Red-Black Coins

Mehdi Salehi, Jeremy Clark, and Mohammad Mannan

Concordia University

Abstract. Abstract goes here.

1 Introductory Remarks

Blah blah blah.

Scope. Blah blah blah.

Contributions. Our primary contributions are as follows.

1. Blah blah blah.
2. Blah blah blah.
3. Blah blah blah.

2 What is RB tokens

There is a growing tendency to issue asset on top of blockchain that represents real world assets such as shares, commodities, and currencies.

One way to implement this kind of tokens is that a company obtains a reserve of the asset and issue tokens that represents a unit of asset. But this design needs custodianship proofs, periodic audits and also trust on the third party.

The question raised here is whether it is possible to find a solution to remove the trust on the third party?

The answer is RB token Dapp. There are two parties involving on each contract of the system. The Red token holder who need a representation of the underlying asset on the blockchain, and Black token holder who bets against the pair value of ETH and the underlying asset.

Therefore, the amount of deposited ETH on each new agreement will grow or shrink depending on the exchange rates of the underlying asset and ETH. Because a blockchain has no inherent knowledge of exchange rates, this mechanism still requires one trustworthy entity called an oracle to write the exchange rates into the blockchain (or consensus can be taken across a set of oracles).

Working Example: Assume Alice wants to create representation of Google share (GOOGL). She sets up a DApp that can hold ETH and issue tokens. The DApp determines how much ETH is equivalent to 1.5 GOGGL, using the current exchange rates, provided to the DApp by a trusted third-party oracle, and Alice deposits this amount of ETH into the DApp. The DApp issues to Alice two tokens, Red and Black. At some future time, the holder of Red token can redeem up to equivalent value of 1 GOOGL in ETH from the deposit and the holder of the Black token gets any remaining ETH. Alice will transfer the Black token to Bob who wants to bet against ETH/GOOGL. When Alice redeems the Red token, it will be worth 1 GOOGL in ETH when the entire deposit of ETH is worth more than 1 GOOGL. If the exchange rate of ETH drops enough or the exchange rate of the GOOGL raise enough (or combinatoion of them), the entire deposit will be worth less than a 1 GOOGL—Alice will get all of the deposit, and the holder of the Black token will get nothing.

There are two risks on the system: Volatility risk of ETH and the underlying asset. Decision on the system depends on the spot exchange rate of ETH and Underlying asset ($\frac{P_{ETH}}{P_{GOOGL}}$).

3 Analysis

4 Systemization

There are a number of stablecoins using crypto-assets as collateral to issue stablecoins which shows a very broad design landscape for indirectly-backed stable coins and different design goals and strategies behind stable coin systems. In this part we will discuss about the mechanism that could be added on top of the RBcoin system discussed on previous section that can be used to change the propetries of the system. The designer of a stable coin may have design goals like Fungibility(I think it should be removed)(Money like tokens could be replaced or sth like that), Stability, Simplicity, and Decentrality.

Firstly, the designer sets the goals of the design and then assign the design parameters of the system to acheive the design goals.

In this part, we propose a systematical design-decision model for indirectly-backed stablecoins. The designer is facing four main design parameters to create a new indictly-backed stable coins which are Maturity date, Counter-party, Collateral risk and interventions.

An overview of the indirectly-backed stablecoins design landscape is in Figure5.

4.1 Maturity Date

The indirectly backed stable systems are agreements between two different parties, a stable party and a volatile party. These two parties should be different because holding both sides of the contract is equal to keeping the underlying asset on the wallet and it is not logical to participate on such a system to just keep the asset.

In this agreement the parties agree to split their deposited asset at a specified date named maturity date. At the maturity date the stable party will receive an exact amount of underlying asset based on the price of the asset at the settlement date and the volitile party will receive the remained part.

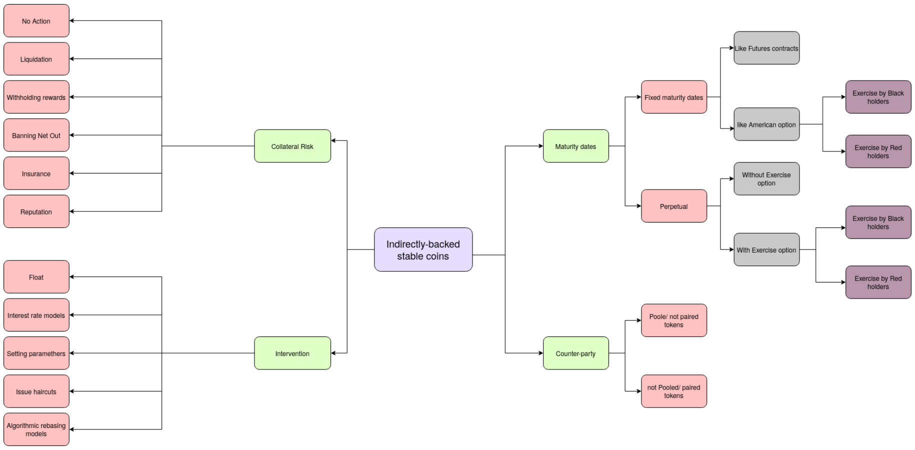

Fig. 1. overview of the indirectly-backed stablecoins design landscape

The first parameter that the designer should decide about is the maturity date. The maturity could be happened at a fixed specific time or could be perpetual.

Fixed Maturity dates The designer can set specific dates for the contracts to be matured for example at the first day of each months. At the day of maturity the deposited assets are devided into two parts. The $1 equivalent amount of the asset goes to the pocket of the stable party (if possible) and the remained is for volatile party. This is simlar to futures contract in Finance.

The designer may let one of the parties to exercise the contract beforr the maturity date. It is very similar to american options. The exerciser could be the black coin holder, red coin holder or both of them.

Perpetual contracts The other way to design the stable coin contracts is to make them as a perpetuty. In this mechanism there is no specific day for the parties to mature the contract. The system may have the option of settlement.

The perpetual stable coin without settlement is not rational because it is like burning the underlying asset to issue stable coins.

For open-ended perpetual stable coins one of the parties has right to request for settlement whenever she wants. The exerciser could be black coin holder or red coin holder.

4.2 Counter party

One of the design parameters is to decide who is the risk taker in each contract. Each newly issued contract is backed by a different vault. Each black coin points its vault because the amount of deposits depend on the black coin holder decision.

The designer could decide whether use a pool for red coins or pair each red coin to its related black coin.

Pooled In this type of design the black coins are pointing to the vaults. Red coins are fungible on the system and there is no differences between them. There is no relations between red coin and the black coin.

In this class, all red coin holders are risk takers of the system and on the unexpected events the take the risks regardless of their issuance contract.

In this case a black coin holder do not know the counterparty and the risk is pooled here.

Paired The designer can create a system in which each red coin and black coins are paired and point to the issued contract. Now the black coin holders now their counterparty and the red coin holder is the risk taker of its own vault. So the risk is not pooled here.

4.3 Collateral Risk

If the price of the underlying asset goes down, the value of deposit falls below collateral ratio. The designers have the choice to react to this situation. We described some of different possible decisions:

Liquidation This variety of design is similar to the marginal accounts in traditional finance. If the underlying asset decreases in price and the value of a vault runs under the collateralization ratio, the system will liquidate the vault.

Liquidation occurs in the case that a vault is the danger area and may not able to pay its obligation. The deposited assets will transfer to the person who takes the responsibility of the debt of the vault. In other words, the liquidator should pay the borrowed red coin (and other obligations in a type of design, such as stability fee in MakerDAO) and receive the vault in exchange.

In liquidation design, the majority of vaults are over-collateralized. If a vault goes under-collateralize it will be liquidated. So, the red coin holders are pretty sure that their coin is backed by a dollar (. They can exchange their asset because the red coins are similar.

Smart contracts cannot trigger themselves. So, there should be an outsider player (like Keepers in MakerDao) to liquidate the warned vaults. They should trace the system to find the under-collateralized vaults and call the liquidation function. Then the keeper will transfer the debt of the vault to the smart contract and receive the deposit of the vault in exchange.

There are design parameters in the liquidation method:

1. Collateralization Ratio: This number shows the factor of over-collateralization. The ratio between the value of the deposits on each vault and the value of borrowed red coins should always be more than the collateralization ratio.

The collateralization ratio is depending on the volatility of the underlying asset. For instance, in the MakerDAO platform, the collateralization ratio for ETH vaults is 1.5. However, in the Synthetix project, it is 7.5 for SNX token, which is more volatile than ETH.

2. Liquidation Incentive: A smart contract is not able to trigger itself. An outsider player named liquidator should pay the transaction fee to call the liquidation function of the smart contract. Some factors influence the costs and profit of liquidators:

   (a) Transaction fee: The liquidator should trigger the liquidation function, send the sufficient red coins, and bid on the auction to win the vault. The user has to pay the transaction fee for these processes. The transaction fee depends on the time of transaction and network congestion.

   (b) Cost of capital: The liquidator pays the obligation by Red coin and receives the deposited coins of the vault. Therefore, the liquidator needs a sufficient amount of red coins for liquidation. There is an opportunity cost associated with the decision of the liquidator to not lend her capital and gain interest.

   In other scenarios, the liquidator may just borrow the fund from lending platforms to liquidate the vault and pay back the loan afterward. There is a cost of borrowing in this scenario as well. So, there is a cost of capital for the liquidator.

   (c) Price Oracles: RB coin systems need the price of the underlying asset in USD. Blockchains have no access to externals data. Oracles are outsider systems that collect the price and push them to the blockchains. Price inefficiency may impose extra costs on the liquidator. For instance, if the price of the asset is $100 on the markets, although the oracle price is $90, the liquidator spends more to provide liquidity from the markets.

   The designer has to incentivize the liquidators to trace the blockchain, find alerted positions, and then send transactions to liquidate them.

   The mechanism of the incentivization is varied between protocols. A majority of platforms give the liquidator discounts on the vaults. For instance, in Single Collateral DAI (SAI), there was a %3 discount on the liquidation process. Other platforms are using auction models to let the market decide about the value of the vault.

3. Auction model: In the case of liquidations, liquidators may come up with a specific warned position and want to liquidate it. The system designer has different options for the decision of picking the winner liquidator.

   The simplest implementation mechanism is the First Come First Serve. However, it won't be fair for the vault holder if the first liquidator bids with a low amount of red coins.

   There are other auction-based mechanisms to find the liquidator. The question raised here is, which method is the most efficient and fair auction model for both bidders and vault holders.

   MakerDao utilizes a mixture of an absolute-auction and a reverse-auction model for the liquidation process.

The absolute auction model is used until the bids cover the debt of the vault. When the bids pass the debt, the auction reversed, the bidders bid on a lower amount of the deposits on the vault for a specific amount of DAI tokens, specified on the absolute auction step.

4. Liquidation penalty: The liquidation penalty is an extra punishment for the black coin holders to care about their debt to collateral ratio. MakerDAO platform charges liquidated vault extra %13 as a punishment for their vault holders. There are two main reasons to add Liquidation penalty on the design:
   (a) To force vault keepers to be over-collateralized
   (b) To mitigate grinding attacks: grinding attack occurs when the position holder deliberately unsafe her black coin and participate in the liquidation auction against her position to buy her deposited assets cheaper.

Using liquidation mechanism as a shield to protect the system provoke criticism. Possibly the black coin holders are freaking out when the price of ETH drops significantly. They may proceed to net out just before the liquidation occurs to their vaults. We called this situation ”early liquidation” of the system.

In this case, the system needs more ETHs to be deposited. The liquidation mechanism is designed to force the black coin holders to inject more ETHs to the system, but the black coin holders withdraw their deposits, and the total collateral of the system drops significantly, which is not the goal of the designers in this situation.

Withholding rewards Majority types of designs like liquidation are disincentivizing bad actors. But, another approach is to encourage users to act properly and incentivizing good actors of the system.

For instance, in the Synthetix project users need collateralize SNX tokens (Synthetix network token) to receive sUSD tokens (Synthetix stable coin pegging a USD). There is no margin call methods or liquidation function on the design. But, there is a reward on the system for users who keep more than the over-collateralization ratio. The Synthetix system has %2 annual inflation on SNX tokens. The inflationary tokens are allocated to the vaults that hold more than the collateralization ratio.

There is another reward for the system. The traders on the exchange of the Synthetix project, pay transfer fees collected and distributed to the vaults holding more than the collateral ratio.

The system incentivizes people to stake their SNX token to be over-collateralized and receive the rewards. So, there is no punishment in the system for bad actors in this class of design.

Banning Black coin holders In the design of indirectly-backed stable coins, the red coins are not redeemable. In other words, the red coin holders cannot give back their red coins to receive $1 of the deposited ETH in exchange. The red coin holder must own (or buy if possible) a black coin to net out a vault and receive the ETH.

In the liquidation scenario, the designer pushes black coin holders to be over-collateralized, applying liquidation punishments. Red coin holders and arbitragers are confident that there is no difference between the red coins because each of the red coins is backed by a sufficient amount of ETHs to be $1 (with high probability).

In another class, the designer removes the liquidation mechanism, prevent black coin holders from withdrawal. In the fungible black coin design class, the designer also forbids the black coin holders from transferring their token.

In this situation, the incentives for black coin holders to be over-collateralized has been decreased, compared to liquidation design class. But, there is a huge incentive left for them to be over-collateralized. If the price of the underlying asset drops, the black coin holders may want to sell their deposited assets to reduce the loss. In this scenario, just black coin holders that have over-collateralized vaults can net out and receive their underlying assets to sell them to the market.

This type of design will increase the fluctuation of the price of the red coin. The market watches the aggregated collaterals on the system and the number of red coins issued by the system and also the price of the underlying asset to evaluate the price of red coins. So when the price of underlying asset drops, the price of red coins will reduce concerning the underlying asset price.

In this scenario, red coin holders are taking parts of the risk of underlying asset volatility risk. On the situation that the price of the asset drops significantly, the value of the stable coin will fall.

Reputation systems In traditional finance, reputation scoring systems are used to decrease or eliminate the collateral needs for a specific financial transaction. Participants are utilizing their reputation as collateral or source of trust for financial services.

For instance, in the FICO credit score system, users can enhance their credit limit by increasing their credit score. There is a default risk on credit systems, but the defaulted person will be punished by credit score reduction. The bad actor loses reputation scores forbidden from using plenty of financial services. Therefore, users have adequate incentives to pay their bills.

A revolution of decentralizing the finance products on top of blockchain technologies began in early 2018, named Decentralized Finance (Defi) movement. There is a myriad of different decentralized financial services out there, such as MakerDAO, Compound, Synthetix, Aave, etc.

There are no differences between users that act properly on Defi platforms and the bad actors. The DeFi ecosystem suffers from a lack of a reputation system or reputation scoring. Using a reputation system will incentivize users to act properly and also reduce the default risk of the system. On the other side of the coin, the users with high-grade reputation scores have new opportunities. So, the cost of defaulting will be increased for high-grade users.

There are barriers to implementing an effective reputation system on blockchains. Lack of strong identities or anonymity is one of them. Also, users can create fake histories. However, these are not impossible to address.

In case that our system concludes a trustworthy reputation system, the designer can use reputation as collateral. We describe two different designs using reputation systems:

1. Reputation-based collateral ratio: In the design of the system, the collateral ratio could be reliant on the reputation of the user. In other words, the collateral ratio is higher for new users (users with no reputation) and lower for users that act properly for a long time.
2. Reputation-based staibility fee In systems like MakerDAO, the DAI borrowers are obliged to pay a fee on their borrowing named stability fee. This stability fee is being set by Maker token holders. In a design based on the reputation, the stability fee could be dependent on the reputation of the user. The reputable user is paying a lower stability fee compared to the new users.

Insurance Insurance models are used to hedge the risk of unexpected events in different systems. Under-collateralization of a vault is an unexpected event on the RBcoin system. The designer could use an insurance model to protect parties from financial loss in the case of under-collateralization.

On the insurance model, the insurer will pay a premium to the insurance company. The company will protect the client from financial loss.

In RBcoins there could be a built-in or outsourced insurance model to protect parties from under collateralization loss. The question raised here is who should pay the premium.

1. Premium pay by Red coin holders: It is very similar to Credit Default Swaps (CDS) on traditional finance. In this design, the approach is that the red coin holders are lending some amount of money to black coin holders. Therefore, black coin holders are borrowing from red coin holders to have a leveraged position on the underlying asset. In this situation, the red coin holders can pay an insurance premium to the contract to protect themselves from the default risk of black coin holders. In the case of under-collateralization, if the black coin holder cannot afford the loss, the insurance contract will pay the loss to the red coin holder.
   This type of design is implemented on the MakerDAO platform. The DAI borrowers are paying a premium so-called stability fee to the system. These fees are collected on a pool named Maker Buffer pool. In the case of liquidation of a CDP, if the winner of the auction pays a lower amount of the obligation of the vault, the difference between the obligation and the paid amount will be paid by the Maker Buffer pool.
2. Premium pay by Black coin holders In this type of design, the black coin holders are paying the insurance premium. It is similar to regular insurance contracts in which the insurer buys an asset and guarantee it by paying a premium to insurance companies. For example, a person purchases a house and insure it. Here the black coin holders are buying a position and pay the insurance premium. If the price of underlying asset drops and the vault going to be liquidated the insurance contract will pay on behalf of the insurer.

3. Premium pay by both In this scenario, both Red and Black coin holders are paying the insurance premium to ensure their positions.

4.4 Intervention

The designer should indicate the level of intervention on the system. There could be some mechanisms to change the level of properties on the system. For instance, the designer may use interest rate models, algorithmic models or secondary tokens to acheive a system property.

Float The desiner may let the system to be free of human or algorithm intervenions. This is the most decentral type of design. This type of design benefits simlicity and decentrality but the red coins has fluctuations.

Interest rate models Interest rates are tools that a system governer has to stimulate the demand or supply side of a system. The designer of indirectly-backed stable coins can use interest rate models on red coins or black coins (two different rates) to adjust the supply and demand of black coins and red coins in the system. This rates could be adjusted by human intervention like DAI or could be fully algorithmic.

Parameter setting All types of the indirectly-backed stable coin system has some parameters in common such as collateral ratio. In specific designs, there are other design parameters added to the system such as maturity dates, insurance premium and rates. The designer may decide to intervene on the system and change these parameter over time. This intervention could be by humans or algorithmic.

Issue haircut The designer should indicate that in case that the price of underlying asset goes down, who is the risk taker of the system. On regular system risk taker of the system is black coin holders till the price falls strongly and the black coins worth zero, then the red coin holders take all the risk.

The designer has other option to divide the risk between red coin holders and black coin holders. The designer could set hair cut parameter a (¡ 1). It means that if the price of the underlying asset falls 1 percent the redcoin holder now takes a percent of the risk and the the black coin holder takes 1-a percent.

This haircut parameter could be changed during the time by human intervention or algorithmic.

Algorithmic rebasing models The designer may use rebasing models to change the number of tokens in a way that at the end of each day the price of redcoins is exactly a dollar.

5 Introduction

There exist different types of stable coins which are categorized to backed stablecoins and algorithmic mechanism stablecoins. Backed stablecoins could be directly backed by a fiat currency or indirectly backed by another volatile asset (for example backed by ETH). In this type one solution to mitigate the volatility is to overcollateralize the deposited asset. In this paper, we propose an imaginary stablecoin model that uses indirectly backed mechanism namely RBcoin (stands from Red Black coin).

RBcoin is a Decentralized Application (DApp) which holds ETH and issue tokens. The DApp determines how much ETH is equivalent to $1.50 USD using the current exchange rate, provided to the DApp by a trusted third party oracle, and Alice deposits this amount of ETH into the DApp. The DApp issues Alice two places in a line — each place is a transferable token Red token and Black token. At some future time, the holder of the first place in line can redeem up to $1.00 USD worth of the deposited ETH at the going exchange rate, and the holder of the second place in line gets any remaining ETH. Alice will transfer the first place in line (as a stable coin called Red coin) to Bob for $1.00 and will hold or sell the second place in line (Black coin). When Bob redeems the Red coin, it will be worth $1 USD in ETH when the entire deposit of ETH is worth more than $1 USD. If the exchange rate drops enough, the entire deposit will be worth less than $1 USD — Bob will get all of the deposit and the holder of the second place in line will get nothing.

The price of ETH to USD is volatile and there is a chance that ETH drops a lot and results in a bad situation in which our Red stable coin worth lesser than $1. In this paper, we analyze the impact of different design factors of the RBcoin model on the failure rate of stability of Red coin. Also, we will talk about features of RBcoins like fungibility, governance, balance mechanism for demand and supply, and implications of regulation on these types of stable coins.

6 Analysis on RBcoins

In this section we analyze stability of RBcoin by changing design and estimation paramethers. We change each factor one by one and check the results of these changes on Redcoin and Blackcoin price estimations.

We use Geometric Brownian Motion (GBM) along with Monte Carlo method for our ETH/USD price simulations. The number of Monte-Carlo method simulations is 1000 and default paramethers used for each simulation is $1.5 collateral amount in ETH and 100 days for estimation. In some parts we will change these default paramethers to see the result of changes.

We use data on the price of ETH/USD from coingecko and the period of our data is from 1 Januery 2018 to 4 May 2020.

Figure 1 shows the result of Monte Carlo simulations on ETH/USD price for 100 future days. Figure 2 shows the histogram ETH/USD output results of 1000 different simulations of Monte-Carlo method of ETH/USD prices in day 100 of simulations. It supposed to be a Log-Normal distribution.

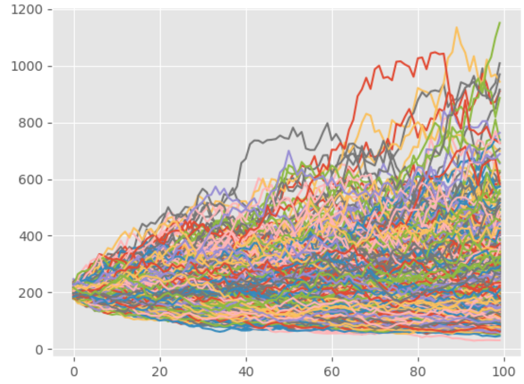

Fig. 2. Monte Carlo forcasts of ETH/USD for 100 days

	Red Coin	Black Coin
Big drop on ETH	<$1	Zero
Little drop on ETH	$1	Much lower than $0.5
Without changes	$1	$0.5
Little rise on ETH	$1	Much higher than $0.5
Big rise on ETH price	$1	Much Much higher than $0.5

Table 1. Impact of ETH volatility on RBcoin

The mean of all 1000 Monte-Carlo simulations for day 100 of estimations is 1.6999126476323942 and the standard deviation is 0.9957392528773387.

Figure 3 is log of outputs in figure 2 to show that the distrubution of log of outputs is a normal shape distribution.

In next sections we will analyze the outputs of Red and Black coin for each set of simulations and then analyze the impact of each design factor on Red and Black coins.

6.1 Impact of ETH/USD volatility on the Red and Black coin

The price of Ether is volatile from its Initial Coin Offering (ICO) until today. The highest historical price of ETH was $1,360 in early 2018 but today's price of ETH on May 4th is $214. ETH price change may have different impacts on the price of our Red and Black coin on RBcoin DApp. In Table 1 we show the impact of changes of ETH/USD on Blackcoin and Redcoin.

So naturally, the question will arise: How often each scenario will occur?

To answer this question we analyze the results of day 100 simulations for three different scenarios as below:

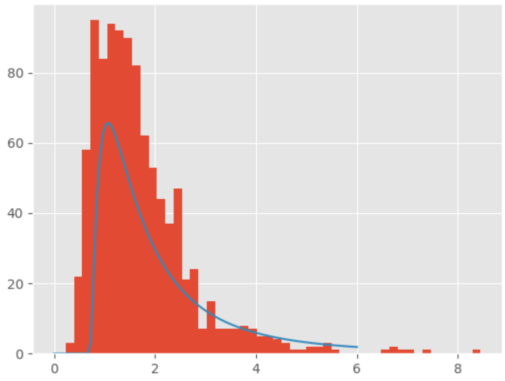

Fig. 3. Histogram of ETH prices in day 100 of simulations

Significant drop on ETH price The worst-case scenario is when the price of ETH in the US dollar drops sharply. So the value of deposited ETH in our RBcoin DApp is bellow $1. In this situation, the Black coin has zero price and the Red coin is worth bellow $1 and not yet pegging a dollar.

In one experiment 237 outcomes out of 1000 simulations have results bellow $1 which tells us the probability of instability on RBcoin is about 23.7%. The mean for the Redcoins in this situation is 0.7683783229826656.

A little drop on ETH price In this situation, the Redcoin price is $1. Because the ETH price is dropped and consequently the equivalent value of the deposited amount of ETH in the dollar is dropped so the value of the Black coin is dropped a lot.

In an experiment 302 simulations out of 1000 results in a bit drop on ETH after 100 days. In this scenario the mean of these 302 outcomes for the Black coin is 0.2458290144866682 with the standard deviation of 0.1366094047375821.

Rise in ETH price If the price of ETH in USD goes up the Redcoin will be stable so its value will be $1. Therefore because ETH price goes up and the Redcoin is stable and the value of deposited ETH is equal to the summation of Redcoin and Blackcoin value, the value of the Black coin will go up on a higher rate compared to the changes in ETH/USD. For example, assume a situation in which the price of ETH in dollar changes α percents and Alice (who deposited ETH on RBcoin DApp) deposited $C amount of ETH as a collateral to RB coin DApp So we have:

$$ValueofDepositedETH = Blackcoin + Redcoin$$

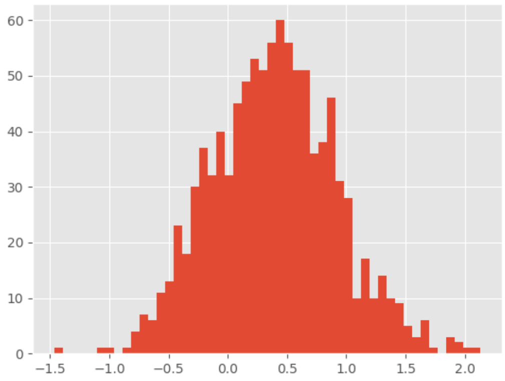

Fig. 4. Histogram of log of ETH prices in day 100 of simulations

By assuming that the value of deposited ETH will not drop bellow $1 the value of Red coin is $1. And because of α percent changes in ETH value in the dollar, the value of Deposited ETh is C * α.

$$ValueofBlackcoin = C\alpha - 1$$

If Bob bought Black coin from Alice on day 0, he paid C-1 for the Black coin. In this situation for calculation return ratio for Bob on day 100 we have :

$$\begin{aligned} Return &= \frac{C\alpha - 1}{C - 1} \\ &= \alpha + \frac{\alpha - 1}{C - 1} \end{aligned} \tag{1}$$

Using Equation 1 and the fact that che changes on ETH price in dollar is α percent we can define leverage ratio for investment on Black coin as:

$$\begin{aligned} LeverageRatio &= \frac{Return}{\alpha} \\ &= \frac{C\alpha - 1}{C\alpha - \alpha} \end{aligned} \tag{2}$$

The leverage Ratio will be equal to zero when ETH price drops by $\frac{1}{C}$. The maximum possible leverage ratio in RBcoin with collateral amount C will be:

$$\lim_{\alpha \to \infty} \frac{C\alpha - 1}{C\alpha - \alpha} = \frac{C}{C - 1}$$

For instance, for collateral amount C equals to $1.5 like DAI Collateral Debt Position (CDP) the leverage ratio formula will be:

$$LeverageRatio = 3 - \frac{2}{\alpha}$$

Regarding Equation 2 Leverage Ratio of the Black coin position will be increased when ETH value in the dollar goes up.

So the leverage ratio of the Black coin for $1.5 collateral is depending on the change of ETH price after the contract. Using this equation for α equals to $\frac{2}{3}$ the Leverage ratio becomes zero. The reason is that if the ETH price drops 33.33% then the value of deposited ETH is $1 and so the Black coin price will be zero.

Another interesting fact is that the highest Leverage ratio in the Black coin position will be 3 and it is when the price of ETH goes up a lot compared to the time of the contract.

In the previous part, we analyze the leverage ratio of the Black coin assuming α percent changes on ETH price. In this part, we combine the results of our Monte-Carlo simulations which shows ETH price changes estimations and the Leverage Ratio formula. In an experiment of 1000 simulations we analyze two different situations. In first we use simulation outcomes in which the resulted amount of ETH on day 100 is higher than $1.5 (which means α is higher than 1). In this situation the mean of all resulted Leverage Ratios are 2.0756085371941726 with standard deviation of 0.24043476162253544. In another scenario, we pick all outcomes with resulted in ETH higher than $1 (which means the value of the Black coin is non-zero). In this scenario the mean of all resulted Leverage Ratios are 1.8120987004369604 with standard deviation of 0.4117814399925659.

All of this description has an assumption that Alice deposited $1.5 as collateral. If Alice decides to deposit a higher amount as collateral the Leverage ratio will be decreased and it is logical because Alice takes a lower risk for lower reward.

Maybe some description needed???.

6.2 Impact of Over-Collaterallization Ratio

Stablecoins that are indirectly backed by crypto-assets like ETH are prone to a risk of the volatility of the asset. This risk is addressed by over-collateralization of the volatile asset. For example, in DAI stablecoin the collateralization ratio is 1.5 like our imaginary model RBcoin. After depositing that amount the depositor receives two places in line. A stablecoin (Red coin) and a leveraged coin (Black coin). But there is a debate on this ratio. Does 1.5 over-collateralization ratio is high enough to mitigate the risk of volatility? Could the over-collateralization ratio be lower than this amount to help the new depositors? In this section, we analyze the impact of the over-collateralization ratio on the stability of RBcoin DApp and the value of Red and Black coin.

In Table 2 we analyze the outcomes for different amount of collateral by depositor.

	$1.05	$1.25	$1.5	$1.75	$2
Mean of outcomes	1.2256	1.4339	1.6987	1.9044	2.3053
Stdev of outcomes	0.7894	0.8593	1.0116	1.1236	1.2886
Number of cases with zero blackcoins	471	349	244	175	99
Average of Redcoins bellow $1	0.6843	0.7111	0.7344	0.7909	0.7610
Mean of Leverage for non-zero Black coins	7.7507	2.4710	1.8236	1.5826	1.5101

Table 2. Impact of Collateral Ratio on RBcoin

	100	200	300	365
Mean of outcomes	1.6320	1.9082	2.1779	2.2390
Stdev of outcomes	0.9272	1.7857	2.3276	3.4074
Number of cases with zero blackcoins	251	318	307	430
Average of Redcoins bellow $1	0.7311	0.6380	0.5771	0.5542
Mean of Leverage for non-zero Black coins	1.8033	1.9466	2.0047	2.0667

Table 3. Impact of simulation days in Analysis

6.3 Impact of simulation days in RBcoin analysis

One of the parameters in our experiments is the day of simulations. It is obvious that by increasing the number of days of predictions the standard deviation of results will be increased. Therefore by using Geometric Brownian Motion and Monte-Carlo because of increasing standard deviation the results of the output depend on the total estimation of these models. It means if these methods overall predict that the price will go up then by increasing the day of prediction the average price results on last day will be increased and vice versa if the overall estimation is that the price will drop then by increasing the days of the simulation the average of the results prices on last day will be dropped.

In Table 3 we analyze some outcomes of the Monte-Carlo method for different days of predictions.

6.4 Impact of early Liquidation

This stability mechanism might enable a third-party to trigger a redemption (for a fee) if they notice a deposit is close to losing more value than the face value of the coins (before the coin holder does). Note that while allowing third parties to trigger a redemption seems like a sensible service, if the coin holders are not monitoring the situation, they will end up holding ETH, instead of an AliceCoin, which is still losing value. Thus this mechanism does not protect holders of the stablecoin at all — it is really only about maintaining the reputation of the stablecoin. The stablecoin can claim it has never broken its peg to the dollar but it is an illusion, because as soon as it is about to lose value, it turns back into its collateral and then loses values under the name of the collateral instead of the stablecoin. If the holder isn't paying attention, they actually lose more by having it triggered than they would breaking the buck.

7 Design Landscape

The purpose of designing a crypto-asset backed stablecoin is to create a stable asset out of a volatile asset. There are a number of stablecoins using crypto-assets as collateral to issue stablecoins which shows a very broad design landscape for indirectly-backed stable coins.

In this part, we propose a systematical design-decision model for indirectly-backed stablecoins. There are some key design decisions for each core feature. We describe core features and the key design decisions related to the main features, and also we will discuss the pros and cons of each feature.

An overview of the indirectly-backed stablecoins design landscape is in Figure 5.

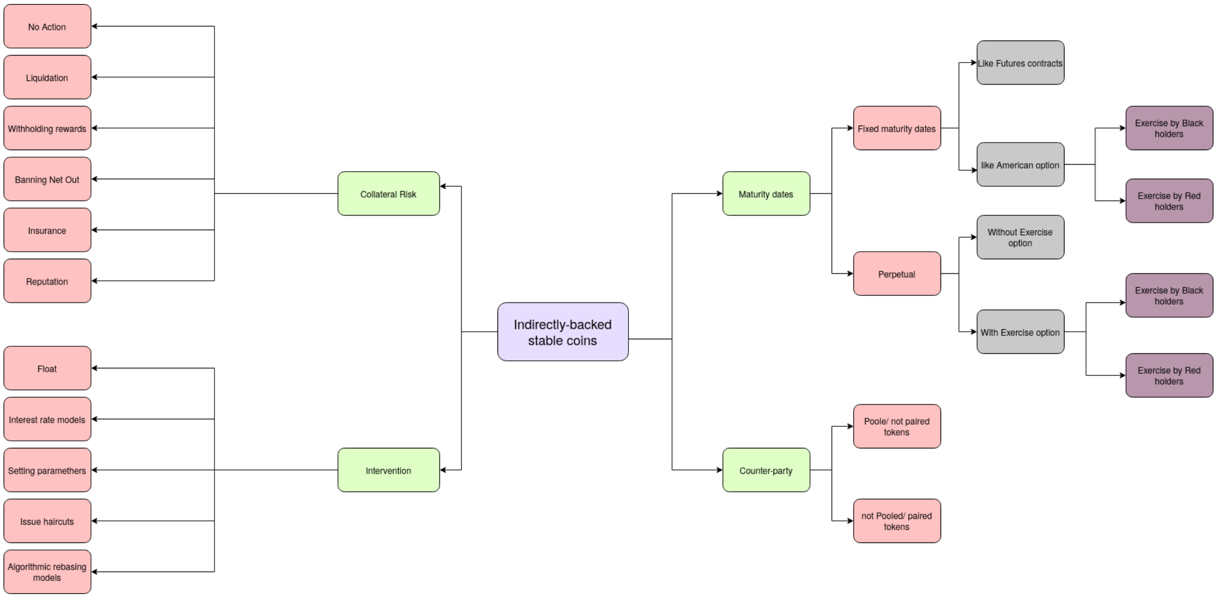

Fig. 5. overview of the indirectly-backed stablecoins design landscape

8 Fungibility

Fungibility or Interchangeability refers to the feature of an asset to be exchanged by the same asset type with equal quality and quantity. For instance, dollar bills are fungible because people can exchange the same amount of dollars without any frictions.

The first design decision is whether the tokens on the systems should be fungible or should be non-fungible.

Fungiblity decision is devided into two parts:

- Red coins Fungibility
- Black coins Fungibility

We will discuss them seperately on next sections.

8.1 Red coins Fungibility

The Red coins, the stable coin of the system, could be fungible or non-fungible. All currently implemented indirectly-backed stablecoins are using fungible stablecoin design. However, it could be non-fungible as well.

Non-fungible Red coins A stablecoin system designer could allow red coins to be non-fungible. For instance, each token could be backed by a different amount of ETHs without limitations on the system such as collateral ratio, liquidation and etc.

In this design class, the Red coin and Black coin should be pair-wise. Because each pair is backing by a different vault and a specific amount of deposited ETH.

There should be a system parameter for each red coin, depends on its vault to distinct the coins. For example, each red coin could be marked by debt to collateral ratio, the number of minted red coins divided by the value of deposited ETH on the related vault, which clarifies the safeties of the coin. So the buyer could have speculation on the price of each red coin base on the debt to collateral ratio.

Some reasons push designers to make red coins fungible. The first reason is usability. Assume that Alice wants to buy 100 red coins. On the other side, Bob wants to sell just 30 coins, Carol wants to sell 50 and David wants to sell 20 red coins. Now Alice should make a price speculation of three different coins and buy them at different prices which is not convenient for her.

The other issue with the non-fungible red coins is price discovery. Markets and crowd wisdom help to aggregate different opinions on the value of an asset. The aggregated results will discover the efficient price of the asset. In non-fungible design, there is not a straight relation between the price of each red coin and the specific characteristic of them like the debt to collateral ratio. So, Each person has speculation for each coin. Because of non-fungibility, the aggregations would not happen and so the real price will not be discovered.

The other reason is that stable coin users are willing to use the stable coins as a money. So, they need stable coins serve as a unit of account which means that you can price other goods or assets using the stable coin. In non-fungible design each red coin has a specific price. So, users can not price other goods based on the stable coin.

8.2 Fungible Red coins

As mentioned in the previous part, stable coin designers put all their effort to create stable coin systems including fungible red coins. There are different mechanisms to bring fungibility into red coins. We classify them into two key designs discussed in the next sections.

- Under-collaterallization
- Separate maturity dates

Collateral Value Assurance One of the methods to bring fungibility into red coins is to set a lower limit for vaults (Collateralization ratio). If the value of deposited ETH in a vault drops beneath a specific amount, then the system decides to take an action.

In this circumstance, there is a minimum amount of ETHs (collateral ratio) backing each red coin. It secures the fungibility of red coins. Red coin holders are sure that there is at least a dollar in the vault for their red coin (strongly expected). There is no difference between their red coin and the red coin of other people in this circumstance.

We will discuss various designs that differ on how they secure the vaults from the under-collateralization in the next sections. Some of them are incentivizing vault keepers to keep their deposit more than collateralization ratio and some of them are disincentivizing the bad actors of the system.

Liquidation This variety of design is similar to the marginal accounts in traditional finance. If the underlying asset decreases in price and the value of a vault runs under the collateralization ratio, the system will liquidate the vault.

Liquidation occurs in the case that a vault is the danger area and may not able to pay its obligation. The deposited assets will transfer to the person who takes the responsibility of the debt of the vault. In other words, the liquidator should pay the borrowed red coin (and other obligations in a type of design, such as stability fee in MakerDAO) and receive the vault in exchange.

In liquidation design, the majority of vaults are over-collateralized. If a vault goes under-collateralize it will be liquidated. So, the red coin holders are pretty sure that their coin is backed by a dollar (. They can exchange their asset because the red coins are similar.

Smart contracts cannot trigger themselves. So, there should be an outsider player (like Keepers in MakerDao) to liquidate the warned vaults. They should trace the system to find the under-collateralized vaults and call the liquidation function. Then the keeper will transfer the debt of the vault to the smart contract and receive the deposit of the vault in exchange.

There are design parameters in the liquidation method:

1. Collateralization Ratio: This number shows the factor of over-collateralization. The ratio between the value of the deposits on each vault and the value of borrowed red coins should always be more than the collateralization ratio. The collateralization ratio is depending on the volatility of the underlying asset. For instance, in the MakerDAO platform, the collateralization ratio for ETH vaults is 1.5. However, in the Synthetix project, it is 7.5 for SNX token, which is more volatile than ETH.
2. Liquidation Incentive: A smart contract is not able to trigger itself. An outsider player named liquidator should pay the transaction fee to call the liquidation function of the smart contract. Some factors influence the costs and profit of liquidators:
   (a) Transaction fee: The liquidator should trigger the liquidation function, send the sufficient red coins, and bid on the auction to win the vault. The user has to pay the transaction fee for these processes. The transaction fee depends on the time of transaction and network congestion.
   (b) Cost of capital: The liquidator pays the obligation by Red coin and receives the deposited coins of the vault. Therefore, the liquidator needs a sufficient amount of red coins for liquidation. There is an opportunity cost associated with the decision of the liquidator to not lend her capital and gain interest.
   In other scenarios, the liquidator may just borrow the fund from lending platforms to liquidate the vault and pay back the loan afterward. There is a cost of borrowing in this scenario as well. So, there is a cost of capital for the liquidator.
   (c) Price Oracles: RB coin systems need the price of the underlying asset in USD. Blockchains have no access to externals data. Oracles are outsider systems that collect the price and push them to the blockchains. Price inefficiency may impose extra costs on the liquidator. For instance, if the price of the asset is \$100 on the markets, although the oracle price is \$90, the liquidator spends more to provide liquidity from the markets.

   The designer has to incentivize the liquidators to trace the blockchain, find alerted positions, and then send transactions to liquidate them.

   The mechanism of the incentivization is varied between protocols. A majority of platforms give the liquidator discounts on the vaults. For instance, in Single Collateral DAI (SAI), there was a %3 discount on the liquidation process. Other platforms are using auction models to let the market decide about the value of the vault.
3. Auction model: In the case of liquidations, liquidators may come up with a specific warned position and want to liquidate it. The system designer has different options for the decision of picking the winner liquidator.

   The simplest implementation mechanism is the First Come First Serve. However, it won't be fair for the vault holder if the first liquidator bids with a low amount of red coins.

There are other auction-based mechanisms to find the liquidator. The question raised here is, which method is the most efficient and fair auction model for both bidders and vault holders.

MakerDao utilizes a mixture of an absolute-auction and a reverse-auction model for the liquidation process.

The absolute auction model is used until the bids cover the debt of the vault. When the bids pass the debt, the auction reversed, the bidders bid on a lower amount of the deposits on the vault for a specific amount of DAI tokens, specified on the absolute auction step.

4. Liquidation penalty: The liquidation penalty is an extra punishment for the black coin holders to care about their debt to collateral ratio. MakerDAO platform charges liquidated vault extra %13 as a punishment for their vault holders. There are two main reasons to add Liquidation penalty on the design:
   (a) To force vault keepers to be over-collateralized
   (b) To mitigate grinding attacks: grinding attack occurs when the position holder deliberately unsafe her black coin and participate in the liquidation auction against her position to buy her deposited assets cheaper.

Using liquidation mechanism as a shield to protect the system provoke criticism. Possibly the black coin holders are freaking out when the price of ETH drops significantly. They may proceed to net out just before the liquidation occurs to their vaults. We called this situation ”early liquidation” of the system.

In this case, the system needs more ETHs to be deposited. The liquidation mechanism is designed to force the black coin holders to inject more ETHs to the system, but the black coin holders withdraw their deposits, and the total collateral of the system drops significantly, which is not the goal of the designers in this situation.

Withholding rewards Majority types of designs like liquidation are disincentivizing bad actors. But, another approach is to encourage users to act properly and incentivizing good actors of the system.

For instance, in the Synthetix project users need collateralize SNX tokens (Synthetix network token) to receive sUSD tokens (Synthetix stable coin pegging a USD). There is no margin call methods or liquidation function on the design. But, there is a reward on the system for users who keep more than the over-collateralization ratio. The Synthetix system has %2 annual inflation on SNX tokens. The inflationary tokens are allocated to the vaults that hold more than the collateralization ratio.

There is another reward for the system. The traders on the exchange of the Synthetix project, pay transfer fees collected and distributed to the vaults holding more than the collateral ratio.

The system incentivizes people to stake their SNX token to be over-collateralized and receive the rewards. So, there is no punishment in the system for bad actors in this class of design.

Banning Black coin holders In the design of indirectly-backed stable coins, the red coins are not redeemable. In other words, the red coin holders cannot give back their red coins to receive $1 of the deposited ETH in exchange. The red coin holder must own (or buy if possible) a black coin to net out a vault and receive the ETH.

In the liquidation scenario, the designer pushes black coin holders to be over-collateralized, applying liquidation punishments. Red coin holders and arbitragers are confident that there is no difference between the red coins because each of the red coins is backed by a sufficient amount of ETHs to be $1 (with high probability).

In another class, the designer removes the liquidation mechanism, prevent black coin holders from withdrawal. In the fungible black coin design class, the designer also forbids the black coin holders from transferring their token.

In this situation, the incentives for black coin holders to be over-collateralized has been decreased, compared to liquidation design class. But, there is a huge incentive left for them to be over-collateralized. If the price of the underlying asset drops, the black coin holders may want to sell their deposited assets to reduce the loss. In this scenario, just black coin holders that have over-collateralized vaults can net out and receive their underlying assets to sell them to the market.

This type of design will increase the fluctuation of the price of the red coin. The market watches the aggregated collaterals on the system and the number of red coins issued by the system and also the price of the underlying asset to evaluate the price of red coins. So when the price of underlying asset drops, the price of red coins will reduce concerning the underlying asset price.

In this scenario, red coin holders are taking parts of the risk of underlying asset volatility risk. On the situation that the price of the asset drops significantly, the value of the stable coin will fall.

Reputation systems In traditional finance, reputation scoring systems are used to decrease or eliminate the collateral needs for a specific financial transaction. Participants are utilizing their reputation as collateral or source of trust for financial services.

For instance, in the FICO credit score system, users can enhance their credit limit by increasing their credit score. There is a default risk on credit systems, but the defaulted person will be punished by credit score reduction. The bad actor loses reputation scores forbidden from using plenty of financial services. Therefore, users have adequate incentives to pay their bills.

A revolution of decentralizing the finance products on top of blockchain technologies began in early 2018, named Decentralized Finance (Defi) movement. There is a myriad of different decentralized financial services out there, such as MakerDAO, Compound, Synthetix, Aave, etc.

There are no differences between users that act properly on Defi platforms and the bad actors. The DeFi ecosystem suffers from a lack of a reputation system or reputation scoring. Using a reputation system will incentivize users to act properly and also reduce the default risk of the system. On the other side of the coin, the users with high-grade reputation scores have new opportunities. So, the cost of defaulting will be increased for high-grade users.

There are barriers to implementing an effective reputation system on blockchains. Lack of strong identities or anonymity is one of them. Also, users can create fake histories. However, these are not impossible to address.

In case that our system concludes a trustworthy reputation system, the designer can use reputation as collateral. We describe two different designs using reputation systems:

1. Reputation-based collateral ratio: In the design of the system, the collateral ratio could be reliant on the reputation of the user. In other words, the collateral ratio is higher for new users (users with no reputation) and lower for users that act properly for a long time.
2. Reputation-based staibility fee In systems like MakerDAO, the DAI borrowers are obliged to pay a fee on their borrowing named stability fee. This stability fee is being set by Maker token holders. In a design based on the reputation, the stability fee could be dependent on the reputation of the user. The reputable user is paying a lower stability fee compared to the new users.

Insurance Insurance models are used to hedge the risk of unexpected events in different systems. Under-collateralization of a vault is an unexpected event on the RBcoin system. The designer could use an insurance model to protect parties from financial loss in the case of under-collateralization.

On the insurance model, the insurer will pay a premium to the insurance company. The company will protect the client from financial loss.

In RBcoins there could be a built-in or outsourced insurance model to protect parties from under collateralization loss. The question raised here is who should pay the premium.

1. Premium pay by Red coin holders: It is very similar to Credit Default Swaps (CDS) on traditional finance. In this design, the approach is that the red coin holders are lending some amount of money to black coin holders. Therefore, black coin holders are borrowing from red coin holders to have a leveraged position on the underlying asset. In this situation, the red coin holders can pay an insurance premium to the contract to protect themselves from the default risk of black coin holders. In the case of under-collateralization, if the black coin holder cannot afford the loss, the insurance contract will pay the loss to the red coin holder.
   This type of design is implemented on the MakerDAO platform. The DAI borrowers are paying a premium so-called stability fee to the system. These fees are collected on a pool named Maker Buffer pool. In the case of liquidation of a CDP, if the winner of the auction pays a lower amount of the obligation of the vault, the difference between the obligation and the paid amount will be paid by the Maker Buffer pool.
2. Premium pay by Black coin holders In this type of design, the black coin holders are paying the insurance premium. It is similar to regular insurance

contracts in which the insurer buys an asset and guarantee it by paying a premium to insurance companies. For example, a person purchases a house and insure it. Here the black coin holders are buying a position and pay the insurance premium. If the price of underlying asset drops and the vault going to be liquidated the insurance contract will pay on behalf of the insurer.

3. Premium pay by both In this scenario, both Red and Black coin holders are paying the insurance premium to ensure their positions.

Separate Maturity Dates This kind of design employs the idea of Futures in traditional finance. Each contract is an agreement between a volatile and a stable party. They deposit an amount of ETHs on the system (Q). The strike price (K) is the dollar value of ETHs that the parties agree that the stable player will receive at the maturity date (M). The remained ETHs on the vault will go to the pocket of the volatile party.

For a specific amount of pooled ETHs, two tranches are created, the stable token and a volatile token (black token). Tranching in traditional finance is used when several securities are created from a pool of other assets, carrying different risks. The junior tranche (volatile token) takes the majority of the risk and the senior tranche (stable coin) takes a lesser risk.

The stable tokens are not fungible because each represents a different maturity date. To create a fungible stable coin, the stable tokens with different maturities are bundled to create the Red coin, stable coin of the system. The amount of red coins each user receives is depending on the maturity date and the strike price of the deposited stable coin.

For example, in the Lien project, the agreement between parties is that at the maturity day, the stable token holder will receive k USD if the deposited ETH worth k USD, and the surplus will belong to the volatile token holder. If the value of deposited ETH dropped below k USD then the stable token worth below K USD and the volatile token worth zero. There are different specified maturity dates every 2 weeks. When a party receives a stable token, she will deposit it on a smart contract named iDOL to receive the stable coin (iDOL token). The iDOL contract bundles stable tokens with different maturities and strike prices and issues a stable coin out of this basket.

8.3 Black coins Fungibility

The Black coins, volatile coin of the system, could be fungible or non-fungible.

Non-fungible Black coin In the majority of implemented indirectly-backed stable coin systems, such as DAI and sUSD black coins are non-fungible. The vaults in these projects are covering various amounts of ETHs. Consequently, the vaults are not fungible.

Non-fungibility of black coins is one of the primary obstacles of the currently implemented projects. These systems are designed to attract users who need stability along with the features of cryptocurrencies.

If Alice decides to issue new stable coins, first she requires to create a pair of a red coin and a black coin. She obliged to keep the black coin because black coins are not transferable. So, the users that need stability should wait till another person who is willing to open a leveraged position, create a new vault, and want to sell her red coins to the market.

The other problem of this kind of design is the control of the demand and supply of stable red coins. If the demand for red coins suddenly increases in markets, the price of red coins in markets will be increased. This is an opportunity for arbitragers to make a profit because the price of red coins is pegging a dollar. The arbitragers issue new red coins that cost $1, sell the red coins to the market to make a profit. But, the problem raised here, because if the arbitrager creates a new vault, then she should hold a non-fungible black coin position. So, the arbitragers are not confident about the price of the red coins. Therefore, there is no motivation for them to make arbitrage on red coin markets.

The designers of the MakerDAO platform are using interest rate models to control the supply and demand for red coins and black coins. This core design feature will be explained in detail, in the next sections.

Fungible Black coin Making black coins fungible is the way to solve the mentioned problem. If Alice wants a red coin, she can open a new vault, sell her black coin to the market, and then decide to use it or keep her red coin.

The fungibility of black coins could boost the market capitalization of indirectly-backed stable coins because people who are willing to use stable coins can issue new stable coins without friction.

In this sort of design, there is no need to adjust interest rates to control the demand and supply of red coins because if the price of recoins increases in a market, the arbitragers can create new vaults, sell the issued black coin to the markets and sell the newly generated red coin, which worths a dollar, to a person who is buying them more than a dollar. The arbitrager also could implement these steps in just one transaction, using the meta transaction method to save money on the transaction fees.

The problem with this type of design is when the demand for red coins increases, and there is no demand for black coins. So, the arbitrager should sell the newly generated black coin lower than the issued price.

However, it uses free-market decisions to calculate the price of red and black coins, which means if the price of red coin increases and there is no demand for black coins, the price of red coins will exceed a dollar.

The other problem with this type of design is the transaction fee for arbitragers. Because the arbitragers are using meta transactions, they should pay high transaction fees for the arbitrage, which may not be profitable in such cases.

8.4 Underlying asset

The first decision that a designer should take is choosing the asset that the issuer use as collateral to issue new stable coins.

There is a strong dependency between the risk related to the underlying asset and the design parameters of an indirectly-backed stable coin.

The stable coins could be backed by a single asset, like SAI (the first version of DAI), sUSD, USDx. Or by a basket of different crypto assets like DAI. In multi-collateral backed stable coins, several design parameters depend on the assets used as collateral on the system.

The purpose of using a basket of assets as collateral is to lower the risk impact of each asset on the stable coin. But the designers may forget the fact that there is a strong correlation between the price of assets. It means as the market of cryptocurrencies falls, all tokens drop in price.

The underlying assets have two types:

- *Exogenous Asset*: Assets that have uses outside of the stable coin systems and just a portion of them are using as collateral on the stable coin system. For instance, ETH, BAT token, and KNC token are collateral options in the MakerDAO platform. These assets are designed to serve other projects, but users can use them as collateral to issue new DAI tokens. Another example is Binance token (BNB) used in the USDx protocol.
- *Endogenous Asset*: This class of assets is designed just to be used on the stable coin system. It means the majority of the assets are locked or used on the system. The Synthetix Network Token (SNX) is an example of endogenous assets. The SNX token is created to be used as collateral to issue new sUSD tokens, the stable token in the Synthetix project.

8.5 Supply adjustment

There is a class of stable coins named Money Supply Adjustment stable coins. In this type of design, the stability comes from the adjustment of the supply of the stable coin. In other words, in the case that the price of stable coin exceeds $1, the system will increase the amount using a mechanism to reduce the price of the stable coin and vice versa.

There is a difference between supply adjustment in indirectly-backed mechanism and Money Supply Adjustment method. In Money Supply Adjustment, there is just one coin (Stable coin) that the designer tries to adjust its supply. But, in Indirect-backed stable coins, there are two different tokens, red and black, that their quantity should be modified.

In a bunch of indirectly-backed stable coins, the designer uses the supply adjustment mechanism to ensure the stable coin's price stability. For instance, in the MakerDAO project, there are two system parameters, Stability fee and Dai Saving Rate (DSR), to adjust the supply of the Dai stable coin.

There is a smart contract named DAI Saving contract or DSR contract. DAI token holders can lock their DAI tokens on the DSR contract and receive interest on the deposited DAI. It is very similar to Saving Accounts in banking. The stability fee is the fee that the Dai borrowers must pay back to the system.

The MakerDAO system uses a combination of these two rates to adjust the DAI tokens and CDPs' supply. The stability fee is the tool to adjust the CDPs (black coins) and the amount of ETHs locked in the system. Decreasing the stability fee is an opportunity for users to create new CDPs with a lower cost of borrowing DAI tokens (red coins). If the Maker token holders conclude that the system needs new vaults, they can reduce the stability fee. On the other hand, decreasing the DSR rate encourages the users that locked their DAI tokens on the DSR contract to withdraw their tokens and supply them to the market, which increases the supply of the DAI tokens.

The MKR token holders, governance token of the MakerDAO platform, can change. So the supply adjustment on the MakerDAO system is a human intervention mechanism. It has a conflict with the decentralization vision of the platform. Because the stability of the tokens is strongly dependant on the DSR and Stability fee, and humans are setting these two. However, the MakerDAO platform uses Decentralized Autonomous Organizations (DAO) to decentralize governance, but there is a critique, which we will discuss in the governance section.

The question here is, why do we need these two rates to adjust the supply of the DAI tokens. Assume that the demand for DAI tokens increases. The total supply of DAI should be increased, or the DAI price will exceed one dollar due to the supply and demand rule. So, arbitragers have an opportunity to make a profit. They can issue new tokens worth one dollar and sell them on the market, which increases the supply and reduce the price of the DAI token. However, there is a problem with arbitragers. They should create a CDP to issue new DAI tokens, and the CDPs are not transferable. So, the arbitragers cannot issue new tokens in this situation, because they cannot sell the black coins. In this case, the Maker token holders have two choices:

- *Reduce the DSR rate*: If a significant amount of DAIs locked in the DSR contract, Maker token holders could vote to reduce the DSR rate. Consequently, the users who locked their tokens on the DSR contract will withdraw their token from the smart contract, the supply of DAI will be increased, and the price will be reduced.
- *Reduce the Staibility fee*: In case that the deposited amount on the DSR contract is not enough to respond to the demand, new DAI tokens should be issued and supplied to the market to stabilize the DAI price. In such a case, the Maker voters must reduce the stability fee to reduce the cost for users to create new CDPs and DAI tokens.
  In this case, the DSR rate is essential, as well. Because it is possible that users create new CDPS and DAIs and then instead of supplying newly generated DAI to the market, deposit them on the DSR contract. So the relation between DSR rate and Stability fee is essential.

The critique here is that DAI stable coin is mostly a human intervention-based stable coin. The other solution to supply adjustment is to make Black coins (CDP in MakerDAO protocol) fungible. As discussed before, the arbitragers can issue new tokens if they find arbitrage opportunities and sell the other token (Black coin) to the market. It is a trade-off between the level of intervention on the system and the stability of the Red coins. Because without any involvement, the price of red coins has more fluctuations, but we let the market decide the price.

The more humans intervene on the system, the more risk of corruption and bribery. The other way to remove humans' involvement in the system is to replace it with automated mechanisms. The designers can use the idea behind Money Supply Adjustment models to automate this part or invent a method to change the system's rates automatically.

8.6 Governance

The decisions about the future of the project are of importance in the design of the system. There is a spectrum of governance models for the future of the project. The right spot of the spectrum is when the project's founders make the proposals and changes in the system. This method is the most centralized type of governance design. The other side of the spectrum is when the system does not use governance models, i.e., the developers deploy the code to the blockchain and leave the project. So, there won't be changed in the future.

In the middle of the spectrum, the designer tries to decentralized the governance of the project. In these projects, the creators distribute governance tokens by a mechanism such as Initial Coin Offering (ICO) or Yield Farming. Then, the governance token holders are responsible for voting on the change proposals of the systems.

For instance, the MKR token is the governance token of the Maker system. Each token represents a vote for future proposals. There are critiques about the governance model of the Maker platform:

- *Technocracy instead of Democracy*: There is a debate on this type of design about information asymmetry. The governance token holders who gain from the technical background has more information about the smart contracts, processes, and logic behind the protocol. This information asymmetry could help the professional voters get their way on the proposals and votes. In other words, for plans that have benefits for them, they use their knowledge to convince the other voters to vote on the proposals.
  The ordinary users in these systems will follow the technocrats on the voting, and it gives the technocrats higher decision power than what they have on their pockets.
- *Level of Centralization*: One of the key points in designing a DAO for the governance of a project is the voters' level of decentralism. The privacy characteristic of the blockchains makes it hard to track the identity of token owners. If a malicious user owns a significant portion of the governance token, then the system is susceptible to governance attacks, and the malicious user can vote and execute the proposals to maximize the profit.

8.7 Implications on Regulatory