Red-Black Coins

Mehdi Salehi, Jeremy Clark, and Mohammad Mannan

Concordia University

Abstract. A number of Ethereum projects for stablecoins and synthetic assets use the same core mechanism for fixing the price of an asset. In this paper, we distil this shared approach into a primitive we call red-black coins. We use a model to demonstrate the primitive's financial character-istics and to reason about how it should be priced. Real world projects do not use the red-black coin primitive in isolation but lay on other mechanisms and features to provide fungibility and to reduce exposure to price drops. One mechanism is called liquidation, however liquidation is hard to analyze as it relies on human behaviour and could produce unintended economic consequences. Therefore we additionally develop a design landscape for extending the red-black coin primitives and put forward a research agenda for alternatives to liquidation.

1 Introductory Remarks

Cryptocurrencies like Bitcoin (BTC) and Ether (ETH) are marked by extreme volatility in price relative to the US dollar (USD). As decentralized finance (DeFi) services mature on Ethereum, a critical component to their success is letting users choose between holding ETH and holding a stablecoin that targets USD (or some other metric of stability) in price.

Some stablecoins work like a hypothetical vending machine [3]: Alice deposits two 'coins' from a volatile currency (*e.g.,* a cryptocurrency like ETH) into the machine and it returns to her two new coins—a 'black' coin that is stable and a 'red' coin that is even more volatile in price than the original coins Alice put in. Together, the red and black coins are equal in value to the two input coins. The machine cannot reduce overall price volatility, but it can push volatility from the black coin onto the red coin.

Consider the following example of such a stability mechanism. An asset is chosen that is considered stable by definition (*e.g.,* the US dollar). The vending machine is implemented as a decentralized app (DApp; *a.k.a.,* smart contract) on a blockchain (*e.g.,* Ethereum). Alice deposits an amount of ETH worth $1.50 USD into the DApp. The DApp references a trusted oracle service for the current ETH/USD exchange rate to enforce this. The DApp holds the ETH as a deposit for future redemption, and returns to Alice a red coin and a black coin (*e.g.,* as ERC-20 tokens). Alice can sell one or both coins. In the future, the owner of the black coin can redeem it for ETH from the DApp, and receive the equivalent of $1.00 USD. This assumes the initial deposit of $1.50 USD worth of ETH is still worth at least $1.00 USD at redemption time—if not, the black coin owner

receives all of the collateral. The red coin holder receives any remaining ETH after the black coin holder is paid.

The key idea is that the black coin will nearly always be worth the equivalent of $1.00 USD. This is true when ETH/USD increases in value, stays the same, or declines moderately. Only if it declines significantly does the black coin start to experience volatility in price—its redemption value will decrease at the same rate as ETH/USD itself. For the red coin, the redemption value increases and decreases as ETH/USD itself increases and decreases, however the gains and losses are amplified. This is an overview; we return to these details below.

Synthetic Assets. The red-black coin primitive can be generalized to produce black coins that match the price of any financial asset, not just a currency like the USD, simply by changing the price that the oracle references. For example, a black coin for one share of the company Apple (APPL) would use an ETH/APPL price feed (possibly constructed by bridging ETH/USD and APPL/USD prices) and otherwise be exactly the same. These black coins are "synthetic assets" because they expose the holder to the price movements of the asset but do not afford the holder any other benefits of holding the financial instrument (*e.g.,* shareholder votes or dividends for equities; physical delivery for futures; or the ability to settle a loan, or option contract on the asset). What a red coin represents in this example is less natural than for a stablecoin: it is a bet that ETH will increase in price faster than APPL.

Relation to Dai. At the time of writing, the stablecoin Dai has (i) a market cap of $800M (the largest of all non-centralized stablecoins); (ii) its parent service, Maker, locks $1.2B worth of ETH (the third largest DeFi service, and the largest stablecoin); and (iii) it is the most supplied and most borrowed asset on the DeFi lending service Compound.[1] Dai uses the red-black coin primitive—black coins are called Dai and a red coin is a Vault (*née* collateralized debt position or CDP). However the system is immensely more complicated because it adds a number of features that the basic red-black coin primitive lacks: (1) interchangeability (fungibility) of black coins across multiple producers, (2) a liquidation process to incentivize red coin holders to increase the collateralized ETH as ETH/USD declines or face an auction that automatically settles a red-black pair, and (3) fees to balance supply/demand of black and red coins that are adjustable through a distributed governance. Other projects built on the red-black primitive (for both stablecoins and synthetic assets) include Synthetix's sUSD [2], Kava's USDX [3], UMA [4], and BitUSD [5].

Liquidations. The worst-case scenario for a red-black coin is a decline in the value of ETH/USD. As a primitive, red-black coins simply force the holders to take on

---

[1] https://compound.finance/markets

[2] https://docs.synthetix.io/litepaper/

[3] https://www.kava.io/

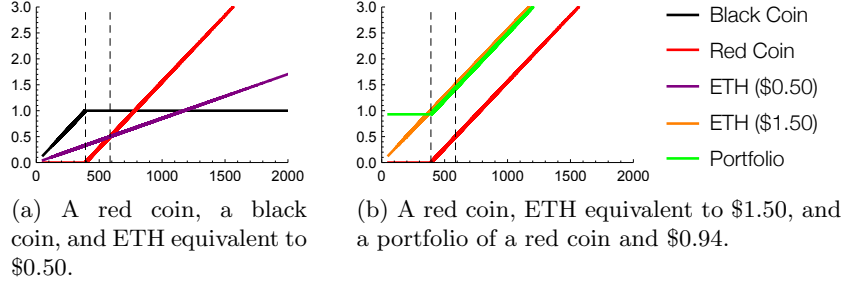[4] https://docs.umaproject.org/

[5] https://github.com/bitshares

this risk. By contrast, liquidations are the main preventative mechanism used by full-fledged systems like Dai. Liquidations are controversial: many vault holders have lost ETH due to liquidations, they require special monitoring tools (*e.g.,* DeFiSaver.com), any analysis includes assumptions about how humans behave and how fast market actions can be taken, and maligned incentives (*e.g.,* return DAI for ETH when ETH/DAI is in decline) can lead to economic crises and deleveraging spirals [5,9]. Liquidations failed Dai on Ethereum's "Black Thursday" event in March 2020 and required a bail-out. In this paper, red-black coins can be thought of as "Dai without liquidations". Since liquidations have a downside, it is important to weigh these against what they contribute. To understand what they contribute, we must first thoroughly understand red-black coins and their shortcomings. Further it might be possible that liquidations are not the best tool to address any shortcomings—we consider alternatives in Section 3.

1.1 Contributions and Related Work

We reference some financial instruments and terminology throughout the paper; we refer the reader elsewhere for full explanations of these [6]. Several systemization of knowledge papers cover stablecoins [11,10,3]. Our notion of a red-black coin is inspired by the 'indirectly-backed' classification from [3] and "exogenous collateral" type of "non-custodial" stable coins in [7]. In the other two [11,10], the mechanism is described as allowing a user to 'borrow' USD from themselves using their ETH as collateral—we find this perspective less intuitive. None of the three SoKs provide deep coverageThis is a bit vague, analysis, or modelling of the stability mechanism in this paper, and instead focus on surveying several different types of stablecoins and mechanisms. Maker is considered a decentralized finance (DeFi) project and it (and other DeFi projects) has been studied from orthogonal angles including attacks/measurements on governance and oracles, attacks using flash loans, and modelling liquidity crises [4,5,12,9]. In [7], stable coins are categorized into two main classes: custodial and non-custodial. They introduced three potential risks for non-custodial stable coins (governance, mining, and manipulations) and utilize a capital structure model to assess the risk under different scenarios.

In this paper, we isolate and study the red-black coin primitive to better understand its characteristics, which seems prudent before analyzing more complex systems. We use the ETH price model from [5] to model how risky red and black coins are under different scenarios. We then examine the necessity of the extra infrastructure projects like what Maker adds to the red-black coins— precisely what does the added complexity (*e.g.,* stability fees, liquidation, global shutdown, *etc.*) achieve and what are the design alternatives for the same functionality? We assume that the market for red and black coins are perfectly liquid to have a simple model to analyze. In [8] and [9], authors explored the effect of supply and demand and the possibility of market collapse due to the feedback effects on liquidity and volatility from deleveraging effects during crises. There is an assumption in the related works that the "liquidation process" is a building block for non-collateral stable coins which we argue against it in this paper.

(a) A red coin, a black coin, and ETH equivalent to $0.50.

(b) A red coin, ETH equivalent to $1.50, and a portfolio of a red coin and $0.94.

Fig. 1. Redemption value in USD (y-axis) as the price of ETH (x-axis) changes.

In addition to our work, there are other "two coin" solutions to implement stablecoins. For instance, Cao et al. [2] proposed a new model in which the stable coin is similar to the coupon bond in traditional finance and the other coin is similar to leveraged positions. They used traditional option theory models to analyze their system.
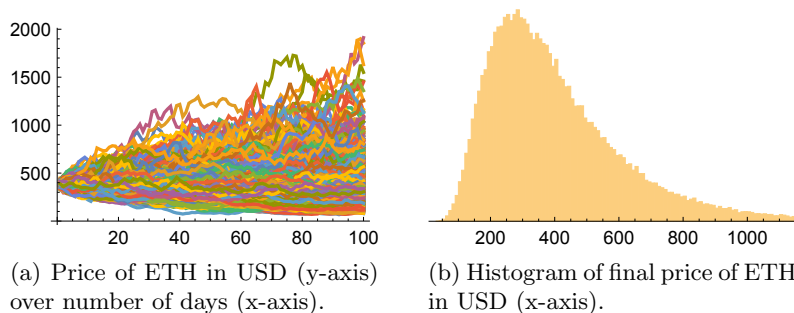
2 Financial Characteristics

In this section, we answer questions about the financial characteristics of the red-black primitive. Consider a black coin that targets $1 USD when 1 ETH is $381.56 USD, and the DApp holds 0.00393126 ETH (worth $1.5 USD). Assume for now that (i) a red-black coin is a (non-fungible) contract between two individuals, and (ii) no one intervenes when ETH/USD declines enough that black coins starts to lose value (no liquidations). Figure 1(a) shows how much a black coin is worth (y-axis) as the price of ETH varies (x-axis). The starting point ($381.56 USD) is marked and if the price of ETH increases (rightward), the black coin is always worth $1. If the value of ETH decreases (leftward), the black coin is still stable until the value of ETH hits $254.37 (marked)—at this point, 0.00393126 ETH starts to become worth less than $1 and the black coin 'breaks the buck.'

Figure 1(a) also shows the redemption value of a red coin. When created, a red coin is redeemable for $0.50 USD. A user with $0.50 USD can choose between purchasing a red coin or purchasing ETH (also shown). In both cases, the user profits when ETH increases and loses when ETH decreases in price. However the slope of red coin is greater. This indicates it is a *leveraged* position in ETH.

2.1 How much should you pay for a black coin?

Consider a black coin that is purchased today when ETH is $381.56 USD. How much will it be worth in 100 days? In most future worlds, the black coin will be worth $1. In some future worlds (when ETH is worth less than $254.37), the

(a) Price of ETH in USD (y-axis) over number of days (x-axis).

(b) Histogram of final price of ETH in USD (x-axis).

Fig. 2. ETH/USD Monte Carlo simulation results.

black coin will break the buck. But even here, it takes a 'haircut' on value as opposed to being worthless (*e.g.,* it can be redeemed for, say, \$0.90).

The average value of a black coin for different possible outcomes can be estimated if we have a statistical model for ETH price movements. In finance, many statistical models have been proposed for many assets. Pricing ETH remains an open research problem. Until future research from the finance community advocates for the most appropriate model, we will sketch in some concrete numbers using Geometric Brownian Motion (GBM), which underlies the Black-Scholes model for pricing options [1] and has been used for ETH in other work [5]. We omit the details of the model itself (covered in nearly every financial textbook [14]). We fit the model to the historical 'closing' prices of ETH for 1000 days prior to 18 Sept 2020[6] and obtain $\mu = 0.000744754$ (an upward drift in price over time) and $\sigma = 0.0524172$ (a measure of volatility). If we simulate the next 100 days using Monte Carlo, we obtain the results in Figure 2. For the parameters of this example, the Average value of the black coin is \$0.94 USD at the maturity date. Our model can be adjusted for the initial price, over-collateralization ratio (section 2.2), and days until redemption. It is available in Python and Mathematica.[7]

As shown in Figure 2(b), the expected return is log-normal. When we model more than 100 days, the variance increases and the Average redemption value of a black coin decreases: \$0.94 USD after 100 days, \$0.85 USD after 200 days, and \$0.80 after 1 year. This does not mean the black coin is worth less over time, it means the risk it falls out-of-the-money increases the more time you give it.

2.2 Why would you want a red coin?

While a stablecoin has utility to the holder, it is less clear what the utility of a red coin is. A red coin is a *leveraged* position in ETH, which means that both gains and losses are amplified—compare the slope of the red coin value with a

---

$0.50 ETH investment at the same starting point ($381.56 USD) in Figure 1(a). Leverage is popular with investors. Investing in a red coin is equivalent to investing $0.50 along with borrowing $2 \times \$0.50$ in ETH (*i.e.,* 3:1 leverage). If the over-collateralization ratio is decreased from 1.50 to 1.10, then leverage for the red coin increases to 11:1. However, the black coin becomes riskier and its 100-day Average value drops from $0.94 to $0.86. For a $2.00 collateralization, red coin leverage is 2:1, and the black coin Average value is $0.98.

Speculators seek out red coins but what about a user that wants to hold ETH without any leverage? She seemingly has no interest in red (or black) coins. Consider two scenarios: (a) she holds $1.50 worth of ETH; and (b) she takes her $1.50 worth of ETH, issues and sells a black coin (*e.g.,* for $0.97 USD), and holds the red coin. She actually has a small portfolio of a red coin and close to $1 USD. The redemption value of (a) and (b) are depicted in Figure 1(b), along with the red coin by itself. The portfolio is actually an attractive investment—she has 'insurance' against catastrophic loss during a devaluation of ETH for a small fixed 'fee'—the $0.03 USD difference between what she received for the black coin ($0.94) and what the DApp pays out to the black coin holder ($1.00). Additionally, she produced a stable black coin, which has external benefit to the decentralized economy.

3   Research Agenda: Extending Red-Black Coins

Red-black coins are primitives. Before deploying them, other aspects of their design should to be considered. Design decisions include the maturity/redemption policy, how to make black and red coins fungible, and interventions to prevent the black coin from breaking the buck. One path through the decision tree leads to a design like Dai, however there are many other decisions that could result in very different stablecoins that have not been thoroughly explored by academics or the DeFi community to our knowledge. We do not propose a specific alternative but see our contribution as setting a research agenda.

3.1   Fungibility

Assume Alice creates a red/black coin, selling the red coin to Carol. Later, Bob creates a red/black coin, selling the red coin to David. Alice's black coin is not identical to Bob's black coin. Because they were created at different times, the ETH/USD exchange rate is different, and thus the amount of collateral in ETH in the DApp will be different. The more collateral, the more a black coin is worth (recall Section 2.2). Such coins are not interchangeable or *fungible* which adds effort to valuation and exchange.

One design option is to **(1) forgo fungibility** and have each coin pair be its own individual contract between two counter-parties (*a.k.a.,* over-the-counter (OTC) contracts). This is the difference between, say, a forward and futures contract [6]. A second option is to **(2) pool the collateral** of the red coins so that each black coin is a claim against the pool. A pool can be unfair: the losses

are democratized to all black coin holders. When pooled, Alice might obtain a black coin before an ETH/USD price bubble; all the black coins issued during the rising bubble are backed by significantly less collateral and when the bubble bursts (consider the case that it reverts to the pre-bubble price), the pool could become under-collateralized, impacting Alice. Had Alice used an OTC contract instead, her red coin would acquire and lose value with the bubble but not be under-collaterialized after bursting.

A third option is to additionally offer **(3) red coin fungibility**. Since red coins have variable collateral (based on when they were created), two conditions need to be added to its transfer function: (i) red coins with less than a specified collateral are not transferable, and (ii) red coins with more than the specified collateral will transfer the surplus to the sellers address while transferring it. While this is not possible with vaults in Dai currently, it seems feasible to add.

3.2   Redemption

A policy for redeeming the collateralized ETH is the next design decision. Note that the DApp can autonomously distribute the collateral without the participation of the red or black coin holder, however someone needs to trigger a function call against the DApp to finalize the process.

Red-black coins could **(1) mature on a pre-specified date** (*e.g.,* the first day of a specified month). At any given time, red/black coins in circulation would have one of a few different expiration dates, while still allowing some degree of fungibility. Coin holders would shorten or extend their coins by trading for a coin with a different maturity date. This is precisely how futures mature [6], and yTokens are based on the same principle [13]. After maturity, the DApp would lock all transfer functions and only allow withdrawal by the coin holders. The first to ask for a withdrawal would trigger the DApp to look up the ETH/USD price as of the maturity date and split the collateral accordingly.

Alternatively, red-black coins could be redeemed at any time **(2) on demand by the black coin holder**, or **(3) red coin holder**, **(4) either**, or **(5) both**. Options (in the US style) work on the principal of (2) or (3) [6,14]. Allowing either to redeem is unlike anything we could find in traditional finance—we speculate it would add uncertainty without any clear gain. Requiring both to agree to redemption could be done by agreement, or (consistent with futures contracts [6]), a red coin holder could acquire a (fungible) black coin and redeem the (netted-out) pair.

3.3   Under-collateralization

When the ETH/USD exchange rate drops enough that under-collateralization is possible, the system could **(1) do nothing** and let the black coin holder price the risk of this into the coin. If the design attempts further mitigation, the DApp could operate like a margin trading account and require red coin holders to top-up their collateral. If they do not, it is **(2) liquidated** (*e.g.,* sold by auction for black coins). The challenge is incentivizing users to sell USD-pegged black coins

for ETH when ETH/USD is in decline (a counter-cyclic investment). In Dai, because collateral is pooled, liquidation is essential because under-collateralized red coins hurt all black coin holders. When collateral is not pooled, liquidation is useless for black coin holders because both ETH and black coins decrease in value at the same rate (recall Figure 1) so it is simpler to do nothing.

Liquidation does not incentivize topped-up collateral unless it is accompanied by a **(3) punishment** (otherwise red coin holders might try to buy their liquidated assets from themselves at a discount). Beyond charging a fee, a stablecoin system might also withhold rewards (some systems used a secondary token for providing governance and providing rewards) or block red coin transfers until collateral is restored. In traditional financial markets, it is also the case that a trader's margin is inadequate to settle their account, they are still legally liable for the difference. A stablecoin accompanied by a **(4) reputation system** could mandate that red coin holders settle any obligation, however the potential loses for a red coin holder becomes unbound. A different approach is to obtain **(5) insurance** or financial coverage for the event of a decline in ETH/USD. This could be actual insurance, whether decentralized or from a traditional brokerage, or an offsetting financial investment that hedges the currency exchange risk.

The last approach is **(6) bail out** any losses through sales of a secondary token. This was used recently by Maker for Dai holders when its normal procedures of (2) and (3) were not adequate for dealing with a sharp, unexpected decline in the price of ETH on 12 Mar 2020 ('black Thursday'). While the auction was successful and recollateralized the pool, it cannot be guaranteed that minting new tokens will be adequate for offsetting any incurred debt. This event also exposed the lack of understanding and underestimation of risk by many vault (*i.e.,* red coin) holders who faced losses under (3), and raises the question of whether a system should be designed that is more forgiving to red coin holders in turbulent markets.

3.4 Autonomy

A design based on the red-black coin primitive that is OTC and does not liquidate is entirely autonomous. It can be instantiated in a DApp and operate without human intervention. While black coins are price-stable under most market conditions, traders who are time-sensitive may forgo obtaining a good price in order to trade quickly. This particularly is influential for stablecoins which provide a low-friction avenue in and out of speculative positions on the price of ETH. Since red and black coins are issued in the same proportion, supply/demand imbalances between them could also add volatility to the black coin price. This could potentially be addressed in the design.

A non-interventionist approach would let the red and black coin price **(1) float freely**. This avoids adding complexity to the design—in fact, a design goal might be to design a system that traders can easily understand and grasp the risk of. This could thwart potential lawsuits, such as a recent class action suit

against Dai.[8] An alternative is to further stabilize prices by **(2) setting rates and fees** at various points in the system. For example, if black coin holders can redeem at any time, a fee could be charged to the black coin holder and paid to the red coin holder. If redemption requires both a red and black coin, the fee could be collected by the DApp. This principle is used by central banks for targeting interest rates, and is used in Maker to control the spot market for Dai. It is a struggle to set fees in the context of a decentralized and autonomous organization—while allowing decisions to be voted on is a first step, it does not guarantee that token holders are independent, informed, and not unduly influenced by the 'expert' recommendations.

4   Concluding Remarks

In this paper, we distil complex stablecoin systems into one of their core primitives, the red-black coin and provide a detailed study of its characteristics and possible extensions. It would be useful to have research results on the most suitable financial model for the ETH/USD price rate (*e.g.,* drift-diffusion or GARCH) for us to use in work like this paper. Future work could also examine the benefits of building a Dai alternative, still based on red-black coins but using different design parameters. Two examples that seem interesting are: (a) a more understandable system that reduces the amount of intervention, and (b) a system with fungible red coins that can be traded freely. Finally, while our paper answers the question of how much you should pay for a black coin, the analysis is much more complicated for Dai—with pooled collateral, liquidation, and bailouts, Dai is less risky than a simple black coin but the risk that these countermeasures systemically fail is not zero.

References

1. Black, F., Scholes, M.: The pricing of options and corporate liabilities. Journal of Political Economy **81**(3) (1973)
2. Cao, Y., Dai, M., Kou, S., Li, L., Yang, C.: Designing stable coins. Tech. rep., Duo Network Whitepaper (2018)
3. Clark, J., Demirag, D., Moosavi, S.: Demystifying stablecoins. In: Communications of the ACM. vol. 63 (July 2020)
4. Gu, W., Raghuvanshi, A., Boneh, D.: Empirical measurements on pricing oracles and decentralized governance for stablecoins. In: Cryptoeconomic Systems (2020)
5. Gudgeon, L., Perez, D., Harz, D., Livshits, B., Gervais, A.: The decentralized financial crisis. In: CVCBT (2020)
6. Harris, L.: Trading and exchanges: market microstructure for practitioners. Oxford (2003)
7. Klages-Mundt, A., Harz, D., Gudgeon, L., Liu, J.Y., Minca, A.: Stablecoins 2.0: Economic foundations and risk-based models. In: Proceedings of the 2nd ACM Conference on Advances in Financial Technologies. pp. 59–79 (2020)

---

[8] CoinDesk: `https://t.co/iJET1JGJib`

8. Klages-Mundt, A., Minca, A.: (In) stability for the blockchain: Deleveraging spirals and stablecoin attacks. arXiv preprint arXiv:1906.02152 (2019)
9. Klages-Mundt, A., Minca, A.: While stability lasts: A stochastic model of stablecoins. Tech. rep., arXiv (2020)
10. Moin, A., Sekniqi, K., Sirer, E.G.: SoK: A classification framework for stablecoin designs. In: Financial Cryptography (2020)
11. Pernice, I.G.A., Henningsen, S., Proskalovich, R., Florian, M., Elendner, H.: Monetary stabilization in cryptocurrencies: Design approaches and open questions. In: CVCBT (2019)
12. Qin, K., Zhou, L., Livshits, B., Gervais, A.: Attacking the DeFi ecosystem with flash loans for fun and profit. Tech. Rep. 2003.03810v2, arXiv (2020)
13. Robinson, D., Niemerg, A.: The yield protocol: On-chain lending with interest rate discovery. Tech. rep., Yield.is (Apr 2020)
14. Seydel, R.U.: Tools for computational finance. Springer, fourth edn. (2009)