Designing Stable Coins*

Yizhou Cao[1], Min Dai[2,3], Steven Kou[2,3], Lewei Li[1], and Chen Yang[4]

[1]FinBook, 148955, Singapore

[2]Risk Management Institute, National University of Singapore, 119613, Singapore

[3]Department of Mathematics, National University of Singapore, 119076, Singapore

[4]Department of Mathematics, ETH Zürich, 8092 Zürich, Switzerland

Abstract: Stable coins, which are cryptocurrencies pegged to other stable financial assets such as U.S. dollar, are desirable for payments within blockchain networks, whereby being often called the "Holy Grail of cryptocurrency." However, existing cryptocurrencies are too volatile for these purposes. By using the option pricing theory, we design several dual-class structures that offer fixed income stable coins (class A and A′ coins) pegged to a traditional currency as well as leveraged investment instruments (class B and B′ coins). When combined with insurance from a government, the design can also serve as a basis for issuing a sovereign cryptocurrency.

JEL codes: G10, O30, E40.

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

*Corresponding author: Min Dai, 10 Lower Kent Ridge Road, Singapore 119076. Tel: +65 6516 2754. Email: matdm@nus.edu.sg.

1 Introduction

How to create a digital currency was a long-standing open problem for many years, due to two main challenges: First, as people can easily copy music and movie files, how to prevent people from copying digital currency token electronically? Secondly, how to avoid the double spending problem in which a single digital currency token can be spent more than once to settle liabilities. A revolution in FinTech was that the two problems can be solved by using blockchains.

A blockchain is a decentralized (peer to peer) and distributed network that is used to record, after miners' verification, all transactions which can be viewed by every users, thus allowing people to verify and audit transactions in a transparent and inexpensive way. The records cannot be easily altered retroactively.[1] Furthermore, a blockchain confirms with very high probability that each unit of value was transferred only once, solving the double spending problem without a trusted authority[2]. The first blockchain was conceptualized in Nakamoto (2008), and was implemented in 2009 as the core component of the first cryptocurrency, Bitcoin.

Another breakthrough came in late 2013 when Vitalik Buterin extends the idea of Bitcoin to create the Ethereum platform on which people can write smart contracts. This is a very important technology advance, as many types of clerk works, such as public notary, import and export paper works, certain legal and accounting documentations, can be programmed as smart contracts which can be tracked and executed automatically on the Ethereum platform. The cryptocurrency generated and circulated on the Ethereum platform is Ether (with the

[1] In fact, any alternation of the records will trigger the alteration of all subsequent blocks, and unless there is a collusion of majority users of the network, it is impossible to change the records.

[2] Even if an attacker has 10% success probability of finding the next block, in the standard 6 block verification scheme, the chance of the attacker will ever be successful in double spending is only about 0.0005914. Note that the calculation 0.0002428 in Nakamoto (2008) was wrong and was corrected in a recent paper by Grunspan and Perez-Marco (2018).

trading symbol ETH).

Currently, there are over 1000 crytocurrencies traded in exchanges; see, e.g, the list on coinmarketcap.com. Some of them are based on public blockchains, such as Bitcoin and Ether, and others on private blockchains, such as Ripple. In fact, one can buy crytocurrencies from online exchanges or at ATM machines worldwide, just like buying standard financial securities or foreign currencies. All cryptocurrencies share three important features. First, a payment from one user to another is processed in a decentralized way without any intermediary. Second, all transaction records are stored in the networks and can be viewed by every user. Third, they allow anonymous payments.

This paper attempts to design stable coins, which are cryptocurrencies pegged to other stable financial assets such as U.S. dollars, by using concepts from the option pricing theory. Stable coins are desirable to be used as public accounting ledgers for payment transactions within blockchain networks, and as crypto money market accounts for asset allocation involving cryptocurrencies.

1.1 Stable Coins

One major characteristic (or drawback) of cryptocurrencies is their extreme volatility. Figure 1 illustrates the price of Ether in U.S. dollars, ETH/USD, from October 1, 2017 to February 28, 2018. During this period, ETH/USD has an annualized return volatility of 120%, which is more than 9 times that of S&P 500 during the same period (13%).

The extremely large volatility means that a cryptocurrency like ETH cannot be used as a reliable means to store value. It is risky to hold the currency even for a single day due to this fluctuation. Even if retailers accept the cryptocurrency for payments, they may have to exchange it immediately into traditional currencies to avoid risk.

A stable coin is a crypto coin that keeps stable market value against a specific index or asset, most noticeably U.S. dollar. Stable coins are desirable for at least three reasons:

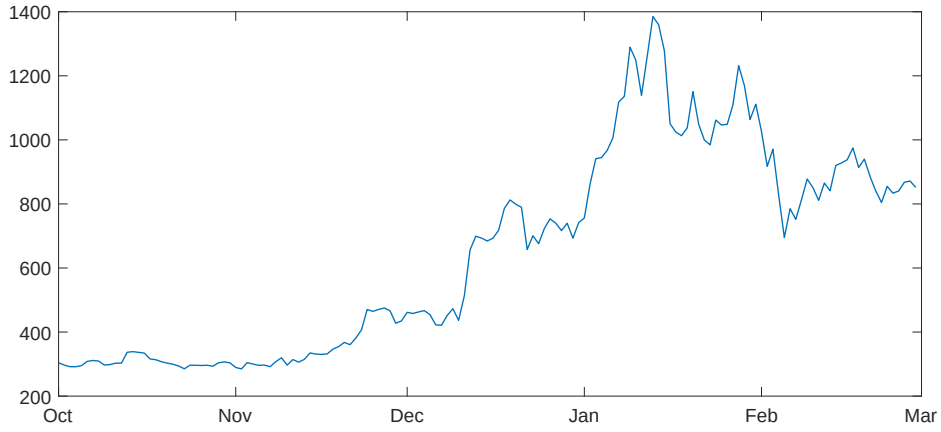

Figure 1: ETH/USD Price from 1 Oct 2017 to 28 Feb 2018

- They can be used within blockchain systems to settle payments. For example, lawyer or accountants can exchange their stable coins generated by smart contracts automatically for the services they provide within the system, without being bothered by the exchange fees from a cryptocurrency to U.S. dollar, which can range from 0.7% to 5%.

- They can be used to form crypto money market accounts, for the purpose of doing asset allocation for hundreds cryptocurrencies.

- They can be used by miners or other people who provide essential services to maintain blockchain systems to store values, as it may be difficult and expensive for them to convert mined coins into traditional currencies.

However, as we can see, existing cryptocurrencies are too volatile to be served as stable coins. In fact, how to create a good stable coin is called the "Holy Grail of Cryptocurrency" in the media (Forbes, March 12, 2018, Sydney Morning Herald, Feb 22, 2018, Yahoo Finance, Oct 14, 2017)

There are four existing types of issuance of stable coins. The first type is an issuance backed by accounts in real assets such as U.S. dollars, gold, oil, etc. More precisely, these stable coins represent claims on the underlying assets. For example, Tether coin is claimed

to be backed by USD, with the conversion rate 1 Tether to 1 USD (see Tether (2016)). However, it is very difficult to verify the claim that Tether has enough reserve in U.S. dollar, especially on a daily basis.[3] There are other tokens claimed to link to gold (e.g. Digix, GoldMint, Royal Mint Gold, OzCoinGold, and ONEGRAM), although the claims are also hard to verify. Recently in February 2018, the government of Venezuela issued Petro, a cryptocurrency claimed to be backed by one barrel of oil.

The second type is the seigniorage shares system, which has automatic adjustment of the quantity of coin supply: When the coin price is too high, new coins are issued; when the coin price is too low, bonds are issued to remove tokens from circulation. A typical example of this type is Basecoin (see Al-Naji (2018)). However, the difficulty of maintaining the right balance of supply and demand of a stable coin is at the same level of difficulty faced by a central bank issuing fiat currency.

The third type is an 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 a smart contract, if the Ether price reaches $110. One can also combine the idea of over-collateralization and seigniorage by issuing more coins if the coin price is too high, and allow people to borrow the coin, which gives borrower to buy back the coin if the coin price is too low, thus pushing the price higher. Examples of this type include the DAI token issued by MakerDAO; see MakerTeam (2017). A drawback of this type is the relative large collateral size.

The last type is government-backed stable coins. Besides Venezuela, other countries are considering issuing cryptocurrencies, including Russia and China. Canadian government also did Project Jasper involving the "CAD-coin", in which a Blockchain network is built for domestic interbank payment settlements. There is a virtual currency working group under

[3] In fact, U.S. regulators issued a subpoena to Tether on December 6, 2017, on whether $2.3 billion of the tokers outstanding are backed by U.S. dollars held in reserve (Bloomberg news, January 31, 2018).

the Federal Reserve System in U.S., which uses the "Fedcoin" internally. As commented by Garratt (2016), "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 they are never worn out. They can be tracked and taxed automatically by the blockchain technology. They can facilitate statistical works, such as GDP calculation and collecting consumer data. Furthermore, they can simplify legal money transfers inside and outside blockchains. Finally, as pointed out by Bech and Garratt (2017), the main benefit of a retail central bank backed cryptocurrency is that it would have the potential to provide the anonymity of cash. The first countries that adopt stable coins will likely see the inflow of money from people who want stable currencies on blockchains.

However, a main drawback of issuing stable coins purely by governments is the cost. More precisely, does a government have enough expertise in maintaining a computer system, is a government willing to put enough reserve to back up a stable coin fully, and how does a government control supply and demand of a stable coin in a global anonymous blockchain network (which can be quite different from a fiat currency network)?

1.2 Our Contribution

We use the option pricing theory (c.f. Duffie (2010); Hull (2017); Ingersoll (1987); Jarrow and Turnbull (1999); Shreve (2004)) to design several dual-class structures that offer entitlements to fixed income stable coins (Class A coins) pegged to a traditional currency as well as leveraged investment opportunities (Class B coins). The design is inspired by the dual-purpose funds popular in the U.S. and China. More precisely, due to downward resets, a vanilla A coin behaves like a 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′ . Unlike traditional currencies, these new class A coins record all transactions on a blockchain without centralized counterparties.

We show that the proposed stable coins have very low volatility; indeed the volatility of class A′ coin is so low that it is essentially pegged to the U.S. dollar. Table 1 reports the volatility of ETH, S&P 500 index, Gold price, U.S. Dollar index, class A and A′ coins, respectively.

Table 1: Annualized Volatility of Our Stable Coins versus Common Market Indices

Index	ETH	S&P 500	Gold	US$ Index	Class A Coin	Class A′ Coin
Volatility	120.49%	13.15%	9.44%	5.76%	2.37%	0.87%

Annualized volatility is calculated from 1 Oct 2017 to 28 Feb 2018.

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 an extremely short time period.[4] Therefore, to be truly stable, stable coins need a guarantee in Black Swan events.

A policy implication of this paper is that a public-private partnership may be formed to issue stable coins backed by a government. More precisely, by designing a set of stable coins using the option pricing theory via private market forces, the government only needs to back up the stable coins in extreme cases of Black swan events, just like what the U.S. government does for the FDIC insurance for private money market accounts in U.S.

[4]The intuition here is similar to that of the risk of the top tranche of a CDO contract. If the correlations of all firms covered within the CDO are close to 1, then one firm's default leads to almost all other firms' default, resulting in a significant drop of the top tranche value.

1.3 Literature Review

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 2. These differences require a different modeling, which is summarized in Panel B of Table 2.

Table 2: Contract and Model 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	Reset Barriers	Lifespan	Underlying 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 Coins	Fixed Income	Payments affect the exchange ratio but not the underlying asset	Yes	Infinite	USD denominated cryptocurrency

Panel B: Model Comparison

	Pricing Model
Dual-Purpose Fund in U.S. Ingersoll (1976) Jarrow and O'Hara (1989)	Black-Scholes PDE
Dual-Purpose Fund in China Dai, Kou, Yang, and Ye (2018)	Periodic PDE, constant upper barrier
Our Vanilla A and B Coins	Periodic PDE, time-dependent upper barrier

The dual-purpose funds in U.S. include those studied in Ingersoll (1976) and the prime and scores studied in Jarrow and O'Hara (1989).

The blockchain technology behind cryptocurrencies can create significant economic benefits in many applications. Cong and He (2018) showed that the blockchain technology can provide and maintain "decentralized consensus", which improves the functioning of the whole system, reduces information asymmetry, and enhances competition. Yermack (2017) pointed out that blockchains may offer to corporation shareholders lower trading costs and more visible ownership records and transfer of shares. Malinova and Park (2017) designed a financial market based on the blockchain technology that can give investors alternative ways of managing the visibility of their holdings and trading intentions.

There are many papers and media articles discussed pros and cons of cryptocurrencies. Using cryptocurrencies as a payment method has several benefits. First, as pointed out in Harvey (2016), the core innovation of cryptocurrencies like Bitcoin is the ability to publicly verify ownership, instantly transfer the ownership, and to do that without any trusted intermediary. Therefore, cryptocurrencies reduce the cost of transferring ownership. Also, the blockchain technology makes the ledger easy to maintain, reduces the cost of networking (see Catalini and Gans (2016)), and is robust against attackers.[5] The distributed ledger can result in a fast settlement that reduces counterparty risk and improves market quality (see Khapko and Zoican (2018)). Furthermore, since the transaction is recorded to the blockchain anonymously, cryptocurrencies help to protect the privacy of their users. The underlying technology of cryptocurrencies may one day strengthen the menu of electronic payments options, while the use of paper currency is phased out (see Rogoff (2015)).

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. As pointed out in Grinberg (2011), Bitcoin is

[5]Indeed, an attacker needs to race with his CPU power against the whole system; if he fails behind in the beginning, the probability of his catching up diminishes exponentially as the race goes on (see Nakamoto (2008) and Grunspan and Perez-Marco (2018)).

unlikely to play an important role in the traditional e-commerce market, since consumers typically do not care about the anonymity that Bitcoin provides; instead, they prefer a currency they are familiar with for most goods and services, and they want fraud protection. 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. Furthermore, Blockchain systems are not as trustworthy as they seem to be. Without an intermediate, individuals are responsible for their own security precautions. Finally, it is difficult to value cryptocurrencies like Bitcoin[6].

Here we want to point out that despite significant drawbacks of cryptocurrencies, it is generally agreed that the blockchain technologies are here to stay. However, blockchain technologies automatically generate cryptocurrencies for the purpose of charging the services provided by the system (such as fees incurred by all programming codes which are run on the Ethereum network), crediting essential services to the system (such as the verification services provided by miners[7]), and of exchanging credits for services. Therefore, cryptocurrencies will not disappear as long as blockchain technologies exist. Thus, designing suitable stable coins is essential for the blockchain system to perform financial functions efficiently and for doing asset allocation across different cryptocurrencies generated by different blockchain systems. In this regard, governments can provide an essential role in helping design a better financial ecosystem of blockchains.

[6]By considering the equilibrium in the case where Bitcoin is the only currency in the economy and the case with two currencies, Garratt and Wallace (2018) found that the value of Bitcoin lies upon self-fulfilling beliefs, and the set of beliefs that can be self-fulfilling needs to be huge.

[7]Easley, O'Hara, and Basu (2017) and Huberman, Leshno, and Moallemi (2017) study mining fees on the Bitcoin system.

2 Product Design

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

2.1 Vanilla Class A and B Coins

Our stable coin has a dual-class split structure which, combined with smart contract rules and market arbitrage mechanism, provides the holders of each class with principal-guaranteed fixed incomes and leveraged capital gains, respectively. The Class A Coin behaves like a bond and receives periodical coupon payments. The Class B Coin entitles leveraged participation of the underlying cryptocurrency. Simply put, this split structure means that the holders of Class B coins borrow capital from the holders of Class A coins and invest in a volatile cryptocurrency. Furthermore, a set of upward and downward reset clauses is imposed, where downward resets reduce default risk of Class B to protect Class A, and upward resets ensure a minimum leverage ratio of Class B to make Class B attractive to leverage investors.

For illustration we choose ETH as the underlying cryptocurrency, and the initial leverage ratio is set to 2.[8] Class A and B coins can be created by depositing ETHs to a custodian smart contract.[9] Upon receiving two shares of underlying ETH at time t, the Custodian contract will return to the depositor $\beta_t P_0$ of Class A and Class B coins each, where P_0 is the initial price of underlying ETH in USD at the inception of the coins ($t = 0$), and β_t is the

[8] The design of a contract with a general initial leverage ratio is discussed in Appendix A.

[9] A custodian smart contract can perform 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 stable coins' net values, and execution of Reset events. The deposited underlying cryptocurrency is kept by the custodian smart 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 coins issued through third party applications such as Etherscan.io.

time-t conversion factor. We set $\beta_0 = 1$, which means that two shares of ETH can initially exchange for P_0 shares of Class A and Class B each. The conversion factor β_t changes only on upward/downward resets or regular payout dates, and the change rule will be introduced later. To withdraw ETH at time t, holders of Class A and Class B coins can send, e.g., $\beta_t P_0$ shares of Class A and Class B coins each to the Custodian contract, then the contract will deduct the same amount of Class A and Class B coins, and return to the sender two ETHs. For instance, if the initial ETH/USD price is 500 and $\beta_t = 1$, then two 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 two shares of ETH. Figure 2 illustrates this split structure.

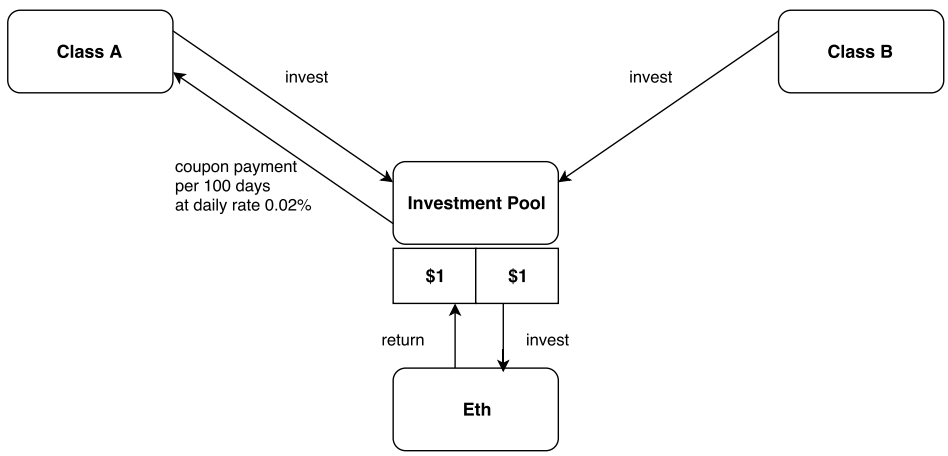

Figure 2: Class A and B, Initial Split. At time t, one share of Class A and B each invests \$1 in ETH. The initial ETH price is $P_0 = \$500$, and the prevailing conversion factor $\beta_t = 1$. So two shares of ETH exchange for 500 shares of Class A coins and 500 shares of Class B coins.

To describe the cash flow of Class A and B coins, we introduce the net asset dollar values of Class A and B coins, V_A and V_B. Thanks to the exchange between ETH and Class A/B coins, the following parity relation holds at any time:

$$V_A^t + V_B^t = \frac{2P_t}{\beta_t P_0}, \tag{2.1}$$

where P_t is the prevailing price of underlying ETH in USD. The net asset value of Class A

coins at time t is defined as

$$V_A^t = 1 + R \cdot v_t, \tag{2.2}$$

where R is the *daily* coupon rate, and v_t is the number of days from the inception, last reset, or last regular coupon payout date. The above design ensures that the initial net asset values of Class A and B coins are both equal to one dollar.

2.1.1 Regular Payout

Assume regular coupons are paid every T days. When $v_{t-} = T$, i.e., $V_A^{t-} = 1 + RT$, a regular payout is triggered, then the holder of each Class A coin receives payment with dollar value RT,[10] and the net asset value of Class A resets to \$1, namely, $V_A^{t+} = 1$. Since no cash flow occurs for Class B coin upon regular payout, the net asset value of Class B remains unchanged, that is, $V_B^{t-} = V_B^{t+}$. Noting that the parity relation (2.1) always holds across regular payout, we deduce that the conversion factor β experiences a jump upon regular payout:

$$\beta_{t+} = \frac{2P_t}{2P_t - \beta_{t-} P_0 RT} \beta_{t-}.$$

For instance, assuming $R = 0.02\%$, $T = 100$, and $P_0 = \$500$, a regular coupon payout occurs at time t when $P_t = \$450$ and $\beta_{t-} = 1$, then Class A receives \$0.02 coupon payment, and the conversion ratio is reset to $\beta_{t+} = 1.011$, which indicates that two shares of ETH can exchange for 505.62 shares of Class A and 505.62 shares of Class B after the regular payout. This is illustrated in Figure 3.

2.1.2 Upward Reset

An upward reset is triggered when the net asset value of Class B coins reaches the predetermined upper bound, denoted by $\mathcal{H}_u$. On an upward reset time t, net asset value of both

[10] Payments are made in the form of underlying ETH from the Custodian contract. For instance, upon regular payout, the holder of each Class A coin receives underlying ETH with amount $\frac{RT}{P_t}$.

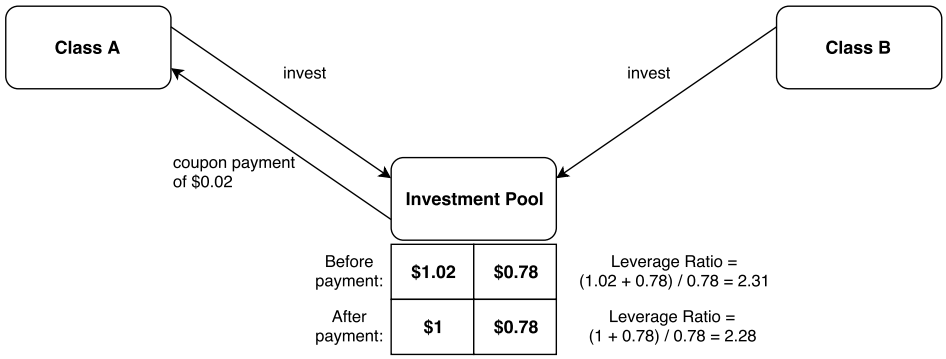

Figure 3: Class A and B, Regular Payout. After 100 days, the ETH price drops to \$450, so that total investment of one Class A coin and one Class B coin becomes \$1.8, within which \$1.02 belongs to Class A. A regular payout takes place, and Class A receives \$0.02 coupon payment. New exchange ratio: 2 shares of ETH now correspond to 505.62 ($= 500 \times \frac{2\times450}{2\times450-500*0.02}$) shares of Class A and 505.62 shares of Class B, yielding $\beta_{t+} = 1.011$.

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, and conversion factor β_{t+} is reset to P_t/P_0 so that after the upward reset two shares of ETH can exchange for P_t share of class A and B. For instance, as illustrated in Figure 4, after another 50 days, the ETH price grows to \$760.96, so the net asset value of the Class B grows to $\mathcal{H}_u \equiv \$2$, triggering an upward reset. The holders of Class A and B receive payments with amount \$0.01 and \$1, respectively. Two shares of ETH now correspond to 760.96 shares of Class A and 760.96 shares of Class B, yielding $\beta_{t+} = 1.52$.

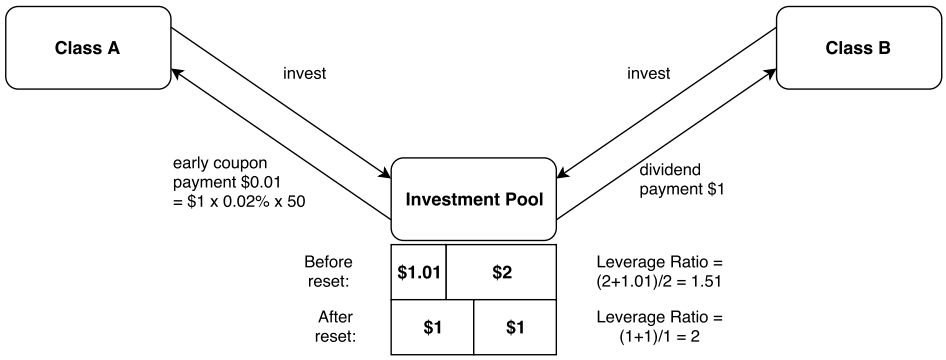

Figure 4: Class A and B, Upward Reset. After 50 days, the ETH price grows to \$760.96, and Class B NAV grows to \$2, triggering an upward reset. Class A NAV equals \$1.01, where \$0.01 is 50-day accrued coupon. On this date, Class A receives \$0.01 coupon payment, and Class B receives \$1 dividend payment. New exchange ratio: 2 shares of ETH now correspond to 760.96 shares of Class A and 760.96 shares of Class B, yielding $\beta_{t+} = 760.96/500 = 1.52$.

2.1.3 Downward Reset

A downward reset is triggered when the net asset value of Class B coins reaches the predetermined lower bound, denoted by $\mathcal{H}_d$, On a downward reset time t, Class A holders receive a payment with dollar value $V_A^t - \mathcal{H}_d$, and $1/\mathcal{H}_d$ shares of Class A and B are merged into one share of Class A and B, respectively, so that the net asset value of both classes resets to \$1. The conversion factor β_{t+} resets to P_t/P_0, that is, two ETHs can exchange for P_t shares of Class A and B after the reset. For instance, as illustrated in Figure 5, after another 50 days, the ETH price drops to \$479.40, so that the net asset value of Class B drops to $\mathcal{H}_d \equiv \$0.25$, 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. Two shares of ETH now correspond to 479.40 shares of Class A and 479.40 shares of Class B, yielding $\beta_{t+} = 479.40/500 = 0.96$.

Under a black swan event, the net asset value of Class B coins V_B^t is likely lower than $\mathcal{H}_d$ or even becomes negative upon downward reset. In the case of $V_B^t > 0$, we can simply replace $\mathcal{H}_d$ by V_B^t for the above description of cash flow and operations on downward reset. If $V_B^t \leq 0$, then both classes are fully liquidated, the holders of Class B receive nothing, and the holders of Class A receive the payment $V_A^t - |V_B^t|$.

No arbitrage implies that the market prices of Class A and B coins also satisfy the parity relation:

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

where W_A and W_B are the market prices of the Class A and B coins, respectively. This has an interesting implication: Suppose the demand of Class B coins is low, then the market value of Class B coins would be low, and the above parity relation implies that the market value of the Class A coins would be high.

Class A coin behaves like a bond. Although Class A has a fixed coupon rate and its

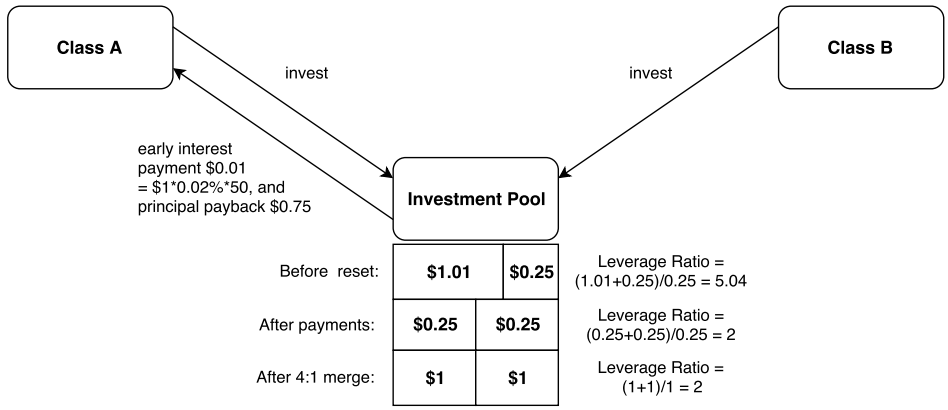

Figure 5: Class A and B, Downward Reset. After another 50 days, the ETH price drops to \$479.40, and Class B NAV drops to \$0.25, triggering an downward reset. Again, Class A NAV equals \$1.01, where \$0.01 is 50-day accrued coupon. On this date, Class A receives \$0.01 coupon payment, as well as \$0.75 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 $\beta_{t+} = 0.96$.

coupon payment is periodic and protected by the downward resets, its value is still volatile on non-coupon dates. This is because the coupon rate is usually higher than the risk-free rate, and on a downward reset, a portion of Class A coin will be liquidated, then the holder of Class A will lose high coupons that would be generated from this portion. Therefore, a potential downward reset will make the price of Class A volatile. We will propose two types of more stable coins: A′ coins (Section 2.2) and A0 coins (see Appendix D).

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′ coin and one Class B′ coin. Conversely, one Class A′ coin and one B′ coin can be merged into two 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 be 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

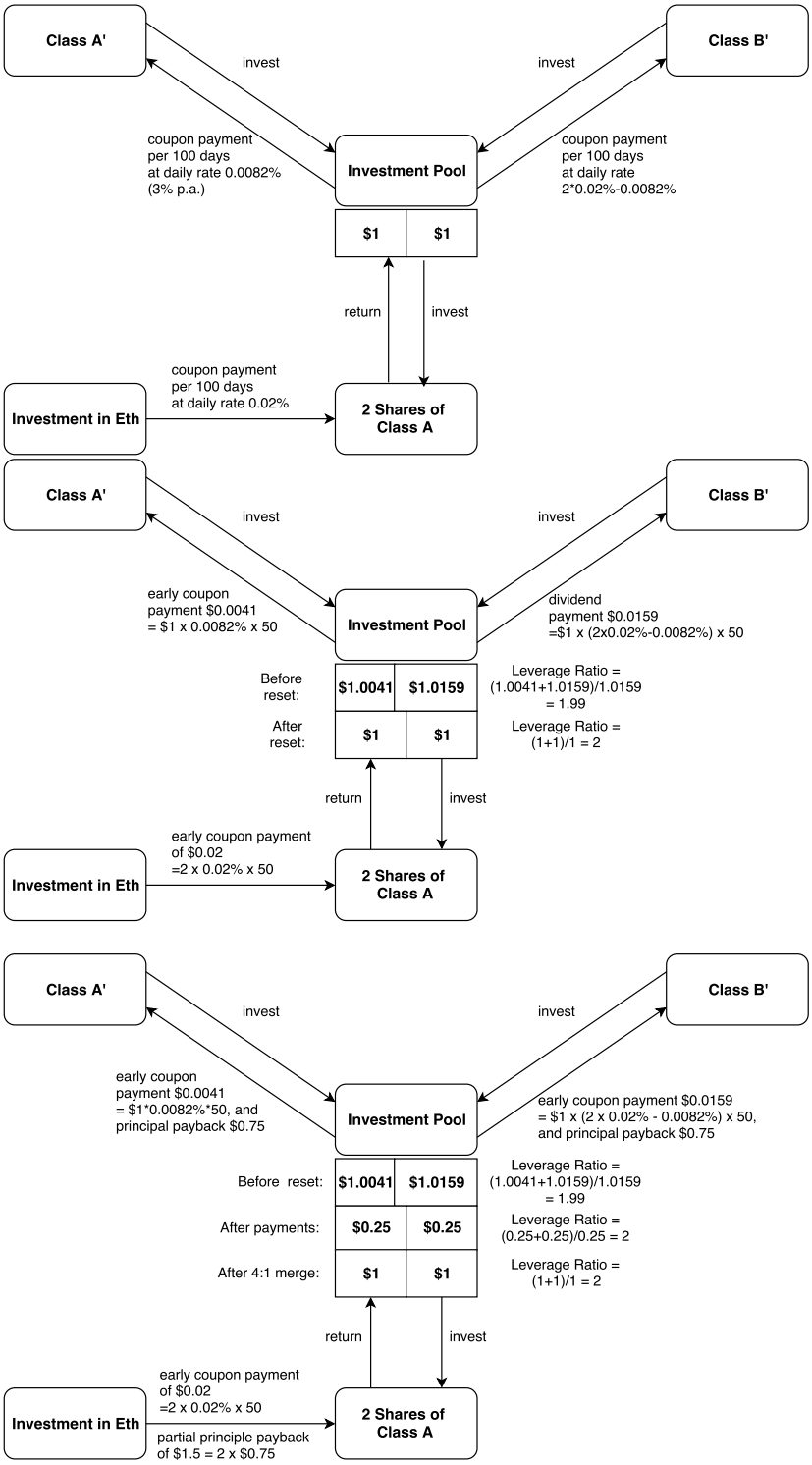

Figure 6: **Top Figure:** What happens to Class A′ on a regular payout date of A. On regular payout dates for Class A (per 100 days), 2 shares of A receives coupon payment \$0.04, i.e. at daily rate 0.02%. \$0.0082 is paid to A′ and \$0.0318 to B′ . **Middle Figure:** Upward Reset of Class A′ . After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

A$'$ gets coupon at the rate R' on regular payouts, upward and downward reset (provided that the net asset value of Class B is positive then), and Class B$'$ gets coupon at the rate $2R - R'$ on upward reset. On downward resets, each share of both Class A$'$ and B$'$ is reduced to $(V_B^t)^+$ share, and Class A$'$ gets the value of the liquidated shares (i.e., $1 - (V_B^t)^+$ 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 net asset value $1 + R't$, or the remaining total asset for A$'$ and B$'$, $2(1 + Rt - |V_B^t|)$, whichever is smaller. Class A$'$ behaves like a money market account, 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 Differences from the Dual-Purpose Fund Contract

There are four main differences between our stable coin with dual-purpose funds in China. First, in China a dual-purpose fund and its underlying fund share the same fund managers, hence the fund managers re-scale the price of the underlying fund upon upward and downward resets and regular payouts, in order to easily ensure the no arbitrage parity relation between the dual-purpose fund and the underlying fund. Since we cannot change the underlying ETH price, we instead change the exchange ratio of the shares between the underlying ETH and Class A and B coins in our case, to maintain no-arbitrage across upward and downward resets and regular payouts.

Second, 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 asset value of B share down-crossing $\mathcal{H}_d$. In contrast, for our stable coin, the triggering conditions of both upward and downward resets are all based on the net asset value of Class B coins. This is because unlike the re-scaled underlying fund price in China, the underlying ETH price is not so appropriate as the net asset value of Class B to measure the leverage ratio of Class B.

Third, the underlying funds of Chinese dual-purpose funds incur management fees, whereas

the underlying ETH does not. Finally, the periodic payout of dual-purpose fund is annually at a fixed date (e.g. first trading day of each year), while the periodic payout of our Class A coins happens when a pre-specified time has passed from the last reset or payout event, which reduces the frequency of payouts, making the coins more stable.

3 Valuation

This section is devoted to the valuation of coins described in Section 2, including Class A, B, A′ , and B′ coins. We study their fair values 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

Denote the relative price $S_t = P_t/(\beta_t P_0)$. Let W_A^t and W_B^t be the market value of Class A coins and B coins, respectively. Then the parity relation can be rewritten as $W_A^t + W_B^t = 2S_t$, which allows us to focus on the valuation of Class A coins.

Since the future cash flow of the coins depends on the cumulative time from last payment (namely, last reset or last regular payout), rather than the calendar time, in the remaining of this chapter we shall relabel the last payment time as 0, so that $t \in [0, T]$ denotes the time from last payment. Denote by $H_d(t) = \frac{1}{2}(1 + Rt) + \frac{1}{2}\mathcal{H}_d$ and $H_u(t) = \frac{1}{2}(1 + Rt) + \frac{1}{2}\mathcal{H}_u$ the downward reset barrier and the upward reset barrier (associated with S_t), respectively. Hence the downward (upward) reset is triggered when S_t hits $H_d(t)$ ($H_u(t)$). It is easy to see $H_d(t) \leq S_t \leq H_u(t)$ if S_t changes continuously. By design, S returns to 1 on every reset date, and is reduced by $\frac{1}{2}RT$ on every regular payout date.

Using the standard option pricing theory, the market value of Class A coins, $W_A^t \equiv$

$W_A(t,S)$, is given recursively as[11]

$$\begin{aligned} W_A(t,S) = E_t\Big[& e^{-r(T-t)}[RT + W_A(0, S_T - RT/2)] \cdot \mathbf{1}_{\{T<\tau\wedge\eta\}} \\ & + e^{-r(\tau-t)}[R\tau + W_A(0,1)] \cdot \mathbf{1}_{\{\tau\le T\wedge\eta\}} \\ & + e^{-r(\eta-t)}[R\eta + 1 - |V_B^\eta| + (V_B^\eta)^+ W_A(0,1)] \cdot \mathbf{1}_{\{\eta\le T\wedge\tau\}}\Big], \end{aligned} \tag{3.1}$$

where r is the risk-free rate, random times τ and η represent the first upward and downward reset date from t, respectively (i.e., $\tau = \inf\{\xi \ge t : S_\xi \ge H_u(\xi)\} \equiv \inf\{\xi \ge t : V_B^\xi \ge \mathcal{H}_u\}$ and $\eta = \inf\{\xi \ge t : S_\xi \le H_d(\xi)\} \equiv \inf\{\xi \ge t : V_B^\xi \le \mathcal{H}_d\}$), and E_t is the expectation computed under a risk-adjusted measure and under the initial condition $S_t = S$. For example, one can assume that P follows a geometric Brownian motion under the risk-adjusted measure:

$$dP_t = rP_t dt + \sigma P_t d\mathcal{B}_t, \tag{3.2}$$

where $\mathcal{B}_t$ is a one-dimensional standard Brownian motion.[12]

The value of Class A coin can be determined as above in a recursive manner, since the holders still get (certain shares of) Class A coin as well as coupons after reset or regular payout. On the right hand side of (3.1), the first term indicates that on the regular payout date T, holders get coupon payment RT and a new Class A coin for which the time from last payment returns to 0 and S is reduced by $RT/2$; the second term indicates that upon upward reset time τ, holders get coupon payment $R\tau$ and a new Class A coin for which the time from last payment returns to 0 and S becomes 1; and the third term indicates that upon downward reset time η, holders receive coupon payment $R\eta$, withdrawal value $1 - |V_B^\eta|$,

[11] We denote $x \wedge y = \min\{x, y\}$.

[12] If one assumes that complete hedging is possible, then the risk adjust measure is exactly the risk-neutral measure. However, even if one does not use the complete hedging argument, the standard option pricing theory using the rational expectations still gives the same dynamics, except that the risk free rate r is now endogenously determined in equilibrium by other factors, e.g. an outside endowment process; see, e.g. Kou (2002).

and $(V_B^\eta)^+$ shares of new Class A coin for which the time from last reset returns to 0 and S becomes 1.

It is straightforward to estimate W_A through (3.1) using Monte Carlo simulation, which is also suggested by Adams and Clunie (2006) to deal with the complexities in fund contracts. Due to the high volatility of the underlying cryptocurrency price, it is important to achieve real-time calculation of W_A. However, a simulation-based method is not so efficient for this purpose, since the cash flow of Class A coins has an infinite horizon and a weakly path-dependent nature. Therefore, in the following we propose an efficient PDE-based estimation method to compute W_A under the geometric Brownian assumption (3.2). Since there is no overshoot by a diffusion process, V_B always equals $\mathcal{H}_d$ on downward reset. Therefore, (3.1) can be simplified to

$$\begin{aligned} W_A(t,S) = E_t\Big[& e^{-r(T-t)}(RT + W_A(0, S_T - RT/2)) \cdot \mathbf{1}_{\{T<\tau\wedge\eta\}} \\ & + e^{-r(\tau-t)}(R\tau + W_A(0,1)) \cdot \mathbf{1}_{\{\tau\le T\wedge\eta\}} \\ & + e^{-r(\eta-t)}(R\eta + 1 - \mathcal{H}_d + \mathcal{H}_d W_A(0,1)) \cdot \mathbf{1}_{\{\eta\le T\wedge\tau\}}\Big]. \end{aligned} \tag{3.3}$$

It can be shown that W_A is governed by the following periodic PDE with nonlocal terminal and boundary conditions (see Appendix B):

$$-\frac{\partial W_A}{\partial t} = \frac{1}{2}\sigma^2 S^2 \frac{\partial^2 W_A}{\partial S^2} + rS\frac{\partial W_A}{\partial S} - rW_A, \qquad 0 \le t < T,\ H_d(t) < S < H_u(t) \tag{3.4}$$

$$W_A(T,S) = RT + W_A(0, S - \frac{1}{2}RT), \qquad H_d(T) < S < H_u(T) \tag{3.5}$$

$$W_A(t, H_u(t)) = Rt + W_A(0,1), \qquad 0 \le t \le T \tag{3.6}$$

$$W_A(t, H_d(t)) = Rt + 1 - \mathcal{H}_d + \mathcal{H}_d W_A(0,1), \qquad 0 \le t \le T. \tag{3.7}$$

It is easy to see that the terminal and boundary conditions (3.5) – (3.7) are directly related with the cash flow of Class A coins. Note that these conditions depend on the solution W_A itself. Such nonlocal terminal and boundary conditions make the PDE problem significantly

different from the classical Black-Scholes model, leading to challenges in both theory and computation. On the theoretical aspect, due to the nonlocal conditions, the linkage between the stochastic representation (3.3) and the PDE problem (3.4) – (3.7) is not straightforward, and no analytical solution is available. On the numerical aspect, the nonlocalness makes the problem nonlinear, which motivates us to propose an efficient iterative procedure to find numerical solutions (see Appendix C).

3.2 Class A′ and B′ Coins

Denote by $W_{A'}(t,S)$ and $W_{B'}(t,S)$ the market prices of Class A′ and B′ coins, respectively. Since two shares of Class A coin exchange for one A′ coin and one B′ coin, i.e., $2W_A(t,S) = W_{A'}(t,S) + W_{B'}(t,S)$, in the following we only discuss the valuation of Class A′ coin. Under the risk-neutral pricing framework, $W_{A'}(t,S)$ is given recursively as

$$\begin{aligned} E_t\Bigg[& e^{-r(T-t)}(R'T + W_{A'}(0, S_T - RT/2)) \cdot \mathbf{1}_{\{T<\tau\wedge\eta\}} \\ & + e^{-r(\tau-t)}(R'\tau + W_{A'}(0,1)) \cdot \mathbf{1}_{\{\tau\le T\wedge\eta\}} \\ & + e^{-r(\eta-t)}\left(\min\{R'\eta + 1 - (V_B^\eta)^+, 2(R\eta + 1 + V_B^\eta)^+\} + (V_B^\eta)^+ W_{A'}(0,1)\right)\mathbf{1}_{\{\eta\le T\wedge\tau\}}\Bigg], \end{aligned} \tag{3.8}$$

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 $\frac{R'\eta-1}{2} - R\eta \le V_B^\eta \le 0$, A′ is fully liquidated, and still receives full net asset value; otherwise, A′ is fully liquidated and takes a loss by receiving $2(1+R\eta+V_B^\eta)^+$ which is smaller than its net asset value $1+R\eta$. 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 net asset value in this case, provided $V_B^\eta \ge \frac{R'\eta-1}{2} - R\eta$; only when $V_B^\eta < \frac{R'\eta-1}{2} - R\eta$ will Class A′ take a loss.

Assuming that P_t follows a geometric Brownian motion, it is easy to see that (3.8) reduces to

$$
\begin{aligned}
E_t\Bigg[& e^{-r(T-t)}(R'T + W_{A'}\ (0, S_T - RT/2)) \cdot \mathbf{1}_{\{T<\tau\wedge\eta\}} \\
& + e^{-r(\tau-t)}(R'\tau + W_{A'}(0,1)) \cdot \mathbf{1}_{\{\tau\leq T\wedge\eta\}} \\
& + e^{-r(\eta-t)}\left(R'\eta + 1 - \mathcal{H}_d + \mathcal{H}_d W_{A'}(0,1)\right) \cdot \mathbf{1}_{\{\eta\leq T\wedge\tau\}}\Bigg].
\end{aligned}
$$

Similar to the linkage between (3.3) and (3.4)-(3.7), we deduce that $W_{A'}(t,S)$ satisfies the following PDE:

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

4 Numerical Examples

For illustration, we use Ethereum (ETH) as the underlying cryptocurrency, during the period from 1 Oct 2017 to 28 Feb 2018.[13] We further assume that the price is monitored on a *daily* basis, and the upward and downward resets are performed according to the end-of-day

[13]The dual class structure of the stable coin is independent of the choice of underlying cryptocurrency; however, 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.

prices. The default model parameters are given as follows.

$$R = 0.02\% \text{ (7.3\% p.a.)} \qquad R' = 0.0082\% \text{ (3\% p.a.)} \qquad \mathcal{H}_u = 2 \quad \mathcal{H}_d = 0.25$$

$$r = 0.0082\% \text{ (3\% p.a.)} \qquad \sigma = 0.0628 \text{ (120\% p.a.)} \qquad T = 100.$$

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 7 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 coins 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 7 at the end of January: as the downward reset approaches, the value of Class A also goes down, especially when the model underestimates the ETH volatility (by setting $\sigma = 0.0262$ per day (annualized 0.5)).

Figure 8 shows the simulated paths from Class B coins. Note that Class 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 9 that the market value of Class A′ coins 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

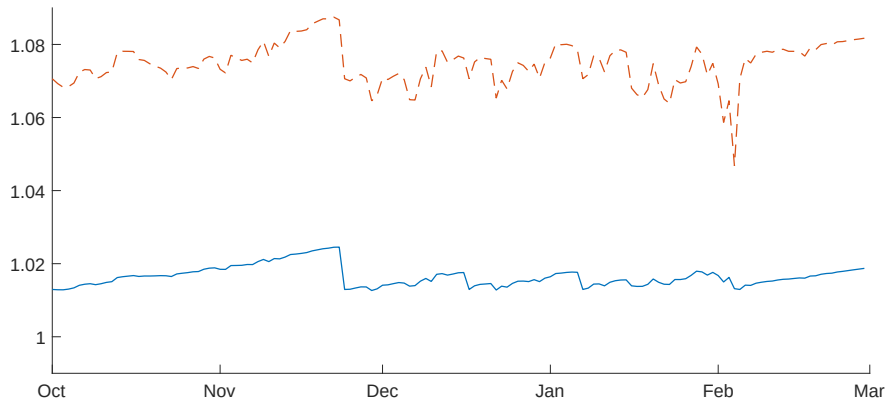

Figure 7: Simulated class A Market Value. $\sigma = 0.0628$ for the blue solid curve, $\sigma = 0.0262$ for the red dashed curve. Parameters: $R = 0.02\%, \mathcal{H}_d = 0.25$, $\mathcal{H}_u = 2$, $T = 100$, $r = 0.0082\%$ per day (3% per year). Upward reset takes place on 24 Nov 2017, 17 Dec 2017,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

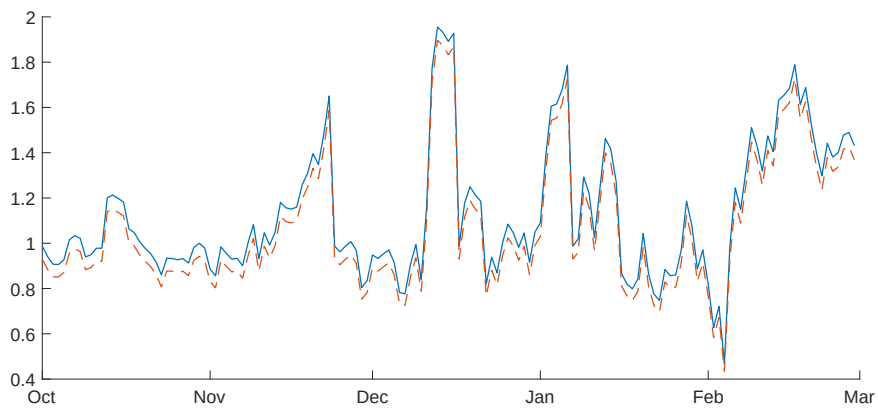

Figure 8: Class B Market Value. $\sigma = 0.0628$ for the blue solid curve, $\sigma = 0.0262$ for the red dashed curve. Parameters: $R = 0.02\%$, $\mathcal{H}_d = 0.25$, $\mathcal{H}_u = 2$, $T = 100$, $r = 0.0082\%$ per day (3% per year). Upward reset takes place on 24 Nov 2017, 17 Dec 2017, and 7 Jan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

de-trend the value of Class A$'$ by its net asset value 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 0.87%, which is comparable to that of the short term U.S. treasury bill, 0.96% (912828K2 Govt, from April 2015 to February 2018).

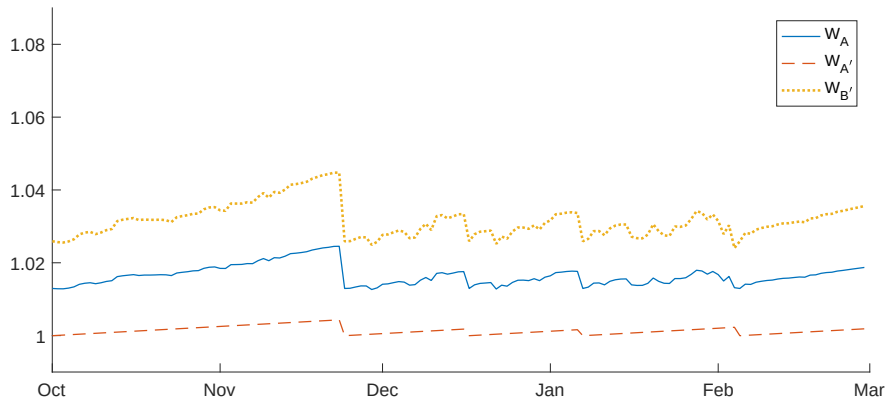

Figure 9: Market Value of Class A′ (red) and B′ (yellow), compared with Class A (blue). Annualized volatility of Class A′ and B′ are 0.0087 and 0.0403, respectively. Parameters: $R = 0.02\%$ per day, $\mathcal{H}_d = 0.25$, $\mathcal{H}_u = 2$, $R' = 0.0082\%$ (3% per year), $T = 100$, $\sigma = 120\%$ per year, $r = 0.0082\%$ per day. Upward reset takes place on 24 Nov 2017, 17 Dec 2017, and 7 Jan 2018. Downward reset takes place on 5 Feb 2018.

4.3 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 net asset value of Class A coins $V_A^\eta = 2S_{\eta-} \cdot (1-80\%) = 0.4$, while the net asset value 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. Specifically,

$$dP_t/P_{t-} = rdt + \sigma d\mathcal{B}_t + dJ_t,$$

where J is a compound Poisson process with constant intensity 0.2 (per 100 days) and constant jump size -80%. Using simulation based on (3.1) and (3.8), 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.

5 Conclusion

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. By using option pricing theory, this paper designs, 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). The design is inspired by the dual-purpose funds popular in the U.S. and China. 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 the proposed stable coins indeed have very low volatility. Indeed, the class A coin has a volatility comparable to that of the exchange rate of world currencies against U.S. dollar, and the class A$'$ coin essentially is pegged to U.S. dollar. When combined with insurance from a government, the design can also serve as a basis for issuing a sovereign cryptocurrency.

References

Adams, A. T., and J. B. Clunie (2006): "Risk Assessment Techniques for Split Capital Investment Trusts," *Annals of Actuarial Science*, 1, 7–36.

Al-Naji, N. (2018): "Basecoin: A Price-Stable Cryptocurrency with an Algorithmic Central Bank," http://www.getbasecoin.com/basecoin_whitepaper_0_99.pdf.

Bech, M. L., and R. Garratt (2017): "Central Bank Cryptocurrencies," https://papers.ssrn.com/abstract=3041906.

Catalini, C., and J. S. Gans (2016): "Some Simple Economics of the Blockchain," *NBER Working Paper*, http://www.nber.org/papers/w22952.

Cong, L. W., and Z. He (2018): "Blockchain Disruption and Smart Contracts," *To Appear in Review of Financial Studies*.

Dai, M., S. Kou, and C. Yang (2017): "A Stochastic Representation for Nonlocal Parabolic PDEs with Applications," Working Paper.

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.

Duffie, D. (2010): *Dynamic Asset Pricing Theory: Third Edition*. Princeton University Press.

Easley, D., M. O'Hara, and S. B. Basu (2017): "From Mining to Markets: The Evolution of Bitcoin Transaction Fees," Working Paper.

Garratt, R. (2016): "CAD-coin versus Fedcoin," *R3 Report*.

Garratt, R., and N. Wallace (2018): "Bitcoin 1, Bitcoin 2, ...: An Experiment in Privately Issued Outside Monies.," *Economic Inquiry*, forthcoming.

Grinberg, R. (2011): "Bitcoin: An Innovative Alternative Digital Currency," https://papers.ssrn.com/abstract=1817857.

Grunspan, C., and R. Perez-Marco (2018): "Double Spend Races," Working Paper.

Harvey, C. R. (2016): "Cryptofinance," https://papers.ssrn.com/abstract=2438299.

Huberman, G., J. Leshno, and C. Moallemi (2017): "Monopoly without a Monopolist: An Economic Analysis of the Bitcoin Payment System," Working Paper.

Hull, J. C. (2017): *Options, Futures, and Other Derivatives*. Pearson Education.

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.

Ingersoll, J. E. (1987): *Theory of Financial Decision Making*. Rowman & Littlefield.

Jarrow, R. A., and M. O'Hara (1989): "Primes and Scores: An Essay on Market Imperfections," *The Journal of Finance*, 44, 1263–1287.

Jarrow, R. A., and S. M. Turnbull (1999): *Derivative Securities: The Complete Investor's Guide*. Thomson Learning.

Khapko, M., and M. Zoican (2018): "Smart Settlement," https://papers.ssrn.com/abstract=2881331.

Kou, S. G. (2002): "A Jump Diffusion Model for Option Pricing," *Management Science*, 48, 1086–1101.

MakerTeam (2017): "The Dai Stablecoin System," https://makerdao.com.

Malinova, K., and A. Park (2017): "Market Design with Blockchain Technology," https://papers.ssrn.com/abstract=2785626.

Nakamoto, S. (2008): "Bitcoin: A Peer-to-Peer Electronic Cash System," https://bitcoin.org/bitcoin.pdf.

Rogoff, K. (2015): "Costs and Benefits to Phasing out Paper Currency," *NBER Macroeconomics Annual*, 29(1), 445–456.

Shreve, S. E. (2004): *Stochastic Calculus for Finance II*. Springer Science Business Media.

Tether (2016): "Tether: Fiat Currencies on the Bitcoin Blockchain," https://tether.to/wp-content/uploads/2016/06/TetherWhitePaper.pdf.

Yermack, D. (2017): "Corporate Governance and Blockchains," *Review of Finance*, 21(1), 7–31.

Online Supplement

Designing Stable Coins

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.

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

$$C_B = \frac{M_C P_0 \beta_t (1-c)}{1+\alpha}, \qquad C_A = \alpha C_B, \tag{A.1}$$

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 cryptocurrency in target fiat currency at last reset event, and β_t is the conversion factor set as 1 at inception and its behaviour is detailed later in Section A.1 to A.2.

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

$$M_C = \frac{C(1-c)(1+\alpha)}{\beta_t P_0}. \tag{A.2}$$

The net value of coins are calculated based on the coupon rate, the elapsed time from last reset event, and the latest underlying cryptocurrency price in target fiat currency fed to

the system. In particular:

$$V_A^t = 1 + R \cdot v_t, \qquad V_B^t = (1+\alpha) \cdot \frac{P_t}{\beta_t P_0} - \alpha \cdot V_A^t, \tag{A.3}$$

where R is the daily coupon rate, v_t is the number of days from last reset event, and P_t is the current price of underlying cryptocurrency in target fiat currency. Note that at all time $Q_A^t = \alpha Q_B^t$, where Q_A^t and Q_B^t are the total amount of Class A and Class B coins. The implied leverage ratio is

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

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

A.1 Regular Payout

A regular payout is triggered when $v_{t-} = T$. Upon regular payout:

1. Total amount of both classes coin remain unchanged, $Q_A^{t+} = Q_A^{t-}$ and $Q_B^{t+} = Q_B^{t-}$
2. Net asset value of Class A reset to 1 USD
3. Class A holder will receive certain amount of underlying cryptocurrency from the Custodian contract. Such amount for each Class A coin is $U_A = \frac{V_A^t - 1}{P_t}$
4. Conversion factor $\beta_{t+} = \beta_{t-} \cdot \frac{(1+\alpha)P_t}{(1+\alpha)P_t - \alpha\beta_{t-}P_0\left(V_A^t - 1\right)}$

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.2 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 coins remain unchanged, $Q_A^{t+} = Q_A^{t-}$ and $Q_B^{t+} = Q_B^{t-}$.

2. Net asset value of both classes reset to 1 target fiat currency.

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

4. Conversion factor β_{t+} is reset to P_t/P_0.

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.3 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 coins is reduced to $Q_B^{t+} = Q_B^{t-} \cdot (V_B^t)^+$.

2. Total amount of Class A coins 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 cryptocurrency from the Custodian contract. Such amount of each Class A coin is: $D_A = \frac{V_A^t - V_B^t}{P_t}$ if $V_B^t \geq 0$, and $D_A = \frac{V_A^t + V_B^t/\alpha}{P_t}$ if $V_B^t < 0$

5. Conversion factor β_{t+} is reset to P_t/P_0.

Total value in the system is unchanged after reset:

$$
\begin{aligned}
& D_A \cdot P_t \cdot Q_A^{t-} + Q_A^{t+} \cdot V_A^{t+} + Q_B^{t+} \cdot V_B^{t+} \\
=& \left[\left(V_A^t - V_B^t\right) \cdot \mathbf{1}_{V_B^t \geq 0} + \left(V_A^t + V_B^t/\alpha\right) \cdot \mathbf{1}_{V_B^t < 0} \right] \cdot Q_A^{t-} + Q_B^{t+} \cdot \alpha \cdot 1 + Q_B^{t+} \cdot 1 \\
=& V_A^t \cdot Q_A^{t-} - (V_B^t)^+ \cdot Q_B^{t-} \cdot \alpha - (V_B^t)^- \cdot Q_B^{t-} + Q_B^{t-} \cdot (V_B^t)^+ \cdot \alpha + Q_B^{t-} \cdot (V_B^t)^+ \\
=& V_A^t \cdot Q_A^{t-} + V_B^t \cdot Q_B^{t-} \ .
\end{aligned}
$$

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

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

$$
\alpha \cdot W_A^t + W_B^t = \alpha \cdot V_A^t + V_B^t \ ,
$$

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

B Derivation of the Pricing Equation

Using contract design under general split ratio $\alpha > 0$, similar to (3.1), the value of Class A coins is described by the stochastic representation

$$
\begin{aligned}
W_A(t,S) = E_t \Bigg[& e^{-r(T-t)} (RT + W_A(0, S_T - \alpha RT/(1+\alpha))) \cdot \mathbf{1}_{\{T < \tau \wedge \eta\}} \\
& + e^{-r(\tau - t)} (R\tau + W_A(0,1)) \cdot \mathbf{1}_{\{\tau \leq T \wedge \eta\}} \\
& + e^{-r(\eta - t)} (R\eta + 1 - |V_B^\eta| + (V_B^\eta)^+ W_A(0,1)) \cdot \mathbf{1}_{\{\eta \leq T \wedge \tau\}} \Bigg].
\end{aligned}
\tag{B.1}
$$

Note that (B.1) becomes (3.1) when $\alpha = 1$. In this section, under the geometric Brownian motion assumption, we show that (B.1) defines a unique bounded function W_A, which is exactly the solution to the PDE problem (3.4) – (3.7) when $\alpha = 1$. We denote v_s and Y_s as the time from last regular payout or reset 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 (thanks to the geometric Brownian motion assumption), reflecting the partial payback of Class A principal. In this remaining of this section, we focus on the right limit process S_{t+}, which is still denoted as S_t for simplicity of notations. 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, we have

$$
\begin{aligned}
&dS_t = rS_t dt + \sigma S_t d\mathcal{B}_t, \\
&S_{\zeta_i} = S_{\zeta_i -} - \frac{\alpha}{\alpha+1} R v_{\zeta_i -}, \quad S_{\tau_i} = S_{\eta_i} = 1, \quad v_{\tau_i} = v_{\eta_i} = v_{\zeta_i} = 0,
\end{aligned}
$$

where $\mathcal{B}$ is a Brownian motion under the risk-neutral measure.

First, we derive the following proposition, which expresses the stochastic representation (B.1) into a non-recursive form.

Proposition 1. *Equation (B.1) defines a unique solution $W_A(t,S)$ for $0 \le t \le T$, $H_d(t) \le S \le H_u(t)$, which can be written as*

$$
\begin{aligned}
W_A(t,S) = E_t^{(t,S,1)} \Bigg[&\sum_{\zeta_i \ge t} e^{-r(\zeta_i - t)} Y_{\zeta_i -} RT + \sum_{\tau_i \ge t} e^{-r(\tau_i - t)} Y_{\tau_i -} R v_{\tau_i -} \\
&+ \sum_{\eta_i \ge t} e^{-r(\eta_i - t)} Y_{\eta_i -} (R v_{\eta_i -} + 1 - \mathcal{H}_d) \Bigg],
\end{aligned}
\tag{B.2}
$$

where $E_t^{(u,s,y)}$ is the $\mathbb{Q}$-expectation computed under the initial condition $v_{t-} = u$, $S_{t-} = s$, and $Y_{t-} = y$.[14]

Proof of Proposition 1. Without loss of generality we prove the case $T = 1$. We prove this theorem in three steps.

[14] If t and S are such that t is a regular payout or downward/upward reset date, the right hand side of (3.1) is viewed as the value of the time-t payment plus the expectation with the value of state variables immediately after the jump (if applicable) as time-t starting values.

Step 1: To see that W_A given by (B.2) satisfies (B.1), note that (B.2) implies

$$
\begin{aligned}
W_A(t,S) = E_t^{t,S,1}\Bigg[& \sum_{t\le\zeta_i<\tau_1\wedge\eta_1} e^{-r(\zeta_i-t)}Y_{\zeta_i-}R + e^{-r(\tau_1-t)}Y_{\tau_1-}Rv_{\tau_1-}\cdot\mathbf{1}_{\{\tau_1<\eta_1\}} \\
& + e^{-r(\eta_1-t)}Y_{\eta_1-}(Rv_{\eta_1-}+1-\mathcal{H}_d)\cdot\mathbf{1}_{\{\eta_1<\tau_1\}} \\
& + e^{-r(\tau_1\wedge\eta_1-t)}Y_{\tau_1\wedge\eta_1}E_{\tau_1\wedge\eta_1}^{(0,1,Y_{\tau_1\wedge\eta_1})}\Bigg(\sum_{\xi_i\ge\tau_1\wedge\eta_1} e^{-r(\zeta_i-\tau_1\wedge\eta_1)}\frac{Y_{\zeta_i-}}{Y_{\tau_1\wedge\eta_1}}R \\
& + \sum_{\tau_i>\tau_1\wedge\eta_1} e^{-r(\tau_i-\tau_1\wedge\eta_1)}\frac{Y_{\tau_i-}}{Y_{\tau_1\wedge\eta_1}}Rv_{\tau_i-} \\
& + \sum_{\eta_i>\tau_1\wedge\eta_1} e^{-r(\eta_i-\tau_1\wedge\eta_1)}\frac{Y_{\eta_i-}}{Y_{\tau_1\wedge\eta_1}}(Rv_{\eta_i-}+1-\mathcal{H}_d)\Bigg)\Bigg],
\end{aligned}
$$

where $E_{\tau_1\wedge\eta_1}^{(u,s,y)}$ denotes the conditional expectation computed at time $\tau_1\wedge\eta_1$ with $(v,S,Y)_{\tau_1\wedge\eta_1} = (u,s,y)$. As a result,

$$
\begin{aligned}
& E_{\tau_1\wedge\eta_1}^{(0,1,Y_{\tau_1\wedge\eta_1})}\Bigg[\sum_{\xi_i\ge\tau_1\wedge\eta_1} e^{-r(\zeta_i-\tau_1\wedge\eta_1)}\frac{Y_{\zeta_i-}}{Y_{\tau_1\wedge\eta_1}}R + \sum_{\tau_i>\tau_1\wedge\eta_1} e^{-r(\tau_i-\tau_1\wedge\eta_1)}\frac{Y_{\tau_i-}}{Y_{\tau_1\wedge\eta_1}}Rv_{\tau_i-} \\
& \quad + \sum_{\eta_i>\tau_1\wedge\eta_1} e^{-r(\eta_i-\tau_1\wedge\eta_1)}\frac{Y_{\eta_i-}}{Y_{\tau_1\wedge\eta_1}}(Rv_{\eta_i-}+1-\mathcal{H}_d)\Bigg]\Bigg] \\
& = E_0^{(0,1,1)}\Bigg[\sum_{\xi_i\ge0} e^{-r\zeta_i}Y_{\zeta_i-}R + \sum_{\tau_i\ge0} e^{-r\tau_i}Y_{\tau_i-}Rv_{\tau_i-} \\
& \quad + \sum_{\eta_i\ge0} e^{-r\eta_i}Y_{\eta_i-}(Rv_{\eta_i-}+1-\mathcal{H}_d)\Bigg] \\
& = W_A(0,1),
\end{aligned}
$$

where the first equality follows from the Markov property of (v,S,Y) and the fact that time 0 cannot be an interest payment date given $(v,S,Y)_0 = (0,1,1)$. Plugging this equation into

the previous equation, we get

$$
\begin{aligned}
W_A(t,S) &= E_t^{(t,S,1)}\Bigg[\sum_{t\le\zeta_i<\tau_1\wedge\eta_1} e^{-r(\zeta_i-t)}Y_{\zeta_i-}R + e^{-r(\tau_1-t)}Y_{\tau_1-}Rv_{\tau_1-}\cdot\mathbf{1}_{\{\tau_1<\eta_1\}} \\
&\quad + e^{-r(\eta_1-t)}Y_{\eta_1-}(Rv_{\eta_1-}+1-\mathcal{H}_d)\cdot\mathbf{1}_{\{\eta_1<\tau_1\}} + e^{-r(\tau_1\wedge\eta_1-t)}Y_{\tau_1\wedge\eta_1}W_A(0,1)\Bigg] \\
&= E_t^{(t,S,1)}\Bigg[\sum_{\zeta_i<\tau_1\wedge\eta_1} e^{-r(i-t)}R + e^{-r(\tau_1-t)}R(\tau_1-\lfloor\tau_1\rfloor+W_A(0,1))\cdot\mathbf{1}_{\{\tau_1<\eta_1\}} \\
&\quad + e^{-r(\eta_1-t)}(R(\eta_1-\lfloor\eta_1\rfloor)+1-\mathcal{H}_d+\mathcal{H}_dW_A(0,1))\cdot\mathbf{1}_{\{\eta_1<\tau_1\}}\Bigg]
\end{aligned}
$$

by the definition of v, Y, and ζ. This yields (B.1).

Step 2: Next we show that any solution W_A satisfying (B.1) is a bounded function of (t,S) in $0\le t\le 1$, $H_d(t)\le S\le H_u(t)$. Indeed,

$$
\begin{aligned}
W_A(t,S) &= E_t^{(t,S,1)}\Bigg[\sum_{1\le i<\tau\wedge\eta} e^{-r(i-t)}R + e^{-r(\tau-t)}\Bigg(R(\tau-\lfloor\tau\rfloor) \\
&\quad + W_A(0,1))\cdot\mathbf{1}_{\{\tau<\eta\}} \\
&\quad + e^{-r(\eta-t)}(R(\eta-\lfloor\eta\rfloor)+1-\mathcal{H}_d+\mathcal{H}_dW_A(0,1)\Bigg)\cdot\mathbf{1}_{\{\eta<\tau\}}\Bigg] \\
&\le E_t^{(t,S,1)}\Bigg[\sum_{1\le i<\tau\wedge\eta} e^{-r(i-t)}R \\
&\quad + e^{-r(\tau\wedge\eta-t)}(R+\max\{W_A(0,1),1-\mathcal{H}_d+\mathcal{H}_dW_A(0,1)\})\Bigg] \\
&\le \frac{e^{-r}R}{1-e^{-r}} + (R+\max\{W_A(0,1),1-\mathcal{H}_d+\mathcal{H}_dW_A(0,1)\}) := \overline{K}.
\end{aligned}
$$

Note that the right hand side does not depend on t or S.

Step 3: To see the uniqueness, for any W_A satisfying (B.1), by defining the first interest

payment time $\theta_1 = \tau_1 \wedge \eta_1 \wedge 1$, we get

$$
\begin{aligned}
W_A(t,S) &= E_t^{(t,S,1)}\Bigg[e^{-r(\theta_1-t)}\Bigg((R + W_A(0, S_{\theta_1-} - \alpha R/(1+\alpha))) \cdot \mathbf{1}_{\{\theta_1<\tau_1\wedge\eta_1\}} \\
&\quad + (R(\theta_1 - \lfloor\theta_1\rfloor) + W_A(0,1)) \cdot \mathbf{1}_{\{\theta_1=\tau_1\}} \\
&\quad + (R(\theta_1 - \lfloor\theta_1\rfloor) + 1 - \mathcal{H}_d + \mathcal{H}_d W_A(0,1)) \cdot \mathbf{1}_{\{\theta_1=\eta_1\}}\Bigg)\Bigg] \\
&= E_t^{(t,S,1)}\Bigg[e^{-r(\theta_1-t)}\Bigg(R \cdot \mathbf{1}_{\{\theta_1=\zeta_1\}} + Rv_{\theta_1-} \cdot \mathbf{1}_{\{\theta_1=\tau_1\}} \\
&\quad + (Rv_{\theta_1-} + 1 - \mathcal{H}_d) \cdot \mathbf{1}_{\{\theta_1=\eta_1\}} + Y_{\theta_1} W_A(v_{\theta_1}, S_{\theta_1})\Bigg)\Bigg].
\end{aligned}
$$

Therefore,

$$
\begin{aligned}
&W_A(t,S) \\
&= E_t^{(t,S,1)}\Bigg[\Bigg(\sum_{\zeta_i\le\theta_1} e^{-r(\zeta_i-t)} Y_{\zeta_i-} R + \sum_{\tau_i\le\theta_1} e^{-r(\tau_i-t)} Y_{\tau_i-} R v_{\tau_i-} \\
&\quad + \sum_{\eta_i\le\theta_1} e^{-r(\eta_i-t)} Y_{\eta_i-}(Rv_{\eta_i-} + 1 - \mathcal{H}_d) + e^{-r(\theta_1-t)} Y_{\theta_1} W_A(0, S_{\theta_1})\Bigg)\Bigg].
\end{aligned}
$$

By plugging the expression for $W_A(0,1)$ into the right hand side and using the Markov property, one gets

$$
\begin{aligned}
W_A(t,S) &= E_t^{(t,S,1)}\Bigg[\Bigg(\sum_{\zeta_i\le\theta_1} e^{-r(\zeta_i-t)} Y_{\zeta_i-} R + \sum_{\tau_i\le\theta_1} e^{-r(\tau_i-t)} Y_{\tau_i-} R v_{\tau_i-} \\
&\quad + \sum_{\eta_i\le\theta_1} e^{-r(\eta_i-t)} Y_{\eta_i-}(Rv_{\eta_i-} + 1 - \mathcal{H}_d)\Bigg) \\
&\quad + e^{-r(\theta_1-t)} Y_{\theta_1} E_{\theta_1}^{(v_{\theta_1}, S_{\theta_1}, Y_{\theta_1})}\Bigg[\Bigg(\sum_{\theta_1<\zeta_i\le\theta_2} e^{-r(\zeta_i-\theta_1)} \frac{Y_{\zeta_i-}}{Y_{\eta_i}} R \\
&\quad + \sum_{\theta_1<\tau_i\le\theta_2} e^{-r(\tau_i-\theta_1)} \frac{Y_{\tau_i-}}{Y_{\theta_1}} R v_{\eta_i-} \\
&\quad + \sum_{\theta_1<\eta_i\le\theta_2} e^{-r(\eta_i-\theta_1)} \frac{Y_{\eta_i-}}{Y_{\theta_1}}(Rv_{\eta_i-} + 1 - \mathcal{H}_d) + e^{-r(\theta_2-\theta_1)} \frac{Y_{\theta_2}}{Y_{\theta_1}} W_A(v_{\theta_2}, S_{\theta_2})\Bigg)\Bigg]\Bigg].
\end{aligned}
$$

Thus,

$$
\begin{aligned}
&W_A(t,S)\\
&= E_t^{(t,S,1)}\Bigg[\Bigg(\sum_{\zeta_i\le\theta_2} e^{-r(\zeta_i-t)}Y_{\zeta_i-}R + \sum_{\tau_i\le\theta_2} e^{-r(\tau_i-t)}Y_{\tau_i-}Rv_{\tau_i-}\\
&\quad + \sum_{\eta_i\le\theta_2} e^{-r(\eta_i-t)}Y_{\eta_i-}(Rv_{\eta_i-}+1-\mathcal{H}_d) + e^{-r(\theta_2-t)}Y_{\theta_2}W_A(v_{\theta_2},S_{\theta_2})\Bigg)\Bigg].
\end{aligned}
$$

Repeating this for N times, we get

$$
\begin{aligned}
W_A(t,S) = E_t^{(t,S,1)}\Bigg[&\sum_{t\le\zeta_i\le\theta_N} e^{-r(\zeta_i-t)}Y_{\zeta_i-}R + \sum_{t\le\tau_i\le\theta_N} e^{-r(\tau_i-t)}Y_{\tau_i-}Rv_{\tau_i-}\\
&+ \sum_{t\le\eta_i\le\theta_N} e^{-r(\eta_i-t)}Y_{\eta_i-}(Rv_{\eta_i-}+1-\mathcal{H}_d) + e^{-r(\theta_N-t)}Y_{\theta_N}W_A(v_{\theta_N},S_{\theta_N})\Bigg],
\end{aligned}
\tag{B.3}
$$

where θ_N denotes the N-th interest payment time. Thanks to the boundedness of W_A, we have

$$
\begin{aligned}
0 &\le \lim_{N\to\infty} E_t^{(t,S,1)}\left[e^{-r(\theta_N-t)}Y_{\theta_N}W_A(v_{\theta_N},S_{\theta_N})\right]\\
&\le \overline{K}\cdot\lim_{N\to\infty} E_t^{(t,S,1)}\left[e^{-r(\theta_N-t)}\right] = 0.
\end{aligned}
$$

Here, to see the last equality, it suffices to note that (1) for two consecutive regular payouts ζ_i,ζ_{i+1}, we have $\zeta_{i+1}-\zeta_i\ge T$, therefore $E_t^{t,S,1}\left[e^{-r(\zeta_{i+1}-\zeta_i)}\right]\le e^{-rT} := K_1 < 1$; (2) for two consecutive upward resets τ_i,τ_{i+1}, we have $E_t^{t,S,1}\left[e^{-r(\tau_{i+1}-\tau_i)}\right] = E_0^{0,1,1}\left[e^{-r\tau_1}\right] := K_2 < 1$; (3) for two consecutive downward resets η_i,η_{i+1}, we have $E_t^{t,S,1}\left[e^{-r(\eta_{i+1}-\eta_i)}\right] = E_0^{0,1,1}\left[e^{-r\eta_1}\right] := K_3 < 1$. Consequently, for $k\ge 1$, we have

$$
E_t^{t,S,1}\left[e^{-r(\theta_{3k+3}-\theta_{3k})}\right] \le K_1\wedge K_2\wedge K_3 < 1,
$$

since there must be two regular payouts, upward resets or downward resets in $\theta_{3k},\ldots,\theta_{3k+3}$. Therefore,

$$
E_t^{t,S,1}\left[e^{-r(\theta_{3k+3}-t)}\right] \le e^{rt}\cdot(K_1\wedge K_2\wedge K_3)^k \to 0,\ \text{as } k\to\infty,
$$

and the claim follows from the monotonicity of (θ_k). Therefore, by sending $N \to \infty$, we infer that the right hand side of (B.3) converges to (B.2). This shows that any W_A is equal to the right hand side of (B.2), which gives the uniqueness of W_A satisfying (B.1). □

Theorem B.1. *W_A is the unique classical solution*[15] *to the following partial differential equation on $\{(t,S) : 0 \le t < T, H_d(t) < S < H_u(t)\}$*

$$-\frac{\partial W_A}{\partial t} = \frac{1}{2}\sigma^2 S^2 \frac{\partial^2 W_A}{\partial S^2} + rS\frac{\partial W_A}{\partial S} - rW_A, \qquad 0 \le t < T, H_d(t) < S < H_u(t) \tag{B.4}$$

$$W_A(T,S) = RT + W_A(0, S - \frac{\alpha}{1+\alpha}RT), \qquad H_d(T) < S < H_u(T) \tag{B.5}$$

$$W_A(t, H_u(t)) = Rt + W_A(0,1), \qquad 0 \le t \le T \tag{B.6}$$

$$W_A(t, H_d(t)) = Rt + 1 - \mathcal{H}_d + \mathcal{H}_d W_A(0,1), \qquad 0 \le t \le T. \tag{B.7}$$

Proof of Theorem B.1. Proposition 1 shows that we can rewrite (B.1) in a non-recursive form as

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

where $E_t^{(u,s,y)}$ is the $\mathbb{Q}$-expectation computed under the initial condition $v_{t-} = u$, $S_{t-} = s$, and $Y_{t-} = y$. So it remains to show that W_A given as (B.2) is the unique classical solution to (3.4) – (3.7). We prove this result based on the stochastic representation result for nonlocal PDE, i.e. Corollary 3.1 in Dai, Kou, and Yang (2017), and in the following we first establish a connection between this theorem and (1).

We first transform S_t to a process $X_t \in [0,1]$:

$$X_t = \Gamma(v_t, S_t) = \frac{S - H_d(v_t)}{H_u(v_t) - H_d(v_t)}.$$

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

For X, the lower and upper limit becomes 0 and 1, respectively. X can be interpreted as the relative distance of S to the lower limit H_d in $[H_d(t), H_u(t)]$. Under this transform, by Ito's formula, we have

$$dX_s = b(v_s, X_s)ds + \sigma(v_s, X_s)d\mathcal{B}_s,$$

where

$$\begin{aligned} b(v,x) &= r(x-1) - \frac{\alpha}{1+\alpha}\frac{R}{H_u(t)-H_d(t)} + \frac{rH_u(t)}{H_u(t)-H_d(t)}, \\ \sigma(v,x) &= \frac{\sigma H_d(t)}{H_u(t)-H_d(t)}. \end{aligned}$$

Besides, after this transform, the definition τ_i, η_i and ζ_i becomes

$$\tau_i = \inf\{s > \tau_{i-1} : X_{s-} \geq 1\}, \eta_i = \inf\{s > \eta_{i-1} : X_{s-} \leq 0\}$$

$$\zeta_i = \inf\{s > \zeta_{i-1} : v_{s-} = T, X_{s-} \in (0,1)\}.$$

On these dates, the change of X is described as

$$X_{\zeta_i} = X_{\zeta_i -}, X_{\tau_i} = X_{\eta_i} = \frac{1-H_d(0)}{H_u(0)-H_d(0)},$$

and on η_i, we have

$$Y_{\eta_i} = \mathcal{H}_d Y_{\eta_i -},$$

due to the reduction in the number of shares.

Now denote $\mathcal{O} = (0,1)$,

$$\begin{aligned} g(x) &= \frac{1-H_d(0)}{H_u(0)-H_d(0)} \cdot \mathbf{1}_{x=0,1}(x) \\ \tilde{\nu}_{t,x} &= \delta_{0,g(x)}(ds, dz) \\ \bar{\nu}(t,x) &= \mathcal{H}_d \cdot \mathbf{1}_{x=0}(x) + 1_{0<x\leq 1}(x) \\ \theta_i &= \inf\{s > \theta_{i-1} : X_{s-} = 0 \text{ or } X_{s-} = 1 \text{ or } v_{s-} = T\} \\ x &= \Gamma(t,S) \\ \tilde{W}_A(t,x) &= W_A(t,S). \end{aligned}$$

Also, the payouts of Class A coins at regular payout or reset dates can be expressed as $\tilde{h}(v_{\theta_i-}, X_{\theta_i-}, \bar{\nu}(X_{\theta_i-}))$, where $\tilde{h}(v, x, u) = 1 - u + Rv$. Using the above definitions, W_A defined in (B.2) can be expressed as

$$\tilde{W}_A(t,x) = E_t^x \left[\sum_{\theta_i \geq t} e^{-r(\theta_i - t)} Y_{\theta_i-} \tilde{h}(v_{\theta_i-}, X_{\theta_i-}, \bar{\nu}(X_{\theta_i-})) \right].$$

where E_t^x means the expectation calculated under $X_{t-} = x$, $v_{t-} = t$ and $Y_{t-} = 1$. Then, Corollary 3.1 in Dai, Kou, and Yang (2017) shows that $\tilde{W}_A$ is the unique classic solution to

$$-\frac{\partial \tilde{W}_A}{\partial t} - \frac{1}{2}\sigma^2(t,x)\frac{\partial^2 \tilde{W}_A}{\partial x^2} - b(t,x)\frac{\partial \tilde{W}_A}{\partial x} = 0 \qquad \text{in } [0,T) \times (0,1) \tag{B.8}$$

$$\tilde{W}_A(T,x) = RT + \tilde{W}_A(0, g(x)) \qquad \text{in } (0,1) \tag{B.9}$$

$$\tilde{W}_A(t,0) = 1 - \bar{\nu}(0) + Rt + \bar{\nu}(0)\tilde{W}_A(0, g(0)) \qquad \text{on } [0,T] \tag{B.10}$$

$$\tilde{W}_A(t,1) = Rt + \tilde{W}_A(0, g(1)) \qquad \text{on } [0,T]. \tag{B.11}$$

By reverting the transform $(t,s) \mapsto (t,x) = \left(t, \frac{s - H_d(t)}{H_u(t) - H_d(t)}\right)$, we conclude that W_A defined in (B.1) is the unique classical solution to (3.4) – (3.7). □

C Numerical Procedure for the Pricing Equation

We propose an iterative algorithm to obtain a numerical solution of the periodic parabolic terminal-boundary value problem (3.4) – (3.7).

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

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

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.

The following theorem ensures the convergence of Algorithm 1.

Theorem C.1. *The sequence $(W_A^{(k)})_{k\ge1}$ defined in Algorithm 1 is monotonically increasing, and it converges to W_A uniformly.*

Proof of Theorem C.1. We follow the notations in Section B. From the proof of Theorem B.1, it suffices to consider the sequence $(\tilde{W}_A^{(k)})$ defined via the transformed equation (B.8) – (B.11) by iteration with $\tilde{W}_A^{(0)} = 0$. Indeed, once we show that $(\tilde{W}_A^{(k)})$ converges uniformly to $\tilde{W}_A$, by reverting the transform $(t, s) \mapsto (t, x) = \left(t, \frac{s-H_d(t)}{H_u(t)-H_d(t)}\right)$, we have that $(W_A^{(k)})$ also converges uniformly to W_A, which establishes the theorem. We shall do it in the following two steps.

Step I. First, we show that the solution $\tilde{W}_A^{(k)}(t, x)$ can be stochastically represented as

$$\tilde{W}_A^{(k)}(t, x) = E_t^x \left[\sum_{t\le\theta_i\le\theta_k} e^{-r(\theta_i - t)} Y_{\theta_i -} \tilde{h}(v_{\theta_i -}, X_{\theta_i -}, \bar{\nu}(X_{\theta_i -})) \right].$$

Indeed, for $k = 1$, by Feynman-Kac representation for diffusion processes, the equation

$$\begin{aligned}
-\frac{\partial \tilde{W}_A}{\partial t} =& \frac{1}{2}\sigma^2(t, x)\frac{\partial^2 \tilde{W}_A}{\partial x^2} + b(t, x)\frac{\partial \tilde{W}_A}{\partial x} - r\tilde{W}_A && 0 \le t < T, 0 < x < 1 \\
\tilde{W}_A(T, x) =& RT && 0 < x < 1 \\
\tilde{W}_A(t, 1) =& Rt && 0 \le t \le T \\
\tilde{W}_A(t, 0) =& Rt + 1 - \mathcal{H}_d && 0 \le t \le T.
\end{aligned}$$

has a unique classical solution $\tilde{W}_A^{(1)} \in C^{1,2}(Q) \cap C(\overline{Q} \backslash D)$, which can be represented as

$$\tilde{W}_A^{(1)}(t,x) = E_t^x \left[e^{-r(\theta_1 - t)} Y_{\theta_1 -} \tilde{h}(v_{\theta_1 -}, X_{\theta_1 -}, \bar{\nu}(X_{\theta_1 -})) \right].$$

This establishes the claim for $k = 1$. Now assume that this claim has been established for $k = i$, $i > 1$. Then we have

$$\begin{aligned}
&E_t^x \left[\sum_{t \le \theta_j \le \theta_{i+1}} e^{-r(\theta_j - t)} Y_{\theta_j -} \tilde{h}(v_{\theta_j -}, X_{\theta_j -}, \bar{\nu}(X_{\theta_j -})) \right] \\
&= E_t^x \left[e^{-r(\theta_1 - t)} Y_{\theta_1 -} \tilde{h}(v_{\theta_1 -}, X_{\theta_1 -}, \bar{\nu}(X_{\theta_1 -})) \right] \\
&\quad + E_t^x \left[e^{-r(\theta_1 - t)} E_{\theta_1}^{v_{\theta_1}, X_{\theta_1}, Y_{\theta_1}} \left[\sum_{\theta_1 < \theta_j \le \theta_{i+1}} e^{-r(\theta_j - \theta_1)} Y_{\theta_j -} \tilde{h}(v_{\theta_j -}, X_{\theta_j -}, \bar{\nu}(X_{\theta_j -})) \right] \right] \\
&= E_t^x \left[e^{-r(\theta_1 - t)} Y_{\theta_1 -} \tilde{h}(v_{\theta_1 -}, X_{\theta_1 -}, \bar{\nu}(X_{\theta_1 -})) + e^{-r(\theta_1 - t)} Y_{\theta_1} \tilde{W}_A^{(i)}(v_{\theta_1}, X_{\theta_1}) \right],
\end{aligned}$$

where the last equality is from the Markov property and time-homogeneity of (v, X, Y). On the other hand, from the Feynman-Kac representation, the equation

$$\begin{aligned}
-\frac{\partial \tilde{W}_A}{\partial t} =& \frac{1}{2}\sigma^2(t,x) \frac{\partial^2 \tilde{W}_A}{\partial x^2} + b(t,x) \frac{\partial \tilde{W}_A}{\partial x} - r\tilde{W}_A && 0 \le t < T, 0 < x < 1 \\
\tilde{W}_A(T,x) =& RT + \tilde{W}_A^{(i)}(0, g(x)) && 0 < x < 1 \\
\tilde{W}_A(t,1) =& Rt + \tilde{W}_A^{(i)}(0, g(1)) && 0 \le t \le T \\
\tilde{W}_A(t,0) =& Rt + 1 - \mathcal{H}_d + \mathcal{H}_d \tilde{W}_A^{(i)}(0, g(0)) && 0 \le t \le T.
\end{aligned}$$

has a unique classical solution, $\tilde{W}_A^{(i+1)}$, which can be represented as

$$\begin{aligned}
\tilde{W}_A^{(i+1)}(t,x) = E_t^x \Big[& e^{-r(\theta_1 - t)} Y_{\theta_1 -} \tilde{h}(v_{\theta_1 -}, X_{\theta_1 -}, \bar{\nu}(X_{\theta_1 -})) \\
& + e^{-r(\theta_1 - t)} Y_{\theta_1} \tilde{W}_A^{(i)}(v_{\theta_1}, X_{\theta_1}) \Big].
\end{aligned}$$

Therefore,

$$\tilde{W}_A^{(i+1)}(t,x) = E_t^x \left[\sum_{t \le \theta_j \le \theta_{i+1}} e^{-r(\theta_j - t)} Y_{\theta_j -} \tilde{h}(v_{\theta_j -}, X_{\theta_j -}, \bar{\nu}(X_{\theta_j -})) \right],$$

and the claim is proved by induction.

Step II. Next we prove the uniform convergence of $(\tilde{W}_A^{(k)})$ to $\tilde{W}_A$. To see this,

$$
\begin{aligned}
&|\tilde{W}_A^{(k)}(t,x) - \tilde{W}_A(t,x)| \\
&= \left| E_t^x \left[e^{-r(\theta_k - t)} \sum_{\theta_j > \theta_k} e^{-r(\theta_j - \theta_k)} Y_{\theta_j -} \tilde{h}(v_{\theta_j -}, X_{\theta_j -}, \bar{\nu}(X_{\theta_j -})) \right] \right| \\
&\leq \bar{K} \cdot \sup_{(t,x) \in [0,T) \times (0,1)} E_t^x \left[e^{-r(\theta_k - t)} \right],
\end{aligned}
$$

where $\bar{K}$ is as defined in the proof of Proposition 1.

We claim that the right hand side converges to 0. Suppose this claim is proved, we then have the uniform convergence of $(\tilde{W}_A^{(k)})$ in $[0,T) \times (0,1)$. Using the terminal and boundary conditions of the equation for $\tilde{W}_A^{(k)}$, $(\tilde{W}_A^{(k)})$ also converges uniformly on $[0,T] \times [0,1]$.

To verify the claim, it suffices to note that (1) for two consecutive regular payouts ζ_i, ζ_{i+1}, we have $\zeta_{i+1} - \zeta_i \geq T$, therefore $E_t^x \left[e^{-r(\zeta_{i+1} - \zeta_i)} \right] \leq e^{-rT} := K_1 < 1$; (2) for two consecutive upward resets τ_i, τ_{i+1}, we have $E_t^x \left[e^{-r(\tau_{i+1} - \tau_i)} \right] = E_0^{g(1)} \left[e^{-r\tau_1} \right] := K_2 < 1$; (3) for two consecutive downward resets η_i, η_{i+1}, we have $E_t^x \left[e^{-r(\eta_{i+1} - \eta_i)} \right] = E_0^{g(0)} \left[e^{-r\eta_1} \right] := K_3 < 1$. Consequently, for $k \geq 1$, we have

$$
E_t^x \left[e^{-r(\theta_{3k+3} - \theta_{3k})} \right] \leq K_1 \wedge K_2 \wedge K_3 < 1,
$$

since there must be two consecutive regular payouts, upward resets or downward resets in $\theta_{3k}, \ldots, \theta_{3k+3}$. Therefore,

$$
\sup_{(t,x) \in [0,T) \times (0,1)} E_t^x \left[e^{-r(\theta_{3k+3} - t)} \right] \leq e^{rt} \cdot (K_1 \wedge K_2 \wedge K_3)^k \to 0, \text{ as } k \to \infty,
$$

and the claim follows from the monotonicity of (θ_k). □

D 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 10 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 cryptocurrency, 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 coins, 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 coins as coupon, they have a relatively longer period of time to liquidate the coins 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 cryptocurrency, they can monitor the market actively and spot a good opportunity to liquidate the underlying cryptocurency.

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

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

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

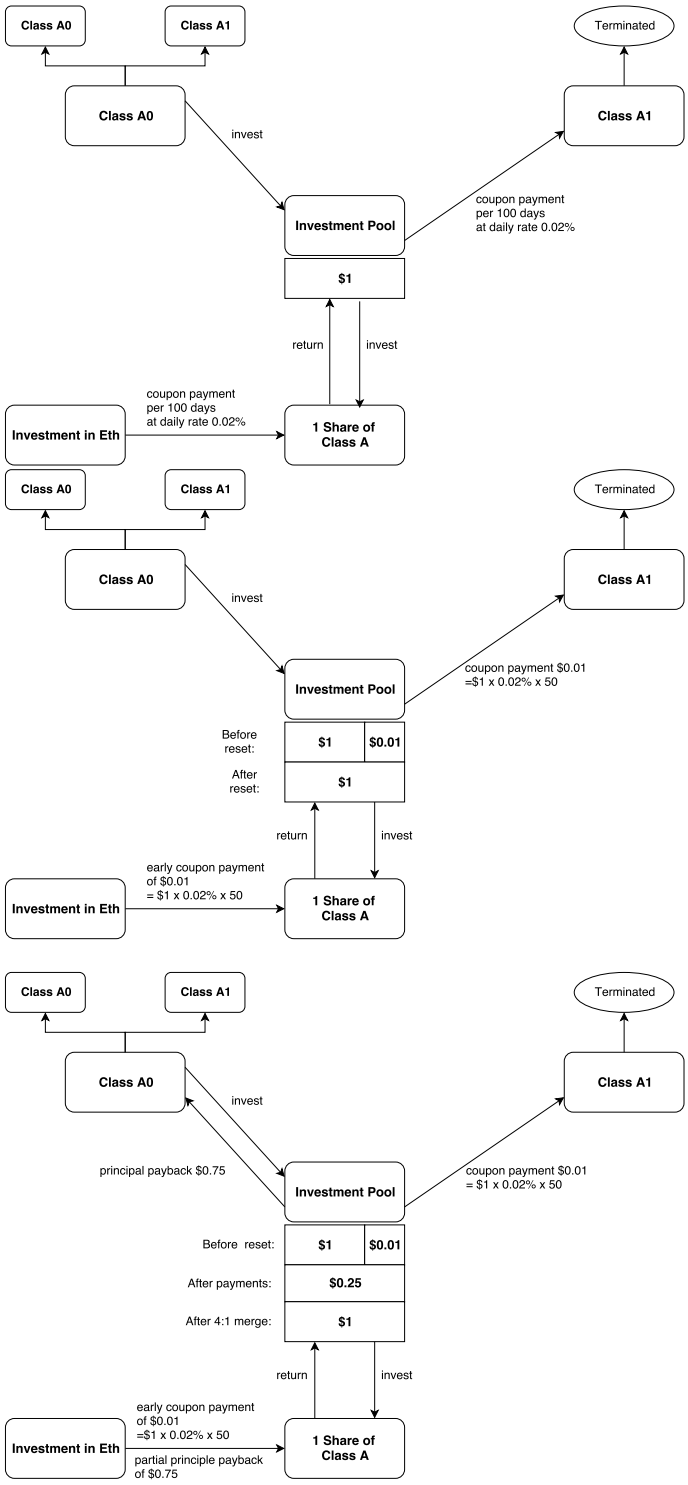

Figure 10: **Top Figure:** Class A0 receives no coupon. Class A1 receives all the coupon payment. After the coupon payment, Class A1 is terminated, and 1 Class A0 is split into 1 new Class A0 and Class A1. **Middle Figure:** Upward Reset of Class A0. After 50 days, Class B's net asset value grows to $2, triggering an upward reset. **Bottom Figure:** After another 50 days, Class B's net asset value drops to $0.25, triggering a downward reset.

the following PDE

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

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

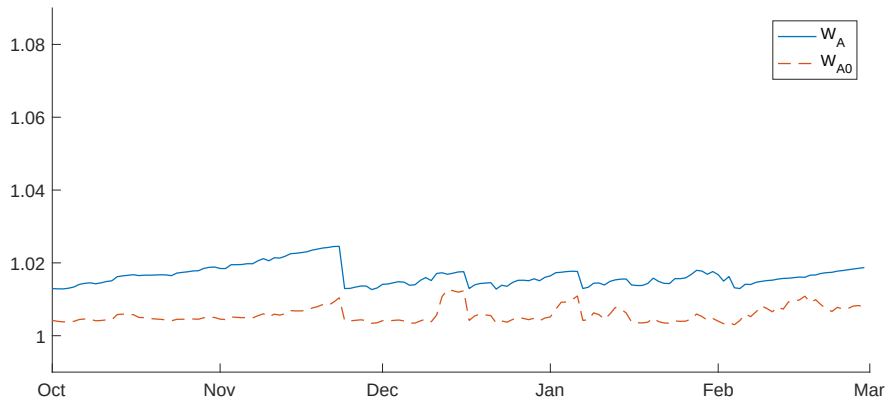

Figure 11: Market Value of Class A0 compared to Class A. Annualized volatility of Class A0 is 0.0254. Parameters: $R = 0.02\%, \mathcal{H}_d = 0.25, \mathcal{H}_u = 2, T = 100, \sigma = 120\%$ per year, $r = 0.0082\%$ (3% per year). Upward reset takes place on 24 Nov 2017, 17 Dec 2017, and 7 Jan 2018. Downward reset takes place on 5 Feb 2018.

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 0.0412 for $\alpha = 1$, as compared to that of W_A, which is 0.0531. 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 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 that of W_A, which is 0.0571. Note that with $\alpha = 2$, the net asset value of B is $3S_t - 2(1 + Rv_t)$, making B more sensitive to S.

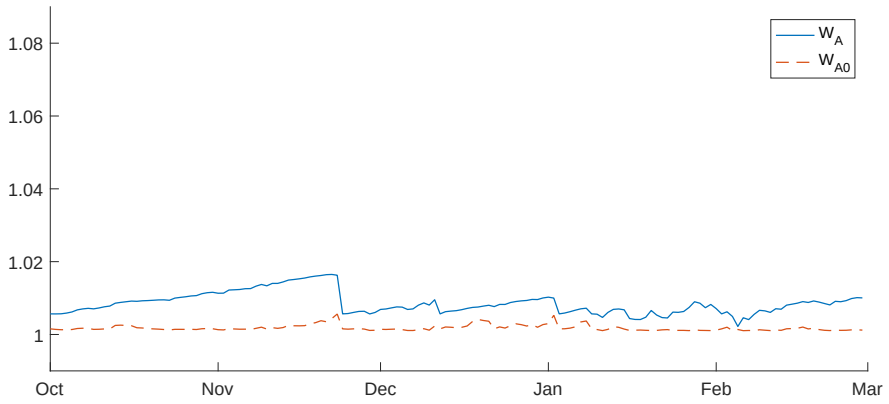

Figure 12: Market Value of Class A0 (principal only class) compared to Class A, where the split ratio between Class A and B coins is 2:1. Annualized volatility of Class A is 0.0125. Parameters: $R = 0.02$ per day, $\mathcal{H}_d = 0.25$, $\mathcal{H}_u = 2$, $T = 100$, $\sigma = 120\%$ per year, $r =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