Designing Stable Coins

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

Version 0.9.0
April 4, 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

1.1 Stablecoins and Fixed Income Assets

Since their inception, crypto currencies aim to create an alternative financial system comparable to fiat financial systems. In a fiat system, money or credit exists in a few different forms: actual currency in circulation and fixed income assets such as time deposits and money market funds, which are the foundation for the rest of the financial market to build on. The crypto market is at primitive stage as it lacks coins or tokens comparable to fiat money due to their huge price volatility, and thus there are no established fixed income assets either.

A Stable token, also known as stablecoin, is a crypto-token that keeps stable market value against a specific index, most noticeably US Dollar. There have been a few attempts to create stable tokens: Tether claims to have 1:1 USD collateral in its centralized bank accounts [9]; Basecoin tries to control money supply by playing an algorithmic version of central bank [10]; MakerDAO uses decentralized over-collateralization to maintain confidence of its Dai stablecoin [11].

Most stable token designs to date face a common problem: their holders bear variable levels of counter-party risks, but there is little incentive or even additional cost to hold these tokens. We believe a crypto-token with low price volatility and stable income is a superior safe haven asset and is essential for a more robust crypto market.

1.2 Risk Segmentation

In the fiat market, risk segmentation exists in every level of market. At asset class level, risk averse investors choose fixed income products while risk seeking investors choose equity or commodity. Within the fixed income market, conservative investors choose safe haven assets such as government bonds while aggressive players choose high yield bonds, or otherwise known as junk bonds.

Although most of crypto assets are considered highly speculative, there still exist different segments of risk appetites. The existence of margin trading in exchanges like BitFinex and Huobi Pro demonstrates the need of leverage from aggressive crypto investors. Similarly, safe haven assets providing low volatility and stable income will be appealing to institutional players, short-term pessimistic investors and ICO project teams. However, to our best knowledge, there is no viable product at the moment.

The price volatility cannot be eliminated, but can be transferred. Through a structured contract, a risk-seeking investor can get exposed to higher leverage with limited assets, while a risk-averse investor can avoid unwanted price fluctuations by entering the other side of the contract. The financial market has created many products satisfying different risk segments, some of which can be very practical for crypto market participants.

1.3 Leveraged Funds

Leverage is the strategy of using borrowed capital to increase the potential return of an investment [7]. Retail investors have less access to leverage methods such as margin loans and financial derivatives, which promotes the creation of leveraged fund products.

An interesting class of leveraged funds is the dual-purpose funds, also known as primes and scores, which are mutual funds that are split into two classes of shares by design: low risk shares and high risk shares. They were designed to provide investors with the opportunity of repackaging their investment incomes and capital flow in accordance with their preferences. Dual-purpose funds first appeared in U.S. in 1965, but faded out in early 1990s due to a change in the tax code that resulted in double taxation [2]. The valuation of dual-purpose funds in U.S. was investigated theoretically and empirically in [4] and [5].

The dual-purpose fund was introduced in China in 2010 and it quickly became one of the most popular leveraged products there, reaching market size of 500 billion CNY (80 billion USD) at its peak. A Chinese dual-purpose fund usually takes an open-end index-tracking fund as underlying and has two classes of shares: the low risk A shares behave like a perpetual bond with periodical coupon payments, and the high risk B shares are essentially a closed-end fund magnifying the exposure of the underlying index. A set of upward and downward reset clauses is imposed to reduce the risk of both shares [2].

We are inspired by the Chinese dual-purpose fund for three reasons: (i) both the income and leveraged shares answer unfulfilled demands of crypto-currency investors; (ii) the market mechanism, pricing formula, and arbitrage method prove to work in real market; and (iii) the structure can be efficiently implemented by Smart Contracts.

1.4 Smart Contract

Smart Contract was first proposed by Nick Szabo in 1994, who described it as “a set of promises, specified in digital form, including protocols within which the parties perform on these promises”.

The idea has not received commercial adoption due to lack of trustworthy execution environment, until the appearance of blockchain technology. Released in 2015, Ethereum implements a nearly Turing-complete language on its blockchain, a prominent smart contract framework. The Ethereum white paper describes smart contracts as “cryptographic boxes contain value and only unlock it if certain conditions are met". It also lists financial derivatives as the most common application of a smart contract, and introduces a rough idea about creating stable-value currencies through a hedging contract [8].

Up until now, the most popular stablecoin solution has been issuer-backed assets. And it is almost a market consensus that such issuers are not always trustworthy. We agree with Ethereum authors’ argument that, a decentralized market of speculators and arbitragers powered by smart contract, could be an alternative solution.

This paper aims to propose an alternative approach of creating stable value tokens, providing a different set of trade offs between price stability, holder incentive and supply flexibility. We believe the solution will be very useful for broader adoption of the crypto market.

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 Overview

DUO a dual-class token 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.

Class A Token also known as the Income Token, continuously accumulates interests based on its original net value at last Reset event. It will also receive token payments at each Reset event.

Class B Token also known as the Leverage Token, entitles leveraged participation of the underlying digital assets.

The Custodian smart contract performs multiple tasks that facilitate key mechanism of the system, including: creation and redemption of DUO tokens, safekeeping the underlying digital assets (e.g. ETH), calculation of tokens' net values, and execution of Reset events.

2.2 Creation and Redemption

2.2.1 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 equal amount of Class A and Class B tokens. Such amount C can be calculated by:

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

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 and its behaviour is detailed later in Section 2.3

The deposited underlying tokens are kept by the Custodian contract, as collateral of the Class A and Class B tokens 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.

2.2.2 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 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:

$$M_C = \frac{2C}{P_0 \cdot \beta} \ . \tag{2}$$

2.2.3 Net Value

The net values of tokens are calculated based on the coupon rate, the elapsed time from last Reset event, and the latest underlying token price in USD fed to the system. In particular,

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

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.

2.2.4 Implied Leverage Ratio

Class B has the following leverage ratio:

$$L_B^t = \frac{P_t}{P_0 \cdot \beta} \cdot \frac{2}{V_B^t}.$$

Note that at inception or after contingent resets, above simply reduces to $L_B^0 = 2$.

2.3 Resets

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.

2.3.1 Contingent Upward Reset

When underlying token price rises, the Class B token's leverage ratio reduces. An upward reset is triggered when the Net Value of Class B token reaches upper limit $\mathcal{H}_u$. The reset will restore the leverage ratio to 2. By increasing Class B's leverage ratio, the structure retains attraction to leverage-seeking users.

Upon upward reset:

1) Total amount of both classes token remains unchanged.

2) Net Value of both classes resets to 1 USD.

3) Both classes' holders will receive certain amount of underlying token from the Custodian contract. Such amount for each Class A token is $\frac{V_A^{t-}-1}{P_t}$ and for each Class B token is $\frac{V_B^{t-}-1}{P_t}$.

4) Conversion factor β is reset to 1.

Total value in the system is unchanged after reset. For details, see Appendix A.6.

2.3.2 Contingent Downward Reset

When the underlying token price falls, the Class B token's leverage ratio increases. A Downward Reset is triggered when the Net Value of Class B token reaches lower limit $\mathcal{H}_d$. Similar to an Upward Reset, a Downward Reset restores the leverage ratio. By reducing leverage ratio and restoring Net Value, the structure strengthens principal protection to Class A holders. Additionally, a Downward Reset will reduce the total supply of Class A and Class B tokens by roughly $1 - \mathcal{H}_d$.

Upon downward reset:

1) Total amount of both classes token is reduced to $Q^{t+} = Q^{t-} \cdot V_B^{t-}$.

2) Net Value of both classes resets to 1 USD.

3) Class A holders will receive certain amount of underlying token from the Custodian contract. Such amount of each Class A token is: $\frac{V_A^{t-}-V_B^{t-}}{P_t}$.

4) Conversion factor β is reset to 1.

Total value in the system is unchanged after reset. For details, see Appendix A.7.

2.3.3 Regular Payout

When a given time period has passed from the last reset time, V_A^{t-} grows to upper limit $\mathcal{H}_p$, a regular payout is triggered to reduce the Net Value of Class A to 1, while Net Value of Class B is unchanged.

Regular payout:

1. Total amount of both classes token remain unchanged.

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 $\frac{V_A^{t-}-1}{P_t}$

4. Conversion factor $\beta^{+} = \beta^{-} \cdot \frac{2P_t}{2P_t - P_0 \cdot \beta^{-} \cdot \left(V_A^{t-} - 1\right)}$.

5. Unlike contingent resets, P_0 does NOT reset to P_t.

Total value in the system is unchanged after reset. For details, see Appendix A.8.

2.4 Market Mechanism

2.4.1 Premium and Discount

Like all fixed income products, Class A is expected to trade on premium or at discount with respect to its net value, depending on market condition. When Class A trades on premium, that generally indicates a higher demand for income over leverage and thus Class A buyers are getting lower yield. On the contrary, when Class A trades at discount, that implies a higher demand for leverage over income and thus Class A buyers are paying less and getting higher yield. In an orderly market, Class A's market price can be used to derive the current market cost of funding. As net values draw closer to resets, Class A might trade closer to its net value as traders start exploiting arbitrage opportunities.

2.4.2 Market Arbitrage

The dual class tokens are two-way fungible to the underlying token (i.e. ETH). Thus, a price parity shall hold as below:

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

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

Along with Equation (3) in Section 2.2, the following relation should hold:

$$P_A^t + P_B^t = 2 \cdot \frac{P_t}{P_0 \cdot \beta} \ .$$

On open market, arbitrage opportunity exists when Class A and Class B tokens trade away from their net values and the above equation is likely violated on either side.

2.5 Differences from the Dual-Purpose Fund Contract

Although the contract of DUO is inspired by dual-purpose funds, it is different from dual-purpose funds in U.S. and China in the aspects shown in Table 1.

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

	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	Periodic payments on upward reset dates	Yes	Infinite	Stock Index
DUO	Fixed Income	Periodic payments on upward reset dates	Yes	Infinite	USD denominated crypto-currency value

The dual-purpose funds in U.S. include those studied in [4] and the prime and scores studied in [5].

There are three main technical difference between DUO with dual-purpose funds in China. (1) During the upward and downward resets, the underlying funds in China will change their values by issuing more shares. In contrast, here the underlying ETH price will never change by the resets. (2) For 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. (3) Chinese dual purpose funds have service fees for the underlying asset, where here the underlying ETH does not.

Both the dual-purpose funds and DUO values can be characterized in terms of partial differential equation (PDE). However, their PDEs differ in the following aspects.

Table 2: Model Comparison of DUO and Dual-Purpose Fund in U.S. and China

	Pricing Method	Domain of PDE
Dual-Purpose Fund in U.S.	Black-Scholes PDE	Half bounded ($S > 0$)
Dual-Purpose Fund in China	Periodic PDE with nonlocal terminal and boundary conditions	Bounded, with time-dependent lower bound and time-independent upper bound
DUO	Periodic PDE with nonlocal terminal and boundary conditions	Bounded, with time-dependent lower and upper bound

3 Valuation

Denote W_A and W_B as the market value of Class A and Class B, respectively. Denote $S_t = P_t/(P_0 \cdot \beta)$ as the relative price of the underlying token. By the design of contract, S returns to 1 on every contingent 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 is given recursively as

$$\begin{aligned} W_A(t,S) = E_t \Bigg[& \sum_{1 \le i < \tau \wedge \eta} e^{-r(i-t)} RT + e^{-r(\tau-t)} (R\tau + W_A(0,1)) \cdot \mathbf{1}_{\{\tau<\eta\}} \\ & + e^{-r(\eta-t)} (R\eta + 1 - V_B^{\eta-} + V_B^{\eta-} W_A(0,1)) \cdot \mathbf{1}_{\{\eta<\tau\}} \Bigg], \end{aligned} \tag{4}$$

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. $W_A(t,S)$ denotes the market value of Class A token with time from last interest payment $0 \le t \le 1$, with $H_d(t) \le S \le H_u(t)$ and $0 \le t < T$, where $H_d(t) = \frac{1}{2}(1 + Rt) + \frac{1}{2}\mathcal{H}_d$, and $H_u(t) = \frac{1}{2}(1 + Rt) + \frac{1}{2}\mathcal{H}_u$. 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 $V_B^{\eta-}$ token, and the time from last reset changes to 0 and S to 1.

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.

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:

$$\begin{aligned}
-\frac{\partial W_A}{\partial t} &= \frac{1}{2}\sigma^2 S^2 \frac{\partial^2 W_A}{\partial S^2} + rS\frac{\partial W_A}{\partial S} - rW_A, \quad t \in [0,T),\ S \in (H_d(t), H_u(t)) && (5)\\
W_A(T,S) &= RT + W_A(0, S - \frac{1}{2}RT), && (6)\\
W_A(t, H_u(t)) &= Rt + W_A(0,1) && (7)\\
W_A(t, H_d(t)) &= Rt + 1 - \mathcal{H}_d + \mathcal{H}_d W_A(0,1). && (8)
\end{aligned}$$

The main feature of the above PDE problem is the nonlocal terminal and boundary conditions (6) – (8), where the given data also depend 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.[1] Finally, the terminal condition (6) corresponds to the regular payout, where Class A receives coupon payment RT and S is reduced by $\frac{1}{2}RT$.

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

4 Extensions

To make the stable token defined in Section 2 even more stable, we consider two extensions on the DUO contract, which split Class A token into two further classes of token.

4.1 A=A0+A1

This extension splits Class A further into two sub-classes: A0 and A1. At the creation of DUO, each Class A token is split into one Class A0 token and one Class A1 token. On the next reset date t, Class A1 receives the coupon payment $V_A^{t-} - 1$ for Class A, and then Class A1 is terminated. Class A0 receives ETH token with value $(1 - V_B^{t-})^+$ as liquidation payment, and is then split into $1-(1-V_B^{t-})^+$ Class A0 token and $1-(1-V_B^{t-})^+$ Class A1 token, until the next reset when Class A1 receives payment and A0 is split again, so on and so forth.[2] At any time, the quantity of Class A0 and A1 maintains 1:1. Based on this construction, at any time, the value of Class A1 equals the expected discounted value of Class A's next payment on the next reset date, and the value of Class A0 equals the difference between values of Class A and A1, or the expected present value of all future payments except the first one.

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.

Under the risk-neutral pricing framework, the market value of Class A1 token is given as

$$W_A(t,S) = E_t\left[e^{-r(\zeta - t)} RT \cdot \mathbf{1}_{\{\zeta \le \tau, \eta\}} + e^{-r(\tau - t)} R\tau \cdot \mathbf{1}_{\{\tau < \eta, \zeta\}} + e^{-r(\eta - t)} R\eta \cdot \mathbf{1}_{\{\eta < \tau, \zeta\}} \right],$$

where the first regular payout time ζ, the first upward reset time τ and the first downward reset time η are defined in the same way as (4). W_{A1} corresponds to the following PDE

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

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

[2] Note that when $V_B^{t-} \ge 1$, Class A0 does not receive any underlying token and maintains the same quantity.

4.2 A=A′ +B′

This second extension splits Class A into two sub-classes: Class A′ and B′. Class A′ and B′ invest in Class A token. At any time, two Class A token can be split into one Class A′ and one Class B′ token. Conversely, one Class A′ and B′ token can be merged into 2 Class A token. The net asset value of Class A′ is defined as $V_{A'} = 1 + R't$, where t is the time since last reset, and the net asset value of Class B′ is defined as $V_{B'} = 1 + 2Rt - R't$.

Class A′ and B′ reset *when and only when* Class A resets. All payments to Class A′ and B′ (in the form of underlying token) consist of the payments made to the Class A in which A′ and B′ invest. Specifically,

- On regular payout ζ, Class A′ and B′ receive $R'T$ and $2RT - R'T$, respectively, in the form of underlying token;
- On upward reset τ, Class A′ and B′ receive payment with value $R't$ and $2Rt - R't$, respectively, in the form of underlying token;
- On downward reset η, Class A′ and Class B′ receive $R't + 1 - V_B^{\eta-}$ and $2Rt - R't + 1 - V_B^{\eta-}$, respectively, in the forms of underlying token, and each one Class A′ and B′ becomes $V_B^{\eta-}$ share.

When Class A′ and Class A have the same coupon rate, i.e. $R' = R$, then Class A, A′ and B′ have the same cash flow and hence the same value, provided no extreme event occurs (the net asset value of Class B does not jump to a negative level). In practice, R' is typically smaller than R and close to the risk-free rate. For instance, $R' = 0.03$ p.a.

Under the risk-neutral pricing framework, the value of Class A′ is given as

$$\begin{aligned} W_{A'}(t,S) = E_t \Bigg[& \sum_{1 \le i < \tau \wedge \eta} e^{-r(i-t)} R'T + e^{-r(\tau - t)}(R'\tau + W_{A'}(0,1)) \cdot \mathbf{1}_{\{\tau < \eta\}} \\ & + e^{-r(\eta - t)}(R'\eta + 1 - V_B^{\eta-} + V_B^{\eta-} W_{A'}(0,1)) \cdot \mathbf{1}_{\{\eta < \tau\}} \Bigg], \end{aligned} \tag{9}$$

where τ, η are the first upward or downward reset (whichever comes first) of Class A (or equivalently, Class A′ and B′) after t, respectively.

$W_{A'}$ satisfies the following PDE, which is the same to (5) – (8) except for changing R to R' for the coupon payment:

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

Given $W_{A'}$, the value of Class B′ is given as $2W_A(t,S) - W_{A'}$.

Although Class A′ and A look similar under normal situations, under extreme scenario in practice, Class A′ is safer than Class A. Consider the scenario when the underlying value suddenly drops to a level $P_t < \frac{P_0}{2}(1+Rt)$. In this case, the net asset value of Class B, V_B, becomes negative. A downward reset will be triggered, when Class A gets all the remaining value $\frac{2P_t}{P_0}$, Class B gets nothing, and all Class A and B tokens are liquidated. This means that Class A will suffer a loss (getting a liquidation value $\frac{2P_t}{P_0}$ smaller than its net asset value $1+Rt$) if P_t suddenly drops below $P_t < \frac{P_0}{2}(1+Rt)$. In comparison, under the same scenario, Class A$'$ and B$'$ will get $\frac{4P_t}{P_0}$ in the form of underlying token from Class A. Therefore, Class A$'$ will have a loss if and only if $\frac{4P_t}{P_0} < 1+R't$, or equivalently, $P_t < \frac{P_0}{4}(1+R't)$, and when $\frac{P_0}{4}(1+R't) < P_t < \frac{P_0}{2}(1+Rt)$, Class A$'$ will get full payment $1+R't$ while Class A will have a loss.

5 ETH Examples

For illustration, we hereby uses Ether (ETH) as the underlying token and apply below default parameter values:

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

The following assumptions are used:

1. Price is monitored on **daily** basis.

2. Upward and downward resets are performed according to end-of-day prices.

3. Coupon payouts are given at the end of the day in terms of ETH, and reinvestment of ETH payout is not considered.

ETH/USD price data from 1 Oct 2017 to 28 Feb 2018 is used. In this period, ETH started from 303.95 USD to low of 284.92 USD and high of 1,359.48 and ended at 851.5, as illustrated in Figure 1 below.

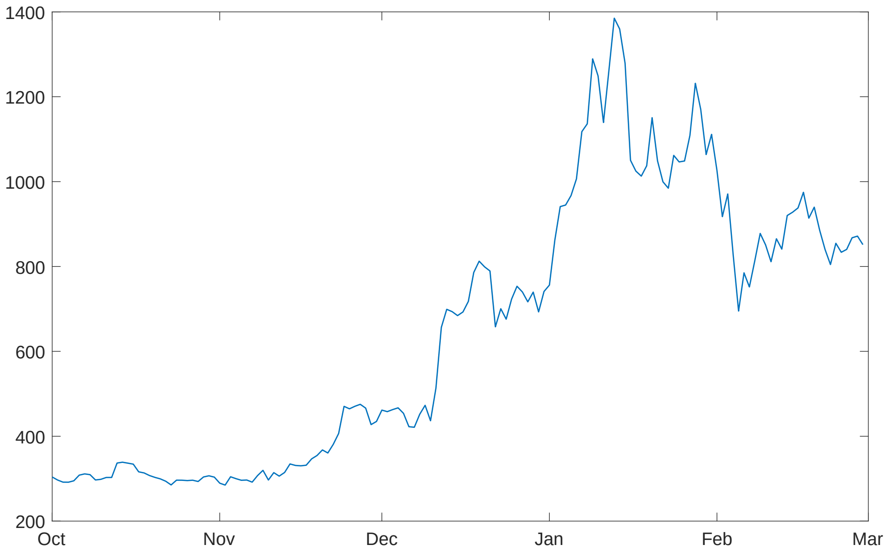

Figure 1: ETH/USD Price from 1 Oct 2017 to 28 Feb 2018

5.1 Market Values of Class A and Class B

We first compute the market values of class A and class B shares, based on the geometric Brownian motion assumption and on the historical prices of ETH. Figure 2 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 2 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 3 shows the simulated paths from class B shares. 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).

5.2 Market Value of Class A0

Figure 4 shows the simulated path for the prices of class A0, the principal only part of A. 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 $\alpha : 1$, $(\alpha > 1)$, 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 5 illustrates the price of A0 with $\alpha = 2$.

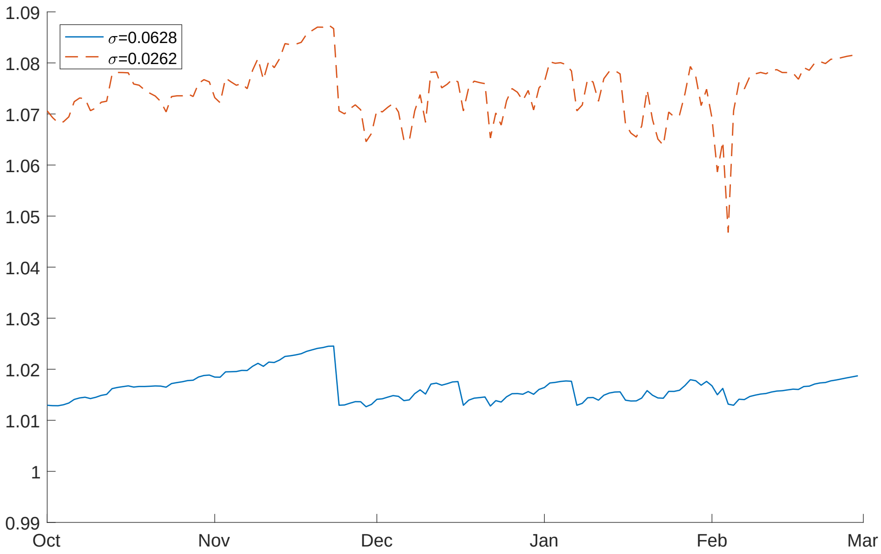

Figure 2: Simulated class A Market Value. Parameters: $R = 0.02\%, \mathcal{H}_d = 0.25$, $\mathcal{H}_u = 2$, $\mathcal{H}_p = 1.02$, $T = 100$, $r = 0.0082\%$ per day (3% per year). Upward reset takes place on 24 Nov 2017, 17 Dec 2017, and 7 Jan 2018. Downward reset date takes place on 5 Feb 2018.

5.3 Market Value of Class A′ and B′

We can see from Figure 6 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 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).

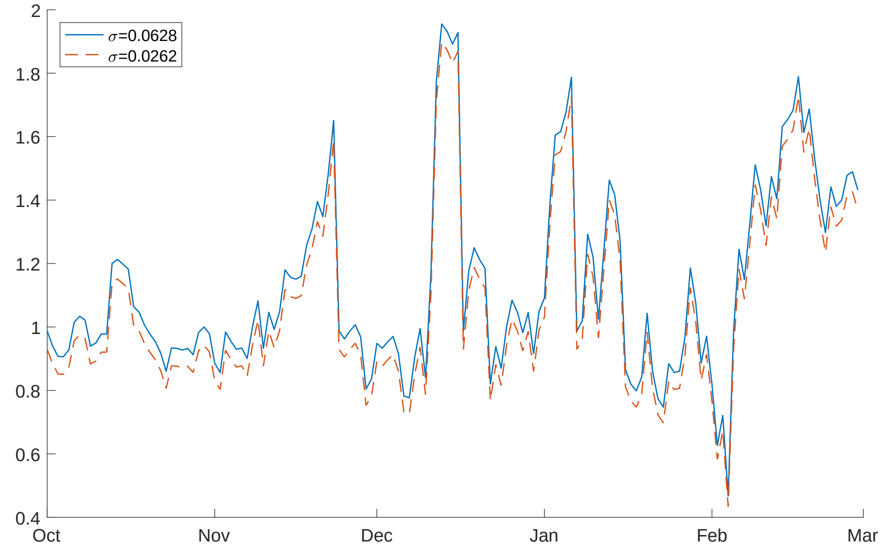

Figure 3: Class B Market Value. Parameters: $R = 0.02\%$, $\mathcal{H}_d = 0.25$, $\mathcal{H}_u = 2$, $\mathcal{H}_p = 1.02$, $T = 100$, $r = 0.0082\%$ per day (3% per year). Upward reset takes place on 24 Nov 2017, 17 Dec 2017, and 7 Jan 2018. Downward reset date takes place on 5 Feb 2018.

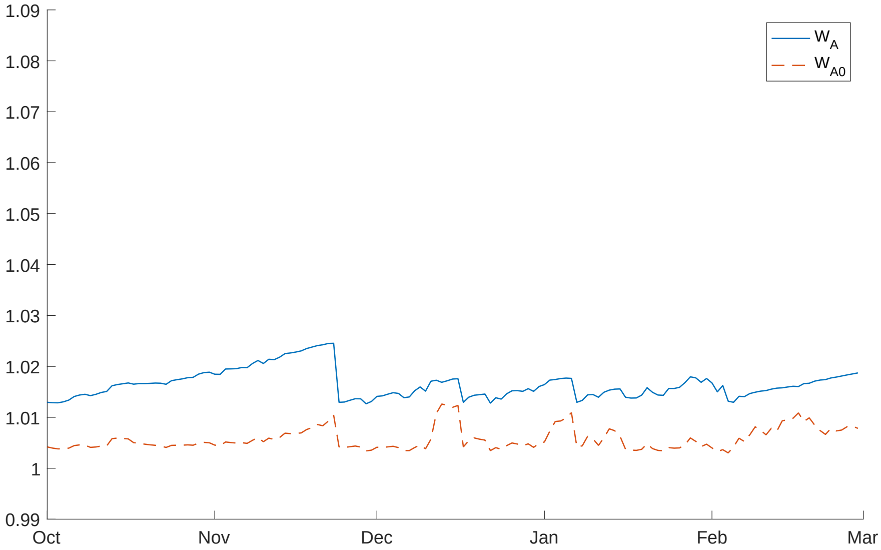

Figure 4: Market Value of Class A0 compared to Class A. Annualized volatility of Class A0 is 0.0255. Parameters: $R = 0.02\%, \mathcal{H}_d = 0.25, \mathcal{H}_u = 2, \mathcal{H}_p = 1.02, T = 100, \sigma = 120\% per year, r = 0.0082\%$ (3% per year). Upward reset takes place on 24 Nov 2017, 17 Dec 2017, and 7 Jan 2018. Downward reset date takes place on 5 Feb 2018.

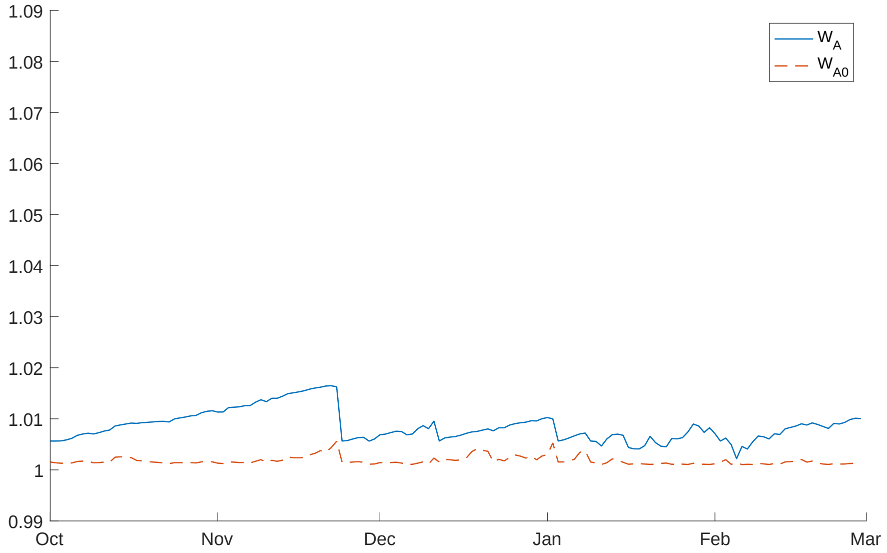

Figure 5: Market Value of Class A0 (principal only class) compared to Class A, where DUO is split into Class A and Class B token with a split ratio 2:1. Annualized volatility of Class A is 0.0125. Parameters: $R = 0.02$ per day, $\mathcal{H}_d = 0.25$, $\mathcal{H}_u = 2$, $\mathcal{H}_p = 1.02$, $T = 100$, $\sigma = 120\%$ 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.

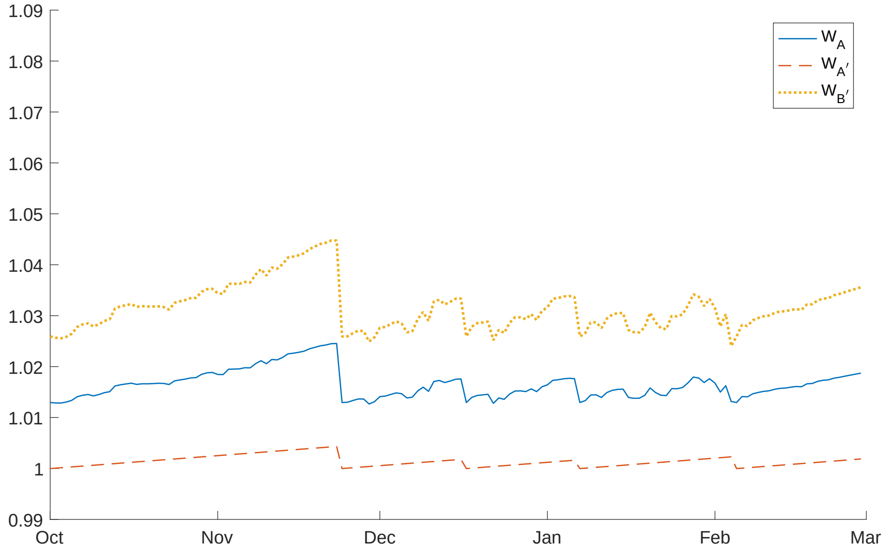

Figure 6: Market Value of Class A′ (red) and B′ (blue), compared with Class A (black). Annualized volatility of Class A′ and B′ are 0.0087 and 0.0403, respectively. Parameters: $R = 0.02\%$ per day, $\mathcal{H}_d = 0.25$, $\mathcal{H}_u = 2$, $\mathcal{H}_p = 1.02$, $R' = 0.0082\%$ (3% per year), $T = 100$, $\sigma = 120\%$ 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.

6 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.

Base Rate Discovery

Arbitrary rate can be used for Class A coupon and it will be traded on premium or at discount based on the market required rate of return. However, it is desirable that Class A trades close to its net value, which means the coupon rate for Class A should be chosen close to the market rate. Currently there are few observable proxies in the market. Several centralized exchanges allowing margin trading are charging USD borrow rates in the range of 20% to 40% per annum.

As discussed in Section 2.4.1, the market premium or discount of Class A token may imply USD's borrow rate in this market. As the structure gains attractions, its implied rate could serve as an indication for other USD borrow practice in crypto market.

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.

Appendix A Product Design with Genearl 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:

$$\begin{array}{rc} C_B = & \frac{M_C \cdot P_0 \cdot \beta \cdot (1-c)}{1+\alpha} \\ C_A = & C_B \cdot \alpha \ , \end{array} \tag{10}$$

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:

$$M_C = \frac{C \cdot (1-c) \cdot (1+\alpha)}{P_0 \cdot \beta} \ . \tag{11}$$

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:

$$\begin{array}{rc} V_A^t = & 1 + R \cdot t \\ V_B^t = & (1+\alpha) \cdot \frac{P_t}{P_0 \cdot \beta} - \alpha \cdot V_A^t \ , \end{array} \tag{12}$$

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 $V_B^t \geqslant \mathcal{H}_u$. 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:

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

A.7 Contingent Downward Reset

A downward reset is triggered when $V_B^t \leqslant \mathcal{H}_d$. 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 $Q_A^{t+} = Q_B^{t+} \cdot \alpha$.
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:

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

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

A.8 Regular Payout

A regular payout is triggered when $V_A^t \geqslant \mathcal{H}_p$. 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 $\beta^+ = \beta^- \cdot \frac{(1+\alpha)\cdot P_t}{(1+\alpha)\cdot P_t - P_0\cdot\alpha\cdot\beta^-\cdot\left(V_A^{t-}-1\right)}$
5. Unlike contingent resets, P_0 does NOT reset to P_t

Total value in the system is unchanged after reset:

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

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

In this section 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 solution*[3] *to the following partial differential equation on* $\{(t,S) : 0 \leq t < T, H_d(t) < S < H_u(t)\}$

$$-\frac{\partial W_A}{\partial t} = \frac{1}{2}\sigma^2 S^2 \frac{\partial^2 W_A}{\partial S^2} + rS\frac{\partial W_A}{\partial S} - rW_A \tag{13}$$

$$W_A(T,S) = RT + W_A(0, S - \frac{1}{2}RT) \tag{14}$$

$$W_A(t, H_u(t)) = Rt + W_A(0,1) \tag{15}$$

$$W_A(t, H_d(t)) = Rt + 1 - \mathcal{H}_d + \mathcal{H}_d W_A(0,1). \tag{16}$$

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

Proof of Theorem B.1. Using Theorem E1.1 in [2], we can rewrite (4) in a non-recursive form as

$$\begin{aligned} W_A(t,S) = E_t^{(t,S,1)} \Bigg[&\sum_{\zeta_i \geq t} e^{-R(\zeta_i - t)} Y_{\zeta_i -} RT + \sum_{\tau_i \geq t} e^{-R(\tau_i - t)} Y_{\tau_i -} r v_{\tau_i -} \\ &+ \sum_{\eta_i \geq t} e^{-R(\eta_i - t)} Y_{\eta_i -} (r v_{\eta_i -} + 1 - \mathcal{H}_d) \Bigg], \end{aligned} \tag{17}$$

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 [3] shows that (17) 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). □

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

By using a similar proof as Theorem C.1 in [2], 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.

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] 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.*

[3] Dai, M., S. Kou, and C. Yang. 2017. A Stochastic Representation for Nonlocal Parabolic PDEs with Applications. *Working Paper.*

[4] 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.

[5] Jarrow, R. A., and M. O'Hara. 1989. Primes and Scores: An Essay on Market Imperfections. *The Journal of Finance* 44:1263-1287.

[6] Black, F., and M. Scholes. 1973. The Pricing of Options and Corporate Liabilities. *Journal of Political Economy* 81:637-654.

[7] Leverage. *https://www.investopedia.com/terms/l/leverage.asp*

[8] White Paper: A Next-Generation Smart Contract and Decentralized Application Platform. *https://github.com/ethereum/wiki/wiki/White-Paper*

[9] Tether: Fiat currencies on the Bitcoin blockchain. *https://tether.to/wp-content/uploads/2016/06/TetherWhitePaper.pdf*

[10] Basecoin: A Price-Stable Cryptocurrency with an Algorithmic Central Bank. *http://www.getbasecoin.com/basecoin_whitepaper_0_99.pdf*

[11] The Dai Stablecoin System. *https://makerdao.com/whitepaper/DaiDec17WP.pdf*