Towards a Stable Tokenized Medium of Exchange

Alexander Lipton
Chief Technical Officer, Sila Inc[1] and Connection Science Fellow, MIT

"…procedere con estrema cautela nell'accettare brillanti novità tecniche che non siano ancora collaudate da una esperienza pratica sufficientemente lunga…"
Admiral Domenico Cavagnari[2]

"Tres sunt modi, prout michi uidetur, quibus aliquis potest in moneta lucrari, absque hoc quod exponat eam in usu suo naturali: unus per artem campsoriam, custodiam uel mercanciam monetarum, alius est usura, tercius monete mutacio. Primus modus uilis est, secundus malus, et tercius peior. "
Nicholas Oresme[3]

ABSTRACT

Existing banking and payment systems, while still functioning, are rapidly becoming obsolete and misaligned with the new challenges of the modern economy. While open access Internet Protocols have unleashed a wave of creativity and growth in numerous fields, banking is not one of them. The reason stems mostly from the fact that internet protocols for money and identity, while sorely needed, are conspicuously absent at present. We argue that a regulatorily compliant fiat-backed token, which can be viewed as an electronic analogue of cash, can help to fill this gap. Experience suggests that all decentralized crypto coins are inherently unstable, which makes them less than useful for commercial applications. Contrary to often-made claims, it is not possible to build a truly decentralized stable token. We argue that any potentially successful stable token has to be at least partially centralized, with varying degrees of decentralization. We describe four approaches to building stable tokens including fully collateralized custodial tokens, partially collateralized custodial tokens, tokens overcollateralized with cryptos, and dynamically stabilized tokens, and conclude that only fully collateralized tokens can be stable, even under extreme circumstances. We also introduce narrow banks and describe their important role as anchors of a diverse digital banking ecosystem and potential emitters of central bank backed digital cash.

[1] Sila is an intuitive, secure, and accessible suite of developer tools for building financial applications. At the heart of Sila is a new regulatory-compliant, fiat-backed tokenized means of exchange - the Sila Token. This token is pegged to the USD via a centralized, 100% reserve held in USD-based instruments, and is guaranteed to be stable and retain its value even in the most extreme volatility environments which afflict financial systems. The Sila token will be used as the base for a fintech API platform that will enable fast, regulatory-compliant payments and other uses of money with minimal reliance on the traditional banking system. Sila's structure and function will resemble that of a narrow bank, while using partnerships with chartered banks to perform day-to-day operations and be regulatory compliant. In the longer run, Sila will apply to get direct access to national payment systems operated by Central Banks by acquiring the necessary licenses. Further details are given in [49].

[2] *"…proceed with extreme caution in accepting brilliant technical innovations that are not yet tested by a sufficiently long practical experience… "* Admiral Domenico Cavagnari (1876 - 1966).

[3] *"It seems to me that there are three ways in which profit may be made from money, without laying it out for its natural purpose; one is the art of the moneychanger, banking or exchange, another is usury, a third alteration of the coinage. The first way is contemptible, the second bad and the third worse."* Nicholas Oresme (1320-1382).

1. INTRODUCTION

The Global Financial Crisis (GFC) has clearly demonstrated that existing banking and payment systems, while still working, are outdated and are struggling to support the constantly changing requirements of the modern world. It would be an understatement to say that the GFC turned into a wasted opportunity to reorganize the world financial ecosystem. Too-big-to-fail banks dramatically increased (not decreased!) in size, disproportionally amplifying their share of the banking business, while the number of banking institutions significantly decreased. For instance, the size of JPMorgan's balance sheet is presently nearly twice as large as it was at the end of 2006, at the onset of the crisis; similarly, the balance sheets of China's four systemically important banks have more than tripled over the same period. The clearing of many over-the-counter derivatives was mandatorily transferred to central clearing counterparties (CCPs), which have become potential points of failure for the system as a whole. This situation is further exacerbated by the high level of interconnectedness of CCPs, due to their having so many general clearing members in common.

While ostensibly better capitalized, banking institutions have increased in complexity to such a degree that their stability and credit worthiness cannot be established with certainty, neither by regulators nor by depositors, investors, and, somewhat surprisingly, by their own management. The balance sheets of Tier 1 banks have become so opaque that their complexity is beyond quantitative analysis. As a result of this complexity, many banks and other financial institutions have become too-big-to-manage. Tier 1 banks have to spend billions of dollars annually (and their smaller competitors hundreds of millions) developing, validating and maintaining complex models and information technology (IT) systems, which are used to demonstrate to their regulators banks' compliance with capital and liquidity requirements. The Comprehensive Capital Analysis and Review (CCAR) is an annual rite of passage which every systemically important bank has to pass.

The situation is not helped at the macro level by the fact that established macroeconomic tools, such as dynamic stochastic general equilibrium modeling (DSGE), which are routinely used by central banks to model the economy and determine their monetary policies, essentially ignore the banking sector altogether, by viewing it as a mere intermediary for other economic actors.

The frustration of the general public with the *status quo* is palpable. Manifestations of this frustration can be seen in various aspects of social and economic life and, most directly, in the incredible rise and spectacular fall of cryptocurrencies.

In this paper we argue that not all is lost. More specifically, we show that, if used deliberately, new technologies, including blockchains and distributed ledgers, can bring much needed competitive pressures to bear on the incumbents by allowing newly formed fintech companies to enter the market, thus providing considerable benefits to the general public.

In the near future, assuming that newcomers understand banking and its role in society, and with the hope that regulators will finally allow competition between various business banking models, we expect to see hotly contested races between fractional reserve banks and narrow banks (NBs); digital cash and physical cash; fiat currencies and asset-backed cryptocurrencies; and, most importantly, centralized payment systems and distributed payment systems. The outcome of these races will reshape the entire financial ecosystem going forward. In a few years, it might change beyond recognition.

2. THE BANKING SYSTEM

2.1. Overview

Civilization is not possible without money and banking, and vice versa. For several centuries, banking provided the essential lubrication for the wheels of commerce. However, the very rapid technological developments of the last two decades have made the banking industry in its present form outdated. In addition, taken as a whole, it is no longer sufficiently profitable or attractive to investors [2]. This situation opens a unique opportunity for newcomers, armed with the latest technological tools, to compete with and potentially overtake incumbents, similar to the way Amazon is trouncing retail incumbents.

One of the biggest impediments in the path of unleashing creativity and developing new business models in banking, rather than mending existing legacy businesses, is the absence of successful open access Internet Protocols (TCP/IP) for money and identity. While TCP/IP are responsible for the phenomenal proliferation of the Internet, which inspired and promoted completely new business models in numerous fields such as commerce, social media, communications etc., banking lags far behind. Moreover, even though the aforementioned technical factor is important, another vital ingredient for developing a new banking infrastructure is missing: many fintech companies, especially in the crypto space, lack a proper understanding of finance in general, and money creation processes in particular. This absence of financial proficiency leads to unfulfilled naïve promises and false jump starts.

Thankfully, recent technological progress opens an avenue for rectifying this situation. Challengers with a sound command of technology and economics can change the system to the benefit of the general public.

2.2. Money

Through the ages, money existed in many forms, stretching from the early electrum coins of Phrygia, to the giant stones of Polynesia, the cowry shells of China, the paper money originating with Kublai Khan, the crypto currencies of today, and to everything in between. Numerous attempts to understand the true meaning of money and from whence it comes have been undertaken by rulers and their tax collectors, traders, entrepreneurs, laborers, economists, philosophers, standup comedians, and ordinary folks.

The Greek philosopher Aristotle articulated legal aspects of money, emphasizing the fact that money is linked to government and government to money, [7]:

> *"But money has been introduced by convention as a kind of substitute for need or demand; and this is why we call it money (νομισμα), because its value is derived, not from nature, but from law (νόμος), and can be altered or abolished at will."*

Nicholas Oresme associated money with information and certification rather than law *per se*, [40]:

> *"When men first began to trade, or to purchase goods with money, the money had no stamp or image, but a quantity of silver or bronze was exchanged for meat and drink and was measured by weight. And since it was tiresome constantly to resort to the scales and difficult to determine the exact equivalent by weighing, and since the seller could not be certain of the metal offered or of its degree of purity, it was wisely ordained by the sages of that time that pieces of money should be made of a given metal and of definite weight and that they should be stamped with a design, known to everybody, to indicate the quality and true weight of the coin, so that suspicion should be averted and the value readily recognized."*

Copernicus generally agreed with Oresme and articulated his requirements for sound money as follows, [51]:

> *"1. It must not be changed in value except after ripe deliberation by the government authorities … . 2. One single place must be chosen for the minting of the money which must be minted in the name of the entire country and not in the name of a single city. … 3. When the new currency is issued, the old currency must be de-monetized and withdrawn from circulation. … 4. It is essential to have an inviolable and unchangeable rule to mint only 20 marks and no more from a pound of silver, deducting only the quantity of silver necessary to cover the expenses of coinage. … 5. Too great a quantity of money must not be issued. … 6. All the different kinds of coins should be issued at the same time. …"*

The German sociologist Simmel emphasized that *"Money represents pure interaction"*, the renowned British economist Keynes pointed out that *"The importance of money flows from it being a link between the present and the future"*, while the American economist Kocherlakota argued that *"Money is memory"*, see [50], [25], [27].

Since late Mediaeval times, money has gradually assumed the form of records in various ledgers. This aspect of money is all important in the modern world. At present, the vast majority of money in circulation is nothing more than a sequence of transactions, organized in ledgers maintained by various private banks, and by central banks who provide the means (central bank cash) and tools (various money transfer systems) used to reconcile these ledgers.

The role played by money in modern society is multi-faceted. However, three main applications are beyond dispute:

- money is a medium of exchange and a means of payments in general, and taxes in particular;
- money is a store of value;
- money is a unit of account.

In fact, anything taken in lieu of tax eventually becomes money. In view of this fact, in a modern legally compliant economy, money has to be linked to identity one way or the other.

In addition, Graziani, [15], and Keen, [24], argue that in a monetary (as opposite to barter) economy:

- money has to be represented by a token;
- money has to be accepted as a means of final settlement of all transactions, which terminates all credit and debt relationships between the parties;
- money should not grant privileges of seigniorage to any agent making a payment, thus requiring the presence of a bank as a third party to any non-cash transaction.

Okamoto and Ohta, [39], succinctly articulated requirements for electronic money as follows:

- On-line payment - can be securely used online;
- Off-line payment - can be securely used off-line;
- Non-forgeability - cannot be copied and reused;
- Anonymity (or pseudonymity?);
- Transferability - can be transferred to others;
- Divisibility - can be subdivided as needed.

2.3. Credit Money Creation and Annihilation

The true nature of money creation and annihilation has been a heated topic of debate for a long time. Currently, the so-called modern monetary circuit theory provides the most convincing explanation of the process. The main conclusion of this theory is that money is created by commercial banks when it is lent to their clients, and destroyed by banks when it is repaid, while interest, which, in effect, comes from the next round of borrowing, stays in the system for good, see [4], [30], [35].[4] Unfortunately, understanding money creation and annihilation is far from trivial.[5] Even among prominent economists, confusion reigns supreme. Here is how Paul Krugman approaches the topic, [28]:

[4] In the case when a borrower defaults, money is not destroyed as expected but remains in the system forever, which is tantamount to forgery.

[5] An astute (if somewhat tangential) observation by Lord Palmerston (1784-1865) springs to mind: "The Schleswig-Holstein question is so complicated, only three men in Europe have ever understood it. One was Prince Albert, who is dead. The second was a German professor who became mad. I am the third and I have forgotten all about it."

> *"Here's my current thought: in some sense money is a really weird thing, which can look to individuals like a real asset - cold, hard, cash - but is ultimately, as Paul Samuelson put it, a "social contrivance", whose value is more or less conjured out of thin air. Mainstream macroeconomics acknowledges the weirdness - in particular, it makes heavy reliance on the ability of central banks to create more fiat money at will - but otherwise treats money a lot like ordinary goods. But that intellectual strategy doesn't come naturally to many people, so there's always a constituency for monetary cranks. "*

However, a quick reflection suggests that the above intellectual strategy causes some consternation principally because it makes no sense, not least because in the developed capitalist economy money is predominantly (but not exclusively) created by private banks - a fact of life, which mainstream macroeconomics stubbornly ignores. One can only repeat after Hegel, [14]: *"Das Bekannte überhaupt ist darum, weil es bekannt ist, nicht erkannt."*[6]

2.4. Bookkeeping and Transactions

In addition to their lending businesses, private banks perform ledger-maintaining and transactional functions for their clients. As part of these efforts, private banks play two very important roles, which central banks are not equipped to perform. They are the system gatekeepers, who provide know-your-customer (KYC) services, and system policemen, who provide anti-money laundering (AML) services. We argue that, in addition to the more obvious areas of application of distributed ledger technology (DLT), such as in digital currencies (DCs) including central bank issued digital currencies (CBDCs), DLT can be used to solve such complex issues as trust and identity, with an emphasis on the KYC and AML aspects. Further, given that all banking activities boil down to maintaining a ledger, judicious applications of DLT can facilitate trading, clearing and settlement, payments, trade finance, and so on. However, if applied without a clear understanding of the underlying business, DLT can make the situation even less satisfactory than it is at the moment.

2.5. Domestic and Foreign Payments

The hallmark of the current financial system is a long chain of middlemen engaged in moving money between a buyer and a seller, not least in the form of correspondent banks. Not surprisingly, middlemen thrive in most situations, especially when foreign exchange transactions are involved. The amount of various fees can easily reach 3% or more, which is a very meaningful amount for most participants[7]. Figure 1, adapted from [12], illustrates the payment and information flows for a typical credit card transaction percolating through the clearing and settlement systems. It shows that this system is very inefficient – in order to move money along just three arrows, multiple flows of information are needed. Besides, the actual settlement process takes place using a separate payment network such as Fedwire®.

[6] "Quite generally, the familiar, just because it is familiar, is not cognitively understood."
[7] For example, web-only retailers often see net margins from as low as 0.5% to 3.5%, see, e.g., [43], [44].

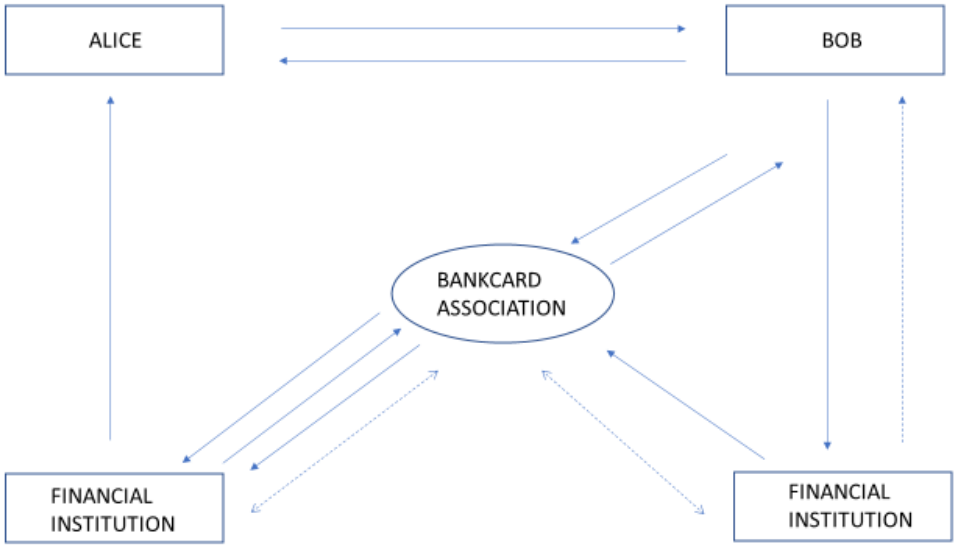

Figure 1. A typical credit card transaction between Alice (a buyer) and Bob (the seller). Alice pays Bob by using her credit card. Solid and dashed lines represent the flows of information and funds, respectively. Adapted from [12].

Needless to say, for foreign exchange payments the situation is even more complex and less satisfactory.

2.6. What is Wrong with the Current Setup?

The biggest issue afflicting the existing banking system is that it is overly complex because of the commingling of three distinct activities:

- creation and annihilation of credit money through lending;
- record keeping;
- execution of transactions.

It is clear that separating these activities is vital for making banking more nimble and efficient. We shall concentrate below on transactional aspects of banking and argue that a judicious use of DLT can be very helpful in bringing transactional banking into the 21st century.

First, we need to understand the inherent riskiness of the current fractional-reserve banking model. It stems from the fact that bank depositors are junior unsecured creditors, and therefore have the lowest priority in the event of a bank liquidation.[8] For small deposits, the danger of default is alleviated by insurance provided by the Federal Deposit Insurance

[8] Devaynes v Noble (1816) 35 ER 781.

Corporation (FDIC); however, for larger deposits, this is not an option. For instance, when in the summer of 2008 IndyMac Bancorp filed for bankruptcy, its large depositors lost a significant portion of their money.

Though the chance of a major bank collapse is not high, it is non-negligible either. By lending money, banks risk both their own capital and depositors' money. FDIC has deposit insurance funds of only $85 billion, which constitutes a little more than 1% of all existing deposits in the US.[9] FDIC funds are not sufficient to cover the losses of even one of the largest 23 banks in the US. In view of the above, one has to conclude that depositors implicitly subsidize banks by hundreds of basis points annually by not being paid interest covering their credit risks. During crises, bankers are acutely aware of the riskiness of banks and stop unsecured lending to each other, so that London Interbank Offered Rate (Libor) breaks. If banks, who understand the inner workings of their brethren, are reluctant to lend money to each other, why should depositors lend money to them for free?

3. Distributed Ledgers

3.1. General Considerations

IBM defines a distributed ledger as follows, [22]: "Blockchain is a shared, distributed ledger that facilitates the process of recording transactions and tracking assets in a business network. An asset can be tangible - a house, a car, cash, land - or intangible like intellectual property, such as patents, copyrights, or branding. Virtually anything of value can be tracked and traded on a blockchain network, reducing risk and cutting costs for all involved."

To appreciate the above definition, it is necessary to articulate the differences between centralized and distributed databases. The hallmark of a centralized database is that storage devices are all connected to a common processor; while in a distributed database, they are independent. Write access in a centralized database is tightly controlled; in a distributed database, many actors have writing privileges. As a result, each storage device maintains its own growing list of ordered records, which, if necessary for the sake of efficiency, can be organized in blocks, which explains the name Blockchain (BC). In a traditional centralized ledger, there is a designated gatekeeper, who collects, verifies, and performs the write requests of multiple parties, while in a distributed ledger (DL) these tasks are distributed. It is not always true that making these tasks distributed works best, since centralization has its undeniable benefits.

The utilization of the DL format requires some extra infrastructural provisions. Cryptography has to be used to maintain the integrity of DLs. Only parties possessing private keys can request updates to the relevant parts of the ledger. Miners (also called notaries) have to verify that users' requests are legitimate. After notarizing legitimate updates, miners broadcast these updates to the whole network, thus ensuring that all copies of the distributed database are in synch.

[9] See https://www.fdic.gov/bank/analytical/qbp/2017mar/qbpdep.html#1.

The idea of a BC is old, since BCs naturally occur whenever power, land, or property change hands. The genealogical trees of royal families are the earliest examples of BCs. Modern technology gives the old idea of BC a new lease of life. DLT opens new possibilities for making conventional banking and trading activities less expensive and more efficient by removing unnecessary frictions. Moreover, if built with skill, knowledge, and ambition, it has the potential for restructuring the whole financial system on new principles. We emphasize that achieving this goal requires overcoming not only technical but also epistemological and political obstacles.

In theory, BC-based payment systems can significantly reduce transaction costs to below 1% as they involve significantly fewer middlemen. For instance, Figure 2, adapted from [33], illustrates a typical bitcoin transaction and shows that the number of steps needed to execute a transaction is much smaller than in Figure 1. However, to do so in practice one needs to overcome several challenges, including regulation, scalability, privacy, and ease of use for all the relevant parties.

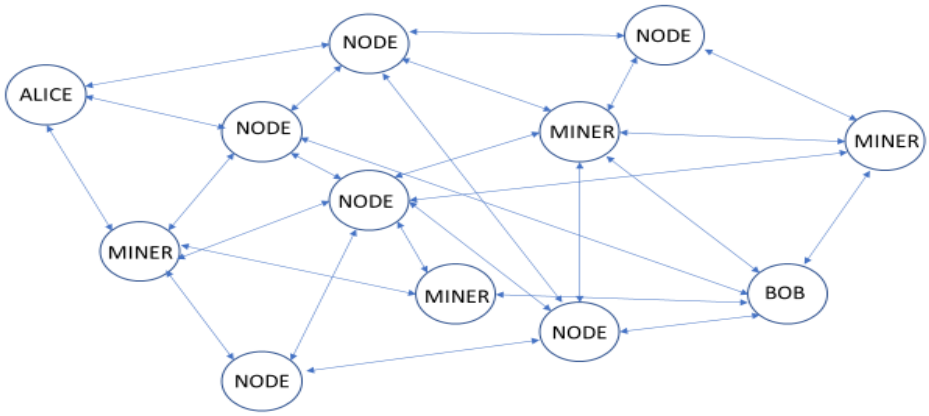

Figure 2. A typical Bitcoin transaction, between Alice (a buyer) and Bob (the seller). Alice broadcasts her intention to send some bitcoins to Bob to the entire Bitcoin network. Miners receive her announcement, verify that she has enough funds, and compete with each other to notarize it. The winning miner receives her reward, broadcasts the update to the entire network, and Bob's Bitcoin account is increased, while Alice's decreased.

Potentially DLT has numerous applications outside of payments. While DCs, including CBDCs, are an obvious venue, other possibilities including exchanges, payments, trade finance, rehypothecation, and syndicated loans, where frictions are particularly high, are attractive candidates as well. However, at present, many applications of DL and related technologies appear to be misguided. In some cases, they are driven by a desire to apply these tools for their own sake, rather than a clear superiority of the result. In other cases,

they are driven by a failure to appreciate that some current systems are shaped by business and other considerations much more than by pure technological reasons.

3.2. Types of Distributed Ledgers

There are several types of distributed databases or ledgers. We list them in increasing order of complexity:

- traditional centralized ledger;
- permissioned private DL;
- permissioned public DL;
- unpermissioned public DL.

To control the integrity of DL, a variety of mechanisms can be used—proof of work, which can potentially be accelerated by sharding or side chains, proof of stake, quorum verification by third parties, among numerous others, see, [38], [56], [42], [36], [48].

3.3. Cryptocurrency Creation and Transactions

Cryptocurrencies took the world by storm. Bitcoin (BTC), described in a seminal paper published in 2008 by Satoshi Nakamoto, [38], was the first in a very long line of cryptocurrencies.[10] A major reason for Bitcoin's initial appeal was the fact that its creation was purely algorithmic in nature. In short succession, Ethereum (ETH), a second-generation, secure, decentralized computing system, was introduced by Buterin [10] and Wood [54]. Ripple (XRP), which is not a derivative of Bitcoin and, for a good measure, not a real cryptocurrency, gained considerable popularity as well, Schwartz *et al.* [48]. Since then, literally thousands of native cryptocurrencies operating on their own purpose-built ledgers, as well as ERC-20 tokens built on top of existing blockchain platforms, have been launched with varying degrees of success.

3.4. What is Wrong with the Current Setup?

Since none of the existing blockchain ecosystems have banks worthy of the name, they have to rely on algorithmic monetary policies for cryptocurrency creation. Regardless of the statements of their creators, in essence, they resurrect, in one way or the other, old ideas of central planning, without fully appreciating the consequences. Moreover, somewhat counterintuitively, newly emerging DLT-based crypto ecosystems suffer from the same drawbacks as the current banking system, because they continue to commingle monetary creation (however primitive and ill-advised) with payments.

[10] *"Was this the face that launched a thousand ships/ And burnt the topless towers of Ilium?"* Christopher Marlowe, Doctor Faustus, Act V, Scene I.

Bitcoin, Ethereum and Ripple have all tried to fill the role of money, but have ended up as a new speculative asset class.[11] In spite of their technical achievements, existing cryptos do not solve the problem for at least four reasons:

- they are not stable enough, even for short transaction times, which prevents their usage for the purposes of conventional commerce;
- they are operationally inconvenient to use for an average economic agent, which is a prerequisite for their wide adoption as money;
- their built-in monetary policies are naïve, simplistic and inflexible;
- last but not least, they are not truly decentralized, while pretending to be so.

Indeed, the only way for an ordinary person to get a bitcoin is via an exchange, which actually adds rather than removes an extra middleman. Here is what the Goldman Sachs 2018 mid-year economic outlook report, [17], declares:

> *"Our view that cryptocurrencies would not retain value in their current incarnation remains intact and, in fact, has been borne out much sooner than we expected. ... We expect further declines in the future given our view that these cryptocurrencies do not fulfill any of the three traditional roles of a currency: they are neither a medium of exchange, nor a unit of measurement, nor a store of value."*[12]

Not surprisingly, the *status quo* in the cryptocurrency land is less than satisfactory.

4. Stable Coins and Their Taxonomy

4.1. Overview

Recent experience shows that all decentralized crypto coins are inherently unstable and thus unsuitable for commercial applications, see Figure 3.

[11] *"We wanted the best, but it turned out as always."* Viktor Chernomyrdin (1938-2010).

[12] Ironically, this view did not preclude Goldman from joining a number of other traditional financial players who have set up their own crypto trading desks.

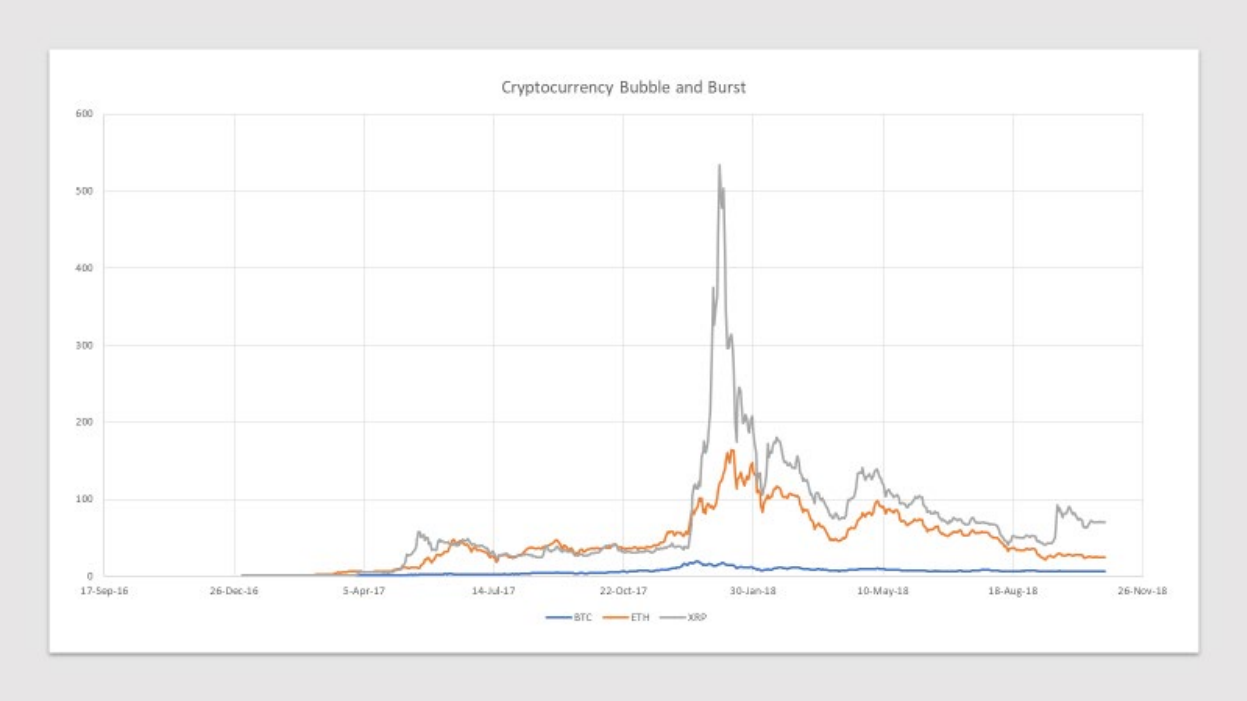

Figure 3. The spectacular rise and inevitable fall of BTC, ETH and XRP. All three are normalized to a value of one on January 1st, 2017.

Given this fact, it is not surprising that a lot of attention is being paid to designing stable crypto coins, which can play a role of tokenized cash. Stable coins come in several flavors. Below, we give a brief discussion of the most visible types.

It is clear that a properly designed stable coin can serve as the cornerstone of a fully digital ecosystem, facilitating fast payments on a commercial scale with minimal reliance on the existing banking system, yet doing so in a regulatory compliant fashion. Such a coin addresses the gaping hole in open access TCP/IP, [49]. A detailed discussion of technical issues related to TCP/IP and stable cryptocurrencies can be found in [20].

We argue that rather than designing monetary policy on its own, which is a challenging task in practice if not in theory, efficient applications of DLT should initially aim at tokenizing existing stable financial instruments denominated in fiat currencies, such as US dollars. Later on, if these efforts are successful, one should be able to tokenize more diverse asset pools, which can serve as a counterbalance to fiat currencies and be very useful for cross-border transfers.

In our estimation and contrary to numerous claims, it is not currently possible to build a truly decentralized stable coin. This is partly because the mere determination of the price of a crypto coin in terms of a fiat currency requires an oracle and automatically breaks decentralization. Such oracles are prone to manipulation and more importantly at odds with the claimed decentralized nature of the coin. Ideally, one should be able to directly observe this price from the blockchain in a distributed fashion. Unfortunately, at present it is not

quite possible for both conceptual and technical reasons.[13] Hence, any potentially successful stable coin has to combine centralized and decentralized features. The degree of centralization vs. decentralization can vary, as explained below.

4.2. Coins Fully Collateralized with Fiat

Custodial coins that are fully collateralized with fiat are relatively centralized as their creation and annihilation is performed by a single party. However, once a coin is created, and before it is destroyed, it can freely move on the corresponding blockchain. Given this semi-centralized design, custodial coins are particularly prone to regulatory influences. In view of this, they must be regulatory compliant in order to be able to survive. Several coins of this nature, including Tether (USDT) and TrueUSD (TUSD), either already exist or are currently being designed, see [47]. We briefly consider a representative example below.

It is easy to see why stable coins are necessary within the cryptocurrency universe. The vast majority of transactions occur on exchanges which are not fully integrated with the existing banking system.[14] Accordingly, having a stable token in order to get in and out of cryptocurrencies quickly and cheaply is a must. Thus, such tokens have been created in order to provide a link between the crypto universe and existing banking system.

However, all these coins have inherent drawbacks. By construction, they are centralized, so their issuers represent a single point of failure and an irresistible attraction for both regulators and hackers (for different reasons, obviously). Operationally, there is no transparency regarding underlying reserves, which makes it difficult for users to trust these coins. Typically, collateralized coins rely on third parties, most notably banks, to keep the corresponding collateral and execute transactions on their behalf, which makes their actual costs excessive and forces them to impose high transaction fees on users. Ironically, reliance on existing legacy banks brings to the forefront the issue of stability of the banking system itself, which an alternative crypto ecosystem is supposed to rectify in the first place.

Unless very carefully structured, fiat-backed coins suffer from high costs of carry for their collateral, which may require storage, transportation, insurance, etc. Low profitability is a major danger in its own right, which cannot be overestimated. For example, creators of custodial stable coins that are reliant on bank balance sheets to hold reserves have to pay a high price to effectively rent those balance sheets (and their capital buffers). This fact vastly reduces their cost-effectiveness, and requires a much larger issued base to reach profitable scale.

Tether is one of the earliest and best known custodial coins. It is issued on the Bitcoin blockchain through the Omni Layer Protocol [52]. As the name suggests, it is supposed to be linked to the underlying fiat currency, such as USD, by virtue of every tether in circulation

[13] Attempts to estimate the consensus price via the so-called Schelling point scheme are impractical at best, since there are no mechanisms to align this price with its external value.
[14] This is partly by necessity, and partly by design.

being collateralized with a dollar held in a dedicated bank account. While simple in theory, in practice the situation is extremely opaque, mostly because it is not known if the corresponding collateral actually exists, where it is held, or who administers it. It goes without saying that, in view of the above, Tether cannot be viewed as regulatory compliant. Besides, as per Tether's legal disclaimer: *"Beginning on January 1, 2018, Tether Tokens will no longer be issued to U.S. Persons."* Not surprisingly, all of the above issues resulted in USDT recently breaking the peg with the USD.

In spite of its glaring shortcomings, one very impressive feature of Tether emanates from its very nature as an essential instrument for speculators. Namely, USDT has an extremely high velocity. Although its capitalization is about sixty times smaller than Bitcoin, the dollar value of BTC and USDT traded per day is broadly comparable. For instance, on August 8, 2018 BTC capitalization and daily volume were $109 Billion and $4.9 Billion, respectively, while for USDT, they were $2.4 Billion and $3.3 Billion. Thus, the velocity of USDT is much higher than the velocity of either BTC or USD. Many observers believe that Tether is actively used to manipulate Bitcoin prices, see, e.g., [19], [29]

4.3. Coins Partially Collateralized with Fiat

Saga is one of a new breed of crypto currencies, which are characterized by time-varying degree of collateralization, starting their life as fully collateralized and eventually becoming fully free-floating [45]. In our opinion, such coins cannot be stable in the long run, regardless of the theoretical arguments put forward by their backers. History has been brutal to such schemes - the moment governments start to manipulate the gold content of their coinage, the value of their coins plummets precipitously. The story of the assignats, used as money during the French Revolution, illustrates this point with extreme clarity, see, e.g., [16]. In the 1970s inflation was triggered after the US dropped the gold peg. Paul Volcker eventually brought it under control by using all the tools available to the Fed, see [18]. It is clear that Saga does not have such tools at its disposal and hence is very prone to a death spiral. Saga's approach can be compared to someone building a sturdy table with four legs, and then, when everyone is happy with the table, starting to remove legs one by one, until the table collapses.

4.4. Coins Over Collateralized with Cryptos

An alternative approach to creating stable coins is to use unstable native crypto coins, specifically ETH, and smart contracts, which guarantee that stable coins, representing a sliver of the total, are massively overcollateralized. This collateral cushion is supposed to create a natural floor for the value of the coin. As with many other crypto ideas, this one can be traced back to conventional financial engineering concepts, specifically, trading on the margin and tranching of collateralized debt obligations (CDO). Under normal conditions, the corresponding coins are indeed stable; however, if there is a sudden drop in the value of the underlying asset, the value of the corresponding "derivative" coin will dip below par. Experience suggests that it is not even necessary for the actual breach of the floor to occur - a mere perception of such a possibility is sufficient to make coins value less than par. One does not need to go far in history for a real-life example - the global financial crisis of 2008

was caused to a large degree by the fact that super-senior CDO tranches lost most of their value, even though they did not suffer any losses due to the presence of a massive underlying buffer. This illustrates the point that market confidence, which is not explicitly taken into account by theoretical models, does play a crucial role in real life. The CDO tranches eventually functioned as designed, as did LTCM trades, which did not prevent their holders from going bankrupt in the interim.

It should be noted that over-collateralization is the opposite of conventional financial practice, such as trading on margin, which is based on the idea of under-collateralization.[15] It seems that many designers of new crypto-coins have totally forgotten why these coins were created in the first place.

In view of the above, crypto-collateralized coins have severe and obvious drawbacks. Since the price evolution of the underlying cryptos, such as ETH, is driven by a jump process, the floor can be breached in the event of a black swan, or more realistically, loss of confidence by the users. Thus, in spite of the fact that coins are over-collateralized, the underlying is so volatile that the peg is not guaranteed. In addition, over-collateralized coins suffer from the negative feedback loop, which arises because forced selling of collateral causes its price to decrease even faster than it would otherwise.

A typical example of stable value coins collateralized by other cryptocurrencies is MakerDai [8], issued by MakerDAO. MakerDai is supported by a very hefty collateral cushion. In the case when the floor is in danger of being breached, collateral is automatically liquidated by profit-seeking nodes, so that MakerDai stability is maintained. As was mentioned earlier, see footnote 15, the amount of collateral needed to keep the scheme going is so large that the underlying economics becomes very challenging.[16]

4.5. Dynamically Stabilized Coins

While the idea of dynamic stabilization of a coin contradicts common sense and historical experience, it has recently gripped the imagination of the investor community and hence is worth investigating in some detail. There are several obvious issues with algorithmically stabilized coins.

Monetary policies underpinning dynamically stabilized coins are derived from obsolete and outdated economic considerations. Either by necessity or by design these policies are vague and either unproven or actually proven by pre-crypto experiences not to work. At the end of the day, centralized mechanisms, such as a centralized reserve, have to be maintained to

[15] Thus, to get $1 worth of a stable coin, a user needs to have $2 or even $3 worth of ETH. This situation should be compared with the conventional margin trading, where a user can have an exposure of $10 worth of equities by posting $1 collateral (say).

[16] MakerDai is not unique in this regard. A typical smart contract requires so much collateral, that its underlying economic rationale is difficult to fathom.

ensure price stability anyway.[17] Historically, all the live projects have suffered drops in value, just breaking their stated *raison d'etre*. In addition, so far no one has been able to design trustless decentralized (price) oracles.

Basis is a representative example of such a coin, see [1]. Stripped of amenities, its algorithm works as follows. If the value of the coin is going up (a relatively easy case), then, not surprisingly, new coins are issued and distributed amongst the holders on a pro-rata basis. If the value of the coin is going down (a more complex case), then bond-like instruments are issued in exchange for coins, which are burned. As a result, the number of coins in circulation goes down and, in theory, their price increases. This is the essence of the concept of seigniorage, as proposed by Robert Sams [46]. When formulated as a cryptocurrency stabilization scheme, this algorithm sounds meaningful. However, if it is rephrased in more familiar terms, for instance, those of a company trying to keep its stock price constant, the algorithm shows its true colors. If the stock price increases, additional stock is issued, thus pushing the stock price down. When the stock price is falling, the company starts to sell bonds, and uses the proceeds to buy its own stock, thus pushing its price up. It is clear that this stabilization scheme represents yet another purely theoretical construction that cannot and does not work in practice, and will collapse when bonds come due - not to mention the fact that selling bonds in the middle of a market panic might be an insurmountable obstacle in the first place.

Algorithms of this type have been known for a long time. For example, Baron Munchausen is famous for using one when pulling himself and his horse out of a mire by his own hair. More recently, similar ideas were entertained by academic economists who proposed a mechanism for fixing the price of gold by a government in terms of its own fiat without keeping any gold in reserve [5]. Needless to say, even with all the coercion mechanisms at their disposal, no government was ever able to achieve such a feat. The probability of a crypto algorithm that lacks such mechanisms succeeding is even lower. Without going too far back in history, the current crisis of the Argentinian peso was accelerated by the increase of interest rates to 60%, which, according to the above theory, is supposed to arrest the currency freefall.

As an aside, the Quantity Theory of Money (QTM), which is used as a foundational concept underpinning Basis, has been discredited for decades, and does not pass scientific analysis, not to mention common sense [30]. The only saving grace is that a similar unflattering observation is true for the majority of traditional macroeconomic theories [31]. As was his habit, Keynes put it in characteristically pithy fashion:

> *"Practical men, who believe themselves to be quite exempt from any intellectual influence, are usually the slaves of some defunct economist. Madmen in authority, who hear voices in the air, are distilling their frenzy from some academic scribbler of a few years back"*

[17] See, e.g., Preson Byrne's blog: https://prestonbyrne.com/2017/10/13/basecoin-bitshares-2-electric-boogaloo/

4.6. Coins Collateralized with Assets

While in a stable economic environment it makes sense to collateralize crypto coins with fiat, in some parts of the world it is not a viable option since the local fiat itself is not stable enough. In these instances, coins collateralized with real assets come to the rescue. Recently, several such coins have been proposed by competing startups, including Digital Trade Coin (DTC) (of which the present author is a co-inventor), Oilcoin, Sweetcoin, Tiberiuscoin, etc., see, e.g., [34], [35], [53]. These coins have significant utility value for supply-chain financing and in well-defined trading environments, such as oil trading or cross-border financing. In addition, several authors convincingly argue that even in the presence of stable fiat, asset-backed coins have considerable advantages by limiting the freedom of central banks to manipulate their currencies, see, e.g., [34].

Fiat currencies, while undeniably useful, are not well suited to the needs of 21st century commerce, especially trade and supply chain finance because of high handling and exchange costs. In addition, the USD, being the world reserve currency, causes serious trade imbalances, which can trigger trade wars and exacerbate the international frictions. To alleviate these ills, several financial authorities have suggested that it makes sense to complement fiat currencies with a supranational currency, such as Spanish *Peso de Ocho*, or Austrian *Thalers*. This supranatural currency will be insulated from adverse actions by single central banks and other parties. By combining the ideas of narrow banking (for stability), digital currencies (for efficiency and transparency), and use of an asset-backed currency for international trade (to reduce trade distortions and inequality), we see the potential for dramatic improvement in the global financial system. Today, for the first time ever, there is a possibility of designing a digital supranational currency backed by a diverse and widely held assets. Such a digital currency could combine the best features of historical currencies, including finality of settlement, partial anonymity, and usability on the web.

Hayek, Keynes, Kaldor, and many other economists, advocated reforming the international monetary system by creating an independent international reserve currency, which remains stable in the long run and does not suffer from the inherent deficiencies of credit-based fiat national currencies, [21], [26], [23].

Zhou Xiaochuan, Governor of the People's Bank of China, advocated the need for such a currency as follows, [55]:

> *"I. The outbreak of the crisis and its spillover to the entire world reflect the inherent vulnerabilities and systemic risks in the existing international monetary system. II. The desirable goal of reforming the international monetary system, therefore, is to create an international reserve currency that is disconnected from individual nations and is able to remain stable in the long run, thus removing the inherent deficiencies caused by using credit-based national currencies. III. The reform should be guided by a grand vision and begin with specific deliverables. It should be a gradual process that yields win-win results for all."*

Recently, an MIT team (of which the present author is a member) have designed an asset-backed digital currency called DTC that is believed to be well suited as a medium of trade and exchange for groups of smaller nations or supranational organizations. DTC is largely immune to policies of central banks controlling the worlds' reserve currencies, and consequently has enormous potential to improve the stability and competitiveness of trading and natural resource producing economies. DTC can serve as a much-needed counterpoint for todays' fiat currencies, and a way forward toward ensuring world-wide financial stability and inclusion, see [34], [35].

4.7. Narrow Banks as Emitters of Digital Cash

In many countries, including the US, cash still plays a major role in the economy. Debit cards, which combine digital and physical aspects of cash, are popular as well. The Fed 2015 Diary of Consumer Payment Choice, [13], observed:

> *"Cash continues to be the most frequently used consumer payment instrument. Cash is widely used in a variety of circumstances. Cash dominates small-value transactions. The average value of cash holdings has grown."*

Similarly, Yves Mersch, Member of the Executive Board of the ECB, in a speech given on 14 February 2018, [11], concluded:

> *"I will conclude by saying that printed euro banknotes will retain their place and their role in society as legal tender for a very long time to come. There is no viable alternative to euro cash. There is good reason to believe that banknotes don't only have to take the form of printed paper, cotton or polymer. However, printed banknotes will remain our core business. And if there is public demand for digital central bank money, this should only be a technical variant of cash."*

While cash is facing competition from other payment instruments[18], results of numerous studies suggest that it remains a resilient form of payment, playing a key and unique role for consumer transactions and other purposes. The amount of currency in circulation, which includes paper currency and coin held both by the public and in the vaults of depository institutions grows at a healthy pace. While the quantity of currency increases steadily, its velocity currently decreases, meaning that money is being used in a less efficient manner. The velocity of money is the number of times a unit of money is spent to purchase goods and services per unit of time, say quarterly. Increasing velocity of money implies that more transactions are occurring between economic agents, while decreasing velocity indicates the opposite.

[18] At the same time, cash is facing competition from other payment instruments. For instance, between 2012 and 2015, the percentage of consumer transactions made with cash decreased by eight percentage points, from 40 to 32 percent. This can be explained by increasing consumer comfort with payment cards and the growth of online commerce.

The absence of physical cash would alleviate societal ills, such as crime, drug trafficking and the like, or, at least, make them more difficult to conduct. It would lubricate the wheels of commerce and help the unbanked to become participants in the digital economy through the use of smartphones, benefitting society at large. On the flip side, with cash abolished, interest rates could be set as negative as central bankers liked; rates would be determined only by policy makers.

A properly constructed NB issuing its own digital currency is a much more palatable and practical solution than CBDC by allowing access to full collateral at any time. This suggests that digital currencies, issued by NBs, could become competitive with fiat currencies for everyday use. Such alternative currencies have a long history of usefulness for smoothing bumps in the financial environment, and if backed by a NB could avoid the bankruptcy problems that have traditionally plagued alternative currencies.

NBs keep all depositors' money as liquid cash deposited with a central bank or liquid government bonds, becoming thereby necessary stabilizers and facilitators of the overall global financial system. There is an acute need for such stabilizers after the GFC, which resulted in a massive concentration of assets in a handful of systemically important banks, thus making the overall financial system less robust. In addition to steadying the whole banking sector, NBs naturally perform the role of record keepers in the economy, while refraining from issuing loans. The Great Depression of 1929 made banks' inability to meet their obligations painfully obvious and brought the idea of a NB to the forefront. Although a practical conversion of fractional reserve banks into NBs was rejected in the forties under enormous political pressure from fractional reserve banks, the idea has always stayed close to the surface, and gained considerable momentum during and after the S&L crisis in the 1980's and 1990's. Not surprisingly, it gained traction again after the GFC. Further details are given in [3], [33], [41].

Several approaches for designing a NB have been summarized in the literature, see, e.g. [41]:

- 100% Reserve Bank (C-PeRB): Assets - central bank reserves and currency. Liabilities - demandable deposits and shareholder equity. Depending on the circumstances, these deposits can either be non-interest-bearing, or interest paying, or interest charging. The latter setup might be necessary if the interest rate paid by the central bank is negative. C-PeRB is financed by a combination of deposits (debt) and shareholders' equity.
- Treasury money market mutual fund (TMMMF): Assets - Treasury bills or repurchase agreements collateralized by Treasury bills. Liabilities - demandable equity shares having a proportional claim on the assets. TMMMF is financed solely by equity.
- Prime money market mutual fund (PMMMF): Assets - short term Federal agency securities, short-term bank certificates of deposits, bankers' acceptances, highly rated commercial paper, and repurchase agreements backed by low-risk collateral. Liabilities - demandable equity shares having a proportional claim on the assets. As before, PMMMF is financed solely by equity.

A detailed design for a NB, including its international dimensions, is given in the Patent Application [6].

4.8. Mixing and Tumbling

Early on, it was recognized that Bitcoin does not provide true anonymity of transactions. While at first glance it would seem this is an issue only for those participants engaging in some sort of nefarious activity, a little reflection indicates that honest participants require enhanced anonymity too. For instance, if a merchant payee has a known public address, all its competitors will gain valuable business insight about the payee's financial well-being by monitoring its transactions on a public blockchain. Likewise, a payer with a large amount of stable tokens will automatically attract unwanted attention. Thus, a reasonable level of anonymity is required for perfectly legitimate reasons. While some approaches involve building distributed ledger designed around enhanced anonymity such as Z-cash, we find them too radical to use in a regulatory-compliant framework. A suitable mixing service is more appropriate, see, e.g., [37].

Given that some centralization is built in to fiat-backed cryptocurrencies from the start, it is natural to benefit from it, and use sponsors as a mixing service. Upon request, they will allow routing of payments via blockchain addresses under their control in a way which will make the central source of funds impossible to deduce for other economic agents. It goes without saying that legitimate authorities that provide a legally binding demand will be able to trace the flow of funds with the same ease as if mixing was not applied. This approach is designed to solve the anonymity problem for payers. For payees it is solved by using the ring key construct. Recall that by using ring keys one can prove that a transaction was signed within a group of addresses without determining a specific signatory.

4.9. KYC and AML Considerations

The importance of KYC and AML requirements for regulatory compliance cannot be overestimated. It is necessary to perform KYC/AML procedures when new tokens are issued or existing redeemed for fiat. Third-party services can be used for these purposes. In principle, KYC is a relatively inexpensive operation, which costs about $0.50 per person. These procedures can be strengthened further, because the exchange of fiat currencies into stable tokens and *vice versa* uses existing bank accounts, whose owners have passed the standard KYC procedures performed by their banks.

Given that stable tokens will circulate on the Ethereum blockchain, and subsequently on other blockchains, all of which keep an immutable record of all transactions, AML can be performed indirectly by analyzing the corresponding transaction social graph. In this regard, stable token transactions are more transparent than conventional physical cash transactions, and are on a par with traditional banking transactions.[19]

[19] It is worth noting that when Bitcoin and Ethereum had just been introduced, criminal elements were extremely excited about illicit usage of cryptocurrencies. However, with time, they realized that the

4.10. Privacy

There is serious hazard of widely used stable tokens being monitored by a repressive surveillance state. If high volumes of cash transactions are completed on a blockchain, then the government can track a considerable portion of its citizens' payments and exert unprecedented control over their lives. To avoid this situation, small cash-like financial transactions must be anonymous, with exceptions to this anonymity allowed in serious criminal investigations or similar situations. When there is an overriding social imperative to override this anonymity, it could be done by using legal court orders and similar tools. Development of the suitable legal infrastructure is of paramount importance for the successful usage of stable tokens as medium of exchange.

5. CONCLUSIONS

In this paper, we discussed the current state of the crypto land and argued that stable crypto tokens, which can be viewed as an electronic analogue of cash, can help to augment the existing TCP/IP with a much-needed mechanism in order to bring existing banking and payment systems into the 21st century. We described three existing approaches to designing such tokens – fiat collateralization, cryptocurrency collateralization, dynamic stabilization – and concluded that only regulatorily compliant fiat-backed tokens are viable in the long run. We also discussed asset-backed cryptocurrencies and argued that in some instances they can provide a much-needed counterpoint for today's fiat currencies, and pave a way forward toward ensuring world-wide financial stability and inclusion.

I am deeply grateful to my MIT colleagues Prof Sandy Pentland and Dr Thomas Hardjono, to my Sila Money partners Shamir Karkal, Angela Angelovska-Wilson, and Isaac Hines, and to my Numeraire Financial colleagues Marsha Lipton and Stewart Inglis for extremely useful and insightful discussions of the topic covered in this paper.

6. GLOSSARY

Algorithmically stabilized cryptocurrency: A cryptocurrency whose price is pegged to fiat by virtue of an algorithmic monetary policy "emulating" conventional monetary policies of central bank.
Anti-money laundering (AML): A set of procedures, laws, and regulations designed to stop generating legal income through illegal actions; AML laws have profound implications for financial institutions and intermediaries.
Asset-backed stable cryptocurrency: A cryptocurrency whose price is pegged to a collateral pool in the form of real assets, such as gold, oil, etc.

immutable record of transactions has opened new avenues for law enforcement agencies to monitor and prosecute their activities. Hence, at present, they are tending back to cash transactions.

Continuous audit of reserves: The process conducted by a third party on behalf of the issuer of any collateralized digital token, proving that assets held by the issuer are equal to or greater than their liabilities, which are calculated from the blockchain exposure.
Cryptocurrency: any open source, cryptographically secured, blockchain-based token. See: http://en.wikipedia.org/wiki/Cryptocurrency
Cryptocurrency platform: A collection of software, hardware and processes supporting the functioning of a cryptocurrency.
ERC-20 token: Tokens designed and used solely on the Ethereum platform; these tokens are standardized, so that they can be shared, exchanged for other tokens, or transferred from one crypto-wallet to another.
Fiat currency: Currency issue by the central bank of a country or a union of countries.
Fiat-backed stable cryptocurrency: A cryptocurrency whose price is pegged to a collateral in the form of fiat currency.
Know-your-client (KYC): A set of procedures used by banks and other financial intermediaries to avoid being used by criminals for money laundering activities and other illegal activities
Mixer or tumbler: A service used to mix potentially identifiable cryptocurrency transactions with others, in order to obscure the original source of funds; they are used to improve the anonymity of cryptocurrencies, which provide a public ledger of all transactions.
Money market mutual fund (MMMF): An open-ended mutual fund that invests solely in short-term debt securities such as short-dated US Treasury bills and commercial paper; safety profiles of most (but not all) of these funds and bank deposits are comparable.
Narrow bank (NB): A proposed type of bank (also called a safe bank), which holds only central bank cash and liquid and short-dated government bonds; such a bank does not issue any loans (except to the government).
Proof of stake (PoS): An algorithm allowing miners to compete against each other based on the amount of coins they possess, in order to add new blocks to the chain and be rewarded.
Proof of work (PoW): An algorithm requiring miners to compete against each other based on the amount of the computational power they possess, in order to add new blocks to the chain and be rewarded.
Quantity theory of money (QTM): A theory which postulates a direct relationship between the quantity of money in an economy and the level of prices for goods and services.
Seniorage: An algorithm using smart contracts to expand and contract the supply of the price-stable currency, trying to emulate the real-life monetary policies of a central bank.
Treasury money market mutual Fund (TMMMF): a MMMF, which invests solely in U.S. Treasury securities, and seeks to provide current income while preserving shareholders' principal.
Utility-backed cryptocurrency: A cryptocurrency which derives its value partially from its real (or perceived) utility, and partially for speculative reasons.
Velocity of money: The number of times a unit of money is spent to purchase goods and services per unit of time.

7. REFERENCES

1. Al-Naji, N., Chen, J., and Diao, L., 2018. Basis: A Price-Stable Cryptocurrency with an Algorithmic Central Bank. White Paper. https://www.basis.io/basis_whitepaper_en.pdf.
2. Begenau, J., and Stafford, E., 2018. Do Banks Have an Edge? SSRN: https://ssrn.com/abstract=3095550
3. Benes, J. and Kumhof, M., 2012. The Chicago plan revisited. Washington, DC: International Monetary Fund.
4. McLeay, M., Radia, A., and Thomas, R., 2014. Money Creation in the Modern Economy. Bank of England Quarterly Bulletin 2014 Q1. SSRN: https://ssrn.com/abstract=2416234
5. Black, F., 1981. A gold standard with double feedback and near zero reserves. Sloan School, MIT.
6. Burkov, S., Dembo, R., and Lipton, A., 2017 Account platform for a distributed network of nodes. U.S. Patent Application.
7. Crisp, R. (Ed.), 2014. Aristotle: Nicomachean Ethics. Cambridge University Press.
8. Dai, 2017. The Dai Stablecoin System, December 2017, https://makerdao.com/whitepaper/DaiDec17WP.pdf
9. Danezis, G. and Meiklejohn, S., 2015. Centrally banked cryptocurrencies. arXiv preprint arXiv:1505.06895.
10. Ethereum, 2018, A Next-Generation Smart Contract and Decentralized Application Platform. White Paper. https://github.com/ethereum/wiki/wiki/White-Paper.
11. European Central Bank, 2018. The role of euro banknotes as legal tender. Speech by Yves Mersch, Member of the Executive Board of the ECB, at the 4th Bargeldsymposium of the Deutsche Bundesbank, Frankfurt am Main, 14 February 2018.
12. Federal Financial Institutions Examination Council, 2016. Retail Payment Systems. It Examination Handbook.
13. Federal Reserve Bank of San Francisco, 2015. Cash Continues to Play a Key Role in Consumer Spending: Evidence from the Diary of Consumer Payment Choice.
14. Findlay, J.N., and Miller, A.V., 1977. Hegel's Phenomenology of spirit. Oxford University Press.
15. Graziani, A, 2003. The monetary theory of production. Cambridge University Press.
16. Goetzmann, W.N., 2017. Money changes everything: How finance made Civilization possible. Princeton University Press.
17. Goldman-Sachs Investment Strategy Group, 2018. Taking stock of our 2018 outlook: (un)steady she goes.
18. Goodfriend, M. and King, R.G., 2005. The incredible Volcker disinflation. Journal of Monetary Economics, 52(5), pp.981-1015.
19. Griffin, J.M. and Shams, A., 2018. Is Bitcoin Really Un-Tethered? Working Paper.
20. Hardjono, T., Lipton, A. and Pentland, A., 2018. Towards a Design Philosophy for Interoperable Blockchain Systems. arXiv preprint arXiv:1805.05934.
21. Hayek, F.A., 1943. A commodity reserve currency. The Economic Journal, 53(210/211), pp.176-184.
22. Gupta, M., 2018. Blockchain for Dummies. 2nd IBM Limited Edition. John Wiley and Sons, Inc.

23. Kaldor N. 2007 Causes of growth and stagnation in the world economy. Cambridge University Press.
24. Keen, S., 2015. What is money and how is it created? Forbes. https://www.forbes.com/sites/stevekeen/2015/02/28/what-is-money-and-how-is-it-created/#61ab998c7df4
25. Keynes, J.M., 1936. The general theory of employment, interest, and money. London: Macmillan.
26. Keynes, J.M., 1943. The objective of international price stability. The Economic Journal, 53(210/211), pp.185-187.
27. Kocherlakota, N. R., 1998. Money is memory. Journal of Economic Theory, 81(2), pp. 232-251.
28. Krugman, P., 2015. There's Something About Money (Implicitly Wonkish), The New York Times, 02.10.2015.
29. Leising, M., Rojanasakul, M., Pogkas, D. and Kochkodin, B., 2018 .Crypto Coin Tether Defies Logic on Kraken's Market, Raising Red Flags. Bloomberg.
30. Lipton, A., 2016. Modern monetary circuit theory, stability of interconnected banking network, and balance sheet optimization for individual banks. International Journal of Theoretical and Applied Finance, 19(06), p.1650034.
31. Lipton, A., 2016. Macroeconomic theories: Not even wrong. Risk, 30(09), p. 29.
32. Lipton, A., 2018. Blockchains and distributed ledgers in retrospective and perspective. The Journal of Risk Finance, 19(1), pp. 4-25.
33. Lipton, A., Hardjono, T. and Pentland, S. 2018 Narrow banks and fiat-backed digital coins. Capco Journal 47: Digitization, pp. 101-116.
34. Lipton, A., Hardjono, T. and Pentland, A., 2018. Digital trade coin: towards a more stable digital currency. Royal Society Open Science, 5(7), p.180155.
35. Lipton, A. and Pentland, A., 2018. Breaking the bank. Scientific American, 318(1), pp. 26-31.
36. Mazieres, D., 2015. The stellar consensus protocol: A federated model for internet-level consensus. Stellar Development Foundation.
37. Meiklejohn, S. and Mercer, R., 2018. Möbius: Trustless tumbling for transaction privacy. Proceedings on Privacy Enhancing Technologies, 2018(2), pp. 105-121.
38. Nakamoto, S., 2008. Bitcoin: A peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf
39. Okamoto, T. and Ohta, K., 1991. Universal electronic cash. In: Annual international cryptology conference, J. Feigenbaum editor. Springer, Berlin, Heidelberg, pp. 324-337.
40. Oresme, N., 1956. The De Moneta of Nicholas Oresme, and English Mint Documents: Translated from the Latin with Introduction and Notes by C. Johnson. Nelson.
41. Pennacchi, G., 2012. Narrow banking. Annual Review of Financial Economics, 4(1), pp. 141-159.
42. Raiden, 2018. Raiden Network Documentation. https://raiden-network.readthedocs.io/en/stable/
43. Rigby, D., 2014. Online shopping isn't as profitable as you think. Harvard Business Review.
44. Ross, S., 2018, What's normal for profit margin in retail sector? Investopedia.
45. Saga, 2018. Saga. White Paper. https://www.saga.org/files/saga-whitepaper.pdf

46. Sams, R., 2015. A Note on Cryptocurrency Stabilization: Seigniorage Shares. Brave New Coin, pp. 1-8.
47. Schor, L., 2018. Stablecoins Explained. https://medium.com/@argongroup/stablecoins-explained-206466da5e61
48. Schwartz, D., Youngs, N. and Britto, A., 2014. The Ripple protocol consensus algorithm. Ripple Labs Inc White Paper.
49. Sila, 2018. Sila: a Stable Fiat-Backed Digital Tokenized Means of Exchange. White Paper.
50. Simmel, G., 2004. The philosophy of money. Routledge.
51. Taylor, J., 1955. Copernicus on the Evils of Inflation and the Establishment of A Sound Currency. Journal of the History of Ideas, 16(4), pp. 540-547.
52. Tether, 2016. Tether: Fiat currencies on the Bitcoin blockchain. White Paper. https://tether.to/wp-content/uploads/2016/06/TetherWhitePaper.pdf
53. Tiberiuscoin, 2017. Tiberiuscoin. White Paper. https://www.tiberiuscoin.com/wp-content/uploads/2018/06/Tiberius-Coin-White-Paper-v3.4.1.pdf
54. Wood, G., 2015. Ethereum: A secure decentralised generalised transaction ledger homestead revision. Yellow Paper. http://gavwood.com/paper.pdf.
55. Zhou X. 2009. Reform the International Monetary System. Basel, Switzerland: Bank of International Settlements.
56. Zilliqa, 2018. The Zilliqa project: a secure scalable blockchain platform. Position Paper. https://docs.zilliqa.com/positionpaper.pdf