International Journal of Service and Knowledge Management
International Institute of Applied Informatics
2020, Vol. 4, No. 2, 71 - 86

What is Stablecoin?: A Survey on Its Mechanism and Potential as Decentralized Payment Systems

Makiko Mita [*], Kensuke Ito [*],
Shohei Ohsawa [†], Hideyuki Tanaka [*]

Abstract

Our study provides a survey on how existing *stablecoins*—cryptocurrencies aiming at price stabilization—peg their value to other assets, from the perspective of *Decentralized Payment Systems* (DPSs). This attempt is important because there has been no preceding surveys focusing on the stablecoin as DPSs, i.e., the one aiming at not only price stabilization but also decentralization. For clarity, we first classified existing stablecoins into four types according to their collaterals (fiat, commodity, crypto, and non-collateralized) and pointed out the high potential of non-collateralized stablecoins as DPSs; then, we further classified existing non-collateralized stablecoins into two types according to their intervention layers (protocol, application) and confirmed details of their representative mechanisms. Utilizing concepts such as *Quantity Theory of Money (QTM)*, *Tobin tax*, and *speculative attack*, our survey revealed the status quo where, despite the high potential of non-collateralized stablecoins, they have no standard mechanism to achieve the stablecoin for practical DPSs.

Keywords: cryptocurrency, decentralized payment system, stablecoin, survey paper

1 Introduction

Since Nakamoto [1] first proposed their theoretical concept, a large variety of *cryptocurrencies*[1] have been issued and actively traded online. After hitting a high of almost $20,000 for one bitcoin in December 2017 [5], the total market capitalization of cryptocurrencies reached $796 billion [6]—equivalent to second place in the world ranking of companies by market capitalization at that time, right after Apple Inc.'s $911 billion [7].

[*] The Graduate School of Interdisciplinary Information Studies, The University of Tokyo, Japan
[†] Daisy, Inc., Tokyo, Japan

[1]The term cryptocurrency has a number of definitions, such as "any form of currency that only exists digitally, that usually has no central issuing or regulating authority but instead uses a decentralized system to record transactions and manage the issuance of new units, and that relies on cryptography to prevent counterfeiting and fraudulent transactions" [2] and "A medium of exchange that functions like money (in that it can be exchanged for goods and services) but, unlike traditional currency, is untethered to, and independent from, national borders, central banks, sovereigns, or fiats" [3]. See Houben and Snyers [4] for other legal definitions.

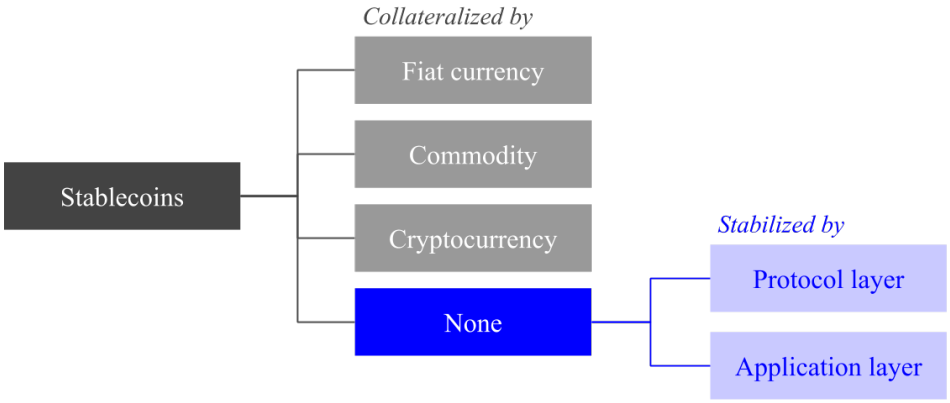

Figure 1: A Classification Tree for Stablecoins

From the perspective of online payment systems, several studies [8][9] have focused on the potential of cryptocurrencies as *Decentralized Payment Systems* (DPSs) that can provide various advantages, such as "(i) the diffusion of control among stakeholders; (ii) the ability to engage in trusted commerce without a centralized intermediary; (iii) the potential to disrupt the rents extracted by centralized intermediaries facilitating commerce; and (iv) global consistency and transparency on a shared ledger" [8][2]. Despite these advantages, however, cryptocurrencies are now difficult to work as practical DPSs due to their *high price volatility*[3]. The high price volatility undermines the three functions of money (i.e., Medium-of-Exchange, Store-of-Value, Unit-of-Account), which results in less demand to own cryptocurrency for online payments. In fact, according to an online survey in 2018 [14], the awareness of cryptocurrency is 74% on average in the eight largest cryptocurrency markets (US, UK, Germany, Brazil, Japan, South Korea, China and India), while its ownership remains 7% on average.

Stablecoin is an approach to address this problem of high price volatility, which is for example defined as "a digital currency that is pegged to another stable asset like gold, or to major fiat currencies like Euros, Pounds or the US dollar" [15][4]. Reflecting the necessity for cryptocurrencies as practical DPSs, the market for stablecoin continues to grow rapidly, more than doubling from $1.4 billion to $3 billion between 2018 and 2019 [18].

Our study aims to provide a survey on how such stablecoins peg their value to other assets, from the perspective of DPSs. This attempt is important because, to the best of our knowledge, there has been no preceding surveys that focuses on the stablecoin as DPSs, i.e., the one aiming at not only price stabilization but also decentralization. For clarity, as Figure 1 depicts, we first classify existing stablecoins into four types according to their collaterals (fiat, commodity, crypto, and non-collateralized)[5] and point out the high potential of non-collateralized stablecoins as DPSs; then, we further classify existing non-collateralized stablecoins into two types according to their intervention layers (protocol, application) and

[2]DPSs develop a variety of protocols to address more specific topics, such as micro payments [10][11] and transparent monetary policy [12].

[3]For specific data on the high price volatility, see, for example, Cryptocurrency Index 30 [13].

[4]Note that there are many other definitions for stablecoin, such as "cryptocurrency that has price stable characteristics" [16] and "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" [17].

[5]This classification is based on the two preceding studies: Zhang et al. [19] and Mancini-Griffoli [20].

confirm details of their representative mechanisms. In addition, to evaluate a variety of stablecoins, the above process leverages three concepts in economics—*Quantity Theory of Money (QTM)*, *Tobin tax*, and *speculative attack*. Our survey consequently highlights the status quo where, despite the high potential of non-collateralized stablecoins, they have no standard mechanism to achieve both price stabilization and decentralization.

The remaining part of this paper is organized as follows. Section 2 covers preliminaries, which includes the introduction of the three useful concepts in economics and the four collateral types to classify existing stablecoins. Section 3 provides an in-depth survey on representative mechanisms in the non-collateralized stablecoin that would have the highest potential as DPSs, by using the layer-based classification. Finally, Section 4 concludes our survey with describing implications and our next steps.

2 Preliminaries

In this section, we first introduce three concepts in economics (QTM, Tobin tax, and speculative attack) which are all useful when considering price-stabilization mechanisms employed in stablecoins. Moreover, we here classify existing stablecoins into four types according to their collateral (fiat, commodity, crypto, and non-collateralized) and point out that the non-collateralized is the best way to implement stablecoins as DPSs.

2.1 Quantity Theory of Money

QTM is a theory of economics that attempts to explain the price level in terms of the amount of money in circulation. A representative model in QTM is the *equation of exchange* which was formulated by Fisher [21][22] as follows:

$$M \cdot V = P \cdot Q, \tag{1}$$

where M is the amount of money supply (in a given period), and V is the velocity of money; P is the price level, and Q is an index of real expenditures on newly produced goods and services. Namely, the left-hand side represents the scale of an economy through money in circulation, while the right-hand side represents it through goods and services in circulation. An implication of this equation is that we can adjust the price level P with M and V if their change has no (or small) effect on Q (i.e., if money is neutral).

From the viewpoint of stablecoins, the QTM is important because it has been a basis of the mechanisms for non-collateralized stablecoins. As we will confirm in Section 3, all non-collateralized stablecoins attempt to stabilize its P by using some mechanism that automatically adjusts M or V in a decentralized manner[6]. Specifically, just as central banks tighten monetary policy against inflation, the mechanism decreases M or V if P becomes too high, and vice versa. Such mechanisms for automatic price adjustment have become more feasible thanks to cryptocurrencies in which we can easily manage transaction records and money supply; on the other hand, there are several related studies preceding cryptocurrencies, including the Tobin tax below.

[6]Note that this P denotes not the price of the stablecoin measured by other currency (e.g., USD) but the price of goods and services measured by the stablecoin. Accordingly, the higher P means the lower value of the stablecoin (i.e., inflation).

2.2 Tobin Tax

Tobin tax is a proposal by Tobin [23][24] in 1972, which aims to stabilize the currency exchange rate by penalizing short-term speculative (noise) trading[7]; specifically, it is a small amount (e.g., 0.5%) of tax imposed on international financial transactions to "throw some sand in the wheels of our excessively efficient international money markets" [24][8].

A variety of studies have analyzed the Tobin tax. For example, McCulloch and Pacillo [25] surveyed related literature and available empirical evidence, then concluded that the Tobin tax can be a major source of revenue without causing market distortions while it may not contribute to the stabilization of exchange rate. To cover its weak contribution to the stabilization, Spahn [26] extended the Tobin tax to the two-tier rate structure (Spahn tax) that imposes a higher tax when financial transactions are taken place outside a predetermined range of exchange rate. Furthermore, Liuzzi et al. [27] leveraged an artificial market to find the optimal rate of the Tobin tax. Their simulation derived the result close to Spahn [26]: a non-negligible level of taxation for highly liquid markets and low (close to zero) levels of taxation for low liquidity markets.

From the viewpoint of stablecoins, the Tobin tax is important because it has been one of the common tools for existing non-collateralized stablecoins. As we will confirm in Section 3, several non-collateralized stablecoins adopt the mechanisms which adjust M and V by imposing some amount of fee on each transaction. Namely, non-collateralized stablecoins inherit the concept of Tobin tax—"throw some sand in the wheels of our excessively efficient international money markets" [24]. In addition, although there are few preceding studies, the Tobin tax should also have implications for collateralized stablecoins, as they have a risk of speculative attack which we will discuss below.

2.3 Speculative Attack

Speculative attack is an action that inactive speculators suddenly sell a large amount of currency to deplete the government's reserves, thereby making the pegged exchange rate fail. Speculators have an incentive to do this attack because they can make big profits from short selling, etc. when the (previously maintained) pegged exchange rate fails.

A variety of studies have analyzed how speculative attacks occur. For example, Krugman [28] was the first study to model the speculative attack targeting a government with insufficient reserves in the foreign exchange market, by extending Salant and Henderson [29]. On the other hand, subsequent studies, such as Obstfeld [30][31] and Chang and Velasco [32], pointed out that speculative attacks (resulting in currency crisis) may occur even in a government with sufficient reserves, by taking into account *self-fulfilling features* in which a speculator actually sells the currency if she predicts that other speculators may sell the currency[9].

From the viewpoint of stablecoins, the speculative attack is important because it has been a main risk for existing stablecoins. Collateralized stablecoins would likely to be subject to speculative attacks, as they have a similar structure to the pegged currencies relying on government reserves. Despite this potential risk, to the best of our knowledge, Routledge and Zetlin-Jones [34] is the only preceding study that addresses the speculative

[7] Tobin first proposed this idea at a lecture held in 1972, while the proceedings of which [23] were compiled in later years.

[8] The Tobin tax and its extensions are often referred to as *Currency Transaction Taxes* (CTTs) or *Financial Transaction Taxes* (FTTs).

[9] See also Diamond and Divig [33] which is the first study to model self-fulfillment in bank runs.

attack in collateralized stablecoins. Non-collateralized stablecoins would also be subject to the attack, as long as speculators can profit from their high price volatility or peg failures in a similar way[10]. Thus, as stablecoins are (by definition) pegged to other stable assets, we must prevent their mechanisms from speculative attacks.

2.4 Fiat-, Commodity-, Crypto-, and Non-Collateralized Stablecoins

Based on preceding studies [19][20], this section classifies existing stablecoins into four types according to their collaterals (Figure 1). In addition, for each type, we briefly explain its mechanism and problem as DPSs, which are summarized in Table 1 below.

The first type is a *fiat-collateralized stablecoin* which uses fiat money (e.g., the US dollar) as collateral. To ensure the stability, it employs a simple and intuitive mechanism that issues new stablecoin on condition that the asset to be pegged is collateralized and, like the gold standard, commits to exchange the stablecoin for collateral at a fixed rate at any time. A representative example of this type is *Tether* [36]—a stablecoin which is promised a one-to-one exchange with the US dollar. Despite this simplicity, however, the fiat-collateralized stablecoin has a problem of requiring a centralized custodian to manage deposited collateral and issue new stablecoins. This is contrary to the aforementioned advantage of DPSs: "the ability to engage in trusted commerce without a centralized intermediary" [8]. We therefore cannot use the fiat-collateralized stablecoin as DPSs due to the lack of decentralization.

The second type is a *commodity-collateralized stablecoin* which uses commodity (e.g., gold, oil) as collateral. Although this type uses different collaterals, it actually employs the same mechanism as the fiat-collateralized stablecoin and thus shares the problem, too. Representative examples of this type are *DigixDAO* [37] and *Petro* [38]—the stablecoins which are pegged to (and collateralized by) gold in the former and oil in the latter. Needless to say, we cannot use the commodity-collateralized stablecoin as DPSs due to the same problem: the lack of decentralization.

The third type is a *crypto-collateralized stablecoin* which uses cryptocurrency (e.g., bitcoin) as collateral. To address the lack of decentralization, it employs a mechanism that uses cryptocurrency (with a decentralized consensus algorithm) for pegging the stablecoin to another stable asset (e.g., the US dollar), which allows any anonymous participants to become a custodian[11]. A representative example of this type is *Dai stablecoin* [43]—a stablecoin pegged to the US dollar but collateralized by the cryptocurrency *Ethereum* [44][45]. On the other hand, the crypto-collateralized stablecoin has another problem that the mechanism, consisting of at least three assets (stablecoin, cryptocurrency as collateral, the asset to be pegged), is inevitably complicated. In particular, to prevent the speculative attack while using cryptocurrencies with high price volatility, the mechanism needs much greater collaterals than the value of newly issued stablecoin, which is a well-known *over-collateralized problem*[12]. Thus, we cannot use the crypto-collateralized stablecoin as DPSs unless we develop some simpler mechanism without the over-collateralized problem[13].

[10] The Bitcoin protocol has a similar risk, called *goldfinger attack* [35] in which miners, even though they have received bitcoin as a reward, damage its value in order to make profits from short selling or holding alternative assets.

[11] Recently, crypto-collateralized stablecoin develops another category referred to as *multi-collateralized stablecoin* which uses a variety of assets simultaneously as collateral (e.g., using gold, bitcoin, and Japanese yen for pegging the stablecoin to the US dollar). For example, see *Libra* [39][40] and *Synthetix* [41][42]

[12] For example, the issuance of new Dai stablecoin requires at least 150% collateral (by default).

[13] Although it is not the main scope of this paper, crypto-collateralized stablecoins have recently developed new mechanisms to avoid the over-collateralized problem, such as *Lien protocol* [46].

Table 1: Characteristics of the Four Collateral Types

Collateralized by	Decentralization	Simplicity
Fiat currency [36]		✗
Commodity [37][38]		✗
Cryptocurrency [43]	✗	
None [47][48]	✗	✗

The fourth type is a *non-collateralized stablecoin* which does not use anything as collateral. As mentioned above, it employs the mechanism that aims to stabilize P by automatically adjusting M and V in a decentralized manner. If such a simple and decentralized mechanism were feasible, the non-collateralized stablecoin could obtain the highest potential as DPSs among the four types. However, can we really design the mechanism of automatic adjustment, even under a variety of risk including the speculative attack? To confirm the feasibility, we in Section 3 provide an in-depth survey on non-collateralized stablecoins, which includes the introduction of representative examples [47][48].

In this section, we have introduced the three concepts and the four collateral types as preliminaries. To summarize, the former implies the importance of preceding discussions in economics to consider price-stabilization mechanisms for exisitng stablecoins, and the latter implies the high potential of non-collaterized stablecoins as DPSs. Table 1 represents characteristics of the four collateral types, which reflects (i) fiat- and commodity-collateralized stablecoins are not decentralized because they require some centralized custodian to manage collaterals; (ii) crypto-collateralized stablecoin is not simple because it consists of at least three assets (stablecoin, cryptocurrency as collateral, and the asset to be pegged). Based on this result, Section 3 focuses on the survey of non-collateralized mechanisms.

3 Non-Collateralized Mechanisms: A Survey

This section provides an in-depth survey on non-collateralized mechanisms, by using the classification according to their two intervention layers: *protocol* and *application* (Figure 1). We here assume that the protocol is a layer related to fundamental consensus-algorithms for the blockchain (e.g., *Proof-of-Work* algorithm and *Nakamoto consensus* in the Bitcoin protocol), while the application is a layer not related to the consensus-algorithm but for various systems running on the protocol[14]. Such layer-based classification became popular, especially after the Ethereum—an alternative protocol subsequent to the Bitcoin protocol—enabled application development on blockchains[15]. To the best of our knowledge, non-collateralized stablecoins need to intervene in either protocol or application layers.

[14]See also the following other definitions: "Protocol layer: consists of the core software building blocks that make up a distributed ledger" [49]; "Application layer: consists of all applications that are built on existing distributed ledger networks" [49]. "The protocol layer lays the foundational structure of the blockchain. It determines the computing language the blockchain will be coded in and any computational rules that will be used on the blockchain" [50]; "The application layer is where networks and protocol are used to build applications that users interact with" [50].

[15]Applications developed on Ethereum are often referred to as *Decentralized Applications (DApps)* [51].

Furthermore, for protocol and application layers, we confirm their representative mechanisms from the perspective of both proposal and implementation, where the former is based on academic articles and the latter is based on white papers for some project.

3.1 Stabilization by Protocol Layer

The survey for protocol layer first confirms two studies, Saito and Iwamura [52][16] and Saleh [54], which both propose modified consensus-algorithms in order for the price stabilization of cryptocurrencies[17]. Subsequently, as a representative implementation, we also confirm the *USDX* project [47] which aims to issue stablecoins pegged with the US dollar.

3.1.1 Proposal

Studies on the protocol for price stabilization have mainly focused on the consensus algorithm which underlies blockchain-based systems. For example, Saito and Iwamura [52] proposes three modifications to Proof-of-Work algorithm in the current Bitcoin protocol[18], aiming for the stable price P through autonomous adjustment of the money supply M and the velocity of money V. The first modification limits the re-adjustment of mining difficulty (i.e., Proof-of-Work targets) only when the block-interval exceeds a certain threshold value[19]. The second modification makes the amount of mining rewards variable according to each scale of the aforementioned re-adjustment, instead of the existing halving rule[20]. These two modifications are intended to adjust the growth rate of M (as mining reward) in line with the fluctuating demand (as hash rate). The third modification imposes a negative interest rate on all bitcoins, which increases in proportion to the time that elapses from the bitcoin issuance just as assets are depreciated over time. This modification not only restrains the ever-increasing M but also intervenes in V because, like the Tobin tax, it collects the negative interest for every transaction[21][22]. Saito and Iwamura [52] tried to make the Bitcoin protocol a practical DPS by the combination of these three modifications.

While Saito and Iwamura [52] proposed a modified Proof-of-Work algorithm, Saleh [54] proposed an alternative algorithm for price stability. He first analyzed Proof-of-Work by the overlapping-generations model [55]—a framework used in economics—and pointed out that it can cause exceptional price volatility and welfare impairment. To solve the problem, Saleh [54] recommends us to adopt *Proof-of-Burn* algorithm[23] in which, to create new blocks, miners need to send a certain amount of their coins to an unspendable (locked)

[16] See also Iwamura et al. [53].

[17] Note that these studies based on the Bitcoin protocol do not apply to stablecoin in the definition by Lund [15], as they do not envision pegging their value to another asset. On the other hand, they are stablecoins in the definition by Tomaino [16] which simply defines stablecoin as "cryptocurrency that has price stable characteristics" [16].

[18] Strictly speaking, while their proposal is based on the Bitcoin protocol, it scopes blockchain-based cryptocurrencies in general.

[19] Regardless of the block-interval, the current Bitcoin protocol re-adjust the mining difficulty for every $2,016$ blocks.

[20] Regardless of the scale of re-adjustment, the current Bitcoin protocol halves the amount of its mining reward for every $210,000$ blocks.

[21] Unlike transaction fees in the current Bitcoin protocol, all bitcoins collected as negative interests will be burned.

[22] Tobin tax and this negative interest are different in that the former fixes its own rate while the latter varies its rate depending on time. The ever-increasing negative interest would also have a positive effect on V because it encourages us to change old coin to new one.

[23] Note that, prior to Saleh [54], Stewart [56] for the first time proposed the concept of Proof-of-Burn in 2012.

address. Here, the Proof-of-Burn adjusts mining difficulty through the amount of coins that should be burned; in other words, his proposal controls M by adjusting the amount of coins burned as mining costs, against the amount of newly issued coins as mining rewards.

One of the problems with these protocols is that their price stabilization does not use market price (e.g., BTC/USD) directly, but uses mining difficulty as a proxy variable. It is still controversial whether the mining difficulty (or hash rate in the case of Bitcoin protocol) can be a proxy variable for market prices [57][58]; however, at least on a yearly basis, there seems to be no explicit correlation between the two [59]. In any case, these protocols can no longer stabilize prices under a chronic deviation between market prices and mining difficulty (i.e., unstable proxy variable). Accordingly, in 3.1.2, we introduce an implementation of the non-collateralized and protocol-based stablecoin, which aims to peg their price directly with the US dollar.

3.1.2 Implementation

Tiutiun et al. [47] proposed the USDX—a project for non-collateralized stablecoin based on the protocol layer. This project has issued a stablecoin called USDY[24], which aims to maintain the same price with the US dollar through the following three mechanisms. The first mechanism is *variable block reward* [47] to adjust the amount of mining rewards, just as the second modification in Saito and Iwamura [52]. On the other hand, to adjust mining rewards, the USDX leverages the USDY/USD price index[25], rather than the mining difficulty. That is, when USDY/USD > 1, the amount of mining rewards (USDY) increases in order for the price reduction (by increasing the growth rate of M), and vice versa. The second mechanism is *lock-in mining* [47] which is a kind of emergency measure, activated only when the state of USDY/USD < 1 persists even if the variable block reward takes the lowest value. To further reduce the money supply M, the lock-in mining allows users to (stochastically) create a new block by temporary locking their own USDY for a predetermined period which varies according to the rigidity of USDY/USD < 1[26]. When users successfully create new blocks with the lock-in mining, they can receive mining rewards (USDY) independent of the variable block reward. The third mechanism is *variable transaction fee* [47], which is the same with the third modification in Saito and Iwamura [52] in that it burns circulating coin with a variable rate to control M and V. On the other hand, the USDX also leverages the USDY/USD price index to determine the rate of transaction fee, rather than the time from the coin issuance. That is, when USDY/USD > 1, the amount of transaction fee decreases in order for the price reduction (by increasing both M and V), and vice versa. The USDX project aims to peg its stablecoin USDY with the US dollar by the combination of the three mechanisms above.

The problem with the USDX is that its mechanism leads to the unstable *purchasing power* (i.e., the amount of USDY $\times$ the current price of USDY) in each wallet. While stablecoin, by definition, focuses on stabilizing its price against other assets, it needs to stabilize the purchasing power of users as well in order to be a practical DPS satisfying the store-of-value. In the case of USDX, the variable block reward and the lock-in mining

[24]This project contains two coins: USDX and USDY, where the former is a type of governance token and the latter is stablecoin pegged to the US dollar.

[25]Here, we have another important problem: how to obtain data outside the blockchain (e.g., the USDY/USD price index) in a decentralized manner while ensuring their reliability? In the context of blockchain, this is often referred to as the *Oracle problem* [60]. Although we will spare you the details, the USDX employs an original mechanism called the decentralized Schelling point Oracle system.

[26]Unlike the Proof-of-Burn, the locked USDY will back to the holders after the predetermined period.

intervene only in the purchasing power of miners who voluntarily join the mechanisms; on the other hand, the variable transaction fee intervenes in that of individuals who do nothing but hold USDY. Furthermore, although the Tobin tax and negative interest rate in Saito and Iwamura [52] do the same type of intervention, the variable transaction fee in USDX would be worse because its fee rate fluctuates unpredictably (according to USDY/USD). Thus, to enable a constant purchasing power, we should controll M and V through mechanisms based on some voluntary action (e.g., mining), and if it were inevitable to use transaction fees, the rates should at least be predictable.

3.2 Stabilization by Application Layer

The survey for application layer, on the other hand, first confirms three studies, Ametrano [61], Morini [62], and Sams [63]. Even though Ametrano [61] and Morini [62] assume direct intervention in each wallet, Sams [63] inherits these studies and proposes another mechanism—*Seigniorage Share*. Subsequently, we also confirm the detail of the *Basis* project [48] as a representative implementation of the Seigniorage Share.

3.2.1 Proposal

Discussions on the application for price stabilization stem from Ametrano [61], which proposed a non-collateralized stablecoin named *Hayek Money*[27]. The gist of the Hayek money is its *rebasement* mechanism [61] that automatically adjusts M by modifying the amount of money stocked in each wallet, according to the data on current price which is updated whenever miners create new blocks. However, as with the USDX project, this simple (and somewhat primitive) mechanism leads to the unstable purchasing power because the rebasement directly modifies the amount of money in each wallet.

To address this problem, Morini [62] argued that the Hayek money should divide its wallet into two types: *Inv wallets* for investment and *Sav wallets* for saving. Here, in order to leave the option of stable purchasing power, the rebasement only intervenes in the Inv wallets (accordingly, M in Inv wallets is subject to the higher fluctuation than the original Hayek money, to cover the adjustment for M in Sav wallets). Namely, Morini [62] allows users to allocate their holding money into both Inv and Sav wallets, thereby offering "the freedom to choose how much they want to be affected by changes of money supply" [62] along with their risk appetite. This mechanism appears to be effective as it only intervenes in the money whose owners have accepted the unstable purchasing power; however, it has another problem. Consider the case where most users predict an increasing trend of P (i.e., a decline in the price of Hayek money). In this case, decreasing M for price-stabilization becomes difficult because speculators would transfer their money from the Inv wallet to the Sav wallet in order to avoid the rebasement. To make matters worse, this Inv-to-Sav transfer will impose the higher decreasing rate on the Inv wallets, which further accelerates the Inv-to-Sav transfer. Therefore, if speculators could freely transfer their money between Inv-Sav wallets (i.e., the Inv/Sav ratio is unstable), it would be difficult to adjust (especially to reduce) M in the Inv wallet[28].

[27] It was named after the denationalization of money [64]—the concept proposed by Hayek.

[28] In response to the problem, Morini [62] suggests collecting a small amount of fee from Sav wallets to decrease M, only if there are extremely few money in Inv wallets. However, needless to say, this is contrary to the original purpose of stabilizing the purchasing power in Sav wallets.

Inhereting the above discussion, Sams [63] proposed a new mechanism for the price stabilization in application layer, named Seigniorage Share. As the name implies, the mechanism aims to automatically adjust M through *shares* with which users can purchase stablecoins. Specifically, when the mechanism detects an increasing trend of P[29], it issues new shares to decrease the current M. Shares are distributed among bidders who burned an arbitrary amount of holding coins in a decentralized auction[30]. Conversely, when the mechanism detects a decreasing trend of P, it issues new coins to increase the current M. Coins are distributed among bidders who burned an arbitrary amount of holding shares in another decentralized auction. In other words, Seigniorage Share is a mechanism that intends for the price stabilization by letting users voluntarily balance the amount of coins and shares, where, unlike the free transfer between Inv-Sav wallets, the coin-share exchange rate is determined in auctions.

3.2.2 Implementation

Al-Naji et al. [48] proposed the Basis—a project for non-collateralized stablecoin based on the application layer. This project has issued a stablecoin called Basis token, which aims to maintain the same rate with the US dollar through the Seigniorage Share. On the other hand, to make the mechanism more practical, the Basis project has made some modifications to the original Seigniorage Share [63]. One of the biggest modifications is to adjust M with another token called *bonds*. Bonds are similar to shares in that they are newly issued to reduce M and are distributed in a decentralized auction (where bonds are sold for prices of less than 1 basis); however, they are not used to purchase stablecoins but, as with real bonds, redeemed at a fixed exchange rate of Bond/Basis = 1 when the mechanism newly issues the Basis token in the future. That is, the mechanism encourages users to purchase the bond by the commitment to redeem it with the newly issued Basis token[31]. This modification—using bonds instead of shares—is primarily for the robustness against the case of high P (i.e., inflation). In the original Seigniorage Share [63], stablecoin would be difficult to recover from extremely high P because the more new shares are supplied, the lower their price and consequently the less power to reduce M. The Basis project attempts to maintain this power to reduce M, by adopting bonds with the commitment to redeem at a fixed exchange rate[32].

However, regardless of this modification, the Basis project and the original Seigniorage Share [63] both have a critical problem which is summarized as follows—"incentives to buy bonds are based on a circular dependency: people will buy the bonds if they think Basis will climb up, but Basis will only climb up if people buy the bonds" [65]. In other words, there is a kind of tautology in the Seigniorage Share that requires a decrease of future P in order to decrease current P (i.e., shares or bonds are in demand). It is highly doubtful that

[29] As with the Hayek money, Sams [63] assumes that the data on current price is updated whenever miners create new blocks. Moreover, Sams [63] mentions the possibility of using mining difficulty as a proxy variable, as in models for protocol layers, in addition to using general oracles that obtain price data from outside the system (e.g., exchanges).

[30] See original article for the detail of decentralized auctions.

[31] It is confusing but the Basis project also uses shares which has a different role from those in Sams [63]. Shares in the Basis project are only issued at the genesis of the blockchain, and shareholders can receive the newly issued Basis tokens, when the mechanism needs to increase M even after all bonds have been redeemed.

[32] In addition, the bonds in the Basis project will expire after five years, even if they are not redeemed with the Basis tokens. This would help maintain the price of new bonds in terms of reducing the amount of existing bonds.

Table 2: Stabilization Mechanisms for Non-Collateralized Stablecoins

	Intervention Layers		**QTM**		**Problems**
	Protocol	Application	M	V	
Proposals					
Proof-of-Work [52]	✗		✗	✗	unstable proxy variable
Proof-of-Burn [54]	✗		✗		unstable proxy variable
Hayek Money [61]		✗	✗		unstable purchasing power
Inv/Sav wallets [62]		✗	✗		unstable Inv/Sav ratio
Seigniorage Share [63]		✗	✗		tautological mechanism
Implementations					
USDX [47]	✗		✗	✗	unstable purchasing power
Basis [48]		✗	✗		tautological mechanism

speculators would buy shares or bonds under such a tautological mechanism. Perhaps due to this problem, the developer team announced the closure of Basis project in December 2018 [66], even though it raised $133 million through *Initial Coin Offering* (ICO).

In this section, we have surveyed non-collateralized mechanisms in protocol and application layers, from the perspective of both proposal and implementation. To summarize, as Table 2 shows, all existing non-collateralized stablecoins are not practical as DPSs due to some problem. In the protocol layer, proposals [52][54] have the problem of unstable proxy variable for market price, and even though an implementation [47] uses price data outside the system, it has another problem of unstable purchasing power (of each wallet). In the application layer, no mechanism has resolved this unstable purchasing power. Despite proposals to increase the type of wallets [62] and tokens [63], speculators would not voluntarily contribute to the price stabilization. This is implied by the closure of a representative project [48] for the application layer[33].

4 Conclusion

In this paper, we for the first time surveyed how existing stablecoins—cryptocurrencies aiming at price stabilization—peg their value to other assets, from the perspective of DPSs. For clarity, our survey first classified existing stablecoins into four types according to their collaterals (fiat, commodity, crypto, and non-collateralized) and pointed out the high potential of non-collateralized stablecoins as DPSs (Table 1); then, it further classified existing non-collateralized stablecoins into two types according to their intervention layers (protocol, application) and surveyed proposals and implementations for each layer (Table 2). This survey focusing on non-collateralized stablecoins pointed out that, due to a variety of problems, all existing mechanisms cannot ensure the constant purchasing power in each wallet which may be owned by speculators.

[33]Despite the closure, non-collateralized stablecoin still has a potential as a DPS and continues to develop new mechanisms such as Terra [67]. Re-investigating the ever-increasing new proposals would be one of the future works of this survey.

This result implies the status quo where, despite the high potential of non-collateralized stablecoins, they have no standard mechanism to achieve both price stabilization and decentralization. Thus, in order to make cryptocurrencies practical DPSs, our next step would be to design some new non-collateralized mechanism that enables a constant purchasing power, while taking into account the aforementioned concepts such as QTM, Tobin tax, and speculative attack. This is achieved if we solve (i) the unstable purchasing power in USDX [47] or (ii) the tautological mechanism in Basis [48], according to our survey on preceding implementations. On the other hand, given the growing number of new proposals, it is also quite possible that someone will achieve the non-collateralized stablecoin with constant purchasing power, through an entirely different mechanism.

Acknowledgements

We would like to express our gratitude to B Cryptos for providing valuable comments and financial support.
We also would like to express our gratitude to referees and participants in IIAI AAI 2019 for providing valuable comments.

References

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[2] C. Dictionary, "Definition of a cryptocurrency," *URL: https://www. merriam-webster. com/dictionary/cryptocurrency*, 2018.

[3] V. A. Maese, A. W. Avery, B. A. Naftalis, S. P. Wink, and Y. D. Valdez, "Cryptocurrency: A primer," *Banking LJ*, vol. 133, p. 468, 2016.

[4] R. Houben and A. Snyers, *Cryptocurrencies and blockchain: Legal context and implications for financial crime, money laundering and tax evasion*. 2018.

[5] CoinMarketCap, "Bitcoin charts." `https://coinmarketcap.com/currencies/bitcoin`. [Accessed: 20-March-2019].

[6] CoinMarketCap, "Global charts." `https://coinmarketcap.com/charts`. [Accessed: 20-March-2019].

[7] B. around the World, "The world's top 50 companies." `https://www.relbanks.com/rankings/worlds-largest-companies`. [Accessed: 20-March-2019].

[8] F. Giulia and V. Pramod, eds., *Decentralized Payment Systems: Principles and Design*, 2019. `http://pramodv.ece.illinois.edu/pubs/Decentralized-Payment-Systems-Principles-and-Design.pdf`, [Accessed: April-03-2019].

[9] R. Kaushal, "Bitcoin: First decentralized payment system," *International Journal Of Engineering And Computer Science*, vol. 5, no. 5, 2016.

[10] A. Xu, M. Li, X. Huang, N. Xue, J. Zhang, and Q. Sheng, "A blockchain based micro payment system for smart devices," *Signature*, vol. 256, no. 4936, p. 115, 2016.

[11] R. Pass and A. Shelat, "Micropayments for decentralized currencies," in *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, CCS '15, (New York, NY, USA), p. 207–218, Association for Computing Machinery, 2015.

[12] G. Danezis and S. Meiklejohn, "Centrally banked cryptocurrencies," *Journal of Cryptology*, 2016.

[13] C. I. 30, "Cryptocurrency index 30: Cci30." `https://cci30.com/`. [Accessed: 5-May-2020].

[14] R. Jakubauskas, "How many people actually own cryptocurrency?." `https://daliaresearch.com/blog/how-many-people-actually-own-cryptocurrency/`, May 2018. [Accessed: 20-March-2019].

[15] J. Lund, "Stable coins: Enabling payments on blockchain through alternative digital currencies." `https://www.ibm.com/blogs/blockchain/2018/07/stable-coins-enabling-payments-on-blockchain-through-alternative-digital-currencies/`, July 2018. [Accessed: 5-May-2020].

[16] N. Tomaino, "Stablecoins: A holy grail in digital currency." `https://thecontrol.co/stablecoins-a-holy-grail-in-digital-currency-b64f3371e111`, April 2017. [Accessed: 5-May-2020].

[17] H. Hassani, X. Huang, and E. Silva, "Banking with blockchain-ed big data," *Journal of Management Analytics*, vol. 5, no. 4, pp. 256–275, 2018.

[18] G. Hileman, "State of stablecoins (2019)," *Available at SSRN*, 2019.

[19] A. R. Zhang, A. Raveenthiran, J. Mukai, R. Naeem, A. Dhuna, Z. Parveen, and H. M. Kim, "The regulation paradox of initial coin offerings: A case study approach," *Frontiers in Blockchain*, vol. 2, p. 2, 2019.

[20] M. T. M. Griffoli, M. M. S. M. Peria, M. I. Agur, M. A. Ari, M. J. Kiff, M. A. Popescu, and M. C. Rochon, *Casting Light on Central Bank Digital Currencies*. International Monetary Fund, 2018.

[21] I. Fisher, "" the equation of exchange," 1896-1910," *The American Economic Review*, vol. 1, no. 2, pp. 296–305, 1911.

[22] I. Fisher, *The purchasing power of money: its' determination and relation to credit interest and crises*. Cosimo, Inc., 2006.

[23] J. Tobin, "The new economy one decade older," *The Jane Lectures on Historical Economics*, 1974.

[24] J. Tobin, "A proposal for international monetary reform," *Eastern economic journal*, vol. 4, no. 3/4, pp. 153–159, 1978.

[25] N. McCulloch and G. Pacillo, "The tobin tax: a review of the evidence," *IDS Research Reports*, vol. 2011, no. 68, pp. 1–77, 2011.

[26] P. B. Spahn, "International financial flows and transactions taxes: survey and options," 1995.

[27] D. Liuzzi, P. Pellizzari, and M. Tolotti, "Optimality of a two-tier rate structure for a transaction tax in an artificial market," in *International Conference on Practical Applications of Agents and Multi-Agent Systems*, pp. 95–106, Springer, 2017.

[28] P. Krugman, "A model of balance-of-payments crises," *Journal of money, credit and banking*, vol. 11, no. 3, pp. 311–325, 1979.

[29] S. W. Salant and D. W. Henderson, "Market anticipations of government policies and the price of gold," *Journal of political economy*, vol. 86, no. 4, pp. 627–648, 1978.

[30] M. Obstfeld, "Rational and self-fulfilling balance-of-payments crises," tech. rep., National Bureau of Economic Research, 1984.

[31] M. Obstfeld, "Models of currency crises with self-fulfilling features," *European economic review*, vol. 40, no. 3-5, pp. 1037–1047, 1996.

[32] R. Chang and A. Velasco, "Financial crises in emerging markets," tech. rep., National Bureau of Economic Research, 1998.

[33] D. W. Diamond and P. H. Dybvig, "Bank runs, deposit insurance, and liquidity," *Journal of political economy*, vol. 91, no. 3, pp. 401–419, 1983.

[34] B. Routledge and A. Zetlin-Jones, "Currency stability using blockchain technology," tech. rep., Society for Economic Dynamics, 2018.

[35] J. A. Kroll, I. C. Davey, and E. W. Felten, "The economics of bitcoin mining, or bitcoin in the presence of adversaries," in *Proceedings of WEIS*, vol. 2013, p. 11, 2013.

[36] T. Limited, "Tether – stable digital cash on the blockchain." `https://tether.to/`, 2015. [Accessed: 27-May-2020].

[37] Digix, "Digix — the future of owning gold is digital." `https://digix.global/#/`, 2014. [Accessed: 27-May-2020].

[38] G. of Venezuela, "El petro - sembrando la soberanía tecnológica." `https://www.petro.gob.ve/`, 2018. [Accessed: 27-May-2020].

[39] TheLibraAssociationMembers, "libra white paper." `https://libra.org/en-US/white-paper/?noredirect=en-US`, June 2019. [Accessed: 3-July-2019].

[40] Z. Amsden, R. Arora, S. Bano, M. Baudet, S. Blackshear, A. Bothra, G. Cabrera, C. Catalini, K. Chalkias, E. Cheng, *et al.*, "The libra blockchain," *URl: https://developers. libra. org/docs/assets/papers/the-libra-blockchain. pdf*, 2019.

[41] S. Brooks, A. Jurisevic, M. Spain, and K. Warwick, "Havven: A decentralised payment network and stablecoin." `https://www.synthetix.io/uploads/havven_whitepaper.pdf`, June 2018. [Accessed: 30-April-2020].

[42] Synthetix.io, "Synthetix litepaper v1.4." `https://www.synthetix.io/uploads/synthetix_litepaper.pdf`, March 2020. [Accessed: 30-April-2020].

[43] MakerDAO, "The dai stablecoin system." `https://makerdao.com/en/whitepaper/sai/`, 2015. [Accessed: 27-May-2020].

[44] G. Wood *et al.*, "Ethereum: A secure decentralised generalised transaction ledger," *Ethereum project yellow paper*, vol. 151, no. 2014, pp. 1–32, 2014.

[45] V. Buterin *et al.*, "Ethereum: A next-generation smart contract and decentralized application platform," *URL https://github. com/ethereum/wiki/wiki/% 5BEnglish% 5D-White-Paper*, vol. 7, 2014.

[46] LienProtocol, "idol white paper." `https://lien.finance/pdf/iDOLWP_v1.pdf`, April 2020. [Accessed: 28-April-2020].

[47] R. Tiutiun, L. Porco, M. Gord, and D. S. Lee, "Usdx: A decentralized monetary policy system," 2018.

[48] N. Al-Naji, J. Chen, and L. Diao, "Basis: a price-stable cryptocurrency with an algorithmic central bank," *Formerly known as: Basecoin Version 0.99*, vol. 7, 2017.

[49] G. Hileman and M. Rauchs, "2017 global blockchain benchmarking study," 2017.

[50] OECD, "Oecd blockchain primer." `https://www.oecd.org/finance/OECD-Blockchain-Primer.pdf`, 2018. [Accessed: 10-May-2020].

[51] S. Raval, *Decentralized applications: harnessing Bitcoin's blockchain technology*. " O'Reilly Media, Inc.", 2016.

[52] K. Saito and M. Iwamura, "How to make a digital currency on a blockchain stable," *Future Generation Computer Systems*, vol. 100, pp. 58–69, 2019.

[53] M. Iwamura, Y. Kitamura, T. Matsumoto, and K. Saito, "Can we stabilize the price of a cryptocurrency?: Understanding the design of bitcoin and its potential to compete with central bank money," tech. rep., Institute of Economic Research, Hitotsubashi University, 2014.

[54] F. Saleh, "Volatility and welfare in a crypto economy," *Available at SSRN 3235467*, 2019.

[55] P. A. Diamond, "National debt in a neoclassical growth model," *The American Economic Review*, vol. 55, no. 5, pp. 1126–1150, 1965.

[56] I. Stewart, "Proof of burn - a potential alternative to proof of work and proof of stake." `https://bitcointalk.org/index.php?topic=131139.0\%202`, 2012. [Accessed: 7-May-2019].

[57] I. Georgoula, D. Pournarakis, C. Bilanakos, D. Sotiropoulos, and G. M. Giaglis, "Using time-series and sentiment analysis to detect the determinants of bitcoin prices," *Available at SSRN 2607167*, 2015.

[58] L. Kristoufek, "What are the main drivers of the bitcoin price? evidence from wavelet coherence analysis," *PloS one*, vol. 10, no. 4, 2015.

[59] T. Vidal, "Hash rate and bitcoin price during mining events: Are they related?." `https://cointelegraph.com/news/hash-rate-and-bitcoin-price-during-mining-events-are-they-related`, May 2020. [Accessed: 10-May-2020].

[60] S. Voshmgir, *Token Economy: How Blockchains and Smart Contracts Revolutionize the Economy*. BlockchainHub, 2019.

[61] F. M. Ametrano, "Hayek money: The cryptocurrency price stability solution," *Available at SSRN 2425270*, 2016.

[62] M. Morini, "Inv/sav wallets and the role of financial intermediaries in a digital currency," *Available at SSRN 2458890*, 2014.

[63] R. Sams, "A note on cryptocurrency stabilisation: Seigniorage shares," *Brave New Coin*, pp. 1–8, 2015.

[64] F. A. Hayek, *Denationalisation of money: the argument refined: an analysis of the theory and practice of concurrent currencies*, vol. 70. Coronet Books Incorporated, 1990.

[65] Q. Wang, "Twitter." `https://twitter.com/QWQiao/status/998213027097989120`, May 2018. [Accessed: 14-May-2020].

[66] N. Al-Naji, "Basis.io." `https://www.basis.io/`, December 2018. [Accessed: 14-May-2020].

[67] E. Kereiakes, M. D. M. Do Kwon, and N. Platias, "Terra money: Stability and adoption," 2019.