

Designing Stable Coins

Yizhou CAO*, Min DAI†, Steven KOU‡, Lewei LI§, Chen YANG¶

Version 0.9.5
April 16, 2018

Abstract

Stable coins, which are cryptocurrencies pegged to other stable financial assets, are desirable for blockchain networks to be used as public accounting ledgers for payment transactions and as crypto money market accounts for asset allocation involving cryptocurrencies, whereby being often called the “Holy Grail of cryptocurrency.” However, existing cryptocurrencies, such as Bitcoins, are too volatile for these purposes. Inspired by the dual purpose funds popular in the US and China, we design, for the first time to our best knowledge, several dual-class structures that offer entitlements to either fixed income stable coins (class A funds) pegged to a traditional currency or leveraged investment opportunities (class B funds). Unlike traditional currencies, the new class A funds record all transactions on a blockchain without centralized counterparties. By using the option pricing theory, we show that proposed stable coins indeed have very low volatility, similar to that of the short term U.S. treasury bonds. When combined with insurance from a government, the design can also serve as a basis for issuing a sovereign cryptocurrency.

Keywords: stable coins, fixed income crypto asset, leveraged return crypto asset, smart contract, option pricing

**Email:* yizhou.cao@finbook.co, CTO and Co-founder of FinBook

†*Email:* matdm@nus.edu.sg. Director, Centre for Quantitative Finance, National University of Singapore

‡*Email:* matsteve@nus.edu.sg. Director, Risk Management Institute, National University of Singapore

§*Email:* lewei.li@finbook.co, CEO and Co-founder of FinBook

¶*Email:* chen.yang@math.ethz.ch, Department of Mathematics, ETH Zurich

1 Introduction

Cryptocurrencies, such as Bitcoin and Ethereum (ETH), are distributed payment systems. They have three important features in common. First, they are a peer-to-peer network, that is, payment from one user to another is processed without any intermediary. Second, they use the Blockchain technology, such that all transaction records are stored by every user. Third, they allow anonymous payment. Anonymous transaction orders are recorded to Blockchain, after miners' verification, and updated to all users immediately.

A Stable Token, also known as stablecoin, is a crypto-token that keeps stable market value against a specific index, most noticeably US Dollar. Stable coins are needed since they can be used within the Blockchain to settle payments, in crypto money market accounts, or by miners who may find that it is difficult to convert the mined coins into traditional currencies in some countries. However, the existing cryptocurrencies are too volatile to be served as stable coins. For instance, the ETH/USD price from October 1, 2017 to February 28, 2018 is shown in Figure 1. During this period, ETH/USD price has an annualized return volatility of 120%, which is more than 9 times that of S&P 500 during the same period (13%).

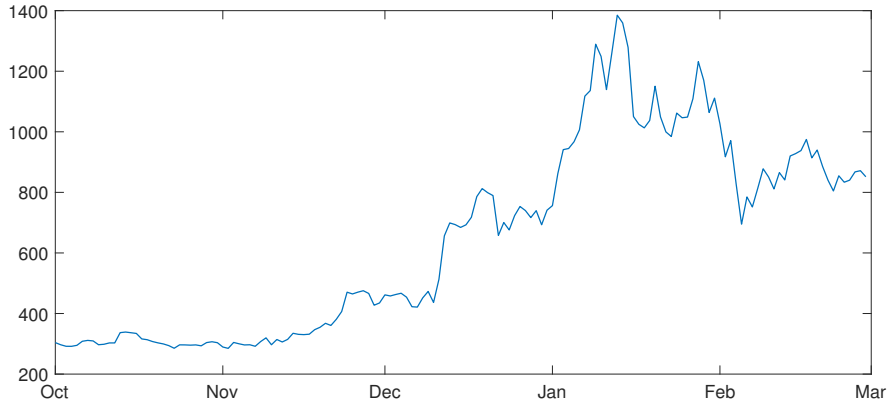


Figure 1: ETH/USD Price from 1 Oct 2017 to 28 Feb 2018

Inspired by the dual purpose funds popular in the U.S. and China, we design, for the first time to our best knowledge, several dual-class structures that offer entitlements to either fixed income stable coins (Class A coins) pegged to a traditional currency or leveraged investment opportunities (Class B coins). Due to downward resets, a vanilla A coin behaves like a corporate bond with the collateral amount being reset automatically. To reduce volatility, the vanilla A coin can be further split into additional coins, A' and B' or A0 and A1. Unlike traditional currencies, these new class A coins record all transactions on a blockchain without centralized counter parties. By using the option pricing theory, we show that proposed stable coins indeed have very low volatility; indeed the volatility of A' and A0 are similar to that of the short term U.S. treasury bonds.

Although our design of stable coins is inspired by dual-purpose funds, it is different from dual-purpose funds in U.S. and China in the aspects shown in Panel A of Table 1. These differences require a more delicate modeling method, which is summarized in Panel B of Table 1.

The design of stable coins can be used alone in most cases, except in the case of Black Swan events, when the underlying cryptocurrency suddenly drops close to zero within

Table 1: Contract Comparison of Our Stable Coins and Dual-Purpose Fund in U.S. and China

Panel A: Contract Comparison					
	Payment Style of A Share	Payment Style of B Share	Leverage Ratio Reset	Lifespan	Reference Asset
Dual-Purpose Fund in U.S.	Dividend	Single payment at wind-up date	No	Finite	Stock/ Stock Index
Dual-Purpose Fund in China	Fixed Income	Payments affect the underlying asset but not the exchange ratio	Yes	Infinite	Stock Index
Our vanilla A and B	Fixed Income	Payments affect the exchange ratio but not the underlying asset	Yes	Infinite	USD denominated crypto-currency value
Panel B: Model Comparison					
	Pricing Method		Domain of PDE		
Dual-Purpose Fund in U.S. [7, 8]	Black-Scholes PDE		Half bounded ($S > 0$)		
Dual-Purpose Fund in China [4]	Periodic PDE with nonlocal terminal and boundary conditions		Bounded, with time-dependent lower bound and time-independent upper bound		
Our vanilla A and B	Periodic PDE with nonlocal terminal and boundary conditions		Bounded, with time-dependent lower and upper bound		

The dual-purpose funds in U.S. include those studied in [7] and the prime and scores studied in [8].

an extremely short time period. This is like the top tranche of a CDO contract. If the correlation of all firms covered within the CDO are close to 1, then one firm defaults leads to almost all other firms default. Therefore, to be truly stable, stable coins need a guarantee in the Black Swan events. When combined with insurance from a government, similar to FDIC insurance, the design can also serve as a basis for issuing a sovereign cryptocurrency via a private-public partnership. By doing so, the government can let the private sector do the job of issuing stable coins, except to provide insurance in rare cases, saving government human and financial resources.

1.1 Pros and Cons of Cryptocurrencies

Using cryptocurrencies as a payment method has several benefits. By design, cryptocurrencies can be used without intermediary, and it has a very low cost. Also, the blockchain technology makes the ledger easy to maintain. Finally, since the transaction is recorded to the blockchain anonymously, cryptocurrencies helps in protecting the privacy of their users.

However, there are also some criticisms of cryptocurrencies. First, a payment system with cryptocurrencies lacks a key feature: the confidence that one can get his money back if he is not satisfied with the goods he purchased. [9] Second, unlike government-backed systems, Bitcoin does not have identity verification, audit standards, or an investigation system in case something bad happens. For instance, one may lose all his deposit in cryptocurrencies should his password get stolen, and there is no remedy. Third, Blockchain systems are not as trustworthy as they seem to be. Without an intermediate, individuals are responsible for their own security precautions. [10]

1.2 Existing Stable Coins

There have been three types of issuance to create stable tokens. The first type is issuance backed by accounts in cash, gold, oil, etc. One has certain assets and issues tokens that represent a claim on the underlying asset. The most famous one is Tether, which 100% backed by USD. The conversion rate is 1 tether USDT equals 1 USD. [13] However, Tether has a major disadvantage: the total assets is about \$62.46 million, but the total liabilities is \$63.014 million, with a negative equity more than half million. There are other tokens claimed to link to gold, e.g. Digix, GoldMint, Royal Mint Gold, OzCoinGold, and ONEGRAM, although the claims are hard to verify. Recently in February 2018, the government of Venezuela issued Petro, a cryptocurrency backed by one barrel of oil.

The second type is issuance backed by over-collateralized cryptocurrencies with automatic exogenous liquidation. For example, one can generate \$100 worth of stable coins by depositing \$150 worth of Ether. The collateral will be sold automatically by the smart contract, if the Ether price reaches \$110. Examples of this type include tokens issued by BitShares and MakerDAO.

The third type is seigniorage shares, which has automatic adjustment of the quantity of coin supply: when the price is too high, new coins are issued; when the price is too low, bonds are issued to remove coins from circulation. Typical example of this type include Basecoin [2], etc.

1.3 Government-backed Stable Coins

Besides Venezuela, other countries are considering issuing cryptocurrencies, including Russia and China. For instance, Canadian government also did “Project Jasper” involving the asset CAD-coin, in which a Blockchain network is built for domestic interbank payments settlement. Also, there is a virtual currency working group under the Federal Reserve System in U.S, which uses the Fedcoin internally. As commented by Rod Garrett [6], “The goal is to create a stable (less price volatility) and dependable cryptocurrency that delivers the practical advantages of Bitcoin even if this means involving the central government and abandoning the Libertarian principles that many believe underlay Bitcoin’s creation.”.

There are several advantages of issuing stable coins by governments. They are cheaper to produce than the cash in bills or coins, and stable coins are never worn out. They can be tracked and taxed automatically by the Blockchain technology. Also, they can facilitate statistical works, such as GDP calculation and collecting consumer data. Finally, they can simplify legal money transfers inside and outside Blockchains. The first countries that adapt stable coins will likely see the inflow of money from people who want stable currencies on Blockchains.

2 Product Design

In this section, we introduce the detailed design of our stable coin, including its creation/redemption, its cash flow, and related arbitrage mechanism. We also point out several differences between the product and the dual-purpose funds.

2.1 Vanilla Class A and B Coins

Our stable coin has a dual-class split structure that, combined with smart contract governed rules and market arbitrage mechanism, provides principal-guaranteed fixed incomes and leveraged capital gains for holders of each class, respectively. The Class A Coin, also known as the Income Coin, continuously accumulates interests based on its original net value at last Reset event. It will also receive token payments at each Reset event. The Class B Coin, also known as the Leverage Coin, entitles leveraged participation of the underlying digital assets.

Class A and B coins can be created by depositing underlying tokens to the Custodian contract.¹ Upon receiving underlying tokens of amount M_C , the Custodian contract will return to the sender equal amount of Class A and Class B coins. Such amount C can be calculated by

$$C = \frac{M_C \cdot P_0 \cdot \beta}{2}, \quad (1)$$

where P_0 is the recorded price of underlying token in USD at last contingent reset event, and β is the conversion factor set as 1 at inception (its behaviour is detailed later). Also, holders of Class A and Class B tokens can withdraw deposited underlying tokens at any time by sending equal amount C of Class A and Class B tokens to the Custodian contract. The contract will deduct Class A and Class B tokens, and return to the sender M_C underlying tokens, where M_C can be calculated by:

$$M_C = \frac{2C}{P_0 \cdot \beta}. \quad (2)$$

For instance, if the ETH/USD price is \$500 and $\beta = 1$, then 2 shares of ETH can create 500 shares of Class A coins and Class B coins each, and 500 shares of Class A and B coins each can be redeemed into 2 shares of ETH. Figure 2 illustrate this split structure.

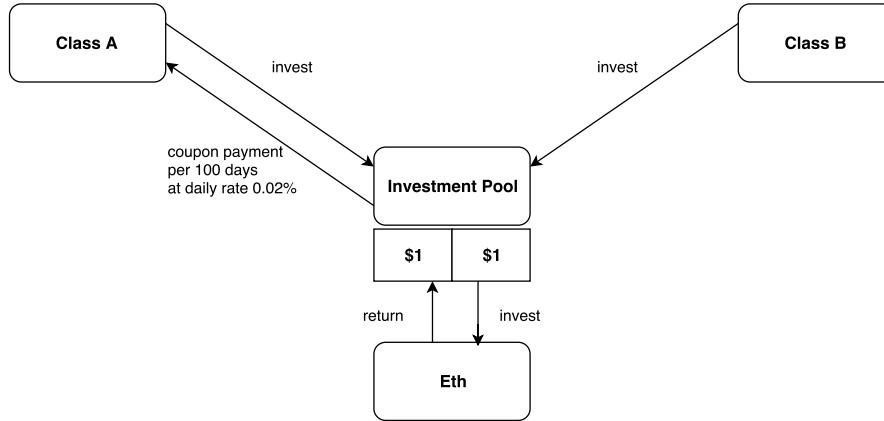


Figure 2: Class A and B, Initial Split. At the beginning, one share of Class A and B each invests \$1 in ETH. The ETH price is \$500, so two shares of ETH correspond to 500 shares of Class A coins and 500 shares of Class B coins. $\beta = 1$.

The net values of Class A and B coins, V_A and V_B , are defined as

$$\begin{aligned} V_A^t &= 1 + R \cdot t, \\ V_B^t &= 2 \cdot \frac{P_t}{P_0 \cdot \beta} - V_A^t, \end{aligned} \quad (3)$$

¹The Custodian smart contract performs multiple tasks that facilitate key mechanism of the system, including: creation and redemption of the stable coin, safekeeping the underlying digital assets (e.g. ETH), calculation of tokens' net values, and execution of Reset events. The deposited underlying tokens are kept by the Custodian contract, as collateral of the Class A and Class B coins issued by the contract. Any user or member of the public can verify the collateral and tokens issued through third party applications such as Etherscan.io.

where R is the *daily* coupon rate, t is the number of days from last reset event, and P_t is the current price of underlying token in USD. The net asset values are used to determine the cash flow of Class A and B.

Next, we describe the cash flow of Class A and B coins. Simply put, the holders of Class B tokens borrow capital from the holders of Class A tokens and invest in a volatile asset (i.e. ETH), which leads the Class B token to possess a continuum of leverage ratios. To reduce risk of both classes, a set of upward and downward reset clauses is imposed. Resets preserve total value in the system.

When a given time period (100 days) has passed from the last reset time, or equivalently, V_A^t grows to upper limit \mathcal{H}_p , a regular payout is triggered. On a regular payout, the total amount of both classes token remain unchanged. The net asset value of Class A reset to 1 USD. Class A holder will receive payment with value $V_A^t - 1$. The conversion factor $\beta_{t+} = \beta_t \cdot \frac{2P_t}{2P_t - P_0 \cdot \beta_t \cdot (V_A^t - 1)}$. For instance, 100 days after the creation, a regular reset occurs and Class A receives \$0.02 coupon payment (assuming $R = 0.02\%$), as illustrated in Figure 3.

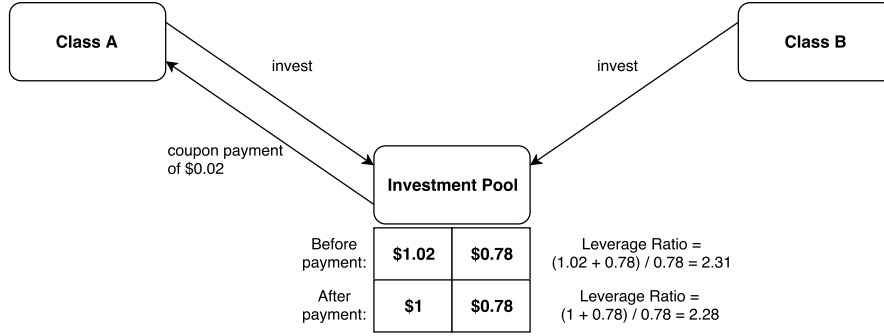


Figure 3: Class A and B, Regular Payout. After 100 days, the ETH price drops to \$450, so that total investment of one Class A coin and one Class B coin becomes \$1.8, within which \$1.02 belongs to Class A. A regular payout takes place, and Class A receives \$0.02 coupon payment. New exchange ratio: 2 shares of ETH now correspond to 505.62 ($= 500 \times \frac{2 \times 450}{2 \times 450 - 500 \times 0.02}$) shares of Class A and 505.62 shares of Class B, yielding $\beta = 1.01$.

An upward reset is triggered when the Net Value of Class B token reaches the upper limit \mathcal{H}_u . On an upward reset, total amount of both classes token remains unchanged, net asset of both classes resets to 1 USD. Class A and B's holders will receive payments of value $V_A^t - 1$ and $V_B^t - 1$, respectively.² Conversion factor β is reset to 1. For instance, as illustrated in Figure 4, after another 50 days, the Class B NAV grows to \$2, triggering an upward reset. Class A and B receive payments with amount \$0.01 and \$1, respectively.

Finally, a Downward Reset is triggered when the net asset value of Class B coins reaches the lower limit \mathcal{H}_d . Similar to an Upward Reset, a Downward Reset restores the leverage ratio. By reducing leverage ratio and restoring net asset value, the structure strengthens principal protection to Class A holders. On a downward reset, each one share of both classes is reduced to $(V_B^t)^+$, where $x^+ = \max\{x, 0\}$ denotes the positive part. The net Value of both classes resets to 1 USD. Class A holders will receive $V_A^t - |V_B^t|$, and the conversion factor β is reset to 1. Note that, under a black swan event such that $V_B^t < 0$, both classes are fully liquidated, and the payment to Class A is lower than V_A^t , that is, Class A takes a loss. For instance, as illustrated in Figure 5, after another 50 days, Class B NAV drops to \$0.25, triggering a downward reset. Class A receives \$0.01 coupon payment and \$0.75 principal payback, and then both classes undergo a 4:1 merger.

²Payments to both classes are made in the form of underlying token from the Custodian contract. For instance, on upward reset, Class A and B receive underlying tokens with amount $\frac{V_A^t - 1}{P_t}$ and $\frac{V_B^t - 1}{P_t}$, respectively.

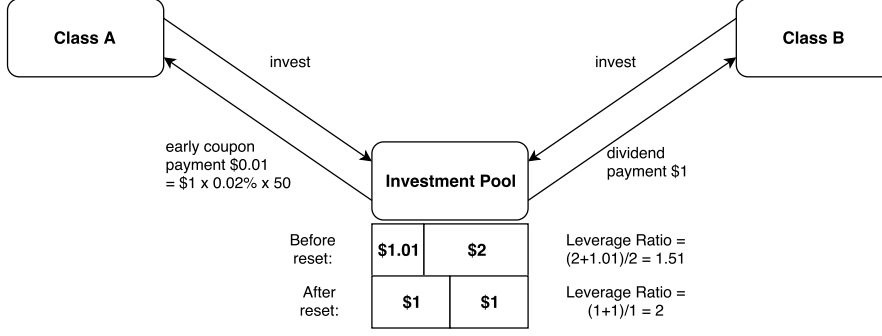


Figure 4: Class A and B, Upward Reset. After 50 days, the ETH price grows to \$760.95, and Class B NAV grows to \$2, triggering an upward reset. Class A NAV equals \$1.01, where \$0.01 is half-year accrued coupon. On this date, Class A receives \$0.01 coupon payment, and Class B receives \$1 dividend payment. New exchange ratio: 2 shares of ETH now correspond to 760.95 shares of Class A and 760.95 shares of Class B, yielding $\beta = 1$.

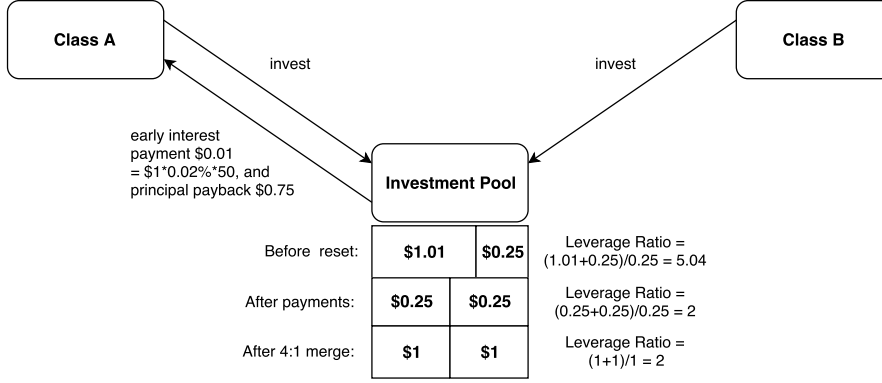


Figure 5: Class A and B, Downward Reset. After another 50 days, the ETH price drops to \$479.40, and Class B NAV drops to \$0.25, triggering a downward reset. Again, Class A NAV equals \$1.01, where \$0.01 is half-year accrued coupon. On this date, Class A receives \$0.01 coupon payment, as well as \$0.75 principal payback. Then, Class A and B each undergo a 4:1 merger, so that both have NAV equal to \$1. New exchange ratio: 2 shares of ETH now correspond to 479.40 shares of Class A and 479.40 shares of Class B, yielding $\beta = 1$.

No arbitrage implies that the prices of Class A and B coins satisfy

$$W_A^t + W_B^t = \frac{2P_t}{\beta_t P_0},$$

where P_t is the USD price of the underlying cryptocurrency, W_A and W_B are the price of the Class A and B coins, and β_t is the conversion ratio. Class A coin behaves like a corporate bond. Although Class A has a fixed coupon rate and its coupon payment is periodic and protected by the resets, its value is still volatile on non-coupon dates. The main risk of Class A is not credit risk, but the risk of a downward reset. On a downward reset, a portion of Class A coin will be liquidated, so the investor will lose the value of future coupons that would be generated from this portion. Therefore, a downward reset will reduce the value of Class A. We propose two classes of more stable coins, the class of A' and B' coins and the class of A0 and A1 coins.

2.2 Class A' and B' Coins

This extension splits Class A into two sub-classes: Class A' and B'. Both classes invest in Class A coins. At any time, two Class A coins can be split into one Class A' and one Class B' coin. Conversely, one Class A' and B' coin can be merged into 2 Class A coins. The split structure for Class A' and B' resembles that for Class A and B: Class

B' borrows money from Class A' at the rate R' to invest in Class A. Here R' is set to close to the risk-free rate r , whereas the rate R for Class A is generally much higher.

Class A' and B' resets *when and only when* Class A resets or gets regular payout. Class A' gets coupon at the rate R' on regular payouts, upward and downward reset (provided the net asset value of Class B then is positive), and Class B' gets coupon at the rate $2R - R'$ on upward reset. On downward resets, each one share of both Class A' and B' is reduced to $(V_B^t)^+$ shares, and Class A' gets the value of the liquidated shares. In the extreme case where $V_B^t \leq 0$, then both Class A' and B' are fully liquidated, and A' receives its full NAV $1 + R't$, or the remaining total asset for A' and B', $2(1 + Rt - |V_B^t|)$, whichever is smaller. Class A' behaves like cash, except in extreme case, when the underlying asset suddenly jumps (not smooth transit) to close to zero. Using the same example as in Section 2.1, Figure 6 illustrates the cash flow of Class A' and B' coins.

2.3 Class A0 and A1 Coins

In this extension, each Class A coin is split into one Class A0 coin and one Class A1 coin. On the next coupon payment date or reset date t , Class A1 receives the coupon payment for Class A, and then Class A1 is terminated. Class A0 is then split into Class A0 coin and Class A1 coin, until the next reset when Class A1 receives payment and A0 is split again, so on and so forth. At any time, the quantity of Class A0 and A1 maintains 1:1. At any time, the value of Class A1 equals the expected discounted value of Class A's next payment on the next reset or coupon payment date. The value of Class A0 equals the difference between values of Class A and A1. Using the same example as in Section 2.1, Figure 7 illustrates the cash flow of Class A0 and A1 coins.

By contract design, the coupon of Class A1 is delivered in the form of the underlying token, whose value in USD may subject to volatile changes due to the high volatility of ETH. In contrast, the coupon of Class A0 is paid in the form of Class A1 token, whose value in USD is much less volatile compared to ETH. Therefore, Class A0 is more suitable for investors with lower risk tolerance or are less active on the market; upon receiving Class A1 tokens as coupon, they have a relatively longer period of time to liquidate the token before its value changes noticeably. In contrast, Class A1 is more suitable for investors who are willing to take certain degree of risk and are more active on the market; so that upon receiving the underlying token, they can monitor the market actively and spot a good opportunity to liquidate the underlying token.

2.4 Differences from the Dual-Purpose Fund Contract

There are four main differences between DUO with dual-purpose funds in China. First, for the coupon payments from the upward and downward resets and regular payouts, the price of a underlying fund in China will change their values, but here the underlying ETH price will never change by the resets. Second, during the regular payout and the upward and downwards resets, the exchange ratio of the shares between the underlying asset and A and B funds will change in our case, to maintain that the related value of the underlying asset is equal to the sum of Fund A and Fund B immediately after these events; in particular, during the regular payout the new exchange ratio will be determined by the coupon rate, and during the upward and downward resets the new exchange ratio will be determined by the prevailing market price of the underlying asset. Third, for

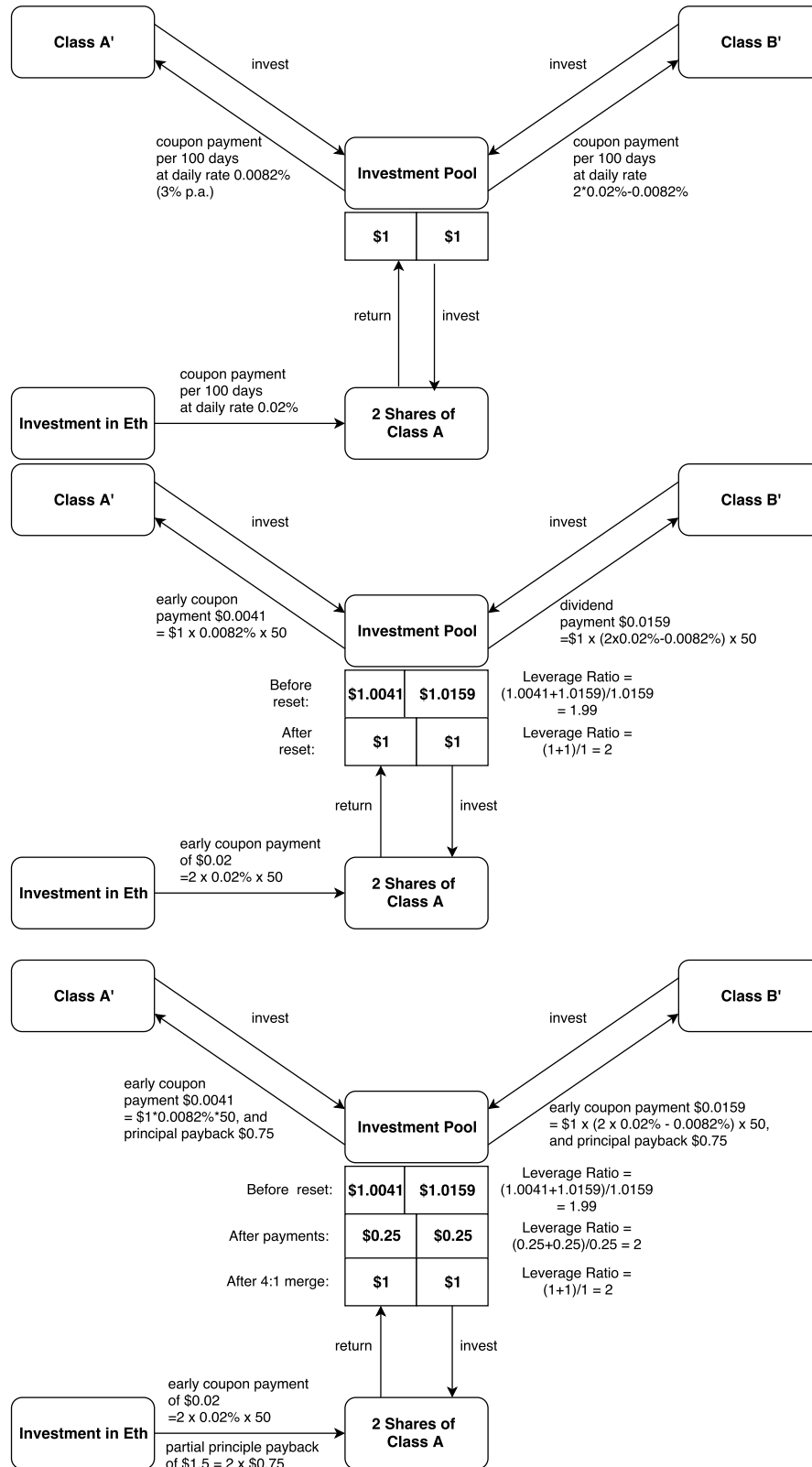


Figure 6: **Top Figure:** What happens to Class A' on a regular payout date of A. On regular payout dates for Class A (per 100 days), 2 shares of A receives coupon payment \$0.04, i.e. at daily rate 0.02%. \$0.0082 is paid to A' and \$0.0318 to B'. **Middle Figure:** Upward Reset of Class A'. After 50 days, Class B's NAV grows to \$2, triggering an upward reset. **Bottom Figure:** Downward Reset of Class B'. After another 50 days, Class B NAV drops to \$0.25, triggering a downward reset.

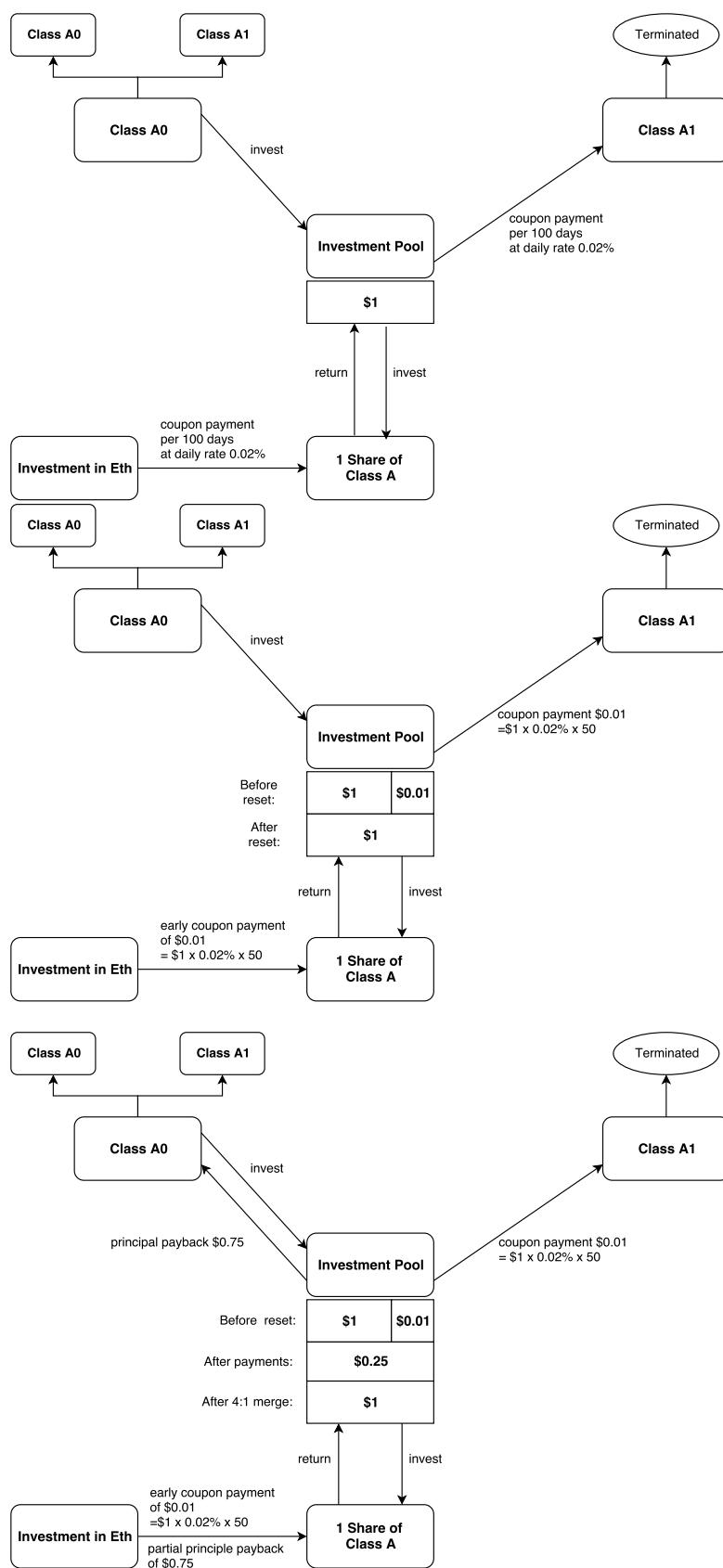


Figure 7: **Top Figure:** Class A0 receives no coupon. Class A1 receives all the coupon payment. After the coupon payment, Class A1 is terminated, and 1 Class A0 is split into 1 new Class A0 and Class A1. **Middle Figure:** Upward Reset of Class A0. After 50 days, Class B NAV grows to \$2, triggering an upward reset. **Bottom Figure:** After another 50 days, Class B NAV drops to \$0.25, triggering a downward reset.

the dual-purpose funds, the upward reset is triggered by the underlying up-crossing \mathcal{H}_u while the downward reset is triggered by the Net Value of B share down-crossing \mathcal{H}_d . In contrast, for DUO, the triggering conditions of both upward and downward resets are all based on the Net Value of Class B token. This brings about symmetry and simplicity to the triggering condition, making it easier to understand. Finally, Chinese dual purpose funds have service fees for the underlying asset, where here the underlying ETH does not.

3 Valuation

In this section, we discuss the valuation of coins we described in Section 2, including Class A and B coins, Class A', B' coins, and Class A0 and A1 coins. For each of them, we describe its risk-neutral value in terms of a stochastic representation, and the corresponding partial differential equation (PDE) under the geometric Brownian motion assumption.

3.1 Class A and B coins

Let the downward reset boundary be $H_d(t) = \frac{1}{2}(1 + Rt) + \frac{1}{2}\mathcal{H}_d$, and upward reset boundary $H_u(t) = \frac{1}{2}(1 + Rt) + \frac{1}{2}\mathcal{H}_u$. Denote $W_A(t, S)$ as the market value of Class A coin with time from last interest payment $0 \leq t \leq T$, with $S_t = P_t/(\beta_t P_0)$, $H_d(t) \leq S_t \leq H_u(t)$. By the design of contract, S returns to 1 on every reset date, and is reduced by $\frac{1}{2}RT$ on every regular payout date.

Under the risk-neutral pricing framework, the current market value of Class A token, $W_A(t, S)$, is given recursively as

$$W_A(t, S) = E_t \left[\sum_{1 \leq i < \tau \wedge \eta} e^{-r(i-t)} RT + e^{-r(\tau-t)} (R\tau + W_A(0, 1)) \cdot \mathbf{1}_{\{\tau < \eta\}} + e^{-r(\eta-t)} (R\eta + 1 - |V_B^\eta| + (V_B^\eta)^+ W_A(0, 1)) \cdot \mathbf{1}_{\{\eta < \tau\}} \right], \quad (4)$$

where E_t is the expectation computed under the risk-neutral measure and under the initial condition $S_{t-} = S$, random times ζ , τ and η represent the first regular payout, upward and downward reset date from t , respectively. Once we calculate W_A , the value of Class B token can be calculated as $W_B = 2S - W_A$.

The value of Class A can be determined as above in a recursive manner, since investors still get Class A token in addition to the payments after a reset. On the right hand side, the first term is value of the all coupons on the regular payout dates before the first reset. The second and third terms describe the cash flow on upward and downward resets. The second term shows that, if the reset is an upward reset, investors get coupon payment, and the time from last reset changes to 0 and S to 1. The third term shows that, if a downward reset comes first, investors receive payment of value $V_A^\eta - |V_B^\eta|$ (including coupon payment of value $V_A^\eta - 1$ and compensation for the quantity reduction $1 - V_B^\eta$), each Class A token reduces to V_B^η token, and the time from last reset changes to 0 and S to 1. As long as $V_B^\eta \geq 0$, Class A receives its accrued coupon and full value for the

quantity reduction, and hence obtains its full NAV. However, under a black swan event when $V_B^\eta < 0$, Class A losses V_B^η of its NAV.

One can estimate W_A via (4) using Monte Carlo simulation, which is also proposed by [1] to deal with the complexities in the fund contract. Due to the high volatility of the underlying token price, it is important to achieve real-time calculation of W_A . However, the efficiency of the simulation-based method is not high enough for this purpose, since the cash flow of Class A token has an infinite horizon and a weakly path-dependent nature. Therefore, in the following we propose an efficient PDE-based estimation method.

Next, we describe a PDE characterization of W_A . We assume that P follows a geometric Brownian motion under the risk neutral measure:

$$dP_t = rPdt + \sigma P_t dW_t,$$

where W_t is a one-dimensional standard Brownian motion. Then, W_A can be characterized in terms of a partial differential equation:

$$-\frac{\partial W_A}{\partial t} = \frac{1}{2}\sigma^2 S^2 \frac{\partial^2 W_A}{\partial S^2} + rS \frac{\partial W_A}{\partial S} - rW_A, \quad t \in [0, T), \quad S \in (H_d(t), H_u(t)) \quad (5)$$

$$W_A(T, S) = RT + W_A(0, S - \frac{1}{2}RT), \quad (6)$$

$$W_A(t, H_u(t)) = Rt + W_A(0, 1) \quad (7)$$

$$W_A(t, H_d(t)) = Rt + 1 - \mathcal{H}_d + \mathcal{H}_d W_A(0, 1). \quad (8)$$

The main feature of the above PDE problem is the nonlocal terminal and boundary conditions (6) – (8), where the given data also depends on the solution W_A itself. Although (5) involves the standard Black-Scholes operator (due to our geometric Brownian motion assumption), the presence of the solution W_A in terminal and boundary data makes the PDE significantly different from the classical Black-Scholes PDE, leading to challenges in both theoretical and numerical aspects. On the theoretical aspect, the existing stochastic representation result is not applicable to PDE (6) – (8) due to the nonlocalness of the terminal and boundary conditions. On the numerical aspect, the nonlocalness in the terminal and boundary data also causes problem since a numerical solution in the interior region depends on the boundary and terminal data, which in turns depends on the numerical solution in the interior region. To solve this, we propose an iterative procedure presented in Appendix C.

The nonlocal terminal and boundary conditions in (6) – (8) are directly related with the cash flow of Class A token. The upper boundary condition (7) at $S = H_u(t)$ corresponds to the upward reset, when early payment Rt is delivered and S resets to 1; the lower boundary condition (8) at $S = H_d(t)$ corresponds downward reset, when early payment $1 - \mathcal{H}_d + Rt$ is delivered to Class A, each Class A token shrinks to \mathcal{H}_d token, and S resets to 1.³ Finally, the terminal condition (6) corresponds to the regular payout, where Class A receives coupon payment RT and S is reduced by $\frac{1}{2}RT$.

³Since P has continuous sample path due to the geometric Brownian motion assumption, we have $V_B^\eta = \mathcal{H}_d$ on downward resets.

3.2 Class A' and B' Coins

Under the risk-neutral pricing framework, the current market value of Class A' token, $W_{A'}(t, S)$ is given recursively as

$$E_t \left[\sum_{1 \leq i < \tau \wedge \eta} e^{-r(i-t)} R' T + e^{-r(\tau-t)} (R' \tau + W_{A'}(0, 1)) \cdot \mathbf{1}_{\{\tau < \eta\}} \right. \\ \left. + e^{-r(\eta-t)} (\min\{R' \eta + 1 - (V_B^\eta)^+, 2(R\eta + 1 + V_B^\eta)^+\} + (V_B^\eta)^+ W_{A'}(0, 1)) \cdot \mathbf{1}_{\{\eta < \tau\}} \right],$$

where τ and η are the first upward and downward reset of Class A (or equivalently, Class A' and B') after t , respectively. On downward reset, if $V_B^\eta > 0$, Class A' receives coupon $R'\eta$, $1 - V_B^\eta$ shares of A' is liquidated, and A' receives the liquidation value; if $\frac{R'\eta-1}{2} - R\eta \leq V_B^\eta \leq 0$, A' is fully liquidated, and still receives full NAV; otherwise, A' is fully liquidated and takes a loss by receiving $2(1 + R\eta + V_B^\eta)^+$ which is smaller than its NAV $1 + R\eta$. Recall that Class A will suffer a loss if $V_B^\eta < 0$ on downward reset, therefore Class A' is safer than Class A since it can still recover its full NAV in this case, provided $V_B^\eta \geq \frac{R'\eta-1}{2} - R\eta$; only when $V_B^\eta < \frac{R'\eta-1}{2} - R\eta$ will Class A' take a loss.

By assuming that P_t follows a geometric Brownian motion, we can also show that $W_{A'}$ satisfies the following PDE. This ODE is the same as that for W_A , except for changing R to R' for the coupon payment:

$$-\frac{\partial W_{A'}}{\partial t} = \frac{1}{2} \sigma^2 S^2 \frac{\partial^2 W_{A'}}{\partial S^2} + rS \frac{\partial W_{A'}}{\partial S} - rW_{A'}, \quad t \in [0, T), \quad S \in (H_d(t), H_u(t)) \\ W_{A'}(T, S) = R' T + W_{A'}(0, S - \frac{1}{2} R T), \\ W_{A'}(t, H_u(t)) = R' t + W_{A'}(0, 1) \\ W_{A'}(t, H_d(t)) = R' t + 1 - \mathcal{H}_d + \mathcal{H}_d W_{A'}(0, 1).$$

Then, the value of Class B' coin is calculated as $2W_A - W_{A'}$.

3.3 Class A0 and A1 Coins

Under the risk-neutral pricing framework, the market value $W_{A1}(t, S)$ of Class A1 coin is given as

$$E_t \left[e^{-r(\zeta-t)} R T \cdot \mathbf{1}_{\{\zeta \leq \tau, \eta\}} + e^{-r(\tau-t)} R \tau \cdot \mathbf{1}_{\{\tau < \eta, \zeta\}} \right. \\ \left. + e^{-r(\eta-t)} (R\eta - (V_B^{\eta-})^-)^+ \cdot \mathbf{1}_{\{\eta < \tau, \zeta\}} \right],$$

where the first regular payout time ζ , the first upward reset time τ and the first downward reset time η are defined as before. On a downward reset, if $V_B^{\eta-} > 0$, A1 gets the coupon payment $R\eta$; if $V_B^{\eta-} \leq 0$, A1 only gets a part of the coupon $(R\eta + V_B^{\eta-})^+ < R\eta$.

By assuming that P_t follows a geometric Brownian motion, W_{A1} is the unique solution of the following PDE

$$\begin{aligned} -\frac{\partial W_{A1}}{\partial t} &= \frac{1}{2}\sigma^2 S^2 \frac{\partial^2 W_{A1}}{\partial S^2} + rS \frac{\partial W_{A1}}{\partial S} - rW_{A1}, \quad t \in [0, T), \quad S \in (H_d(t), H_u(t)) \\ W_{A1}(T, S) &= RT \\ W_{A1}(t, H_u(t)) &= Rt \\ W_{A1}(t, H_d(t)) &= Rt. \end{aligned}$$

Finally, the value of Class A0 coin is calculated as $W_{A0} = W_A - W_{A1}$.

4 Numerical Examples

For illustration, we use Ethereum (ETH) as the underlying token, during the period from 1 Oct 2017 to 28 Feb 2018. We further assume that the price is monitored on a *daily* basis, the upward and downward resets are performed according to the end-of-day prices, and reinvestment of ETH payout as coupon payout is not considered. The default model parameters are selected as follows.

$$\begin{array}{lll} R = 0.02\% \text{ (7.3\% p.a.)} & R' = 0.0082\% \text{ (3\% p.a.)} & r = 0.0082\% \text{ (3\% p.a.)} \\ \mathcal{H}_u = 2 & \mathcal{H}_p = 1.02 & \mathcal{H}_d = 0.25 \\ \sigma = 0.0628 \text{ (120\% p.a.)} & T = 100. & \end{array}$$

4.1 Market Values of Class A and Class B

We first compute the market values of Class A and Class B coins, based on the geometric Brownian motion assumption and on the historical prices of ETH. Figure 8 shows that, although Class A has a fixed coupon rate, and its coupon payment is periodic and protected by the resets, its value is still volatile on non-coupon dates. This should be compared to the behavior of a junk bond, whose value is influenced by its issuer's credit risk. In contrast, the main risk of Class A is not credit risk, but the risk of a downward reset. On a downward reset, a portion of Class A token will be liquidated, so the investor will lose the value of future coupons that would be generated from this portion. Therefore, an approaching downward reset will pull down the value of Class A. This is illustrated in Figure 8 at the end of January: as the downward reset approaches, the value of Class A also goes down, especially when the model underestimates the market volatility (by setting $\sigma = 0.0262$ per day (annualized 0.5)).

Figure 9 shows the simulated paths from class B coins. Note that B has upward resets (on 24 Nov 2017, 17 Dec 2017, and 7 Jan 2018) with dividend payments \$1.0846, \$1.0467, and \$1.1106 and downward resets on (7 Jan 2018).

4.2 Market Value of Class A' and B'

We can see from Figure 10 that the market value of Class A' token is very stable during our sample period, with a value close to 1, except for four downward jumps. These downward jumps correspond to the coupon payment of Class A' on the reset dates of

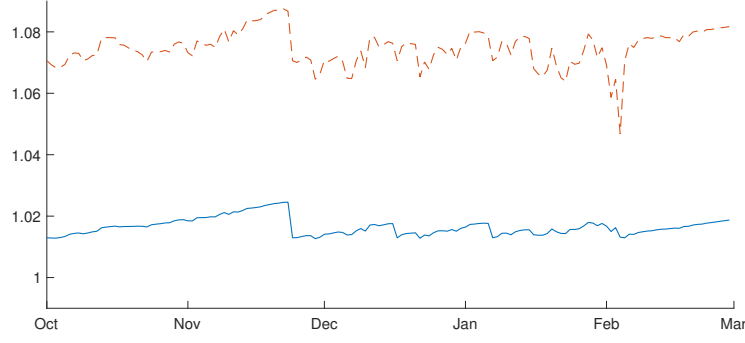


Figure 8: Simulated class A Market Value. $\sigma = 0.0628$ for the blue solid curve, $\sigma = 0.0262$ for the red dashed curve. Parameters: $R = 0.02\%$, $\mathcal{H}_d = 0.25$, $\mathcal{H}_u = 2$, $\mathcal{H}_p = 1.02$, $T = 100$, $r = 0.0082\%$ per day (3% per year). Upward reset takes place on 24 Nov 2017, 17 Dec 2017, and 7 Jan 2018. Downward reset date takes place on 5 Feb 2018.

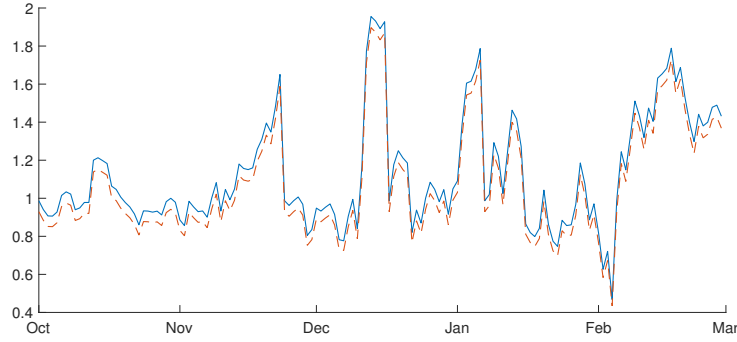


Figure 9: Class B Market Value. $\sigma = 0.0628$ for the blue solid curve, $\sigma = 0.0262$ for the red dashed curve. Parameters: $R = 0.02\%$, $\mathcal{H}_d = 0.25$, $\mathcal{H}_u = 2$, $\mathcal{H}_p = 1.02$, $T = 100$, $r = 0.0082\%$ per day (3% per year). Upward reset takes place on 24 Nov 2017, 17 Dec 2017, and 7 Jan 2018. Downward reset date takes place on 5 Feb 2018.

Class A. If we de-trend the value of Class A' by its NAV and consider $W_{A'} - V_{A'}$, it has an annualized standard deviation of 5.4×10^{-5} , which is much smaller than that of $W_A - V_A$ (0.0178). Even without de-trending, Class A' has an annualized return volatility of 0.0087, which is close to that of the short term U.S. treasury bill, 0.00849 (912828UZ Govt, from April 2013 to February 2018).

4.3 Market Value of Class A0

Figure 11 shows the simulated path for the prices of class A0, the principal only part of A. A0 has an annualized standard deviation of 0.0413 for $\alpha = 1$, as compared to SD of W_A , which is 0.0530. Note that A0 is still volatile. To make A0 more stable, one can increase the split ratio between A and B from 1:1 to a higher split ratio $\alpha : 1$, ($\alpha > 1$),⁴ resulting in a lower leverage ratio for class B which in turn leads to a lower risk for Class A and Class A0, because the risk of downside resets is lower. Figure 12 illustrates the price of A0 with $\alpha = 2$. Class A0 has an annualized standard deviation of 0.0156 for $\alpha = 2$, as compared to SD of W_A , which is 0.0571. Note that with $\alpha = 2$, the NAV of B is $3S_t - 2(1 + Rt)$, making B more sensitive to S .

⁴The contract design and pricing of stable coin with general $\alpha > 0$ is discussed in the appendix.

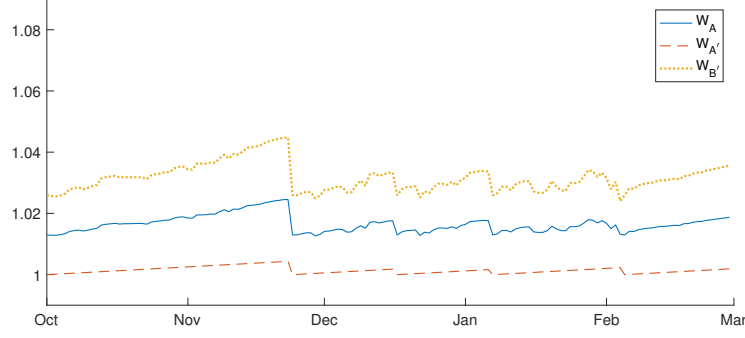


Figure 10: Market Value of Class A' (red) and B' (blue), compared with Class A (black). Annualized volatility of Class A' and B' are 0.0087 and 0.0403, respectively. Parameters: $R = 0.02\%$ per day, $\mathcal{H}_d = 0.25$, $\mathcal{H}_u = 2$, $\mathcal{H}_p = 1.02$, $R' = 0.0082\%$ (3% per year), $T = 100$, $\sigma = 120\%$ per year, $r = 0.0082\%$ per day. Upward reset takes place on 24 Nov 2017, 17 Dec 2017, and 7 Jan 2018. Downward reset date takes place on 5 Feb 2018.

4.4 Black Swan Events

Assume that at time η , an extreme event happens, and there is a 80% sudden drop in the ETH price. Assuming $\beta_{\eta-} = 1$, $P_{\eta-} = P_0 = 500$ (so that the relative price $S_\eta = 1$), and P suddenly drops to $P_\eta = 100$. Then the NAV of Class A coins $V_A^\eta = 2S_{\eta-} \cdot (1 - 80\%) = 0.4$, while the NAV of Class A' coins is $V_{A'}^\eta = 2 \cdot V_A^\eta = 0.8$. A downward reset is triggered, Class A and Class A' are fully liquidated, and they receive \$0.4 and \$0.8 payout, respectively. Therefore, when a sudden drop in ETH price occurs, although both Class A and A' take a loss, A' still recovers a larger value than A.

Now we assume that this kind of downward jump occurs in a jump diffusion model with a Poisson intensity 0.2 per 100 days and constant jump size -80%, then we have at time 0, $W_A(0, 1) = 0.888$ and $W_{A'}(0, 1) = 0.962$; in contrast, if there is no jump risk (intensity equals 0), $W_A(0, 1) = 1.013$, $W_{A'}(0, 1) = 1.000$. Therefore, the presence of extreme jump risk has a smaller impact on Class A' coins.

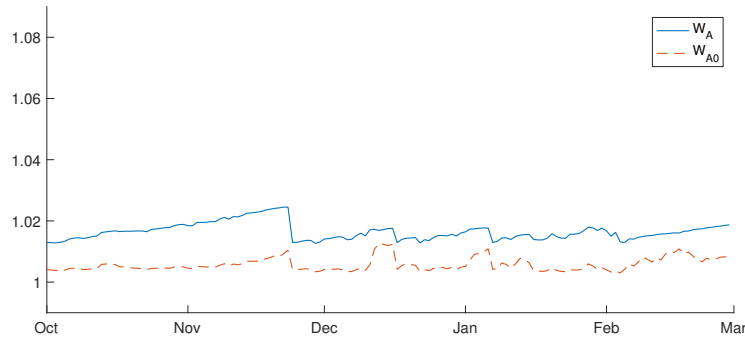


Figure 11: Market Value of Class A0 compared to Class A. Annualized volatility of Class A0 is 0.0255. Parameters: $R = 0.02\%$, $\mathcal{H}_d = 0.25$, $\mathcal{H}_u = 2$, $\mathcal{H}_p = 1.02$, $T = 100$, $\sigma = 120\%$ per year, $r = 0.0082\%$ (3% per year). Upward reset takes place on 24 Nov 2017, 17 Dec 2017, and 7 Jan 2018. Downward reset date takes place on 5 Feb 2018.

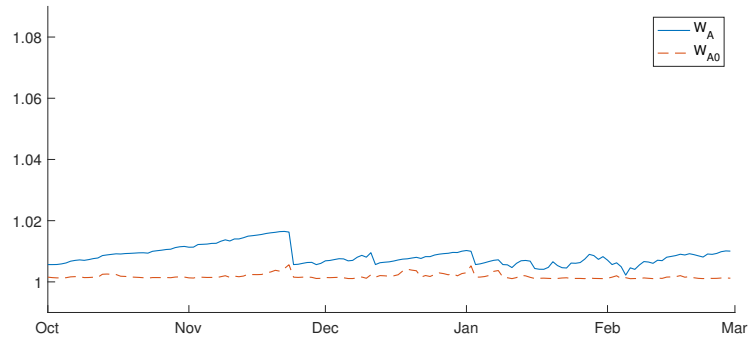


Figure 12: Market Value of Class A0 (principal only class) compared to Class A, where DUO is split into Class A and Class B token with a split ratio 2:1. Annualized volatility of Class A is 0.0125. Parameters: $R = 0.02$ per day, $\mathcal{H}_d = 0.25$, $\mathcal{H}_u = 2$, $\mathcal{H}_p = 1.02$, $T = 100$, $\sigma = 120\%$ per year, $r = 0.0082\%$ (3% per year). Upward reset takes place on 24 Nov 2017, 17 Dec 2017, and 7 Jan 2018. Downward reset date takes place on 5 Feb 2018.

Appendix A Product Design with General Split Ratio

In Section 2, we have described a specific product design where Class A is stable relative to USD as target fiat currency and Class B has initial leverage as 2 ($\alpha = 1$). In addition, transaction cost in creation and redemption is omitted. In this section, a general case is discussed.

A.1 Creation

Dual-class tokens can be created by depositing underlying tokens to the Custodian contract. Upon receiving underlying tokens of amount M_C , the Custodian contract will return to the sender certain amount of Class A and Class B tokens. Such amount C_A and C_B can be calculated by:

$$\begin{aligned} C_B &= \frac{M_C \cdot P_0 \cdot \beta \cdot (1-c)}{1+\alpha} \\ C_A &= C_B \cdot \alpha, \end{aligned} \quad (9)$$

where c is the processing fee of the smart contract, α is a positive number to determine the ratio of A and B, and P_0 is the recorded price of underlying token in target fiat currency at last reset event, and β is the conversion factor set as 1 at inception and its behaviour is detailed later in Section A.6 to A.8.

A.2 Redemption

Holders of Class A and Class B tokens can withdraw deposited underlying tokens at any time by performing a redemption. To do this, the user will send amount of $C \cdot \alpha$ Class A and amount of C Class B tokens to the Custodian contract. The contract will deduct Class A and Class B tokens, and return to the sender M_C underlying tokens, where M_C can be calculated by:

$$M_C = \frac{C \cdot (1-c) \cdot (1+\alpha)}{P_0 \cdot \beta}. \quad (10)$$

A.3 Net Value

The net value of tokens are calculated based on the coupon rate, the elapsed time from last reset event, and the latest underlying token price in target fiat currency fed to the system. In particular:

$$\begin{aligned} V_A^t &= 1 + R \cdot t \\ V_B^t &= (1+\alpha) \cdot \frac{P_t}{P_0 \cdot \beta} - \alpha \cdot V_A^t, \end{aligned} \quad (11)$$

where R is the daily coupon rate, t is the number of days from last reset event, and P_t is the current price of underlying token in target fiat currency.

A.4 Quantity

Below holds in the system at all time

$$Q_A^t = Q_B^t \cdot \alpha,$$

where Q_A^t and Q_B^t are the total amount of Class A and Class B tokens.

A.5 Implied Leverage Ratio

$$L_B^t = \frac{P_t}{P_0 \cdot \beta} \cdot \frac{1 + \alpha}{V_B^t}$$

Note that at inception or after contingent resets, above simply reduces to $L_B^0 = 1 + \alpha$.

A.6 Contingent Upward Reset

An upward reset is triggered when $V_B^t \geq \mathcal{H}_u$. Upon upward reset:

1. Total amount of both classes token remain unchanged, $Q_A^{t+} = Q_A^{t-}$ and $Q_B^{t+} = Q_B^{t-}$.
2. Net Value of both classes reset to 1 target fiat currency.
3. Both classes' holders will receive certain amount of underlying token from the Custodian contract. Such amount for each Class A token is $U_A = \frac{V_A^{t-} - 1}{P_t}$ and for each Class B token is $U_B = \frac{V_B^{t-} - 1}{P_t}$.
4. Conversion factor β is reset to 1.

Total value in the system is unchanged after reset:

$$\begin{aligned} & U_A \cdot P_t \cdot Q_A^{t-} + U_B \cdot P_t \cdot Q_B^{t-} + Q_A^{t+} \cdot V_A^{t+} + Q_B^{t+} \cdot V_B^{t+} \\ &= (V_A^{t-} - 1) \cdot Q_A^{t-} + (V_B^{t-} - 1) \cdot Q_B^{t-} + Q_A^{t-} \cdot 1 + Q_B^{t-} \cdot 1 \\ &= V_A^{t-} \cdot Q_A^{t-} + V_B^{t-} \cdot Q_B^{t-} . \end{aligned}$$

A.7 Contingent Downward Reset

A downward reset is triggered when $V_B^t \leq \mathcal{H}_d$. Upon downward reset:

1. Total amount of Class B token is reduced to $Q_B^{t+} = Q_B^{t-} \cdot V_B^{t-}$.
2. Total amount of Class A token is reduced to $Q_A^{t+} = Q_A^{t-} \cdot \alpha$.
3. Net Value of both classes reset to 1 target fiat currency.
4. Class A holders will receive certain amount of underlying token from the Custodian contract. Such amount of each Class A token is: $D_A = \frac{V_A^{t-} - V_B^{t-}}{P_t}$.
5. Conversion factor β is reset to 1

Total value in the system is unchanged after reset:

$$\begin{aligned} & D_A \cdot P_t \cdot Q_A^{t-} + Q_A^{t+} \cdot V_A^{t+} + Q_B^{t+} \cdot V_B^{t+} \\ &= (V_A^{t-} - V_B^{t-}) \cdot Q_A^{t-} + Q_B^{t-} \cdot \alpha \cdot 1 + Q_B^{t-} \cdot 1 \\ &= V_A^{t-} \cdot Q_A^{t-} - V_B^{t-} \cdot Q_B^{t-} \cdot \alpha + Q_B^{t-} \cdot V_B^{t-} \cdot \alpha + Q_B^{t-} \cdot V_B^{t-} \\ &= V_A^{t-} \cdot Q_A^{t-} + V_B^{t-} \cdot Q_B^{t-} . \end{aligned}$$

Note above used the fact $Q_A^{t-} = Q_B^{t-} \cdot \alpha$.

A.8 Regular Payout

A regular payout is triggered when $V_A^t \geq \mathcal{H}_p$. Upon regular payout:

1. Total amount of both classes token remain unchanged, $Q_A^{t+} = Q_A^{t-}$ and $Q_B^{t+} = Q_B^{t-}$
2. Net Value of Class A reset to 1 USD
3. Class A holder will receive certain amount of underlying token from the Custodian contract. Such amount for each Class A token is $U_A = \frac{V_A^{t-}-1}{P_t}$
4. Conversion factor $\beta^+ = \beta^- \cdot \frac{(1+\alpha) \cdot P_t}{(1+\alpha) \cdot P_t - P_0 \cdot \alpha \cdot \beta^- \cdot (V_A^{t-}-1)}$
5. Unlike contingent resets, P_0 does NOT reset to P_t

Total value in the system is unchanged after reset:

$$\begin{aligned} & U_A \cdot P_t \cdot Q_A^{t-} + Q_A^{t+} \cdot V_A^{t+} + Q_B^{t+} \cdot V_B^{t+} \\ &= (V_A^{t-} - 1) \cdot Q_A^{t-} + Q_A^{t-} \cdot 1 + V_B^{t-} \cdot Q_B^{t-} \\ &= V_A^{t-} \cdot Q_A^{t-} + V_B^{t-} \cdot Q_B^{t-} . \end{aligned}$$

A.9 Market Arbitrage

In the absence of arbitrage, the following price parity shall hold

$$\alpha \cdot P_A^t + P_B^t = \alpha \cdot V_A^t + V_B^t ,$$

where P_A^t is the current price of Class A in target fiat currency, and P_B^t is the current price of Class B in target fiat currency.

Appendix B Derivation of the Pricing Equation

Using contract design under general split ratio $\alpha > 0$, the value of Class A coins is still described by the stochastic representation (4). In this section, under the geometric Brownian motion assumption, we show that (4) defines a unique bounded function W_A , which is exactly the solution to the PDE problem (5) – (8). We denote v_s and Y_s as the time from last interest payment and the number of A shares at time s , respectively. Starting from an initial value 1, Y is reduced by a factor of \mathcal{H}_d on every downward reset dates, reflecting the partial payback of Class A principal. Further denote ζ_i , τ_i , and η_i as the i -th regular payout date, upward reset date, and downward reset date after t , respectively. From the construction of contract,

$$S_{\zeta_i} = S_{\tau_i} = S_{\eta_i} = 1, \quad v_{\tau_i} = v_{\eta_i} = v_{\zeta_i} = 0.$$

Theorem B.1. W_A is the unique classical solution⁵ to the following partial differential equation on $\{(t, S) : 0 \leq t < T, H_d(t) < S < H_u(t)\}$

$$-\frac{\partial W_A}{\partial t} = \frac{1}{2}\sigma^2 S^2 \frac{\partial^2 W_A}{\partial S^2} + rS \frac{\partial W_A}{\partial S} - rW_A \quad (12)$$

$$W_A(T, S) = RT + W_A(0, S - \frac{\alpha}{1+\alpha}RT) \quad (13)$$

$$W_A(t, H_u(t)) = Rt + W_A(0, 1) \quad (14)$$

$$W_A(t, H_d(t)) = Rt + 1 - \mathcal{H}_d + \mathcal{H}_d W_A(0, 1). \quad (15)$$

Proof of Theorem B.1. Note that under the geometric Brownian motion assumption, we always have $V_B^\eta = \mathcal{H}_d$. Using Theorem E1.1 in [4], we can rewrite (4) in a non-recursive form as

$$\begin{aligned} W_A(t, S) = E_t^{(t, S, 1)} & \left[\sum_{\zeta_i \geq t} e^{-R(\zeta_i - t)} Y_{\zeta_i -} RT + \sum_{\tau_i \geq t} e^{-R(\tau_i - t)} Y_{\tau_i -} r v_{\tau_i -} \right. \\ & \left. + \sum_{\eta_i \geq t} e^{-R(\eta_i - t)} Y_{\eta_i -} (r v_{\eta_i -} + 1 - \mathcal{H}_d) \right], \end{aligned} \quad (16)$$

where $E_t^{(u, s, y)}$ is the \mathbb{Q} -expectation computed under the initial condition $v_{t-} = u$, $S_{t-} = s$, and $Y_{t-} = y$. Following the proof in Section 4.1 in [5] shows that (16) is the unique classical solution to the PDE problem (5) – (8). Therefore, W_A defined in (4) is the unique classical solution to (5) – (8). \square

Appendix C Numerical Procedure for the Pricing Equation (5) – (8)

We propose an iterative algorithm to obtain a numerical solution of the periodic parabolic terminal-boundary value problem (5) – (8).

Algorithm 1

1. Set the initial guess $W_A^{(0)} = 0$;
2. For $i = 1, 2, \dots$: Given $W_A^{(i-1)}$, solve for $W_A^{(i)}$, the solution to the equation

$$\begin{aligned} -\frac{\partial W_A}{\partial t} &= \frac{1}{2}\sigma^2 S^2 \frac{\partial^2 W_A}{\partial S^2} + rS \frac{\partial W_A}{\partial S} - rW_A & 0 \leq t < T, H_d(t) < S < H_u(t) \\ W_A(1, S) &= RT + W_A^{(i-1)}(0, S - \frac{1}{2}RT) & H_d(t) < S < H_u(t) \\ W_A(t, H_u(t)) &= Rt + W_A^{(i-1)}(0, 1) & 0 \leq t \leq T \\ W_A(t, H_d(t)) &= Rt + 1 - \mathcal{H}_d + \mathcal{H}_d W_A^{(i-1)}(0, 1) & 0 \leq t \leq T. \end{aligned}$$

3. If $\|W_A^{(i)} - W_A^{(i-1)}\| < \text{tolerance}$, stop and return $W_A^{(i)}$; otherwise set $i = i + 1$ and go to step 2.

⁵By classical solution we mean $W_A \in C^{1,2}(Q) \cap C(\overline{Q} \setminus D)$, where $Q = \{(t, S) : 0 \leq t < 1, H_d(t) < S < H_u(t)\}$ and $D = \{T\} \times \{H_d(T), H_u(T)\}$.

By using a similar proof as Theorem C.1 in [4], one can show that the sequence $(W_A^{(i)})_{i \geq 1}$ defined in Algorithm 1 is monotonically increasing and converges to W_A uniformly.

Appendix D Further Development

This paper has outlined the main design and market mechanism for the dual-class token structure. Further studies can be done in below aspects.

Underlying Price Pair

While the dual class structure is independent of the underlying crypto fiat price pair, the liquidity and popularity of the underlying price pair do impact the viability of the structure as market arbitrage is important to ensure the structure trades as designed. In this paper, ETH/USD is used as the underlying price pair, but other popular ERC20 tokens, such as EOS, ADA, paired with major fiat other than USD, can also be considered.

Optimal Reset Thresholds

It is important to keep leverage for Class B within certain range: not too high so as to protect Class A holders from sudden price drop and not too low so as to keep Class B attractive to leveraged users. However, it is undesirable that resets, especially downward resets, happen too frequently.

There are two main parameters to be determined, the ratio between Class A and Class B shares, α (see Appendix A); and the lower limit of Class B net value, \mathcal{H}_d , that triggers downward resets. The Chinese market over the years has concluded a broadly accepted set of parameters: α is set to 1, meaning the quantities of Class A versus Class B is 1:1; \mathcal{H}_d being 0.25, meaning a downward reset will be triggered if the underlying price dropped approximately 37.5% from last reset. This setup has been tested in extreme market events such as the mid-2015 market crash and the early-2016 circuit breaker turmoil, where the reset clauses were all successfully implemented and protected the interests of Class A holders.

We witness that cryptocurrencies have considerably higher volatility than stock market indices. A series of back testings and Monte Carlo simulations will be performed to investigate the optimal parameters for dual class token structures.

References

- [1] Adams, A. T., and J. B. Clunie. 2006. Risk Assessment Techniques for Split Capital Investment Trusts. *Annals of Actuarial Science* 1:7-36.
- [2] Basecoin: A Price-Stable Cryptocurrency with an Algorithmic Central Bank. http://www.getbasecoin.com/basecoin_whitepaper_0_99.pdf
- [3] Black, F., and M. Scholes. 1973. The Pricing of Options and Corporate Liabilities. *Journal of Political Economy* 81:637-654.
- [4] Dai, M., S. Kou, C. Yang, and Z. Ye. 2018. The Overpricing of Leveraged Products: A Case Study of Dual-Purpose Funds in China. *Working Paper*.
- [5] Dai, M., S. Kou, and C. Yang. 2017. A Stochastic Representation for Nonlocal Parabolic PDEs with Applications. *Working Paper*.
- [6] Garratt, R. 2016. CAD-coin versus Fedcoin. R3 Report 15.
- [7] Ingersoll, J. E. 1976. A Theoretical and Empirical Investigation of the Dual Purpose Funds: an Application of Contingent-claims Analysis. *Journal of Financial Economics* 3:83-123.
- [8] Jarrow, R. A., and M. O'Hara. 1989. Primes and Scores: An Essay on Market Imperfections. *The Journal of Finance* 44:1263-1287.
- [9] Kai Stinchcombe. 2017. Ten years in, nobody has come up with a use for blockchain. <https://hackernoon.com/ten-years-in-nobody-has-come-up-with-a-use-case-for-blockchain-ee98c180100>
- [10] Kai Stinchcombe. 2018. Blockchain is not only crappy technology but a bad vision for the future. <https://medium.com/@kaistinchcombe/decentralized-and-trustless-crypto-paradise-is-actually-a-medieval-hellhole-c1ca122efdec>
- [11] Leverage. <https://www.investopedia.com/terms/l/leverage.asp>
- [12] White Paper: A Next-Generation Smart Contract and Decentralized Application Platform. <https://github.com/ethereum/wiki/wiki/White-Paper>
- [13] Tether: Fiat currencies on the Bitcoin blockchain. <https://tether.to/wp-content/uploads/2016/06/TetherWhitePaper.pdf>
- [14] The Dai Stablecoin System. <https://makerdao.com/whitepaper/DaiDec17WP.pdf>