EasyChair Preprint

№ 1188

What is Stablecoin?: A Survey on Price Stabilization Mechanisms for Decentralized Payment Systems

Makiko Mita, Kensuke Ito, Shohei Ohsawa and Hideyuki Tanaka

EasyChair preprints are intended for rapid dissemination of research results and are integrated with the rest of EasyChair.

June 14, 2019

What is Stablecoin?: A Survey on Price Stabilization Mechanisms for Decentralized Payment Systems

Makiko Mita
Daisy, inc.
Tokyo, Japan
mm@daisy.id

Kensuke Ito
the Graduate School of Interdisciplinary Information Studies
The University of Tokyo
Tokyo, Japan
k-ito@g.ecc.u-tokyo.ac.jp

Shohei Ohsawa
Daisy, inc.
Tokyo, Japan
o@daisy.id

Hideyuki Tanaka
the Interfaculty Initiative in Information Studies and the Graduate School of Interdisciplinary Information Studies
The University of Tokyo
Tokyo, Japan
tanaka@iii.u-tokyo.ac.jp

***Abstract*— Since the first theoretical concept of blockchains was proposed, over 100 digital currencies have been issued by online platformers as cryptocurrencies and traded by online consumers mainly in emerging countries. From the perspective of online payment systems, several studies have regarded blockchains as *decentralized payment systems (DPSs)*, enabling international payment with lower cost and higher traceability with sophisticated peer-to-peer protocols in contrast to other centralized systems. Despite the advantages, DPSs are not chosen by the owners of online shops due to the high volatility of cryptocurrency prices. *Stablecoins* are cryptocurrencies with price stabilization mechanisms to match the price of another currency with lower volatility. Our motivation is to gather various price stabilization mechanisms for the purpose of comparing them from the perspective of implementation and enterprise usage. After dividing the methods into four collateral types (fiat, crypto, commodity, and non-collateralized) and two layers (protocol and application), we show that non-collateralized stablecoin on the application layer is the simplest approach for implementation. Moreover, we discuss their connection with traditional economic studies on Hayek money, Seigniorage Share, and Tobin tax. Some current stablecoin projects are also discussed and compared. This is the first survey of stablecoins to the best of our knowledge.**

Keywords—stablecoin, payment systems, Hayek money, Tobin tax, Seigniorage Share

I. INTRODUCTION

Since the first theoretical concept of blockchains was proposed in 2008, over 100 digital currencies have been issued by online platformers as cryptocurrencies and traded by online consumers. After hitting a high of almost 20,000 dollars[1] for one bitcoin in December 2017, the total market capitalization of cryptocurrencies reached 796 billion dollars[2] the following month. According to the world ranking of companies by market capitalization at that time, cryptocurrencies' market scale would be listed in second place, right after Apple Inc.'s 911 billion dollars[3].

From the perspective of online payment systems, several studies have regarded blockchains as *decentralized payment systems (DPSs)* [16, 19]. DPSs studies are focused because not only is it easy to pay and remit overseas at lower cost, but DPSs also have the possibility to trace all transactions so that monetary policy is carried out in an algorithmic, automatic, and non-discretionary way.

Despite the advantages, most online payment systems have not employed a cryptocurrency as an alternative to a fiat currency. In fact, in eight of the largest cryptocurrency markets (US, UK, Germany, Brazil, Japan, South Korea, China and India), current awareness of cryptocurrency is 74% on average, while its ownership is on average 7%. Most of the owners of online shops do not choose DPSs due to the high price volatility of cryptocurrency.

Stablecoin is proposed to introduce a stabilization mechanism by controlling the exchange rate between cryptocurrency and fiat currency. In fact, several platformers have implemented stabilization mechanisms by issuing stablecoins. According to Hassani et al. [5] who investigate blockchain from the banker's perspective, stablecoin is defined as "*basically a digital token that will have low price volatility as a result of being pegged to some underlying fiat currency, thereby acting as a store of value, a medium of exchange and unit of accounting for blockchain payments."* The "stable" in "stablecoin" is surely about price volatility; however, it is too narrow to define it as "a result of being pegged to some underlying fiat currency." Hassani et al. [5] premise stablecoins

Acknowledgments: We would like to express our gratitude to B Cryptos for providing valuable comments and financial support.

[1] CoinMarketCap "Bitcoin Charts" as of March 20, 2019
https://coinmarketcap.com/currencies/bitcoin/

[2] CoinMarketCap "Global Charts" as of March 20, 2019
Market capitalization is calculated by multiplying the market price per coin by the total amount of coins in circulation.
https://coinmarketcap.com/charts/

[3] Banks around the World "The World's Top 50 Companies"
Market capitalization ranking as of January 17, 2018
https://www.relbanks.com/rankings/worlds-largest-companies

are pegged to a fiat currency; however, it is possible for stablecoins not to peg to a fiat currency.

Our motivation is to gather together various price stabilization mechanisms and compare them from the perspective of implementation and enterprise usage. First, we divide stablecoins into four collateral types—fiat, crypto, commodity, and non-collateralized—according to the literature of Zhang et al. [20] and conclude that the non-collateralized stablecoin is the only way for a stabilized price, decentralization, and nondiscretionary digital currency. Second, we divide non-collateralized stablecoins into two layers (protocol and application) and show that non-collateralized stablecoins on the application layer is the simplest approach for implementation. Moreover, we discuss their connection with traditional economic studies on Hayek money, Seigniorage Share, and Tobin tax (exchange stabilization has been discussed in economics for a long time). Some current stablecoin projects are also discussed and compared in one table. To this end, we demonstrate the following finding:

All stablecoins are not stable in purchasing power.

This paper is organized as follows. In Section II, we review the preliminaries for monetary stabilization in traditional economics (Quantity Theory of Money, Tobin tax, and speculative attack) and show stablecoins with four collateral types (fiat, crypto, commodity, and non-collateralized). In Section III, we survey non-collateralized mechanisms from two technical layers (protocol and application) and show theories and implementation examples for each layer. In conclusion, we summarize the meaning of this paper and state challenges for the future. This is the first survey of stablecoins to the best of our knowledge.

II. PRELIMINARY

We first demonstrate the issue of monetary stabilization in traditional economics, Quantity Theory of Money, Tobin tax, and speculative attack, and show stablecoins with collaterals. This section shows that non-collateral stablecoin is the best way for implementation.

Quantity Theory of Money is a basic concept to control money supply. Tobin tax is a mechanism to stabilize exchanging currencies especially on international financial transactions and applied to cryptocurrency stabilization. Speculative attack is a risk to the fixed exchange rate and a potential risk to any collateralized stablecoin.

A. Quantity Theory of Money

Cryptocurrencies are digital currencies that are traceable for all transactions; that is, we can grasp their amount, velocity of circulation, and other indicators not observable in the current fiat currencies. To control the money supply and stabilize the price of stablecoins, we refer to a prerequisite theory: the Quantity Theory of Money (QTM). QTM (also known as the Equation of Exchange) was originally formulated by the economist Irving Fisher in 1911 [4] as follows:

$$M\,V = P\,Q,$$

where M is the money supply (demand side), V is the velocity of money (demand side), P is the price per unit (supply side), and Q is the quantity produced (supply side).

This theory helps us understand how money moves and how to adjust the money supply. Some (non-collateralized) stablecoins, such as Basis and USDX[4] (details are explained in Subsection III.B) are theoretically based on the Quantity Theory of Money. To design an automatic mechanism to control money supply, it is necessary to stabilize the stablecoin price.

B. Tobin Tax

Tobin tax is a mechanism to stabilize exchanging currencies proposed by James Tobin in 1972 [18]. The Tobin tax concept to "throw some sand in the wheels of speculation" is one of the traditional methods for monetary stabilization proposed before blockchains [18]. It proposes a tax on international financial transactions to control exchange rate volatility. We introduce this traditional stabilization idea of currencies into stablecoin.

McCulloch and Pacillo [8] survey Tobin tax and focus on controlling volatility by imposing a low tax (e.g., 0.2%) on financial transactions. McCulloch and Pacillo [8] conclude that "a Tobin tax is feasible and, if appropriately designed, could make a significant contribution to revenue without causing major distortions." We can set a transaction fee for exchanging stablecoins, like the Tobin tax, for exchanging currencies and to control the volatility of cryptocurrency price, or exchange rate volatility, with fiat currencies. Setting a transaction fee is feasible and it also becomes a good revenue stream for issuers. A transaction fee seems a good approach for stablecoins.

However, Spahn [15] points out that it is "virtually impossible to distinguish between normal liquidity trading and speculative "noise" trading." Spahn [15] expands the Tobin tax to "a two-tier rate structure consisting of a low-rate financial transactions tax, plus an exchange surcharge at prohibitive rates as a piggyback. The latter would be dormant in times of normal financial activities and be activated only in the case of speculative attacks" (Spahn tax) [15]. Spahn [15] prepares a high transaction tax for speculative attacks, which we discuss in the next section as a potential risk to any collateralized stablecoin.

Liuzzi et al. [6] analyze the optimal level of Tobin tax in an artificial market. Liuzzi et al. [6] explain that "depending on the liquidity of the market, two possible regimes of optimal taxation emerge: a non-negligible level of taxation for highly liquid markets and low (close to zero) levels of taxation for low liquidity markets. This outcome resembles the two-tier rate structure discussed by Spahn in his famous contributions." To set an optimal transaction fee for keeping a low volatility, we also need to simulate with an artificial market or start with a small market as an experiment. We should avoid too high

[4] Note that, even though the description uses the project name USDX for the sake of convenience, USDX project especially refers to its stablecoin as USDY.

TABLE I. CHARACTERISTICS OF THE FOUR COLLATERALIZED PATTERNS OF STABLECOINS

Collateralized by	Decentralized	Dual Stability (less-volatile collaterals)
Fiat currency** (e.g., USD)	—	✓
Cryptocurrency (e.g., BTC)	✓	—
Commodity** (e.g., gold)	—	✓
None (mentioned in § III)	✓	✓*

* Non-collateralized stablecoin is dual stable because it is not affected by the price of collaterals.

**Fiat-collateralized and commodity-collateralized have the same characteristics in this table. However, they are different in the issue limit. Fiat currencies do not have an issue limit under the managed currency system. On the other hand, commodities such as gold and petroleum are finite resources and as such have an issue limit.

transaction fee, which impedes money circulation and expands the market scale of cryptocurrencies.

The Tobin tax mechanism suggests how to stabilize stablecoin prices by including transaction fees. We propose a different transaction fee mechanism to incentivize users to stabilize the stablecoin price. When users buy/sell a stablecoin, which makes the stablecoin price part from the other currencies such as the US dollars (USD), we propose a high transaction fee to disincentivize them from buying/selling it. On the other hand, when users buy/sell a stablecoin, which makes the stablecoin price constant to the other currencies such as the US dollars, then we propose a low transaction fee and the users are incentivized to buy/sell the stablecoin more.

C. Speculative Attack

There is a discussion about fixed exchange rates called "speculative attack," which is a potential risk to any collateralized stablecoin. Spahn [15] proposes the Spahn tax to prevent this financial attack (see previous section).

Diamond and Dybvig [3] formulate bank runs in terms of game theory. Diamond and Dybvig [3] address that a bank run can be a Nash equilibrium because when one depositor thinks that other depositors will withdraw their deposits even when they do not need to, the withdrawal makes one depositor's utility increase. To prevent bank runs, Diamond and Dybvig [3] insist on the importance of deposit insurance.

Obstfeld [10] adopts a game theory approach to fixed exchange rate currencies that depends on a reserve fund. Obstfeld [10] points out that to bring a fixed rate tumbling down by aggressive trading for speculation purpose, a speculative attack can be reasonable depending on the reserve rate.

Routledge and Zetlin-Jones [11] discuss collateralized stablecoin and "develop new theory of pegs with less than 100% backing," which is immune to speculative attacks. Their exchange rate adjustment mechanism can contribute to the over-collateralized problem in cryptocurrency-collateralized stablecoin.

Preventing a speculative attack is well studied as an incentive to break fixed exchange rate system. As long as stablecoin is designed to peg to something, it is exposed to the risk of speculative attacks.

D. Collateralized or Non-collaterized

Not only cryptocurrencies, but all currencies need to be trustworthy. We put value not on just a piece of paper or digital figures, but on what they can give us. People do not use a currency without trust. However, trustfulness does not always need collateral. Most of the modern paper currencies are fiat currencies. Fiat currencies were backed by gold until around the end of the 20th century, using the *gold standard system*. However, it was difficult to maintain the gold standard system following World War I when nations shifted to today's *managed currency system*. Fiat currencies are now backed by governments and issued by the central banks. When the government loses trust and people are afraid of risks like inflation, the currency price will go down. Stablecoins also have collateral patterns. In this paper, we organize the patterns of stablecoins and propose the best way to approach stablecoins.

We show the three categories of stablecoin by Zhang et al. [20] and one more category from Mancini-Griffoli et al. [7], and compare each method and, consequently, show that non-collateral coins are the best way for stabilization. We divide each collateralized pattern in Table I by two perspectives: whether it is centralized or decentralized, and *dual stability* (i.e. whether it uses less-volatile collaterals or not). Since non-collateralized stablecoins are decentralized and dual stable, it has the most advantage in realizing decentralized stablecoins.

The first type of stablecoins uses fiat money as collateral [20]. Zhang et al. [20] point out that the "major problem with this form of stablecoins is that it requires some central organization to process all transactions, which is against the principle of decentralization." The fiat-collateralized pattern is not decentralized, which is exactly our critical reason to exclude fiat-collateralized stablecoins from the ideal alternative to fiat currency. We can add the other perspective to this centralized problem. The issuer must prepare the same amount of fiat currency as their stablecoin to ensure their stablecoin is pegged and changeable to the fiat currency, whenever. The greater their stablecoin's economy of scale, the more the issuer must reserve fiat currency unless their users accept partial reservation like legal reserves. This acceptance is possible when the issuer itself is trustful enough, like a central bank. However, fiat-collateralized cryptocurrency cannot part ways with centralization, which is the first and decisive problem.

The second type of stablecoin uses cryptocurrency as collateral [20]. Zhang et al. [20] continue to point out the problem of this second type: "However, due to the fact that cryptocurrencies are volatile, this type of stablecoins is often "overcollateralized." [20] To avoid cryptocurrency fluctuation, the ratio of the stablecoin to the collateral cryptocurrency becomes low [20]. We explain the problem of crypto-collateralized stablecoins from another perspective. The prices of cryptocurrencies fluctuate almost in the same way with each

other[5] compared with the other markets. The main purpose of stablecoin is to stabilize the price [5, 20]; however, cryptocurrencies are too volatile to peg to.

The third type of stablecoin uses a commodity, such as gold or oil, as collateral. Zhang et al. [20] do not refer to this third type of stablecoins. Mancini-Griffoli et al. [7] introduce the "petro" as a commodity-collateralized cryptocurrency. The petro, or petromoneda, was issued by the Venezuelan government in 2018 and collateralized by its oil. This type of stablecoin is not discussed a lot because commodities like gold or petroleum are reserved by the issuers, which is theoretically the same as fiat-collateralized. Commodity-collateralized stablecoin is also not decentralized[6].

The fourth type of stablecoins is "the non-collateralized stablecoins. These stablecoins would remain in the long term a stable value as their algorithms are designed to adjust the supply based on the price, according to theories in monetary economics" [20]. Non-collateralized stablecoins do not need any collateral and their money supply is controlled automatically.

In this section, we reviewed four types of stablecoins. Fiat-collateralized stablecoins is easy to implement, be understood, and be trusted, which results in a lot of approaches and practices of it. As we saw in the paper by Hassani et al. [5], there are cases where stablecoin is defined as "being pegged to some underlying fiat currency." However, the goal of cryptocurrency is to achieve a decentralized intermediary that can be adjusted in an automatic and non-discretionary way. As we pointed out, (1) fiat-collateralized stablecoins are centralized and never decentralized; (2) crypto-collateralized stablecoins are exposed to high price fluctuations of the pegged cryptocurrencies, causing them to be over-collateralized; (3) commodity-collateralized stablecoins are centralized and never decentralized; and (4) non-collateralized stablecoins that have nothing to peg to but have an automatic price stable mechanisms are the only way to establish price stable decentralized cryptocurrencies.

The following section surveys non-collateralized stablecoins. This is meaningful because non-collateralized stablecoins have the greatest potential to achieve a stable price and decentralized cryptocurrency, and few papers have focused on non-collateralized stablecoin.

III. Non-Collateralized Mechanisms: A Survey

This section surveys non-collateralized stablecoins. In general, cryptocurrencies have mainly two layers to their approach: a protocol layer and an application layer. The protocol layer is technically located on a more fundamental layer than the application layer, similar to a PC's operating system. A protocol is a rule to operate a cryptocurrency system and the system must obey the protocol rule. For example, the bitcoin protocol has a rule like "maximum block size is 1 MB." It is possible to change the protocols of cryptocurrencies but the difficulties of

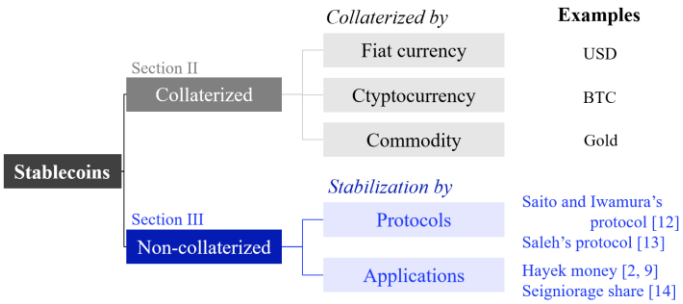

FIGURE I. STABLECOIN CATEGORY TREE

intervening in protocol layers depend on the cryptocurrencies. For example, changing the bitcoin protocol is difficult because it needs most users' agreement. Approaches to protocol layer is categorized into non-collateralized stablecoin from the viewpoint of collateral. The application layer resides in a shallower layer, like applications installed on a PC's operating system. Changing applications is easier than changing protocols. To stabilize the prices of cryptocurrencies, we have possibilities to intervene in the protocol and/or application layers.

The categorization tree are mapped into a tree structure as shown in Fig. I. We have categorized stablecoins into four collateral patterns—fiat, crypto, commodity, and non-collateralized—and divided technical approaches into two layers, application layer and protocol layer, under non-collateralized because it is the only approach to realize a decentralized intermediary that is adjusted in an automatic and non-discretionary way. We surveyed the protocol layer in subsection A and application layer in subsection B, each from the perspective of theory and implementation.

A. Stabilization by Protocols

We will mention two studies and one practical example. Saito and Iwamura [12] and Saleh [13] discuss an update on bitcoin, and Tiutiun et al. [17] show an the implementation example, USDX project, from a stablecoin perspective.

1) Theory

First, Saito and Iwamura [12] propose changes to the protocol layer of blockchain currencies to stabilize their market prices automatically. In their past work, Saito and Iwamura [12] reasoned "that the cause of instability of BTC[7] price is that supply of coins does not respond to demand shocks." Saito and Iwamura [12] suggest an automatic adjustment of BTC supply which responds to the demand. Their proposal involves three changes to the design of blockchain currencies. The first change is limiting the re-adjustment of proof-of-work (PoW) targets[8] only when the block interval exceeds a certain threshold value in order to increase BTC supply when the demand increases. The second change is making mining rewards variable according to the observed over-threshold changes of block intervals instead of the halving rule[9]. The third change is a negative interest as a

[5] CoinMarketCap "Top 100 Cryptocurrencies by Market Capitalization" as of April 8, 2019https://coinmarketcap.com/

[6] There are mix types of four collateralized types such as partially fiat-collateralized stablecoins.

[7] BTC is a currency unit of bitcoin.

[8] Proof-of-work targets are also called difficulty target. The target is about a speed at which new blocks are generated by the network.

[9] Halving rule is that block rewards for mining are cut in half at regular intervals based on the bitcoin protocol.

depreciation rule so that the effective values of coins are depreciated as time elapses. The first change aims to stabilize the price to use, the second change sustains the currency systems by making rewards to miners perpetual, and the third change avoids hoarding coins and incentivizes users to use coins for payment. Saito and Iwamura [12] propose these changes to make a sustainable and actively used currency. However, an automatic adjustment of BTC supply does not maintain users' constant purchasing power ($P \cdot Q$).

Second, Saleh [13] analyzes the characteristics of PoW using the overlapping generations model of economics. Saleh [13] suggests that "PoW induces exceptional volatility and impairs aggregate welfare" and examines an alternative mechanism, the Proof-of-Burn (PoB)[10]. Saleh [13] says that PoB generates blocks not by spending computing resources but by deleting coins, and contributes more price stability and welfare improvement.

These two papers focus on the protocol layer of BTC to propose solutions for improving stability. BTC was originally designed to be supplied based only on its demand. The original protocol does not include any adjustment system to maintain market price stability. These two proposals intend to modify the original protocol of BTC to make it more stable. Implementation

Tiutiun et al. [17] propose a non-collateralized stablecoin named "USDX," which is designed from the protocol layer. They adjust the USDX price through three mechanisms. The first mechanism is the *variable block reward*, which decides mining rewards according to the USDX market price. They decide the rewards according to the price of USDX/USD. The price index USDX/USD is monitored and provided by Oracle. For example, during the *Rising stage*, Oracle monitors that USDX/USD > 1 "and shows a rising trend, implying that the Stablecoin is in short supply. Therefore, the block reward needs to be increased to expand USDX's supply. Then, the block reward is increased" [17]. On the other hand, during the *Decline stage*, Oracle monitors that USDX/USD < 1 "and presents a decreasing trend, implying USDX's supply exceeds demand, so it is necessary to reduce the block reward to reduce Stablecoin's supply. In this case, the block reward is reduced" [17]. The second mechanism is *lock-in mining*. This mechanism is only activated when USDX/USD < 1 and the variable block reward of mechanism 1 has been reduced to the lowest value, but the decline of USDX/USD has not slowed down. Users can choose to participate in the "lock-in mining" and once the mechanism is activated to reduce money supply M (QTM is explained in Subsection II.A) in order to rise USDX/USD, participants' coins are locked and not circulated. Money supply M on the market is reduced by a longer locked period. This mechanism adopts Proof-of-Stake (PoS)[11] in which stablecoins' stake lock period is set to change based upon market price. The third mechanism is the *variable transaction fee*. As discussed in Section 1 (Preliminary) about Tobin tax, transaction fees can influence users' action. Transaction fee changes are based on market prices. For example, when USDX/USD ≤ 1, the transaction fee rises and the velocity of money V and the total amount of USDX in circulation M decrease, which adjusts the USDX/USD closer to 1. The third mechanism might be different from the other two from the viewpoint of purchasing power. The first and second mechanisms do not affect users' purchasing power because they impose duties only on miners. However, the third mechanism might affect users' purchasing power based on arguments regarding Tobin Tax and Hayek money that we mention later.

Saito and Iwamura [9], Saleh [13], and Tiutiun et al. [17] work on the protocol layer to create stable cryptocurrencies with different algorithms such as PoW, PoB, or PoS. However, their approaches do not keep users' purchasing power constant. Stablecoin's constant purchasing power cannot currently be brought by simple intervention in the protocol layer.

B. Stabilization by Applications

We will mention three studies as theories for application layer intervention: Hayek money, Seigniorage Share, and as an implementation example, the Basis project. We explain the importance of price stabilization; however, the real goal is stabilization of users' purchasing power. We use currencies as a medium of exchange for purchasing things such as eggs, vegetables, devices or other medium of exchange. The forcible stable price with one fiat currency may part with this real goal. Constant purchasing power is challenging and there is no implementation that achieves this.

1) Theory

1. Hayek Money

Ametrano [2] introduces "Hayek money" as a new concept of cryptocurrency to automatically stabilize prices by adopting elastic supply policy according to the demand. Hayek money rebases the amount of coin in each wallet by calculating the mean value of the USD/BTC exchange rate. However, the proposal by Ametrano [2] cannot guarantee to keep constant the purchasing power of users, even though it is designed to include stabilization mechanism. If purchasing power diminishes, then users buy fewer goods and services, affecting users severely.

Morini [9] proposes dividing wallets into two types, investment (Inv) and saving (Sav), to solve the purchasing power problem of the Hayek money. Morini [9] gives users "the freedom to choose how much they want to be affected by changes of money supply, by introducing two types of wallets: Inv wallets and Sav wallets." The users who want to take the risk and reward ("risk-bearing users"), will choose investment wallets while users that prefer stability and want to avoid the risk and reward ("risk-averse users") will choose saving wallets. The fluctuations of Inv wallets become large because Inv wallets absorb fluctuations of the Sav wallet. Morini [9] explains this asymmetry would be accepted by the users' discretionary choice of the ratio in the Inv/Sav wallets. However, if users can choose Inv/Sav wallets freely, then the Hayek money adjusts price by the rebasement of the amount of coin in the wallets and the rebasement happens every some time, rational owners of Inv wallets remove their coins from their Inv wallets between two rebasements. Morini [9] also explains this arbitrage would also

[10] The concept of PoB was introduced by Iain Stewart in 2012. https://bitcointalk.org/index.php?topic=131139.0%202

[11] The concept of PoS was first introduced in a paper by Sunny King and Scott Nadal in 2012. They intended to solve the problem of bitcoin mining's high energy consumption.

TABLE II. COMPARISON OF STABILIZATION MECHANISMS FOR NON-COLLATERIZED STABLECOINS.

	Implementation				Intervention				Issue Other Coins
	On-chain		Off-chain		*M*	*V*	*P*	*Q*	
Approaches	Protocol Layer	Application Layer	Wallet	Exchange					
Theory									
Hayek Money [2]	—	—	✓	—	✓	—	—	—	—
Hayek Coin (Sav/Inv) [9]	—	—	✓	—	✓	—	—	—	—
Seigniorage Share [14]	—	✓	—	—	✓	—	—	—	✓
Implementation									
USDX [17]	✓	—	—	—	✓	✓	—	—	—
Basis [1]	—	✓	—	—	✓	—	—	—	✓

be accepted. He insists the existence of risk-bearing investors in the real economy who will exist in the digital economy as well.

Hayek money's auto-rebasement of each wallet by the exchange rate suggests decentralized systematic supply policy to the arbitrary monetary policy by the central bank, and the Inv/Sav wallets approach adjusts users' acceptance of the coin volume fluctuations in their wallets.

2. Seigniorage Share

Sams [14] proposes a new supply adjustment model, named "Seigniorage Share." This proposal challenges users' discretional way to distribute their coins by Morini [9]. When the stablecoin price declines and coin supply needs to decrease, shares are issued and sold with stablecoin in the auction. Conversely, when the stablecoin price rises and coin supply needs to increase, stablecoins are issued and sold with shares in the auction. Sams [14] tries to solve purchasing power problem by the supply adjustment mechanism with users' spontaneous participations in auctions. Seigniorage Shares do not need collateralized assets and theoretically this scheme does not depend on fiat currency or cryptocurrency. However, selling shares when the stablecoin price declines premises users expect they will change their shares into stablecoin in the future, even though the price is falling at that time. There is no guarantee the price is set in the auctions.

Sams [14] introduces the Basis project as an experimental project, but it was closed in 2018 due to difficulties in its relationship with U.S. regulators regarding ICOs and issuing tokens and bonds, and a flaw in the Seigniorage Share's design, tautological scheme. Basis project is the only project which explains its seigniorage share mechanisms in detail as far as we searched.

2) Implementation

Sams [14] poses the Basis project as a real reference case. Basis implements price stability by using the Quantity Theory of Money and Seigniorage Share model. Al-Naji et al. [1] measure the price of Basis and adjust Basis supply accordingly.

Al-Naji et al. [1] define an index like the Consumer Price Index (CPI) to stabilize against fiat currencies and their blockchain system is designed in a decentralized way using the Basis–USD exchange rate via an Oracle system. To adjust the supply of Basis based on QTM, and expand and contract the money supply, Basis makes three classes of tokens based on the idea of Seigniorage Share. (1) Basis tokens (Basis): The core tokens of the system. They are pegged to a target asset or index to be used as a medium of exchange. Their supply is adjusted according to the deviations of the exchange rate in order to maintain the peg. (2) Bond tokens (bonds): These tokens are auctioned off by the blockchain when it needs to reduce Basis supply. Bonds are not pegged to anything and each bond promises exactly 1 Basis at some point in the future under certain conditions. Because newly created bonds are sold on open auction for prices of less than 1 Basis, users can expect to earn a competitive premium for their bond purchase. (3) Share tokens (share): These tokens are only supplied at the genesis of the blockchain. They are not pegged to anything and their value stems from their divided policy. When demand for Basis goes up and new Basis is issued to match demand, users who have shares receive these newly created Basis *pro rata*.

Basis projects are highly expected and raised 133 million dollars through their initial coin offering (ICO) because it is designed well, using fundamental economic theory, QTM, and a new supply adjustment model, the Seigniorage Share, but in vain. The Basis team announced the close of the project and suggested difficulties in the tautologic mechanism design. They write that having "fewer participants in the on-chain auctions adversely affects [sic] the stability of Basis, making Basis intrinsically less attractive to users. Additionally, imposing transfer restrictions on bond and share token auctions materially hurts our ability to build the Basis ecosystem" (Basis official announcement on December 13, 2018)[12]. Though the demand for share expects the future price rise (with the issue of stablecoin), the stablecoin price rise is achieved by the purchase, or demand of its share. Like this, the demand for shares is tautological. In addition, when we think of the process of auction, there is a possibility that the share price might not be set as a result of the auction. This abandonment of the most advanced non-stablecoin project is a distinct example of the Seigniorage Share problem.

Now, we compare approaches to stablecoins with the three items shown in Table II: (1) implementation object on-chain is protocol layer or application layer, and off-chain, wallet or exchange, (2) intervention object is *M*, *V*, *P*, and/or *Q* from QTM, and (3) whether other coins are issued or not.

[12] https://www.basis.io/

These approaches are mapped into a tree structure as shown in Fig. I. We have categorized stablecoins into four collateral patterns—fiat, crypto, commodity, and non-collateralized—and divided technical approaches into two layers, application layer and protocol layer, under non-collateralized because it is the only approach to realize a decentralized intermediary that is adjusted in an automatic and non-discretionary way.

IV. Conclusion

This study surveyed the literature of stablecoin, a cryptocurrency whose value aims to be pegged with a given underlying assets, by introducing some related concepts in economics.

To provide an overview, this study first classified stablecoins into four collateral (fiat, commodity, crypto, and non-collateralized) and pointed the advantage of non-collateralized stablecoin as summarized in Table I. Subsequent to the collateral-based classification, we further divided non-collateralized stablecoin into two types according to the intervention layer (protocol or application) as depicted in Fig. I, to cover more recent discussions. The investigation, which included academic papers [13, 12, 2, 9], indicates that the latest implementation in both types (i.e., USDX [17] for protocol layer and Basis [1] for application layer) cannot sufficiently ensure the constant purchasing power ($P \cdot Q$), which is a prerequisite for stablecoin.

This result implies the *status quo* where, despite the potential utility of non-collateralized stablecoin, we still do not have a method to maintain its purchasing power. This study makes an academic contribution in that it conducted a comprehensive survey of miscellaneous stablecoins, thereby highlighting the difficulties of maintaining purchasing power with current non-collateralized stablecoins. It would, therefore, be our next research topic to consider the non-collateralized stablecoin with a constant purchasing power while taking into account some of the aforementioned economic concepts such as QTM, Tobin tax, and speculative attack.

References

[1] Al-Naji, N., Chen, J., & Diao, L. (2017). *Basis: A Price-Stable Cryptocurrency with an Algorithmic Central Bank.* Basis team.

[2] Ametrano, F. M. (2016). *Hayek Money: the Cryptocurrency Price Stability Solution.* SSRN Electronic Journal. doi:10.2139/ssrn.2425270.

[3] Diamond, D. W., & Dybvig, P. H. (1983). *Bank Runs, Deposit Insurance, and Liquidity.* The University of Chicago Press. The Journal of Political Economy, Vol. 91, No. 3.

[4] Fisher, I., & Brown, H. (1911). *The Purchasing Power of Money.* Yale University.

[5] Hassani, H., Huang, X., & Silva, E. (2018). *Banking with blockchain-ed big data.* Journal of Management Analytics. doi:10.1080/23270012.2018.1528900.

[6] Liuzzi, D., Pellizzari, P., & Tolotti, M. (2017). *Optimality of a Two-Tier Rate Structure for a Transaction Tax in an Artificial Market.* PAAMS 2017: Highlights of Practical Applications of Cyber-Physical Multi-Agent Systems. doi:10.1007/978-3-319-60285-1_8.

[7] Mancini-Griffoli, T., Peria, M. S., Agur, I., Ari, A., Kiff, J., Popescu, A., & Rochon, C. (2018). *Casting Light on Central Bank Digital Currency.*

[8] McCulloch, N., & Pacillo, G. (2011). *The Tobin Tax: A Review of the Evidence.* Institute of Development Studies at the University of Sussex. Brighton BN1 9RE UK: IDS RESEARCH REPORT 68.

[9] Morini, M. (2014). *Inv/Sav wallets and the role of financial intermediaries in a digital currency*. SSRN Electronic Journal.

[10] Obstfeld, M. (1995). *Models of currency crises with self-fulfilling features.* European Economic Review 40.

[11] Routledge, B. R., & Zetlin-Jones, A. (2018). *Currency Stability Using Blockchain Technology.* Society for Economic Dynamics.

[12] Saito, K., & Iwamura, M. (2018). *How to Make a Digital Currency on a Blockchain Stable.* CoRR - Computing Research Repository.

[13] Saleh, F. (2018). *Volatility and Welfare in a Crypto Economy.* seminar, McGill University, Desautels.

[14] Sams, R. (2014). *A Note on Cryptocurrency Stabilisation: Seigniorage Shares.*

[15] Spahn, P. B. (1995). *International Financial Flows and Transactions Taxes: Survey and Options.* IMF.

[16] The Distributed Technology Research Foundation. (2019). *Decentralized Payment Systems: Principles and Design.* The Distributed Technology Research Foundation.

[17] Tiutiun, R., Porco, L., Gord, M., & Lee, D. S. (2018). *USDX: A Decentralized Monetary Policy System.* white paper.

[18] Tobin, J. (1972). *The New Economics, One Decade Older.* Princeton University Press.

[19] Xu, A., Li, M., Huang, X., & Xue, N. (2016). *A Blockchain Based Micro Payment System for Smart Devices.* Suzhou: 1st Conference on Emerging Topics in Interactive Systems.

[20] Zhang, A. R., Raveenthiran, A., Mukai, J., Naeem, R., Dhuna, A., Parveen, Z., & Kim, H. (2018). *The Regulation Paradox of Initial Coin Offerings: A Case Study Approach.* Schulich School of Business, York University. SSRN Electronic Journal.