A Stable Token Based on Dual-Class Structure

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

Version 0.7.0
9 Mar 2018

Abstract

Major crypto-currencies are subject to massive volatility, which makes them attractive to speculators but unsuitable for mainstream use. There have been several attempts on implementing 'stablecoins'. But most of them fail to provide steady returns that's appealing to regular investors.

Inspired by the dual purpose fund that has gained popularity in the US and China, we propose, for the first time to our best knowledge, a dual-class crypto token structure that offers entitlements to either fixed income or leveraged capital appreciation: the income token receives periodical coupon payments with principal protection; the leverage token provides leveraged participation in underlying crypto assets. The whole mechanism is governed by smart contracts run on Ethereum blockchain, without dealing with centralized counterparties. In theory, we justify the income token as an ideal stable token.

For illustration, we employ Ether (ETH) as underlying asset and use its historical prices to demonstrate the performance of our stable token in real world scenarios. We also show how arbitrage activities take place and help maintain price stability of this stable token.

Keywords: stablecoin, dual-class token, fixed income crypto asset, leveraged return crypto asset, smart contract, Ethereum, decentralized asset management

* *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

A wise man ought always to follow the paths beaten by great men,
and to imitate those who have been supreme, so that
if his ability does not equal theirs, at least it will savour of it.
– *Niccolo Machiavelli: The Prince*

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 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[6]; Basecoin tries to control money supply by playing an algorithmic version of central bank[7]; MakerDAO uses decentralized over-collateralization to maintain confidence of its Dai stablecoin[8].

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[4]. 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.[1]

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.[1]

We are inspired by Chinese dual-purpose fund for three reasons: (i) both the income and leveraged shares answer unfulfilled demands of cryptocurrency 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. [5]

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

Everything should be made as simple as possible, but no simpler.
– *Albert Einstein*

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:

$$C = \frac{M_C \cdot P_0}{2} \ , \tag{1}$$

where P_0 is the recorded price of underlying token in USD at last reset event.

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 R 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_R underlying tokens, whereM_R can be calculated by:

$$M_R = \frac{2R}{P_0} \ . \tag{2}$$

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,

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

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

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

Note that at inception or after 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 preserves 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 remain unchanged
2. Net Value of both classes reset 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 $\frac{V_B^{t-}-1}{P_t}$

Total value in the system is unchanged after reset. For details, see Appendix A.1.6.

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 are reduced to $Q^{t+} = Q^{t-} \cdot V_B^{t-}$
2. Net Value of both classes reset 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: $\frac{V_A^{t-} - V_B^{t-}}{P_t}$

Total value in the system is unchanged after reset. For details, see Appendix A.1.7.

2.3.3 Periodic Reset

When a given time period has passed from the last reset time, V_A^{t-} grows to upper limit $\mathcal{H}_p$, a periodic reset is triggered to restore the leverage ratio and net value of both classes. If V_B^{t-} is less than 1, reset will be the same as the Contingent Downward reset. Otherwise, reset will be the same as the Contingent Upward reset.

3 Valuation

Denote W_A and W_B as the market value of Class A and Class B, respectively. We assume that P follows a geometric Brownian motion under the risk neutral measure:

$$dP_t = \rho P dt + \sigma P_t dW_t,$$

where W_t is a one-dimensional standard Brownian motion. Also denote$S_t = P_t/P_0$, then

$$dS_t = \rho S_t dt + \sigma S_t dW_t,$$

where ρ denotes the risk-free rate. Note that $S_\theta = 1$ at any reset time θ, when P_0 is reset to P_θ.

Based on the above specifications, the current market value of A shares under the risk-neutral pricing framework is given recursively as

$$\begin{aligned} W_A(t,S) = E_t^*\Bigg[& e^{-\rho(\zeta-t)}[rT + g(S_{\zeta-}) + (1-g(S_{\zeta-}))W_A(0,1)] \cdot \mathbf{1}_{\{\zeta\le\tau,\eta\}} \\ & + e^{-\rho(\tau-t)}(r\tau + W_A(0,1)) \cdot \mathbf{1}_{\{\tau<\eta,\zeta\}} \\ & + e^{-\rho(\eta-t)}(r\eta + 1 - \mathcal{H}_d + \mathcal{H}_d W_A(0,1)) \cdot \mathbf{1}_{\{\eta<\tau,\zeta\}}\Bigg], \end{aligned} \tag{4}$$

where E_t^* is the $\mathbb{Q}$-expectation computed under the initial condition $S_{t-} = S$, random times ζ, τ and η represent the first periodic, upward and downward reset date from t, respectively, and $g(s) = ((1+\alpha)(1-s) + \alpha rT)^+$. Here $W_A(t,S)$ denotes the market value of A share with time from last interest payment $0 \le t \le 1$, and underlying fund value $H_d(t) \le S \le H_u(t)$, where $H_d(t) = \frac{\alpha}{1+\alpha}(1+rt) + \frac{1}{1+\alpha}\mathcal{H}_d$, and $H_u(t) = \frac{\alpha}{1+\alpha}(1+rt) + \frac{1}{1+\alpha}\mathcal{H}_u$ Note that by labeling the last interest payment date as time 0, t can also be interpreted as the current time.

Since after either an upward or downward reset, investors still get Class A shares in addition to the payments, the right hand side of (4) depends on W_A which makes (4) recursive. On the right hand side of (4), the second and third terms describe the cash flow on upward and downward resets. The second term shows that, if an upward reset comes first, investors get early 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 $V_A^{\eta-} - V_B^{\eta-}$, each share of Class A reduces to $\mathcal{H}_d$ share, and the time from last reset changes to 0 and S to 1. Finally, the first term is value of the cash flow on the periodic reset date. Specifically, when $V_B^{\zeta-} \ge 1$, or equivalently, $(1+\alpha) - \alpha(1+rT) \ge 1$ (so that $g(S_{\zeta-}) = 0$), the cash flow follows that of an upward reset where Class A receives payment of value rT, and the number of Class A remains unchanged; when $V_B^{\zeta-} < 1$, or equivalently, $(1+\alpha) - \alpha(1+rT) < 1$, the cash flow follows that of a downward reset, where Class A receives payment of value $V_A^{\zeta-} - V_B^{\zeta-} = 1 + rT - (1+\alpha)S_{\zeta-} - \alpha(1+rT) = rT + g(S_{\zeta-})$, and each one share of Class A is reduced to $V_B^{\zeta-} = (1+\alpha)S_{\zeta-} - \alpha(1+rT) = 1 - g(S_{\zeta-})$ share.

The following theorem characterizes W_A in terms of a partial differential equation.

Theorem 3.1. *W_A is the unique classical solution*[1] *to the following partial differential equation on* $\{(t,S) : 0 \le t < T, H_d(t) < S < H_u(t)\}$

$$-\frac{\partial W_A}{\partial t} = \frac{1}{2}\sigma^2 S^2 \frac{\partial^2 W_A}{\partial S^2} + \rho S \frac{\partial W_A}{\partial S} - \rho W_A \tag{5}$$

$$W_A(T,S) = rT + g(S) + (1 - g(S))W_A(0,1) \tag{6}$$

$$W_A(t, H_u(t)) = rt + W_A(0,1) \tag{7}$$

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

The proof follows that of Theorem 4.1 in [1] by adopting the change in the terminal condition. 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 $A.4$.

The nonlocal terminal and boundary conditions in (6) – (8) are directly related with the cash flow of A shares. 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 $S = H(t)$ corresponds downward reset, when early payment $V_B - V_A$ is delivered, each one A share shrinks to H_d share, and S resets to 1. Finally, the terminal condition (6) corresponds to the periodic reset, where the payment follows either the upward or downward reset based on whether $V_B \le 1$.

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

4 ETH Examples

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

$$\begin{aligned} r &= 0.02\% \\ \mathcal{H}_d &= 0.25 \\ \mathcal{H}_u &= 2 \\ \mathcal{H}_p &= 1.02 \ , \end{aligned}$$

and below assumptions are used:

1. Price is monitored on **daily** basis
2. Resets are performed according to end-of-day prices
3. The structure starts with 100,000 ETH with no further capital injection
4. Reinvestment of ETH payout from resets is not considered

4.1 Overall Market

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.

At inception, 15,197,500 Class A and 15,197,500 Class B are issued from the 100,000 ETH, total value in the system is 30,395,000 USD.

Three upward resets were triggered on 24 Nov 2017 ($V_B = 2.0846$), 17 Dec 2017 ($V_B = 2.0467$) and 7 Jan 2018 ($V_B = 2.1106$) while one downward reset was triggered on 5 Feb 2018 ($V_B = 0.2379$.). No periodic reset was triggered in the sampling period.

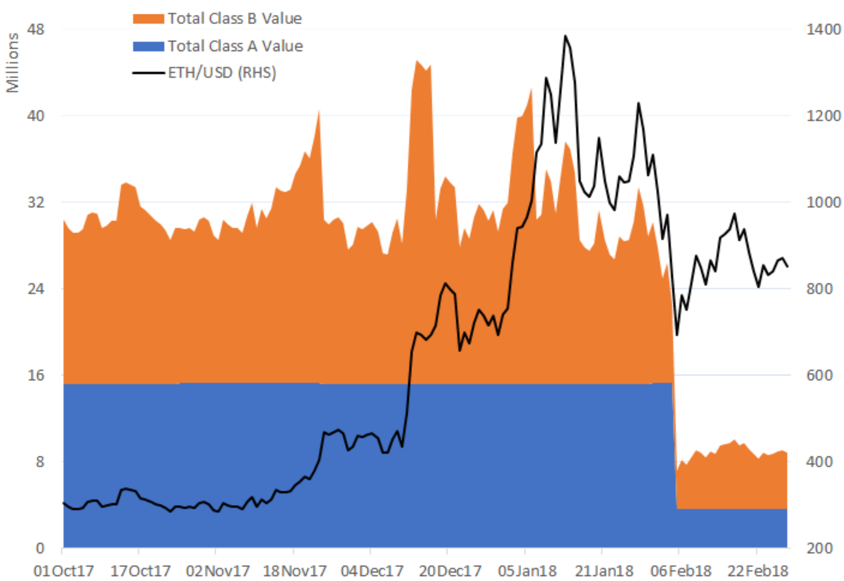

Figure 1: Total Values

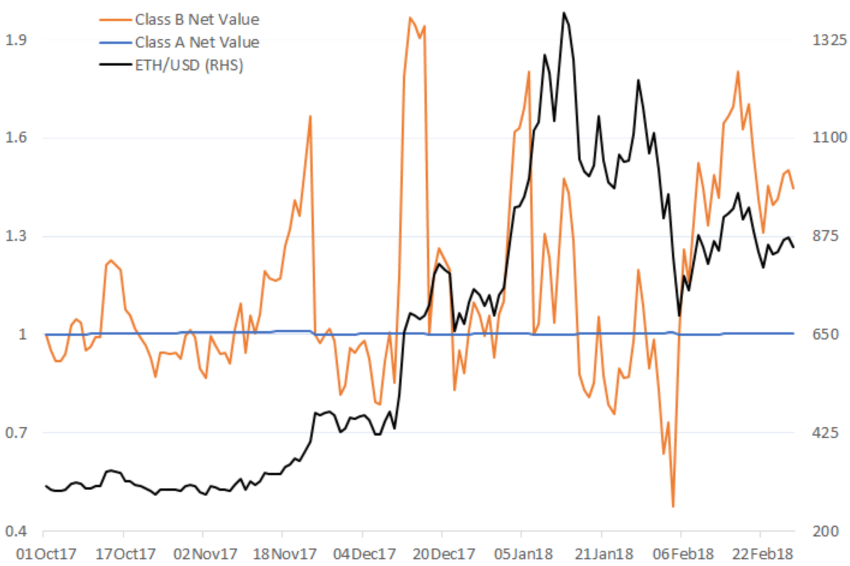

Figure 2: Net Values

Period without Reset The total value of Class A and Class B tokens moves in line with ETH price. Class B tokens get exposed to full price fluctuations of ETH, while Class A token value is stable and slowly appreciating.

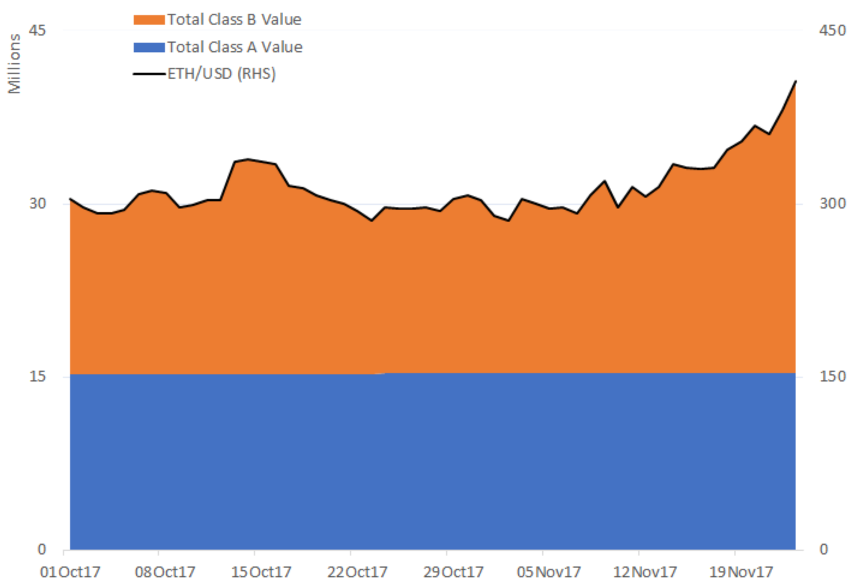

Figure 3: 1 Oct 2017 - 23 Nov 2017 Total Values

Period with Contingent Upward Reset[2] 17 Dec 2017, $V_B = 2.0467$. 97.4049 ETH is paid out to Class A holders and 22,163.7213 ETH is paid out to Class B holders. Remaining System value is at 30,395,000 USD. The total value of Class A, Class B and ETH payout is consistent with ETH price movement.

[2]Chart and numbers are similar for the other two upward resets and thus omitted here.

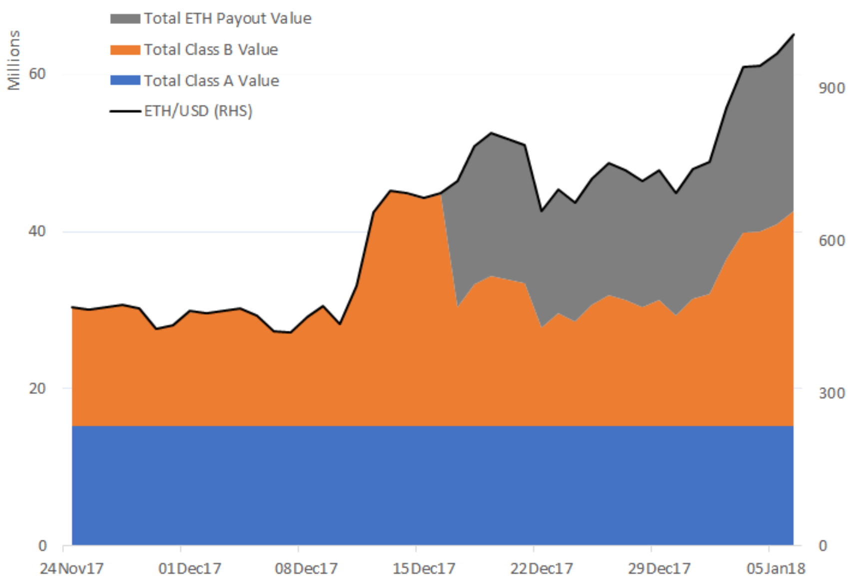

Figure 4: 24 Nov 2017 - 6 Jan 2017 Total Values

Period with Contingent Downward Reset 5 Feb 2018, $V_B = 0.2379$. 16,789.3847 ETH is paid out to Class A holders. total amount of both classes is reduced to 3,615,680.02. Remaining System value is at 7,231,360.04 USD. The total value of Class A, Class B and ETH payout is consistent with ETH price movement.

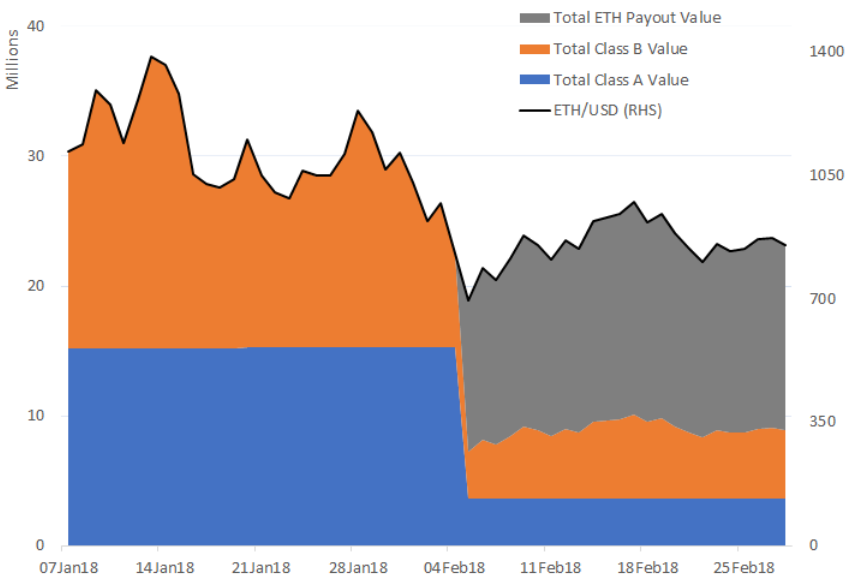

Figure 5: 7 Jan Nov 2017 - 28 Feb 2017 Total Values

4.2 Individual Class Return

Class A stable return from daily coupon and not affected by ETH price movement.

Figure 6: Class A Return

Class B magnified return from ETH price movement due to the embedded leverage.

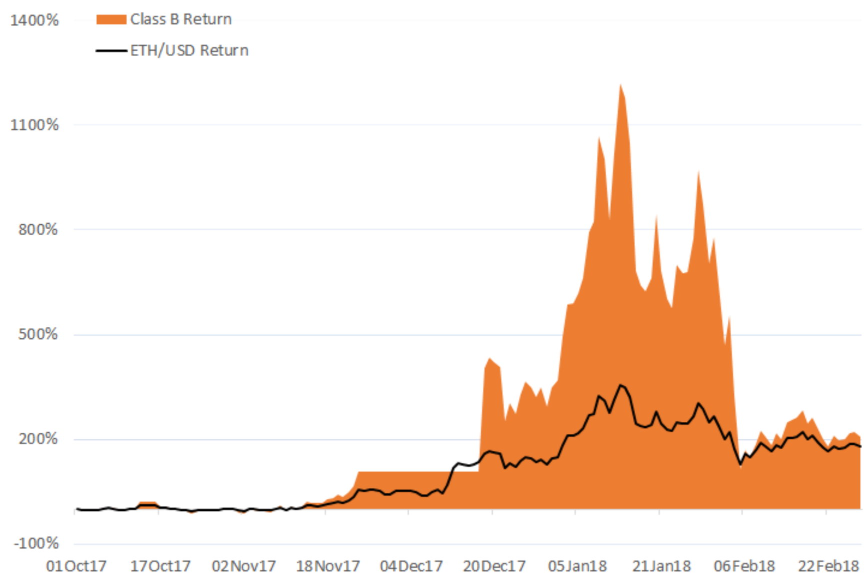

Figure 7: Class B Return

Note In order to achieve above return, ETH payout from resets need to be fully converted back to the corresponding class token. For example, after 24 Nov 2017 upward reset, all ETH received by Class A holder need to be converted into Class A token.

4.3 Market Value

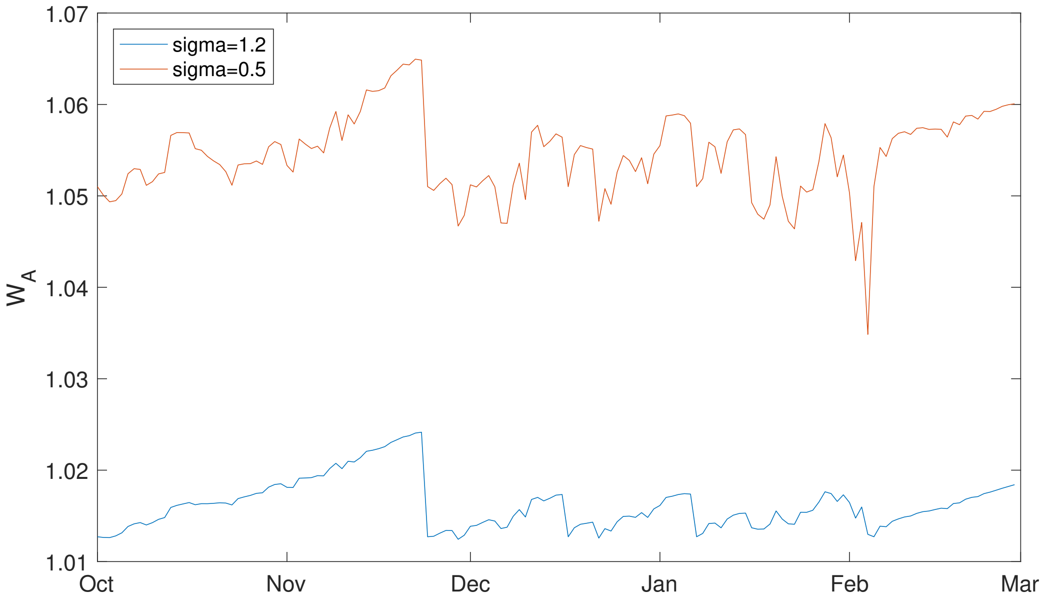

Figure 8: Class A Market Value

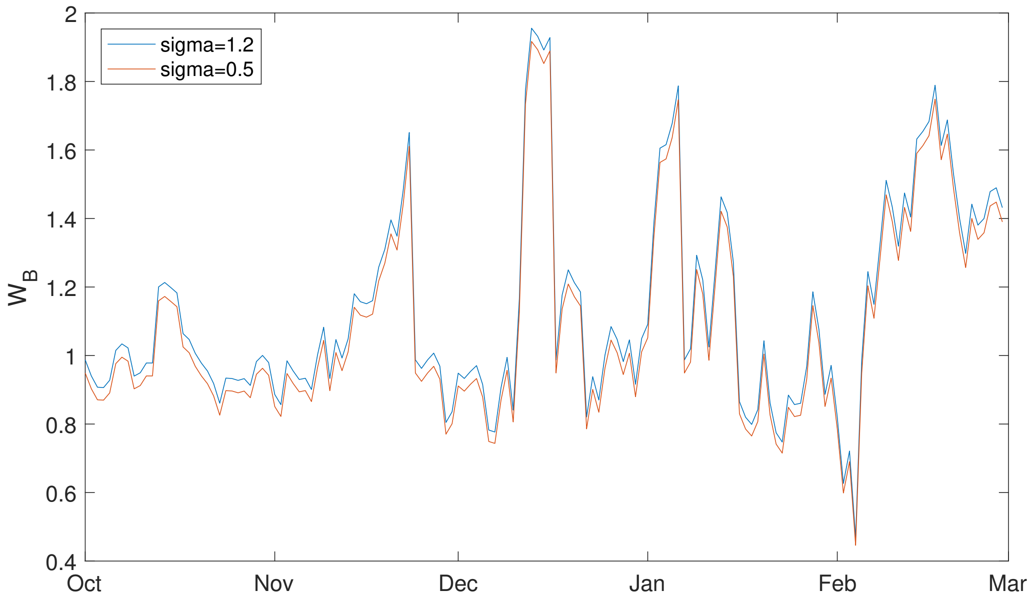

Figure 9: Class B Market Value

5 Market Mechanism

Arbitrage human nature. It's not going to change any time soon.
– *James O'Shaughnessy*

5.1 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.

5.2 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, below should hold:

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

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.

Arbitrage via Creation When combined market price of Class A and Class B tokens are higher than their combined net values, i.e.

$$P_A^t + P_B^t > 2 \cdot \frac{P_t}{P_0} \ ,$$

arbitrage profit can be exploited by perform DUO token creation:

1. Buy 1 underlying tokens from open market for P_t USD equivalent.
2. Send the underlying tokens to the Custodian contract.
3. Based on Equation (1), receive $\frac{P_0}{2}$ Class A and $\frac{P_0}{2}$ Class B tokens.
4. Sell Class A and Class B tokens on open market for $P_0 \cdot \frac{P_A^t + P_B^t}{2}$ USD equivalent.

The expected payoff of above operations is:

$$P_0 \cdot \frac{P_A^t + P_B^t}{2} - P_t = \frac{P_0}{2} \cdot \left(P_A^t + P_B^t - 2 \cdot \frac{P_t}{P_0} \right) > 0 \ .$$

Arbitrage via Redemption When combined market price of Class A and Class B tokens are lower than their combined net values, i.e.

$$P_A^t + P_B^t < 2 \cdot \frac{P_t}{P_0} \ ,$$

arbitrage profit can be exploited by perform DUO token redemption:

1. Buy $\frac{P_0}{2}$ Class A and $\frac{P_0}{2}$ Class B tokens from open market for $P_0 \cdot \frac{P_A^t + P_B^t}{2}$ USD equivalent.
2. Send Class A and Class B tokens to the Custodian contract.
3. Based on Equation (2), receive 1 underlying tokens.
4. Sell underlying tokens on open market for P_t USD equivalent.

The expected payoff of above operations is:

$$P_t - P_0 \cdot \frac{P_A^t + P_B^t}{2} = \frac{P_0}{2} \cdot \left(2 \cdot \frac{P_t}{P_0} - \left(P_A^t + P_B^t \right) \right) > 0 \ .$$

Many other factors also determine whether above arbitrage strategy can be successfully executed, such as bid ask spread of all the 3 components, cost in creation and redemption, and ability to short sell the required components. Please refer to appendix for discussion of a more general case.

6 Further Development

> Patience, persistence and perspiration make an unbeatable combination for success.
> – *Napoleon Hill*

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.

Theoretical Pricing Model

We have illustrated the net values for the dual structure. As market evolves and observable price data becomes available, a theoretical model based on Black-Scholes pricing framework can be developed to derive fair price for the dual structure and explain deviations from net values.

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 5.1, 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.1); 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.

A Appendix

A.1 General Product Design

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. In addition, transaction cost in creation and redemption is omitted. In this section, a general case is discussed.

A.1.1 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:

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

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.

A.1.2 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 $R \cdot \alpha$ Class A and amount of R Class B tokens to the Custodian contract. The contract will deduct Class A and Class B tokens, and return to the sender M_R underlying tokens, whereM_R can be calculated by:

$$M_R = \frac{R \cdot (1-c) \cdot (1+\alpha)}{P_0} \ . \tag{10}$$

A.1.3 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:

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

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.1.4 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.1.5 Implied Leverage Ratio

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

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

A.1.6 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 $U_B = \frac{V_B^{t-}-1}{P_t}$.

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.1.7 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: $D_A = \frac{V_A^{t-} - V_B^{t-}}{P_t}$.

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.1.8 Periodic Reset

A periodic reset is triggered when $V_A^t \geqslant \mathcal{H}_p$. If V_B^{t-} is less than 1, reset will be the same as the Contingent Downward reset. Otherwise, reset will be the same as the Contingent Upward reset.

A.2 General Market Arbitrage

The price parity shall hold as below:

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

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.

Along with Equation (9), (10) and (11) in Section A.1, below should hold:

$$\frac{P_t}{P_0} \cdot (1-c) \leq \frac{\alpha \cdot P_A^t + P_B^t}{1+\alpha} \leq \frac{P_t}{P_0} \cdot \frac{1}{1-c} \ .$$

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

Arbitrage via Creation When combined market price of Class A and Class B tokens are higher than their combined net values, i.e.

$$\frac{\alpha \cdot P_A^t + P_B^t}{1+\alpha} > \frac{P_t}{P_0} \cdot \frac{1}{1-c} \ ,$$

arbitrage profit can be exploited by perform DUO token creation:

1. Buy $\frac{1}{1-c}$ underlying tokens from open market for $P_t \cdot \frac{1}{1-c}$ target fiat currency equivalent.
2. Send the underlying tokens to the Custodian contract.
3. Based on Equation (9), receive $P_0 \cdot \frac{\alpha}{1+\alpha}$ Class A and $P_0 \cdot \frac{1}{1+\alpha}$ Class B tokens.
4. Sell Class A and Class B tokens on open market for $P_0 \cdot \frac{\alpha P_A^t + P_B^t}{1+\alpha}$ target fiat currency equivalent.

The expected payoff of above operations is:

$$P_0 \cdot \frac{\alpha P_A^t + P_B^t}{1+\alpha} - \frac{P_t}{1-c} = P_0 \cdot \left(\frac{\alpha \cdot P_A^t + P_B^t}{1+\alpha} - \frac{P_t}{P_0} \cdot \frac{1}{1-c}\right) > 0 \ .$$

Arbitrage via Redemption When combined market price of Class A and Class B tokens are lower than their combined net values, i.e.

$$\frac{P_t}{P_0} \cdot (1-c) > \frac{\alpha \cdot P_A^t + P_B^t}{1+\alpha} \ ,$$

similar arbitrage profit can be exploited by perform DUO token redemption:

1. Buy $P_0 \cdot \frac{\alpha}{1+\alpha}$ Class A and $P_0 \cdot \frac{1}{1+\alpha}$ Class B tokens from open market for $P_0 \cdot \frac{\alpha P_A^t + P_B^t}{1+\alpha}$ target fiat currency equivalent.
2. Send Class A and Class B tokens to the Custodian contract.
3. Based on Equation (10), receive $1-c$ underlying tokens.
4. Sell underlying tokens on open market for $P_t \cdot (1-c)$ target fiat currency equivalent.

The expected payoff of above operations is:

$$P_t \cdot (1-c) - P_0 \cdot \frac{\alpha P_A^t + P_B^t}{1+\alpha} = P_0 \cdot \left(\frac{P_t}{P_0} \cdot (1-c) - \frac{\alpha \cdot P_A^t + P_B^t}{1+\alpha} \right) > 0 \ .$$

A.3 Derivation of the Pricing Equation

A.4 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* $V_A^{(i-1)}$, *solve for* $W_A^{(i)}$, *the solution to the equation*

$$\begin{array}{rcc} -\frac{\partial W_A}{\partial t} = & \frac{1}{2}\sigma^2 S^2 \frac{\partial^2 W_A}{\partial S^2} + \rho S \frac{\partial W_A}{\partial S} - \rho W_A & 0 \le t < T, H_d(t) < S < H_u(t) \\ W_A(1,S) = & rT + g(S) + (1-g(S)) W_A^{(i-1)}(0,1) & H_d(t) < S < H_u(t) \\ W_A(t, H_u(t)) = & rt + W_A^{(i-1)}(0,1) & 0 \le t \le T \\ W_A(t, H_d(t)) = & rt + 1 - \mathcal{H}_d + \mathcal{H}_d W_A^{(i-1)}(0,1) & 0 \le t \le T. \end{array}$$

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 [1], one can show that the sequence$(W_A^{(i)})_{i \ge 1}$ defined in Algorithm 1 is monotonically increasing and converges to W_A uniformly.

References

[1] 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*.

[2] 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.

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

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

[5] *https://github.com/ethereum/wiki/wiki/White-Paper*

[6] *https://tether.to/wp-content/uploads/2016/06/TetherWhitePaper.pdf*

[7] *http://www.getbasecoin.com/basecoin_whitepaper_0_99.pdf*

[8] *https://makerdao.com/whitepaper/DaiDec17WP.pdf*