‘Global Stablecoin’ Challenges: Response to FSB Consultation Document

Summary

Serviceable Recommendations, Bad Taxonomy

The consultative document contains serviceable “High-Level recommendations to address the regulatory, supervisory and oversight challenges raised by [certain monetary] arrangements”, subject to four regulatory suggestions (pgs. 24, 27) and one set of policy suggestions (pg. 2).

Unfortunately, the ontological domain the recommendations are intended to address is misconceived. Compounding this, the analysis is biased toward, indeed predicated upon, a particular technical approach to implementing the functions and activities of such media – one that may prove to be nothing more than a trendy, but ultimately discredited and abandoned, fad[1]. Viewing the challenge through this combination of distorted lenses has resulted in a deeply flawed taxonomy which should be scrapped outright.

The relevant ontological domain, the “arrangements” that warrant consideration, are those pertaining to the prospect of privately issued (digital) moneys, especially those which might, if permitted, attract international usage for payments. A proposed alternative set of defined terms is provided in Appendix 5.

Willful blindness

There is also a noteworthy irony in the fact that this document highlights efforts to discover appropriate regulation and oversight for media that, other than a remarkably bizarre exceptional category (examined below), at least entail ‘backing’ with assets of some sort – while ignoring the thousands of unbacked (play money and/or unregistered securities) ‘cryptocurrencies’, the most prominent of which owed their creation and emergence to their creators’ overt intent to defy government authority[2], particularly in relation to their provision of powerful anonymity features. This phenomenon of blockchain and so-called Distributed Ledger Technology (DLT)—effectively celebrated and legitimized by this consultative document—has resulted, arguably, in a lost decade of unprecedented malinvestment and rampant criminality. Moreover, in addition to giving the scofflaw creators and promoters of such media a pass (no oversight there!) the document even contemplates models whereby these unbacked anonymous media themselves might serve as the backing for so-called stablecoins. This is a bad idea that should not be countenanced by the FSB.

Facebook/Libra/Novi

It is painfully obvious that the current impetus and sense of urgency on the part of regulators and policy officials to cobble together this consultative document reflects an effort to come to grips with the prospect of Facebook/Libra (and now Novi). The very term “Global Stablecoin”, *the designated topic* examined in this consultative document. was ‘coined’ specifically for this purpose.

[1] Ironically, even Facebook’s new Novi scheme appears likely to employ a “Hosted Wallet” arrangement in which P2P transfers are “off-chain”…meaning that all of the “blockchain” and “DLT“ noise of Libra has practically nothing to do with Facebook’s current strategy to provide in-app payments to its billions of Monthly Active Users (MAU).

[2] This is articulated constantly, though typically glossed over. A recent example by one of Bitcoin’s perennial cheerleaders in Forbes: “Bitcoin has increasingly been adopted by Wall Street and the world's biggest financial institutions since its 2017 price explosion but remains a tool to fight government control”.

It is a certainty that, sooner or later, privately issued brands of money will emerge that attract such significant international usage for payments as to potentially exert systemic effects.

Facebook/Libra/Novi may (or may not) be one of them and, given the fact that Facebook is the prime mover behind the Libra Association, its emergence could pose entity-specific risks. I will therefore explore Facebook/Libra/Novi-specific considerations. To preview however, the key to forestalling a potential Facebook/Libra/Novi nightmare scenario will not lie in embedding tricky de facto Libra-specific poison pills in the needed international framework. Instead, the key will be to be prepared for the lawyered-up stratagems Facebook/Libra/Novi will deploy to make a mockery of whatever privacy, anti-trust and possibly AML/CFT safeguards you come up with.

Forest and trees

I will argue that Facebook/Libra and, in reaction, the FSB, G20, BIS, IMF, BoE and all the rest of you have lost the plot with this "global stablecoin" lingo. The real issue that needs to be addressed is privately-issued money and in particular its role in cross-border payments. Central bank sponsored initiatives examining this area have so far been barking up the wrong tree and the needed breakthrough may well require one or more well-conceived private sector entities, offering alternatives to SWIFT that would extend the efficiencies possible with domestic single-currency clearinghouses to cross border payments.

Indeed, the FSB has articulated[3] the imperative of 'enhancing cross-border payments', going so far as to ask: *"How can the public and private sectors help to catalyse improvements…"* and *"Are there initiatives that public authorities could take to enhance key payment infrastructures…?"*. It may be that one or two authorities will lead on initiatives that indeed help to catalyse projects by such well-conceived private sector entities for such new infrastructures by (a) streamlining regulatory frameworks, especially cross-border; (b) issuing 'challenges', i.e. inviting, publishing and validating proposals, aligned with those streamlined framework(s); and (c) supporting the creation of structures within existing regional/international fora to facilitate wider collaboration, engagement and adoption.

As long as such entities—any of which would be fine with seeking licensing or official permission to operate in multiple jurisdictions, and operating in conformity to such—have no clear path for developing and deploying infrastructure utilities that could be transnational, you are playing into the hands of the un-backed unsound cryptocurrency mongers who seemingly have no need to concern themselves with such niceties as regulatory approval.

Crypto-conceits

As suggested above, the presumption that blockchain and/or so-called Distributed Ledger Technology (DLT) comprise the apotheosis of human technical progress may be invalid. I will offer an alternative, more critical, assessment of the foundational dogmas of crypto-this'nthat. See Appendix 1: Debunking Blockchain and DLT.

Algorithmic chicanery

There is an additional grave flaw in the consultation document, so egregious as to call into question the competence of regulatory authorities who seek to take on responsibility to ensure the effectiveness of "risk management frameworks…with regard to reserve management [and other] requirements." It is the

[3] FSB: 'Enhancing Cross-border Payments - Stage 1 report to the G20', Apr 2020

blithe acceptance of the fraudulent conceit that an exchange rate peg to any designated external anchor asset might be sustainably maintained by "algorithmic" means and/or with an insolvent balance sheet (i.e. partial "backing"). An already deployed implementation of this worse-than-Ponzi scheme 'confidence game' will be examined for purposes of illustration.

Flawed Ontology leads to bad taxonomy

The consultative document, while rightly acknowledging "public policy goals are meant to be technology neutral" adopts a taxonomy that is anything but. The classification scheme and defined terms set forth in the consultative document all derive from two misconceived ontological distinctions, the first of which is premised on unrecognized advocacy of what may be nothing more than a technological fad:

- Account-based vs. token-based money,
- Virtual/digital as a meaningful and/or appropriate criterion for distinguishing government-issued from privately-issued money.

Account-based vs. token-based money

Brunnermeier et al[4], following Kahn and Wong, recites:

"There are two main forms of money: account-based money and token money."

Kahn, Rivadeneyra, Wong[5] express this distinction as:

"Many of these new systems are "token-based" – that is, they rely on identification of the object being transferred as a means of payment rather than relying on identification of the individual whose account is being debited"

And Kahn[6] elaborates:

"It has long been noted that payments arrangements can, generally speaking, be divided into two categories: token-based and account-based systems. The fundamental distinction between the two is identification requirements. In a token-based system, the thing that must be identified for the payee to be satisfied with the validity of the payment is the "thing" being transferred – "is this thing counterfeit or legitimate?" In an account-based system, however, the identification is of the customer – "Is this person who he says he is? Does he really have an account with us?"

Before digging into this alleged account vs. token distinction—which is foundational to the whole ontological/taxonomic edifice that has resulted in this consultative document focused on "stablecoins" as a category of global regulatory attention—it is instructive to note how the high priests of Libra use the terms. The "The Libra Blockchain" technical protocol exclusively uses the word "account(s)" (116 occurrences) and eschews usage of the word "token" (0 occurrences, in any form of the word). (It does however make liberal use of the word "coin(s)" – in every case using it to reference some particular brand of money).

[4] Brunnermeier, 2019; "THE DIGITALIZATION OF MONEY"; NBER Working Paper 26300;

[5] Kahn, Rivadeneyra, Wong, 2018; "Should the central bank issue e-money?"

[6] Kahn, 2016: "How are payment accounts special?"

Token-based vs. account-based is a non-difference. The crypto community, in Emperor's New Clothes[7] fashion, has imprinted credulous less-techie people with the meme that their digital "tokens" are self-contained embodiments of value, analogous to the (anonymous) physical tokens—currency[8], i.e. paper cash and coins—issued/minted by government monetary authorities.

In both 'cases' (account or so-called token), the "thing" or "object" being transferred is a payment instruction, designating payment amount and recipient payment coordinates. Verification of identity—though it may or may not have been a prerequisite to obtaining access credentials for the transaction system/network, depending on whether participation rights are granted on a permissioned basis—does not come into play in the processing and execution of particular transactions. What matters is whether the payment instruction can be authenticated and processed in accordance with the requirements of the system. In both cases, if the instruction is authenticated and the transaction persisted to whatever sort of ledger the system is organized around, some balance—whether styled as a 'wallet' or an 'account' balance—of the recipient/beneficiary of payment will be incremented.

Suppose a system is established that involves all the latest flashy blockchain or DLT atmospherics (perhaps, like >268,000 other brands of 'tokens', it implements the ERC-20 token protocol) but the system is implemented as to require a permissioned wallet tied to a rigorous identity verification and due diligence system. (For example, perhaps the participant's access key must be cryptographically signed by the administrative entity responsible for granting system access permissions as a prerequisite to its activation). Does this mean it has become an account-based system?

Moreover, consider Kahn's notion that entails the payee making a judgment as to whether the thing/object—whatever it is, whether some self-embodied quantum of value or a payment instruction—is non-counterfeit. Payment instructions, whether or not styled as tokens, are not transmitted to the recipients/beneficiaries of payment for evaluation, processing and execution. They are transmitted to some system which is external to the client software on the beneficiary's device, where, if they can be authenticated as valid in accordance with the technical protocol and business rules of that system, are persisted to a ledger resulting in an increment in some balance of the recipient/beneficiary. All that the recipient sees is a notification that payment has been received.

Additional absurdity comes into play in relation to the recipient/beneficiary being able to rely on the notification – whether she is "satisfied" with its validity[9]. Suppose the recipient/beneficiary is a merchant who must determine whether to release goods/services for delivery on the strength of the notification received. With Bitcoin, the ur-crypto where all this token-babel began, a recipient needs to wait until the payment is six blocks deep on the blockchain, an interval of about an hour, to warrant sufficient confidence the payment will not be reversed. Contrast that to the historic counterexample involving an overtly account-based system set forth in Appendix 3. This system, a full decade prior to Bitcoin, provided

[7] Or, more aptly—given the decades-long role of the self-styled "cypherpunks" in promoting "crypto" this and that, most recently blockchain and DLT—'the cool kids' new clothes'.

[8] See discussion below of the FinCEN 2013 exercise in sophistry involving "virtual currency"

[9] Note also how Kahn is concerned with the payee being satisfied in his token litmus test, while the provider of the payment account, presumably the financial institution, is glibly substituted in the last sentence. But neither perspective is relevant to whether the payment instruction is executed. That is strictly dependent on whether the authentication credentials being presented to the authentication protocol pass muster, regardless of who or what might be presenting them.

notifications of payments that had been received, with cash-like finality, which could be cryptographically (and automatically) authenticated by the recipient…the entire payment and notification process requiring less than one thousandth the latency, less than one ten thousandth of the system/infrastructure costs and essentially none of the ecological devastation of a Bitcoin payment.

These ‘token’ misconceptions are so central to the ‘coin’ nonsense that arises from them as to warrant a deeper dive.

The mystique of ‘Tokens’

One is actually hard pressed to find a succinct and precisely abstracted definition of “token” in the computing or cryptographic context expressed in laymen’s terms. More commonly one sees sophomoric explainers such as https://www.bitdegree.org/tutorials/token-vs-coin/. But its technical definition, as a datatype (as in the W3 XML schema), is quite straightforward. See also IBM’s reference.

A token, *functionally*, can be thought of like a ticket, possession of which affords access to a resource. But in the relevant domain of computing, a token is simply a string of characters. Tokens are used in a variety of contexts and applications including the establishment and operation of a network of computers and closely related strategies for securing and authenticating communications.

Use of the term ‘token’, in terms of *which sort of strings* are referred to as tokens, has evolved over time – most likely due to a paucity of synonyms. For example, if you set your preferred internet search utility to a date range prior to, say, January 2008, and search using terms such as ‘cookie’ ‘session’ and ‘token’ you will not uncommonly find “session ID”s (correctly) referred to as tokens. For example, this from Oracle described their “Access Manager Session Service” (for managing visitor/customer access to websites):

“The session token, also known as a sessionID, is an encrypted, unique string that identifies the specific session instance. If the session token is known to a protected resource such as an application, the application can access the session and all user information contained in it. In Access Manager, a session token is carried in a cookie. A cookie is an information packet generated by a web server and passed to a web browser.”

Use of the word “token” to refer to Session IDs is no longer in style, possibly because the term was needed to distinguish an enhancement of TLS[10]—the technology for securing internet connections that superseded Secure Sockets Layer (SSL)[11]—called “token binding”.

This reflects the fact that, more and more in recent decades, applications that entail usage of tokens implement cryptographic techniques such as hash functions and asymmetric encryption involving private/public key pairs, regardless of whether they secure bank-provided apps or other account-based systems. Yet it remains perfectly correct usage to refer to all manner of strings, encrypted or not, as tokens. As of July 2020, Visa continues to offer its Visa Token Service which basically substitutes some other string of characters for a “Primary Account Number (PAN)”, thereby “tokenizing payment cards for e-commerce and mobile payments (HCE and OEM Pay wallets) but also bank account numbers for

[10] Transport Layer Security

[11] The URL’s/URI’s for websites/APIs that support secure connections via technologies such as TLS (and previously by SSL) are prefixed by “https” instead of the “http” used for insecure connections.

ACH/real-time payments, as well as cryptocurrency wallets.” This usage of the term “tokenizing” or tokenization is fully valid from a technical standpoint and does not change the fact that both credit cards and bank accounts are “account-based systems”.

The point of this discussion is that the proposed taxonomy in this document, which contains “coin” and “stablecoin” is based on:

- This bogus distinction between “account-based money” and so-called “token money”[12] that has been imbued on credulous monetary economists by techie people.
- A predisposition among non-technical people to conflate the concepts of “coins” and “tokens” which, though apt in the physical realm, is quite misleading in relation to digital assets,

From token to coin

English speakers have a linguistic predisposition to conflate the concepts of “coins” and “tokens”. Token and coin also end up being used almost interchangeably in crypto-babble. This is evidenced by the innumerable articles, especially about Bitcoin, embellished with seemingly obligatory pictures of little golden colored coins decorated with the ₿ symbol.

But neither Bitcoin transactions nor payments with any other popular cryptocurrency involve anything that could appropriately be referred to as ‘coins’.

There are two essential concepts that comprise coin’ness.

- A coin embodies a fixed discrete number of units of the brand of money in relation to which it is minted. With USD, a dime always embodies ten one-hundredths of a dollar (i.e. cents), unlike a payment, payment message or payment instruction, the amount of which can be specified with a continuous variable.
- A coin is also a bearer medium. Whoever finds and appropriates a lost quarter lying on the sidewalk effectively becomes the owner of the value it embodies. The value of a coin can be realized (e.g. spent) without applying it toward incrementing a ledger balance maintained by a third party (such as depositing it into an account).

Before proceeding, it is worth pausing to also focus a moment on the notion of a bearer medium because it has also attracted a lot of disputatious nonsense. Usage of a bearer medium, such as paper cash or coins, normally enables significant anonymity (if desired) and poor traceability. But the reverse logic, that a system that is not bound to verified identity and which affords anonymity and untraceability is therefore a bearer system, is not correct.

If I intercept a Bitcoin (or any other crypto-) payment instruction that was not directed to an address I control, unlike a coin, it is useless to me.

It is inappropriate to use a term of such specificity as “coin”, especially when the canonical examples of these digital coins are so incongruous with any reasonable sense of what coin’ness might mean. It is mere branding and it is untoward when experts who should know better adopt such usage with the solemnity

[12] The consultation document uses the word “token” as a superset of “coin”, “security” and “utility” tokens.

of courtiers vying with one another in the effusiveness of their flattery of their naked emperor’s new clothes.

There are over 7,500 brands of cryptocurrencies with exchange rates tracked on the https://www.coingecko.com/en page. Looking at just the first 100, seven use the word “coin” in their brand name, three “cash” (one, Bitcoin Cash, uses both) and seven employ “token”. The point is that coming up with a catchy brand name is hard, and one strategy—the alternative to conjuring up something completely novel and non-descriptive (Cardano? Zilliqa?)—is to employ words people already associate with the product or line of business a company is in.

This has happened before: the tortured semantics of “virtual currency”

In 2013, FinCEN issued guidance regarding “virtual currencies”. There were two striking similarities to this current exercise in devising ill-advised neologisms:

- Dread of Facebook, combined with overestimation of its prowess/competence in the domain of alternative moneys,
- Hesitation to call a spade a spade, to wit “what might people think if we refer to such phenomena as ‘privately-issued money’!?”

While the term “virtual currency” had been used as early as 2004 to describe pre-paid sums held on account for purchase of “virtual property” in ‘Massively multiplayer online role-playing games ("MMORPGs")’, it was not until Facebook embraced the notion (for its captive games such as Farmville) and then announced ambitious plans for its ill-conceived Facebook Credits (e.g. “Imagine Facebook Credits as more like a euro, which makes it easy to spend money across countries.”) that FinCEN mobilized to weigh in on the topic.

FIN-2013-G001

Issued Date: March 18, 2013

Guidance Subject: Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies

”FinCEN's regulations define currency (also referred to as "real" currency) as "the coin and paper money of the United States or of any other country that [i] is designated as legal tender and that [ii] circulates and [iii] is customarily used and accepted as a medium of exchange in the country of issuance." In contrast to real currency, "virtual" currency is a medium of exchange that operates like a currency in some environments, but does not have all the attributes of real currency. In particular, virtual currency does not have legal tender status in any jurisdiction. This guidance addresses "convertible" virtual currency. This type of virtual currency either has an equivalent value in real currency, or acts as a substitute for real currency.”

It is instructive and, I will argue, highly relevant to the current context to closely examine this previous semantic exercise.

Sentence 1:

“FinCEN's regulations define currency (also referred to as "real" currency) as "the coin and paper money of the United States or of any other country that [i] is designated as legal tender and that [ii]

CIRCULATES AND [III] IS CUSTOMARILY USED AND ACCEPTED AS A MEDIUM OF EXCHANGE IN THE COUNTRY OF ISSUANCE."

They were mostly on solid ground here. 31 CFR § 1010.100 – General definitions, (m) Currency, was cited accurately, with the addition only of the lower-case Roman numerals.

"THE COIN AND PAPER MONEY OF THE UNITED STATES OR OF ANY OTHER COUNTRY THAT IS DESIGNATED AS LEGAL TENDER AND THAT CIRCULATES AND IS CUSTOMARILY USED AND ACCEPTED AS A MEDIUM OF EXCHANGE IN THE COUNTRY OF ISSUANCE.

Yet they gratuitously added '(also referred to as "real" currency)'. This addition of "real" as a modifier for "currency" could only make sense as a (superfluous and unnecessary) means of distinguishing currency (as defined by law) from counterfeit coins or paper money. But this was not FinCEN's intent in adding "real". What they were attempting to queue up was a distinction between government-issued money and privately issued money which latter, for reasons not elaborated, they were hesitant to call money. But the intent can be inferred. Lacking any US federal definition of "money" and concerned about the atmospherics of referring to privately-issued money as money, they sought to apply laws that explicitly refer only to paper cash and coins to privately issued moneys, even though the only such media of potential significance existed only in digital form. So the word currency was again employed in the second sentence. But this sentence used the word in accordance with its other main, completely different, conventional usage – as a 'brand' of money.

"IN CONTRAST TO REAL CURRENCY, "VIRTUAL" CURRENCY IS A MEDIUM OF EXCHANGE THAT OPERATES LIKE A CURRENCY IN SOME ENVIRONMENTS, BUT DOES NOT HAVE ALL THE ATTRIBUTES OF REAL CURRENCY."

Note the "a" in "like a currency". If referring to the legislatively defined word "currency"—as FinCEN took such pains to anchor its guidance to in the previous sentence—this was like saying "a furniture", "a lingerie" or "a garbage". The word "currency" as defined in US code doesn't work as a plural or rendered as "a currency". One cannot say "In fiscal year 2012, the Bureau of Engraving and Printing delivered approximately 35 million currencies a day". In the plural, or rendered as "a currency", the word means something altogether different. It means a brand of money in the sense that the words euro, yen, ruble, US dollar etc. each designate some particular currency.

The remainder of the sentence, in concert with the following sentence, then indulges in a fanciful riff attempting to differentiate whatever they mean by "virtual currency" from the stuff actually defined in US law and regulation. They rightly point out that this figment "does not have all the attributes of real currency. In particular, virtual currency does not have legal tender status in any jurisdiction."

What has been established here? (A) Virtual Currency isn't government-issued paper cash or pocket change, and (B) it lacks legal tender status (i.e. no one can be compelled to accept it in payments, whether to extinguish debt or for purchase of goods and services). But bank deposits, whether at a commercial bank or even at a government central bank, aren't paper cash either nor, as far as I can determine, are they designated as legal tender in the US or any other country.

They then concluded with a distinction, throwing in the completely undefined (but actually problematic) term "convertible", that continues to fully apply to bank deposits but might quite plausibly exclude certain implementations of privately-issued money, the very stuff they were trying to label as "virtual currency".

“THIS GUIDANCE ADDRESSES "CONVERTIBLE" VIRTUAL CURRENCY. THIS TYPE OF VIRTUAL CURRENCY EITHER HAS AN EQUIVALENT VALUE IN REAL CURRENCY, OR ACTS AS A SUBSTITUTE FOR REAL CURRENCY.”

Unquestionably, bank deposits have an equivalent value in like-denominated paper cash and act as a substitute. Are such bank deposits also “convertible”?

To convert is to transform, to change something into something else, both things being elements of the same more general set, as opposed to exchanging one thing for another thing of a different type.

One can convert liquid water into ice by lowering its temperature or vice versa. Both are still H2O. All that has changed is its form or state. But one cannot convert water into ammonia (NH3).

If I am holding USD deposits in a commercial bank account, the value of the USD deposits is “equivalent” to the same number of units of USD in currency, i.e. paper money, form. My deposit is a substitute for such (non-counterfeit, i.e. “real”) paper money or coin. I can elect to convert some of the USD on the asset side of my balance sheet into USD in another form via an ATM withdrawal. But it is still USD.

Suppose instead I have a EUR-denominated bank account. I cannot simply go to the ATM and withdraw USD from the account. Should I desire USD, there would be an obligatory currency exchange involved, funded from my EUR balance. Similarly, neither the ECB nor a Eurosystem NCB can wave a magic wand and cause some of the EUR monetary liabilities it has created to become transmuted into USD. If one has EUR but wants USD instead, the EUR can only be exchanged for, i.e. used to buy, or posted as collateral to borrow, USD.

But consider a privately-issued digital money established in accordance with a currency board logic anchored to physical gold such that the unit of account adopts the conventional weight units in which physical gold is quantified and the monetary liability is defined as to require the issuer to maintain at least one physical gram of gold, fine content, held in trust to back every monetary ‘gram’ issued and outstanding. There is no fixed equivalence between a specified quantity of this money and the paper cash (currency) of any country, just as there is no such equivalence between USD and EUR. Absent one brand of money being issued in accordance with a currency board arrangement anchored on the other currency, the exchange rate of all currency pairs fluctuates continuously.

The obvious goal of this FinCEN exercise was to conjure up some rubric legitimizing its jurisdiction over privately-issued money. But the semantic logic (outright sophistry) they came up with yielded a closer description of bank deposits than it did of privately-issued moneys anchored to some external asset other than one or other existing brand of money. Had they instead undertaken to articulate some legal basis for asserting regulatory authority over privately-issued money, the ontological domain of actual interest, there would be even less of a need for the current exercise involving so-called stablecoins. And even if such a valid legal basis was found not to exist, the discovery of its absence might have informed legislation to address the gap.

Why does this “Virtual Currency” precedent matter?

Why linger at such length on the 2013 semantic exercise when the current topic is the 2020 consultative document regarding so-called global stablecoins?

- Multiple other nations adopted similar virtual currency nonsense willy-nilly and now have either bad regs or laws on their books.

- The only apparent difference between virtual currency and stablecoins is the crypto assumption. No new class is needed if the true essence is still simply ‘privately-issued money’.
- Bad laws/regulations abrogate responsibility, sloughing off their interpretation to the courts.
- The courts are poor arbiters because the outcome is largely determined by who has the larger budget to lawyer up. Consider the Ripple case where, having sold tens of billions of units of unbacked play money to a gullible/avaricious public, the principals had an effectively unlimited (> 1 billion USD) legal war chest, enabling them to sidestep criminal indictment for their securities, unlicensed money transmission, and money laundering violations and receive only a perfunctory Non-Prosecution Agreement slap on the wrist.

Stablecoin: origins, connotations and ramifications

Official adoption of the term “stablecoin” is a bad idea and “global stablecoin” is even worse.

As matters stand, the term stablecoin is a shibboleth, fraught with connotations that inform a useful heuristic for distinguishing ill-conceived and invalid schemes from sound and sustainable monetary innovations.

The heuristic is: any monetary/payments scheme for which the organizers/promoters and their target market regard “stablecoin” as a positive meme encapsulating an attractive value proposition is more likely unsound – perhaps to the extent of eventually producing losses on the part of its customers and investors.

The stablecoin meme/model is, at least for those content to refer to their products/services as such, more or less a package deal in terms of possible business and revenue models as well as their dependence on crypto ‘rails’. These considerations are addressed below. But first…

Why ‘coin’ a neologism inferior to existing terminology?

The currency board model is a potentially sound logic for the private sector issuance of (Base) Money. With a properly designed system, the exchange value of monetary liabilities issued in accordance with a currency board model closely track the market value of the designated outside anchor asset at a fixed exchange rate. Relatedly, fluctuations in market demand for the money result in increase or decrease in the amount issued and outstanding, rather than deviation from the hard peg.

A so-called “stablecoin”—a neologism, the origins of which are explored below—*could* be described as a medium of exchange that is issued in accordance with a currency board model. But this is not the language of stablecoin promoters and enthusiasts. It is by no means evident they are even familiar with the theory and practice underlying this well-established and long understood term of art.

Origins – It began with Tether

The impetus behind most self-styled stablecoin projects to date has been an ambition to emulate, and wrest market share from, Tether in relation to its role in the speculative trading of unbacked cryptocurrencies. While it may be argued that Libra, classified as a stablecoin in the taxonomy of many analysts, is envisioned as an alternative medium of exchange for routine use as money, it too, as discussed below, was (at least initially) conceived on unsound foundational premises that continue to impede its evolution into a sound and sustainable alternative.

The driving force behind interest in Bitcoin and the almost innumerable unbacked cryptocurrencies that have followed in its wake has been tulip-bubble-like speculation. While bizarre phenomena such as

HODLers[13] have become a cultural spectacle, some speculators with large paper gains sought to realize them by exchanging them for real money. But there was a two-fold problem. No market existed for selling Bitcoin etc. (in any significant quantity) for real money such as USD deposits in a bank account. Moreover, many such speculators avidly sought to evade government detection of their capital gains and the resultant tax liability.

Tether was formed to exploit this opportunity by offering a "token" called USDT which it claimed was entirely backed by USD bank deposits on a 1:1 basis and therefore a perfect proxy for real USD. It has been convincingly asserted that the Tether organizers, in collusion with Bitfinex, a crypto exchange owned and controlled by the same principals, then proceeded via a combination of fraud and market manipulation to engineer the rise of Bitcoin to as high as 20,000 USD/BTC. It is telling that even now, when this fraud is almost universally recognized, that USDT remains the most widely used USD-surrogate (for the crypto community), with over 9 billion USDT[14] in circulation and with USDT the most common component in cryptocurrency trading pairs. In fact, Tether is again gaining market share relative to its much more legitimate would-be successors/competitors.

While it is unlikely any Tether imitator would dare to engage in such overt fraud, most do share multiple characteristics with Tether that both undermine their safety and soundness and drastically reduce the prospect of them ever becoming widely used for routine money payments.

Business model

The apparent proximate business model for the stablecoins anchored to national currencies that have followed in Tether's wake has been to:

- seek market share as a place for customers to park realized but unreported capital gains from crypto speculation,
- generate revenue from remunerative assets held as backing for the monetary liabilities.

Most have expressed the intention, as does Facebook/Libra, of attracting usage as a medium of exchange used for normal payments such as international remittances, online ecommerce, point-of-sale purchases or B2B payments. However, to date, such usage appears to be a relative trickle compared to crypto-speculative trading and Ponzi schemes[15].

The term stablecoin has also been applied to a subset of crypto-based media backed by stored commodities such as gold. The apparent business model of their various promoters entails positioning them as an investment / store of value, effectively placing such entities in direct competition with (typically much better established) dealers in gold bullion and coins. Revenue is primarily derived from selling the media at a mark-up – which in the discussion of revenue models below is classified as provision

[13] HODL means "Hold On for Dear Life" and HODLers tenaciously hold on to their Bitcoin (etc.) stash in hopes of eventually realizing fabulous capital gains or purchasing power.

[14] Tether's claimed USDT "market cap" has abruptly risen from 4.3 billion on March 29, 2020 to over 9 billion

[15] For instance, while Paxos is blessed by the New York DFS and has "distinguished luminaries including Sheila Bair and Senator Bill Bradley" on its board, it's primary usage remains cryptospeculation and Ponzi schemes see also https://decrypt.co/34640/philippines-sec-just-denounced-the-top-ethereum-dapp-as-a-ponzi.

of currency exchange. There is no indication that any such company is cash flow positive, rather all appear to be operating primarily on the basis of money raised from investors.

Revenue model

There are basically three (legal[16]) ways an issuer of money and/or provider of payments services[17] may (as such[18]) generate revenue:

- Provision of exchange services;
- Holding remunerative assets;
- Transaction or other service fees.

Provision of exchange services. An issuer of money (or any other entity) that undertakes to make a market for currency exchange is commonly exposed to exchange rate risk. This risk is exacerbated by the latency and risk of reversal of incoming conventional money payments as well as potential non-performance of customers that renege on funding transactions for which the market has turned in their disfavor. This combination may prevent the provider from timely resort to an external market when needed to offset trading imbalances that result in depletion of currencies in high relative demand and an inability to fulfill obligations.

Tether of course was the same entity as Bitfinex and its principal windfall was derived from engineering speculative capital gains on its occult holdings of Bitcoin (in lieu of the USD it claimed to hold). A more honest imitator may only seek to capture a one-time seignorage by selling newly issued money into exchange markets at a markup. But such a one-time revenue event, in addition to reducing incentive for third party providers of exchange to act as a distribution channel, is insufficient to sustain operations given that the money, analogous to banknotes, may remain in circulation for a long time.

Another model involves ongoing involvement in currency exchange markets in accordance with algorithmic stabilization strategies that, at least on paper, are revenue positive. The notion of algorithmic stabilization is discussed below and in Appendix 2: Algorithmic Stabilization.

Asset portfolio/Balance sheet risk. A stablecoin issuer may contemplate generating income the same way banks do – by holding a portfolio of remunerative assets[19]. But an issuer of money offsetting its monetary liabilities with an asset portfolio that includes uninsured commercial bank deposits, money market mutual funds or ETFs, or even high-grade sovereign debt instruments (treasury bonds) of greater than about 90 days maturity is exposed to the risk of loss and possible insolvency. These risks also apply

[16] It has been very credibly asserted that Tether, by secretly holding Bitcoin (and most likely via outright insolvency when expedient) and working in undisclosed collusion with Bitfinex, also generated windfall profits from manipulating the Bitcoin price.

[17] Whether established as an e-money institution (EMI), Authorised Payment Institution (API), Payments Bank, Stablecoin or you name it.

[18] Providers may garner revenue by more indirect means: from affiliated providers of financial services, advertising or other models fostered by seeking dominance of their app/platform/community. By saying "as such" I am narrowing the focus to exclude these more peripheral strategies.

[19] Notably, prior to February 2002, with one in its succession of business models, Paypal's interest income from remunerative assets held against customer liabilities was a significant source of revenue until ordered by the FDIC to basically stop doing what banks do. It subsequently morphed (the rest of the way) into becoming a credit card intermediary, reliant on transaction fee revenues.

in the case of a government monetary authorities. However, sovereign issuers of money assert freedom from default risk based on government guarantee of "full faith and credit" or similar verbiage.

Most so-called stablecoins, whether operational or planned, are indeed backed by uninsured commercial bank deposits, a smattering of cryptocurrencies, interest bearing securities and/or even holdings of other stablecoins. With the exception of media backed by a stored physical commodity (which typically rely on the exchange model outlined above), interest income generated by the asset portfolio has historically been their principal revenue source. The revenue model for Libra, to the extent plans have been disclosed (or even formulated) appears to be based, to significant degree, on the expectation of interest income.

Special mention, asset portfolio-wise, is warranted for Saga, a stablecoin which, at least initially, appears to be organized in accordance with the concept of a "Market-SDR" - a token backed by a basket of assets intended to mirror the composition of real SDRs and enabling a market value that closely tracks that of the official SDR price. Saga features an illustrious advisory board which includes a Nobel laureate in economics in addition to former senior executives from a major international bank and a government central bank. On the strength of this impressive board, Saga was able to raise $30 million from some of the most sophisticated venture capital firms in existence. Of note, the core of the Saga plan is a scheme to gradually substitute intangible goodwill, described as "inherent value", for up to 90% of the asset portfolio backing its monetary liabilities in circulation. In contrast, of the estimated $64 billion Bernie Madoff bilked from investors, court-appointed receivers eventually recovered over $13 billion (20.3%) – over twice the "reserve ratio[20]" contemplated for this scheme.

Fee-based revenue. The only revenue source for a privately-issued brand of money that would provide for a sustainable business model without incurring the risks of currency exchange or portfolio losses is fees – primarily transaction fees for executing a payment instruction. A fee-based revenue model is fully compatible with institutional arrangements designed to ensure freedom from default risk.

As follows, however, existing stablecoins largely relinquish this potential revenue source to the public blockchain cryptocurrency schemes on which they are piggy-backed.

Dependence on crypto rails

All self-styled stablecoin promoters formulate(d) their schemes informed by belief that blockchain, cryptocurrencies and so-called "Distributed Ledger Technology (DLT)" constitute the future of money, payments and nearly everything else. As a consequence, all or nearly all existing stablecoins designed their schemes in a fashion that makes them wholly reliant on existing cryptocurrency public blockchains[21].

[20] The Reserve Ratio for a depository institution refers to a defined, cash-like, subset of overall assets divided by customer deposits. But, in addition to reserves, a bank's asset portfolio also includes a substantial portfolio of investments such as loans and securities. Saga misuses the term "reserve ratio" to mean the sum total of all its marketable assets divided by the market value of its monetary liabilities. But then, as I see it, the authors of this consultation document misuse the term of art "reserves" in the same way. This topic is addressed immediately below.

[21] Libra, as currently conceived, is an exception to this dependence on crypto-rails of third party systems. Plans call for a new Libra Blockchain that dispenses with legacy blockchain elements such as blocks and the notion of all nodes maintaining an archive of every transaction.

Per the Tether website: "Tethers exist as digital tokens built on bitcoin (Omni and Liquid Protocol), Ethereum, EOS and Tron blockchains."

This dependency is of two-fold significance.

Firstly, it tends to mean that transaction fees for processing payments—the safest potential source of revenue for a Stablecoin scheme provider—are more likely to be captured by elements of the underlying (rails) network.

But there is an operational risk as well. For example, the most common rails via which existing or planned stablecoins circulate is Ethereum, via its support for "ERC-20" tokens. The significance of this is that were Ethereum to cease to exist, as would occur were the price of ETH to collapse below the level where its "miners" (or providers of stakes) can cover their operating costs, ALL stablecoins dependent on it could cease to circulate and, if so, there quite plausibly might be no mechanism enabling holders of such 'tokens' to assert their claims in the liquidation of the underlying assets. It is ironic that while a principal rationale for the whole blockchain phenomenon was avoidance of a "single point of failure", over 268,000 flavors of ERC-20 tokens could well be kaput were the crypto bubble to collapse.

This should be an issue of acute concern because a plausible argument can be advanced that the only factors that are currently preventing all unbacked cryptocurrencies from collapsing are: a) the deluge of new money recently created by the Fed and other central banks, and b) renewed massive fraud on the part of Tether/Bitfinex as it shuffles huge balances of Bitcoin around in lieu of the USD it purports to hold.

This before Tether more than doubled its issuance of USDT in the past three months.

(Mis)use of the term "reserves"

The term "reserve assets" appears 52 times in the consultative document. It is used to refer to all 'assets that are "backing" the value of a stablecoin' and encompasses instruments which entail "credit, liquidity and market risks". This usage of the term "reserve assets" is a bad idea. It would be better to use a term such as "earmarked assets" or, per the convention of the Hong Kong Monetary Authority (HKMA) as noted below, "backing portfolio (BP)".

"Reserves" is a defined term of art in certain contexts. In banking, the word refers to money held on deposit with the central bank in a master account plus vault cash used to stock teller drawers and ATM machines. Such reserves are needed in order for a bank to, respectively, fund/settle outbound payments through a clearinghouse or the settlement platform typically administered by the central bank, or, to immediately meet its obligations to fulfill cash withdrawal orders/requests (whether over the counter or via an ATM machine). In this commercial banking context, the reserves portion of the bank's asset portfolio serves as its own 'money[22] in the bank' while its other, typically more remunerative assets—loans, securities etc.—can be thought of as investments.

[22] There is an additional benefit in holding such *liquid* reserves (direct liabilities of a government monetary authority comprising the epitome of liquidity). Such reserves are also the *safest* possible asset in the sense of "safety" being the certainty of being able to liquidate an asset for money (since they are already the money'est money possible). Liquidity and safety in this case are two sides of the same 'coin'.

In banking, the term “reserve ratio” is also a defined term of art, albeit one being gradually deprecated. For a bank, “reserve ratio” means its quantity of reserves, as defined above, divided by its deposit liabilities. Taking liberties with the term ‘reserves’ provides cover for misuse of the notion of ‘reserve ratio’. Again using Saga as an example, we see a stablecoin issuer using the term (in the same fashion as the consultative document does) to refer to all assets held against its outstanding money (called “SGA tokens”). In fact, the term “reserve ratio” appears 149 times in Saga’s Monetary Model whitepaper although, interestingly, neither “liability” (in any form of the word) nor “balance sheet” are used at all. But were an example balance sheet to be displayed, it would show—once the scheme achieves its projected “market cap” of >=3 trillion (SDR)—total liabilities ten times the earmarked assets held against them. This astounding intent to achieve such insolvency is justified by a sleight-of-hand glossing over how Saga’s usage of “reserve ratio” (like the consultative document’s) is not how the term is used in banking:

“Thereafter [when the “market cap” of SGA tokens passes “20M SDR”], the reserve ratio decreases until it eventually reaches a minimum of 10%, then remains constant. *A 10% reserve ratio is identical to the US Federal Reserve’s current required reserve ratio on banks’ Net Transaction Accounts*.” [Italics added for emphasis].

With government monetary authorities organized as central banks, the word reserves may be used as a standalone term or rendered as “international reserves”. The Bundesbank for example has both usages in its SDDS Plus disclosure of Währungsreserven and offers the succinct definition “Reserves are defined as foreign currency denominated claims on non-euro area countries plus gold, holdings of SDRs and the reserve position in the Fund [i.e. the IMF].” The United States Treasury and the Federal Reserve report (their apparently commingled) “U.S. Reserve Assets” similarly, distinguishing reserves from the portfolio of securities and loans which generate the bulk of the Federal Reserve’s revenue. Again, as with the reserves held by banks, these categories of reserves, unlike more remunerative instruments, all afford perfect freedom from default risk.

Government Monetary Authorities constituted as Currency Boards also make a distinction between the assets backing the monetary base and their investment portfolio. The HKMA expresses this distinction with the terms “Backing Portfolio (BP)” and “Investment Portfolio (IP)” where the “BP holds highly liquid US dollar-denominated assets to provide full backing to the Monetary Base as required under the Currency Board arrangements.” The IP, in contrast “invests” (primarily in the bond and equity markets of the member countries of the OECD) to generate income and capital gains to augment the HKMA’s (very substantial) accumulated surplus held as a buffer against credit, liquidity or market risks that might otherwise impair its solvency.

In the consultative document, “reserve assets” is not listed in the Glossary as a defined term but it is used twice in the “Activity” section of the “Stablecoin arrangement” definition. Again, this is a bad idea from the standpoint of such novel usage producing confusion due to its conflict with established usage.

Why split hairs over sloppy application of this longstanding term of art “reserves” (in both this consultative document and the “official libra White Paper” that it seems to track? It is because “reserves”, as the term has always been used by commercial banks and government central banks, refers exclusively to assets which do **not** entail “credit, liquidity and market risks”. In contrast, deposits or other direct liabilities at/of a government central bank (domestic or foreign), physical gold[23], SDRs – all of these afford perfect freedom from default risk.

This matters because a private sector issuer of a Digital Base Money (DBM), under the auspices of a 'Private-Sector Monetary Authority' (as per the appended definitions in Appendix 5), were it to hold a 100% reserve of one of these *actual* reserve-class assets, and avoid currency mismatch across the balance sheet, would arguably have a stronger balance sheet than any government monetary authority. Such fiduciary arrangements would ensure freedom from default risk without resort to any sort of government guarantee[24].

The contrast between this scenario and an entity holding risk assets, including commercial bank deposits[25], is such as to warrant limiting use of the terms "reserves" and "reserve assets" to entities that actually hold reserves as they have always been defined in the banking context. Usage of the terms "Earmarked assets" or "Backing Portfolio" for all assets held against Monetary Liabilities, a subset of which may be reserve-class assets, would better align with prudential realities.

'Wholesale/Retail' vs. Base Money / Broad Money

The consultative document adopts a convention, which has also been increasingly prevalent in recent discussions of CBDCs or of cross-border payment alternatives, of referring to "retail" and "wholesale" monetary/payment arrangements. Such usage of this terminology should be deprecated. Precise discussion concerning classification and regulation of privately-issued money schemes would be better facilitated by using the long-established terms of art "Base Money" and "Broad Money".

One problem with applying wholesale/retail terminology to monetary/payments arrangements is that it impedes clarity in discussing the boundaries that separate different currencies (brands of money). This is pertinent to the Facebook/Libra discussion even if its organizers profess no current plans for their money to be used by financial institutions as a medium of settlement[26]. It is also relevant to CBDC discussions in that certain implementations of CBDCs could effectively result in a central bank issuing the Base Money

[23] Gold, it may be argued, may entail liquidity and/or market risk if there is currency mismatch across the balance sheet as is the case with all Government Monetary Authorities that hold it. Accordingly, major central banks may carry it on the balance sheet at its original "cost" basis (42 USD/troy ounce in the case of the Fed) or, as in the Eurosystem, offset its appreciation relative to the central bank's own money with revaluation accounts (carried as liabilities). Both result in a huge buffer of unrealized gains that dwarf any financial risk of holding gold.

[24] Fun fact. The US Federal Reserve changed the boilerplate in its "Annual Report…Notes to the Combined Financial Statements of the Federal Reserve Banks…Significant Accounting Policies…Federal Reserve notes" in 2007 from "Finally, Federal Reserve notes are obligations of the United States and are backed by the full faith and credit of the United States government." to, simply, "Finally, Federal Reserve notes are obligations of the United States government." The United States appear to be off the hook. Meanwhile, the status of *deposits* at Federal Reserve Banks continues to be somewhat more ambiguous.

[25] Whether or not covered under a passthrough deposit insurance scheme.

[26] Actually, it is not strictly true that FB/Libra has no overt designs for its various ≋XXX to serve as Base Money. Per the "The Libra Blockchain" technical protocol proposal: "We anticipate that many payment transactions will occur off-chain, for example, within a custodial wallet or by using payment channels." A "custodial wallet" indicates usage of ≋XXX as an asset held as backing against like-denominated and payable Monetary Liabilities of the custodian. Moreover, nothing precludes a consortium of multiple such custodians from using this underlying Base Money as a medium of settlement for intermediated payments between their respective customers.

of two distinct brands of money that do not necessarily trade at parity and which could well require a suitable naming convention enabling people to distinguish one from the other.

Clarity with respect to Base Money vs. Broad Money is (or will be) particularly critical in the case of a private sector entity that undertakes to provide for the issuance of the Digital Base Money of a soundly conceived alternative global currency designed for both end-user P2P payments and to be suitable for banks worldwide to hold on their balance sheets as both a medium of settlement and a reserve asset underlying like-denominated and -payable deposit accounts.

Would a private sector issuer of Money that is hard pegged to a designated anchor brand of government-issued Money be more like a commercial bank (depository institution), an "e-money institution (EMI)" as contemplated in multiple jurisdictions, or a distinct Monetary Authority issuing[27] the Base Money of a separate and distinct brand of money?

Assuming such Money is redeemable[28], with any of these arrangements there would be circumstances in which the institution with outstanding Monetary Liabilities would be obliged to symmetrically shrink its balance sheet, paying out conventional Money and concurrently extinguishing a quantity of its own Monetary Liabilities.

Consider the differences between three flavors of, let's say, GBP-denominated (or GBP-pegged) monetary liabilities:

- GBP-denominated (demand) deposit liabilities of a commercial bank,
- GBP-denominated "electronic money" (e-money) as contemplated in regulations[29] governing an Electronic Money Institution (EMI),
- Privately issued money (which you call Stablecoins) issued in accordance with a currency board arrangement implementing a hard peg to GBP.

The first two are part of the Broad Money supply of GBP. The third, assuming it implements certain protocol elements and institutional arrangements addressed below, would not be. It would be a different brand of money we might refer to generically as eGBP, likely to closely track the exchange value of GBP yet with fluctuations as observed in the HKD/USD exchange rate[30]. In the first two cases, the symmetric shrinkage of the balance sheet referred to above occurs not only with redemption/withdrawal but also with outbound payments. In the third, there is no such thing as an 'outbound' payment, provided that final settlement of payments[31] only occurs on the platform/ledger native to the system.

[27] Or rather 'responsible for the issuance of'…

[28] Redeemable may or may not mean "convertible" as discussed in the "virtual currency" section.

[29] Payment Services Regulations and Electronic Money Regulations promulgated by the FCA.

[30] Again, depending on implementation details, as will be discussed, a CBDC hard pegged to GBP, even if issued by the Bank of England itself, could very well manifest the same eGBP/GBP exchange rate fluctuations as if issued by a foreign or private sector monetary authority.

[31] This includes composite/hybrid transactions such as the Interledger Protocol that entail obligatory in-line currency exchange.

This third variant, whether or not recognized as such or, critically, whether or not other entities actually create Broad Money denominated and payable in it, would be the Base Money of a distinct currency (brand of money), just as the Bulgarian lev (BGN), though hard pegged to EUR, is not EUR.

The fundamental boundary that demarcates one brand of money from another is the medium, i.e. the Base Money, and the platform (ledger) for final settlement of remote payments[32] of such Base Money. If the clearing and/or settlement of a payment might in any circumstance require a transfer of the Digital Base Money issued by a(nother) Monetary Authority on its platform for settling such transfers (most typically, an RTGS platform), the money is part of the Broad Money[33] supply of the already-existing currency rather than constituting the Base Money of a distinct brand of money. The ramifications of this distinction affect interoperability between, and miscibility of, the media of exchange provided by different issuers of such.

Consider WeChat Pay and Alipay. Until fairly recently, these were effectively separate currencies (distinct from each other or from RMB), both organized more or less in accordance with currency board logic. Final settlement of a payment with either system was done on the books of the company, highly similar to a situation where a bank might settle payments between pairs of its own customers on its own books – each transfer having no effect on the asset side of the institution's balance sheet. One ramification of this was that a payer using one of the two brands could not pay a recipient who only used the other. Similarly, if an entity used both, there was no way to combine balances. A customer with 400 RMB-equiv. of WeChat Pay and 600 RMB-equiv. of Alipay needing to make a 500 RMB-equiv. payment would of necessity require: a) the recipient to have accounts in both systems, and, b) two payments.

The historical analogy to this situation was the use of bank notes in the absence of a clearinghouse. Bank notes (in the same domestic currency compartment), each particular to their issuing bank, were commonly valued differently, even though each were required[34] to be redeemable in the same base money.

In both cases, the WeChat Pay/Alipay situation and the bank notes scenario, uniformity and interoperability were achieved with a clearinghouse solution in which all participants used a common medium of settlement. Imposition of the rule, whether by law or convention, of "all payments through the clearinghouse[35]" produced uniformity that transformed what were in effect issuers of multiple distinct currencies into part of the Broad Money supply of the same currency.

What are the ramifications if the Monetary Liabilities of a private sector Monetary Authority are indeed Base Money?

[32] Remote payments as opposed to hand to hand transfers of physical tokens such as paper cash or coin.

[33] One might argue that an e-money issuer, if it does not extend loans, cannot be regarded as Broad Money. If however this EMI holds any assets against its Monetary Liabilities other than bank deposits (such as securities) it is expanding (broadening) the money supply of the brand of money in which it is denominated and payable.

[34] One might say 'nominally required' since the designated base money of the era, full-bodied bullion coins (especially gold), were so ill-suited for routine payments it was rare for anyone to exercise their right of redemption.

[35] In the bank note case, the rule concerned banks accepting (for deposit) or paying out the notes of other banks.

For centuries, an unchallenged truism has been that money is a public good, something that can only be provided by the State[36]. Of course, even as that notion has been broadly and uncritically recited, monetary economists not uncommonly refer to deposit creation (e.g. a loan advance) on the part of banks as privately created money. Moreover, it has long been the habit of smaller banks (or, more accurately, banks on the periphery of payment networks) to hold deposits (credit-based, privately created money) at banks of higher centrality in such graphs (aka correspondent banks) and to use those liabilities as a medium of settlement.

What, if any, functions of money can only be properly performed by the state? Isn't it possible that the most critical functions of money in relation to payments—providing a common medium of settlement and the platform on which transfers of that medium are settled—might be provided just as well, or better, by a private sector entity, a private sector Monetary Authority?

Privately-issued Money

In 2001, Laurence H. Meyer, a Fed Governor, in remarks titled "The Future of Money and of Monetary Policy", addressed the then-emerging possibility of private sector issuance of money.

Notably, he asserted:

"...central banks, at least in developed economies, issue currency and provide clearing services, at least in part, because their services offer features, such as freedom from default risk and finality of settlement, that private providers cannot match[37]."

Is it true that only a government monetary authority can ensure freedom from default risk? And if freedom from default risk is imperative with respect to the medium used for settlement of intermediated payments, how does that square with cross-border payments via SWIFT where most cover payments settle on the books of correspondent banks, many of which are G-SIBs – the network centrality of which poses the greatest source of potentially catastrophic systemic risk? Collectively, these nostro balances are claimed by some to exceed 27 Trillion USD-equivalent.

Freedom from default risk

As noted above, there are two ways to provide (ledger-based) money affording freedom from default risk – a bullet-proof balance sheet, or, a government guarantee.

The strongest possible balance sheet would require a 100% reserve of demand assets (i.e. zero-maturity) with no currency/denominational mismatch across the balance sheet and appropriate trust/custodial arrangements ring-fencing the assets from any/all encumbrances or claims other than backing the money.

[36] As recently (June 17, 2020) asserted by Fed Chairman Powell: "The private sector is not involved in creating the money supply. That's something that the central bank does" as opposed to "private employees who are not accountable solely to the public good".

[37] Unbeknownst to Meyer, e-gold®—a privately issued medium, described by the Financial Times in 1999 as "the only electronic currency that has achieved critical mass on the web"—had been fulfilling those imperatives since its online launch in 1996. e-gold went on by 2006 to serve active customers in over a hundred countries, settling 3 billion (USD-equiv.) worth of P2P payment per annum and amassing gold reserves surpassing those then backing the Canadian Dollar or Mexican Peso.

A list of appropriate such zero-maturity assets would match the examples cited above in reference to the external reserve assets held by the Fed and Bundesbank.

The next best thing would be to do what Libra proposes to do, to hold a very high proportion (in their case 80%) of “very short-term (up to three months’ remaining maturity) government securities issued by sovereigns that have very low credit risk (e.g., A+ rating from S&P and A1 from Moody’s, or higher) and whose securities trade in highly liquid secondary markets” in addition to the denominational and custodial safeguards specified above.

In either case, such a balance sheet would be dramatically safer and more sound than that of any government central bank or commercial bank, including the G-SIBs whose deposits substitute for reserves in the international payments context.

Moreover, it is virtually certain that every major government central bank in the world has passed the point of no return in terms of ever being able to unwind the unconventional policy measures implemented in response to previous crises. Both QE and weakened standards for quality of collateral have reached escape velocity. It would be prudent at this point to make provisions enabling a few private sector lifeboats to be deployed.[38]

Additionally, as further explored in Appendix 2: Algorithmic Stabilization, any arrangement for the issuance of Money other than an issuer whose balance sheet enables the ability to buy back **all** the money it has issued, at par, is basically a confidence game. This applies to any entity engaged in maturity transformation of such magnitude as to face insolvency in the event of a spike in interest rates which, in the case of government Monetary Authorities, might arise from loss of confidence in their future ability to ensure adequately stable purchasing power. Libra, to its credit, plans on balance sheet arrangements that would support stronger ability to shrink its balance sheet (in the event of decreased demand for its money) than any major government central bank.[39]

These safety and soundness considerations weigh in favor of building a transnational regulatory framework that would provide for initiatives such as Libra. But there are other considerations of no less importance that must also be taken into account. One salient concern that has been expressed is the possibility of a global medium that either displaces usage of sovereign domestic currencies or interferes with the transmission and efficacy of monetary policies.

Objection: Interference with “monetary policy transmission”

Concerns with potential “macroeconomic implications including monetary sovereignty issues”, while outside the scope of the FSB consultative document[40] are nevertheless touched upon and are the subject

[38] It would also be prudent for government central banks not to ‘go overboard’ in their zeal to get rid of physical cash. In the event of a catastrophic Carrington-like event, paper cash could be the only stopgap that would avert civilizational collapse pending ability to restore critical networks.

[39] Novi does not specify whether it will maintain 100% backing of the Base Money form of ≈XXX against its like-denominated Monetary Liabilities. But surely that is the plan.

[40] There is extensive concern with “Monetary Policy Transmission” in the October 2019 “G7 Working Group on Stablecoins” report “Investigating the impact of global stablecoins” https://www.bis.org/cpmi/publ/d187.pdf

of a forthcoming IMF report to the G20[41]. The document does observe “a GSC could potentially substitute for domestic currencies, particularly in some EMDEs with volatile domestic currencies”.

There is an ironic aspect to such concerns regarding potential threats to the prerogatives and policy efficacy of domestic Monetary Authorities that may result in exchange rate (and interest rate) volatility. The most destabilizing potential consequence arising from domestic use of, or dependence on, a foreign currency, sometimes forcing domestic monetary authorities to make radical adjustments[42], is occasional abrupt reversal of capital flows, impeding domestic progress toward capital account convertibility and other benefits of a more advanced monetary/financial regime.

The irony is that the status quo, in which the domestic currency of a foreign country (USD), subject only to the discretionary monetary policies of a foreign sovereign, is the perennial source of these whipsaw or “spillover” effects. Usage of an international medium subject to fixed, contractually enforced rules could scarcely be worse.

There is a clearcut and relatively simple solution that would mitigate concerns of a privately-issued global money interfering with monetary policy transmission but to reveal it in these public comments risks divulging commercial secrets. [I am happy to selectively discuss this on a confidential basis.]

Summing up, the Libra plan, other aspects of which are discussed below, deserves high marks in terms of safety and soundness. Moreover, though there are no indications Libra/Novi has figured this part out, there are measures the provider of an alternative global medium can implement that would adequately mitigate the risk of impairment of the prerogatives of domestic Monetary Authorities. However, as matters stand with Libra, other concerns are warranted with respect to both domestic monetary sovereignty and regulatory authority. These are addressed below.

Regarding Libra, and Facebook/Novi

As noted above, the impetus behind the current scramble on the part of regulators to address so-called Global Stablecoins is to come to grips with the Facebook-initiated Libra consortium and its plans to get into the money issuing/payments business. But it would be indelicate to formulate a regulatory rubric explicitly targeting only a single commercial entity.

There are also good reasons to distinguish a potentially global entity from more geographically circumscribed initiatives. It may afford a more consistent regulatory approach to private sector issuers of money and providers of cross-border payments utilities that may be applied on a multi-jurisdictional basis.

Yet there are valid reasons to be concerned when a global behemoth with a track record of massive lobbying of, and, arguably, out-flanking regulators seeks to branch out and set up shop as a Private-Sector Monetary Authority.

The considerations touched on below focus first on Libra, particularly in relation to its intent to eventually support “Unhosted Wallets”. After that are a few observations regarding Novi.

[41] G20 Finance Ministers and Central Bank Governors, in their Communique of Feb 2020, regarding “so-called ‘global stablecoins’” also “look forward to… a report from the IMF on the macroeconomic implications including monetary sovereignty in its member countries – July 2020”.

[42] …including, not uncommonly, highly damaging pro-cyclic interest rate adjustments

But first, a few comments may be in order in relation to whether Facebook's prospects warrant such global mobilization to churn out new regs and otherwise mount the barricades.

Sound and fury, signifying nothing

Facebook, while world leader in its domain of expertise[43], appears to remain a relative tyro with respect to monetary/payment systems. Facebook Credits, which were a dismal bust, have disappeared into the memory hole.

They may be no more clueful this time in terms of fundamentals (though they go to the head of the class in terms of recruiting graduates of the revolving public-private door for compliance and other ambassadorial positions). One indication they may be as lacking in relevant insight as before is their seemingly reflexive embrace of blockchain/DLT dogmas (including a "BFT"[44] consensus protocol classically exemplifying considerations touched on above) and their adoption of all the peculiar usages of terminology as displayed in the FSB consultative document: "coin", "fiat", "stablecoin", "Reserve", "settlement coin" and "convert".

A more coherent approach in building a solution starts with analysis of the problems to be solved and goal definition. With such an approach, choices concerning implementation technologies occur late in the process, partly because tech changes constantly. In fact, to the extent possible, one seeks to be technology-agnostic so a system can be implemented using a variety of technologies.

In Facebook's case, while promotional material for the new Novi wallet makes liberal reference to "blockchain", and "Novi's Approach to Compliance" is content to refer to Libra currencies as cryptocurrencies, it is almost certain that Novi will be a "custodial wallet" implementing a yet-to-be specified/revealed "off-chain" payment mechanism. As an off-chain protocol, it is highly unlikely individual Novi wallets would each be "clients" with "accounts" on the underlying Libra blockchain. It is more likely that Novi, as a VASP—Virtual Asset Service Provider, a category which includes "exchanges and custodial wallets", both of which Novi appears to be—will hold all the ≋XXX backing for Novi balances in its own account(s) on the underlying Libra blockchain. If that is indeed the case, all the brouhaha regarding BFT and whatnot has no direct relevance to payments between Novi wallets. As per Libra[45], "VASPs will facilitate transactions by their users and may record some transactions internally on their own books instead of on the Libra Blockchain". Accordingly, it would be to Facebook's advantage were Novi payments to be implemented via a plain vanilla (i.e. better-engineered) "centrally administered, but highly distributed"[46] architecture/arrangement.

[43] i.e. mining customer information to aid in their manipulation by third parties such as advertisers.

[44] The Libra Byzantine Fault Tolerance (LibraBFT) protocol is classic drink-the-koolade DLT, providing for consensus with respect to "ordering and finalizing transactions among a configurable set of validators…even if at any particular configuration epoch, a threshold of the participants are Byzantine" (DLT-speak for occultly malicious). In the Libra case, this provision for Byzantine Validators comes across a bit like window dressing since at all times at least a two thirds majority of Validators are Founding Members. i.e. "organizations with established reputations, making it unlikely that they would act maliciously". One might reasonably wonder – why bother inviting in a token set of "untrusted" outsiders, especially since implementing this BFT stuff results in transaction latency of about 10 seconds?

[45] Libra White Paper v2.0, Apr 2020, Compliance and the Prevention of Illicit Activity

[46] Debunking Blockchain, D. Jackson, Mar 2018

Returning to Libra, an additional possible indicator of an incoherent approach is inattention to a sustainable revenue model. Even if Libra is not intended to be a cash cow for Association Members, it would be a good idea if it could generate enough revenue to cover costs such as for genuinely effective customer identity verification and due diligence processes. But there is only one reference to "revenue" in the current 29-page Libra White Paper – acknowledging the possible need for transaction fees to cover losses in the event of negative interest rates. As noted below, the direct and indirect costs of proper customer identity verification and due diligence, customer service support, transaction monitoring, compliance with reporting requirements and response to lawful requests may involve biting off more than Members dare chew. There is a not-insignificant chance Libra never launches, at least not as the issuer of distinct new currencies.

Libra-specific issues

There are two areas where Libra, as currently envisioned, may be problematic:

- Unclear designation of responsibility;
- Continued weakness of AML/CFT safeguards.

The buck stops where

The consultative document raises two critical and related concerns with regard to responsibility:

- "effective application and enforcement of a jurisdiction's rules may be difficult as users access services on the Internet and authorities cannot easily locate the provider of the services."
- The "objectives of comprehensive consolidated supervision" are undermined "if there is no entity responsible for the governance of the GSC arrangement or if the back-end core functions (governance, issuance of coins, stabilisation mechanism, or transfer mechanism) of the GSC arrangement are performed by different entities in different jurisdictions."

Private sector provision of the Digital Base Money of an alternative global currency can be conducted in a manner that definitively addresses these concerns. But as matters stand, there is no indication that Libra has any intention of establishing and designating an entity that is ultimately responsible, the place where, as in the memorable phrase of Harry Truman, "The buck stops here". Three examples illustrate how Libra is either being slippery or has simply not thought this through.

Preventing usage in non-approving jurisdictions

Suppose a national government chooses to ban those subject to its jurisdiction from using a particular privately-issued brand of money. The unbacked cryptocurrency community delights in the fact that governments appear to be helpless to prevent such usage. Instead governments resort to the fig leaf of measures to regulate exchange services, as if currency exchange were an obligatory element in every privately-issued money payment transaction.

Libra would appear to be exploiting this pretense that regulating exchange providers (who in turn would be required to implement AML safeguards with respect to their customers) is a sufficient control measure. But it is not. While currency exchange constitutes a disproportionate share of early payments when a new brand of money is first introduced, as network effects develop it becomes increasingly feasible for users to both receive income and pay expenses in that money, with less and less need to exchange to or from local currency.

The issue is the host of end users, or, as Libra phrases it, Unhosted Wallets. While the Libra White Paper has many words regarding its intended "Financial Intelligence Function (FIU-function)", none of them can be taken to mean that Libra will prevent people from using its money except "transactions originating from IP addresses associated with sanctioned jurisdictions".

My suggestion for the FSB and national authorities is to insist on clarity as to whether a private sector provider will prevent usage of its products and services by end users resident in or otherwise subject to the jurisdiction of countries that do not want it in their country.

Service of process

The Libra White Paper has many reassuring words regarding the establishment and responsibilities of its future "Financial Intelligence Function (FIU-function)". But you can't serve a subpoena on a function. And while one might think FIU should stand for "Financial Intelligence Unit", as in a designated entity, it is consistently rendered only as in the preceding sentence.

My suggestion for the FSB and national authorities is to insist on clarity regarding who to contact for service of process or other lawful requests in each jurisdiction.

Customer Service and handling of complaints

The Libra White Paper makes few references to customers/end users and none to "customer service", "customer support" or "complaint"[47]. While "Unhosted Wallets" is presented as the Libra solution to "financial inclusion"—which would suggest Libra anticipates there will be a lot of Unhosted Wallets—it is altogether unclear who the owners of these Unhosted Wallets should reach out to when something goes awry. Examples of things that can result in an end user desperately needing to contact customer support:

- Lost access credentials,
- Compromise of access credentials resulting in an unauthorized transaction draining a Wallet balance,
- Erroneous payment in which the amount was grossly wrong (like an extra zero) or directed to the wrong payment coordinates,
- Complaint regarding another user, such as non-performance or fraud,
- A Wallet that has been administratively blocked or frozen, for unclear reasons or perhaps in error.

My suggestion for the FSB and national authorities is to insist on clarity regarding who is responsible for handling customer service/support. This goes beyond "dispute resolution mechanisms or procedures for seeking redress or lodging complaints".

Gaming regulatory requirements for CIP and CDD

Watered down CIP

Libra offers a lot of soothing words regarding its intention to establish robust and compliant AML/CFT capabilities. Yet it is quite vague with respect to whether any identity verification would be required of the owners/users of Unhosted Wallets or, if so, who would perform it. Instead, emphasis is placed on protocol level controls of "transaction [throughput] and address balance limits" and measures to detect circumvention by a perp controlling multiple wallets. The only (two) references to "identity" per se refer

[47] For that matter, the consultative document only makes a single reference to "complaints".

to a hoped-for "open identity standard", a goal that has managed to elude multiple startups and consortia devoted to that task for over two decades.

If and as Libra proceeds, arguments may be advanced that it does not need to perform actual identity verification and due diligence as required for legacy systems because "The Internet Knows You Better Than Your Spouse Does". This may be true in terms of social networks (and their data-purchasing customers) being able to manipulate individuals (whoever they actually are) in terms of their purchasing, voting in elections or other decisions but that is different than actual identity verification. There are times when the police actually need to go to the right door. And the fact is, most examples of crimes involving purchase of illegal goods/services are small ticket transactions, well under any throughput or balance limits that might be imposed.

Ineffective CDD

Even more important is due diligence of business customers. Without an understanding of what a member business does and how it intends to use the system. the door is wide open to a deluge of Ponzi schemes and goodness knows what else. Libra contemplates all the guest worker remittances that it might facilitate but, at least initially, for every would-be remittance sender there are probably twenty would-be 'Participant Perps'[48] avidly seeking to get in on the ground floor of an "HYIP"[49].

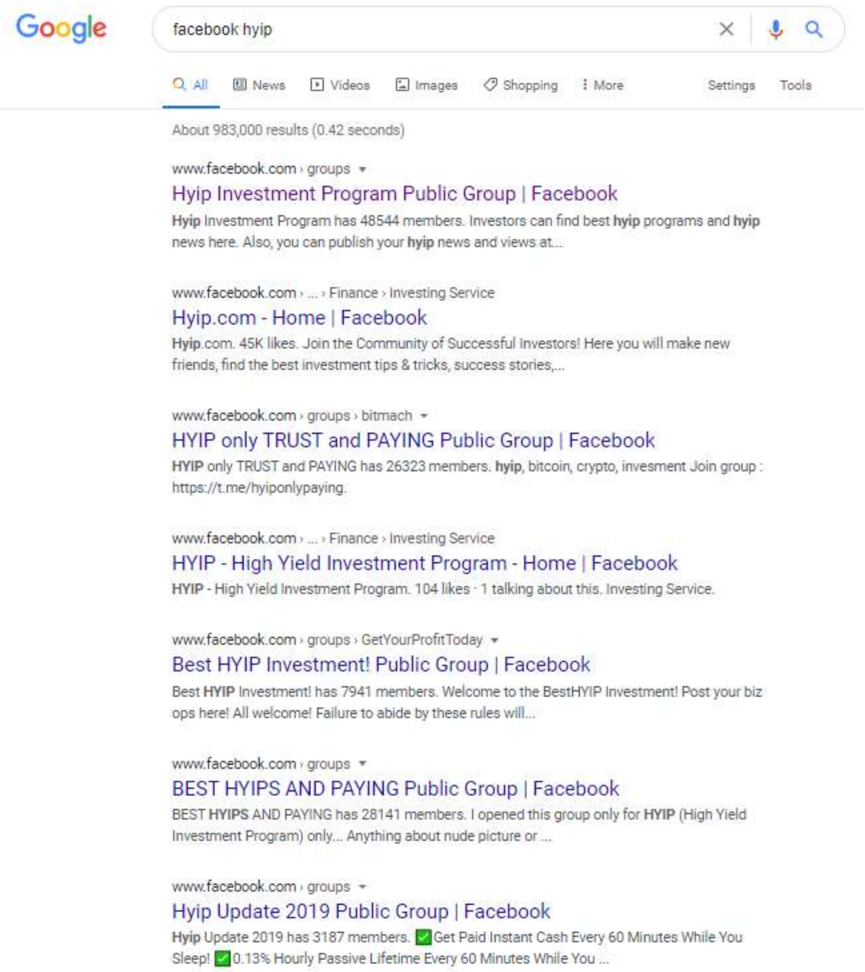
Facebook must contemplate the business risk that the CDD necessary to determine whether a business customer is legitimate may alienate a significant portion of its user base.

I don't have a FB account so I can't check out the following, but a google search using "Facebook" and "hyip" as search terms immediately yields plus or minus 1 million hits[50], the first few of which are:

[48] HYIPs entail two roles: Organizer Perps (who establish and operate the scheme) and Participant Perps who avidly seek out HYIPs, send them money and shill for them, hustling to build their "downstream" before the scheme collapses. Participant Perps are also known as "victims", a shape-shift phenomenon that occurs when expedient which entails an instant transformation from presenting oneself as sophisticated investor living on yacht funded by passive income to blind orphan disabled veteran living in trailer park.

[49] An "HYIP" (High-Yield Investment Program) is an internet-based Ponzi scheme organized on an MLM (Multi-level Marketing) basis.

[50] Facebook may be starting to crack down on the investment scams within its user base. The google search that yielded >1.1 million HYIPs in early June has dropped week by week and now (July 2020) ranges from ~800-900k.



About 983,000 results (0.42 seconds)

www.facebook.com › groups
Hyip Investment Program Public Group | Facebook
Hyip Investment Program has 48544 members. Investors can find best **hyip** programs and **hyip** news here. Also, you can publish your **hyip** news and views at...

www.facebook.com › ... › Finance › Investing Service
Hyip.com - Home | Facebook
Hyip.com. 45K likes. Join the Community of Successful Investors! Here you will make new friends, find the best investment tips & tricks, success stories,...

www.facebook.com › groups › bitmach
HYIP only TRUST and PAYING Public Group | Facebook
HYIP only TRUST and PAYING has 26323 members. **hyip**, bitcoin, crypto, invesment Join group : https://t.me/hyiponlypaying.

www.facebook.com › ... › Finance › Investing Service
HYIP - High Yield Investment Program - Home | Facebook
HYIP - High Yield Investment Program. 104 likes · 1 talking about this. Investing Service.

www.facebook.com › groups › GetYourProfitToday
Best HYIP Investment! Public Group | Facebook
Best **HYIP** Investment! has 7941 members. Welcome to the BestHYIP Investment! Post your biz ops here! All welcome! Failure to abide by these rules will...

www.facebook.com › groups
BEST HYIPS AND PAYING Public Group | Facebook
BEST **HYIPS** AND PAYING has 28141 members. I opened this group only for **HYIP** (High Yield Investment Program) only... Anything about nude picture or ...

www.facebook.com › groups
Hyip Update 2019 Public Group | Facebook
Hyip Update 2019 has 3187 members. ✅Get Paid Instant Cash Every 60 Minutes While You Sleep! ✅0.13% Hourly Passive Lifetime Every 60 Minutes While You ...

One can only imagine the arms race to obfuscate such (currently overt) listings that will ensue should Libra/Novi facilitate the ability to ability to conveniently "invest" in such schemes seamlessly, with no need to exit the comfort and convenience of your WhatsApp or Facebook Messenger App.

Anonymity

As with the cryptocurrency community in general, Libra talks out of both sides of its mouth with respect to anonymity. The Libra White Paper is resplendent with assurances of how its Financial Intelligence ~~Unit~~ Function will prevent abuse. But the techies it has hired to gin up the "Libra Blockchain" need not observe such pretenses when Dad isn't listening or they are speaking in a code he is too dim to grasp. Recall "We anticipate that many payment transactions will occur off-chain, for example, within a custodial wallet or by using payment channels".

In the paper they reference for an updated explication of channels, section "V. ANONYMITY AND PRIVACY", is devoted to techniques for thwarting "an adversary" (i.e. regulators, law enforcement and other snoops) so presumptuous as to try to compromise "unlinkability and untraceability properties".

Novi-specific issues:

Privacy

One of the biggest concerns with Facebook is their history of exploiting data regarding customer behaviors and preferences to facilitate their sale of services such as targeted ads. Their new brightline distinction between Libra and Novi indicates "Aside from limited cases, **Novi will not share account information or financial data with Facebook, Inc. or any third party without customer consent. For example, Novi customers' account information and financial data will not be used to improve ad targeting on the Facebook, Inc. family of products**". [selective bolding in the original].

My suggestion for the FSB and national authorities is to insist on:

- ***a) Clarity and Specificity: as to those "limited cases" in which such information might be shared;***
- ***b) Oversight: regulatory guidelines as to cases where information sharing might occur;***
- ***c) Transparency: anonymized publishing of complete data on such user data sharing events to support both regulators and independent third parties in conducting audits;***
- ***d) Proxies: that each customer must appoint an independent legal proxy to represent their interests and whose approval would be required for such information sharing changes, and/or;***
- ***e) Contract: other limitations as to the effect of end-users 'clicking' their acceptance of, say, 'changes to our privacy policy' that would affect details of those purportedly limited cases.***

It is, however, not especially auspicious that merely visiting the Novi website might lead to infestation with "embedded content" cookies:

Third Party / Embedded Content	These cookies enhance the experience of Website users. These cookies allow you to share what you've been doing on our Site with social media organizations such as Facebook and Twitter. We have no control over the information collected by these cookies.

Transparency

From the Novi FAQ:

"Will Novi charge fees?

What you send is what they get. You can add, send, receive, and withdraw money from your wallet without worrying about hidden charges. Novi is cutting fees to help people keep more of their money."

Was that a yes or a no?

The pretty animated graphic showing a mock-up of a cross-border, cross-currency payment—in which the payer (a Dad-looking chap with a gray beard) spends 100 ≋USD and the recipient (Mateo, a young man). will "get 81.90 ≋GBP"—proclaims "Fees: 0.00". Inquiring minds might be curious to know how much ≋USD Pop would receive were Mateo to immediately spend back his 81.90 ≋GBP. Exchange rate spreads (between these two Libra-currency-variants) apparently don't count as fees.

But this is nothing new. All countries have tolerated this sophistry for decades with conventional remittance services, and banks.

Appendix 1: Debunking Blockchain[51] and DLT

As noted above, the usage of terms such as "crypto-asset", "coin" "validator node" throughout the consultative document are all predicated on the presumption that blockchain and the related notion of Distributed Ledger Technology (DLT) represent epochal breakthroughs in technology that will enable mankind to transcend all the problems of legacy arrangements for money and payments. But this not only misdiagnoses the problems of legacy systems but also advocates a technological approach that is inherently inferior in terms of critical metrics such as latency of transactions and scalability.

While blockchain/DLT continues to be the banner under which many new initiatives are touted, the unmistakable direction of later generation systems is to repudiate all of the original imperatives of blockchain technology – eliminating blocks, cipher block chaining and massive redundancy of records. The anonymity of unbacked cryptocurrencies however, while continuing to be downplayed for credulous regulators, is being hardened. More broadly, with respect to both public unpermissioned and private permissioned networks, the core shibboleth and legacy feature of DLT—the avoidance of centralized administration—continues to be a source of unnecessary complexity and inefficiency arising from the need for "Byzantine" consensus protocols.

While the technology-related aspects of a system are of critical importance, insisting on a particular technical solution as the starting premise or foundation for a system is to put the cart before the horse. Design and implementation of coherent systematic solutions, especially providing for money and payments, requires the integration of well-conceived institutional arrangements, sound monetary principles and sustainable business models or other economic incentives for participants.

To briefly summarize:

1) So-called "Distributed Ledger Technology" embodies a peculiar and aberrant take on the well-established principles of distributed computing that results in absurd inefficiencies that unnecessarily increase costs, hinder scalability and result in pernicious side effects. Blockchain/DLT systems may achieve efficiency and scale only by deviating from canonical blockchain dogmas in the direction of the already well-understood network engineering principles that inform genuinely well-engineered distributed systems.
2) Unbacked cryptocurrencies are play money wholly unsuited to serve as reserve assets or media of settlement. Moreover, existing and proposed blockchain/DLT arrangements are also unsuitable to be used as platforms for the issuance, distribution, circulation, redemption and de-issuance of real money, especially the critical category of Digital Base Money, whether issued by central banks or private sector institutions.
3) Most if not all economically useful use cases that have been proposed as arguments favoring blockchain/DLT technical solutions can be addressed more effectively with systems implementing other technologies.

Core blockchain/DLT dogmas/fallacies

The foundational themes of blockchain/DLT promoters were and remain:

[51] These issues are explored in greater depth in the (draft) analysis "Debunking Blockchain: The case for centrally administered, but highly distributed, financial utilities"

- The ascription of unspecified horrors stemming from any role for “trusted third parties”,
- Misrepresentation of principles for distributed system architectures accompanied by denunciations of “single points of failure” purported to infest any/all systems that do not travel under the banner of blockchain/DLT.

Trust Issues

Trust and/or the lack thereof between third parties has always been a core fixation of game theory, the favored hobbyhorse of cypherpunks – the Cool Kids who instigated the crypto frenzy of the past decade. In the crypto mantra espoused by “Satoshi Nakamoto”, the idea that trusted third parties were a scourge to be avoided at any cost was treated as a given. The only example of the vile deeds that might be perpetrated by such boogeymen was a passing reference to payment repudiation, as if to imply chargebacks in credit-based payment systems were due to some sort of deficiency of technologies relating to data persistence or the determination of whether a submitted transaction/settlement instruction was in conformity with system rules.

The proximate result was Bitcoin, a huge step backward in terms of transaction latency, system scalability, infrastructural overhead and even environmental costs. This was of course followed by innumerable other unbacked cryptocurrencies as promoters sought to cash in the speculative bonanza and geyser of funding from herd mentality investors avid to get a piece of anything involving or, even with a name implying, blockchain.

Ironically, as detailed in the referenced Debunking paper, all these systems were and remain *riddled* with the necessity of trusting all manner of third parties. But rather than eliminating the need for the blindest, most abject trust, the realty with public blockchains is that there is no one who can be held responsible (or even provide customer assistance) when things go wrong. And things will always go wrong from time to time, with any system[52].

In the present context of course—monetary media backed by some sort of asset portfolio—the idea of avoiding responsible third parties is too ridiculous to contemplate. Known parties must be responsible for ensuring suitable earmarked assets are held in appropriate legal/custodial arrangements against real money liabilities. The authors of the consultative document managed to reduce usage of the term “trusted third party” to just one occurrence[53], albeit one that illustrates how this meme continues to be imprinted in the minds of people who should know better.

An additional irony relating to the trust issue is the fact that algorithmic stabilization schemes are given credence in the document. The sustainability of such mechanisms depends on public confidence[54] (i.e. trust), the idea that an ignorant/avaricious or apathetic public, accustomed to deposit insurance and other government mechanisms that reduce the incentive to make personal evaluations of financial risk, will trust the mumbo jumbo of an algorithm sufficiently to indefinitely defer eventual panic and collapse as

[52] A recent example, just one of countless other incidents of loss, involved the host of the (blockchain/DLT oriented) “Protocol Podcast” who irrevocably lost his stash of Bitcoin, assiduously accumulated over seven years, when he downloaded a malicious wallet app from the Google Store.

[53] The specific reference, on p.9, clearly is in contemplation of a consensus mechanism, the remaining bugaboo of so-called “DLT”. The illogic of consensus mechanisms is addressed below.

[54] The traditional term for a scheme that takes advantage of misplaced trust is “con game”.

would occur were people to realize that the entity has insufficient assets to buy back more than a small fraction of the money it has issued.

Single point of failure

The crypto community has made denunciations of a potential single point of failure into a parlor game in which adepts rack up points by pointing them out, real or imagined, and wringing their hands over them. This is done in obedience to the Cool Kids who have managed to inculcate the misconception that avoidance of such was an insight they were first to conceive.

In reality, identifying, analyzing and avoiding potential single points of failure, to the extent practicable when multiple other constraints are taken into consideration, has been part of the DNA of software engineers and network architects as well as their counterparts in the engineering disciplines concerned with physical devices/systems since, well, forever.

Such concern with and sensitivity to potential single points of failure is a subset of a broader need for risk assessment and discovery/implementation of measures to mitigate identified risks.

Consensus mechanisms

As noted, current private network (permissioned) initiatives involving money and payments have for the most part quietly moved away from their blockchain and DLT origins even if, for funding/marketing/promotional purposes they still pose as such. The last vestige of their DLT baggage, if any remains, tends to be incorporation of, or at least provision for, some sort of consensus protocol/mechanism.

The notion of a consensus mechanism warrants close scrutiny, both to expose its foundational logic and the self-serving deceitfulness of vendors seeking to take advantage of the gullibility of decision makers who might select such systems for payments/settlement production environments.

In a payments protocol that implements a DLT model, what sort of questions/determinations require the consensus of mutually distrusting and potentially malicious third parties? Most typically the issue is whether to commit/persist a transaction/event or some other chunk of data to the ledger, database or other persistence mechanism. What are the determinant criteria? Well, what other question can there be other than whether the candidate transaction conforms to system rules?

All computer-based applications, regardless of system design, are based on software logic that determines whether an input is valid and then processes it in accordance with defined system rules. Some implementations may entail some sort of two-phase commit that requires a prescribed number or proportion of servers to 'agree' as a means of ensuring consistency. But all such servers that may be 'voting' are applying the same system rules implemented in the same computer code. This is going to be true whether the servers[55] (nodes) all belong to or are operated under the authority/auspices of an entity

[55] Or "containers", as is increasingly common with modern highly distributed architectures (less so with DLT schemes, though some are starting to catch up).

serving as a centrally administered utility such as a clearinghouse or if the individual nodes belong to mutually distrusting participants such as banks that are all in competition with each other[56].

But the latter case, characteristic of so-called DLT, is problematic. The logic of a plain vanilla two-phase commit arrangement, while by no means trivial, is quite straightforward in comparison to the "Byzantine" consensus mechanisms typical of self-styled DLT schemes. As a general rule, providing for Byzantine Fault Tolerance[57] (where for goodness-knows-what-reason a mutually untrusting set of validators must work together to accomplish what would be so much simpler if the pertinent nodes were under the control of a single administrative entity) adds computational and network-architectural overhead that tends to greatly complicate strategies for reducing transaction latency or supporting massive scalability.

Moreover, organizing a private network in accordance with the latter model leads to what may be thought of a "digital islands". This means that, effectively, all participants in a DLT/private network or specified market (such as the recently touted "Nasdaq Marketplace Service" are obliged to use the same software vendor. The actual DLT tech may have so little to do with DLT per se (and almost certainly no vestige of blockchain) as to be nothing more than marketing jargon. Any claimed efficiencies derive strictly from everyone using the same software. But this comes at a price.

Digital Islands

Contrast two arrangements for clearing/settling payments. One is a centrally administered (albeit highly distributed) utility such as a clearing house. The other is a DLT scheme involving a private network in which participants own/operate or otherwise are associated with or represented by their own nodes.

With the centrally administered utility, one entity is responsible for implementing and operating a system that performs functions regarded as useful to third parties who may matriculate as system participants or customers. It attends to the technical details of ensuring system/network performance and may even proffer some sort of Service Level Agreement warranting metrics such as capacity, availability/uptime or transaction latency. If the data persistence logic implemented by the utility happens to entail a two-phase commit, such technical details are not such as to inspire advocacy and zeal or new regulatory rubrics that incorporate such arcana into new taxonomies. The network maintained by or on behalf of the utility may entail hundreds of nodes, the operation and maintenance of all which are the direct or indirect responsibility of the clearinghouse, which bears responsibility and is liable for operational risk.

[56] For instance, R3's "Corda" marketing material uses jazzy terms that subdivide consensus tasks into "validity consensus" (does a pending transaction conform to system rules?) and "uniqueness consensus" (prevention of double-spends, a task performed by "Notary Clusters", which may or may not be "validating"). But every clearing and settlement system ever implemented, ranging from the banknote exchange operated by the Suffolk Bank in the 1830's to CHIPS, CHAPS, RINGS etc. has provided such functionality. Otherwise, i.e. if it had no means of doing the most fundamental validation and bookkeeping tasks, it would have never become operational.

[57] The blockchain/DLT literature is replete with references to the Byzantine Generals Problem, a favorite concern of game theory aficionados – a set of which Cypherpunks comprise a proper subset. In this predicament, "a group of generals of the Byzantine army [are] camped with their troops around an enemy city. Communicating only by messenger, the generals must agree upon a common battle plan. However, one or more of them may be traitors who will try to confuse the others. The problem is to find an algorithm to ensure that the loyal generals will reach agreement." The situation is further complicated due to the failure of some messages to arrive in a timely fashion or at all.

The centrally administered utility, let's say a clearinghouse, commonly exposes a set of APIs. This enables the utility's participants/customers to choose from a host of competing vendors that offer banking software products/services, all of which build to interface to the API, enabling their customers to make use of the clearinghouse.

Alternatively, a jurisdictional authority or a group of financial institutions may elect to establish a DLT-based system for clearing/settlement of payments. In this case, each direct participant maintains or is associated with a node or set of nodes for which it most likely pays a subscription/licensing fee to whichever DLT scheme provider has managed to assemble this cohort of customers. The banks or broker-dealers that have their various nodes can be likened to children on an amusement park ride that whirls little cars around, each with its own pretend steering wheel, enabling the kiddies to imagine that their fiddling with their little steering wheel is in some way controlling something[58]. But each node implements whatever system logic it is designed to implement, as occurs with the various nodes in the centrally administered system. If there are parameters that can be modulated, they do NOT affect the decision whether particular transactions, such as those of between a pair of untrusted competitors, will be committed to the ledger. All that has been accomplished by the DLT arrangement, and its DLT consensus mechanism has been to force all participants to enrich the winning scheme provider, even as other jurisdictions/cohorts may have selected other, incompatible scheme providers.

The resultant emergence of digital islands, each organized around its particular arcane Rube Goldberg consensus mechanism-based private network, may then give rise to an additional layer of complexity as schemes are proposed to enable interoperability[59] between the islands.

What has commonly been de-emphasized in reports of the numerous "proofs of concept" and other trials of DLT schemes for clearing and settlement of payments is that none perform as well as existing systems and none appear to be massively scalable unless the actual DLT bits (i.e. need for consensus models) are quietly ditched.

Moreover, in relation to the biggest problem in payments – cross-border, cross-currency payments – it couldn't be more obvious that the real issue hasn't been benighted tech, crippled by a dearth of blockchain until Satoshi came down from the mountaintop and showed us the way. It's always been the lack of a suitably well-conceived and soundly implemented common medium of settlement, one that, unlike USD, fulfills the need for a global common good.

[58] For example, see the Libra discussion above detailing how untrusted Validators in Libra's variant of the "Hotstuff" BFT consensus model, though they may feel like they are doing something important, are always outvoted by Libra Founding members.

[59] For instance the International Chamber of Commerce recently announced its Digital Trade Standards Initiative to "facilitate technical interoperability among the variety of blockchain-based networks", and thereby "connect existing digital islands".

Appendix 2: Algorithmic stabilization

Algorithmic stabilization schemes rest on the following premises/principles:

- While theoretically possible that a large proportion or all holders of certain demand liabilities may all at once demand their immediate redemption, for instance in a cascading panic typified by an old-timey bank run, they normally don't. Their disinclination to run (the inverse of their propensity to panic and run) is a function of their confidence.
- Confidence may be fostered by a variety of means such as by having an advisory board of high reputation luminaries, using integral and derivative symbols in your pricing model (with extra points for Monte Carlo simulations) and, especially, by demonstrating the ability to immediately honor and fulfill demand obligations. It is therefore expedient, initially, to maintain the ability to immediately honor all obligations. Later, as confidence becomes more habitual, fewer people are likely to pay much attention or care if the ability to meet all obligations is gradually hollowed out (examples being the Bank of Amsterdam, Bernie Madoff and, apparently, Wirecard).
- Stochastic estimation of the risk of a cascading, contagion-driven, run provides a statistical basis for determining how large a buffer should be maintained to quell the outbreak of a run. It is the same sort of calculation/estimation of synthetic maturity that informs liquidity coverage ratios (and used to be used for formulating required reserve ratios).
- Third party providers of currency exchange services constitute a reservoir of liquidity that diminish the need for the issuer to backstop markets by serving as the market of last resort, the one entity that can and will buy back money at par even if no one else can or will.

The inherent cynicism of this sort of confidence game was ably articulated[60] and exploited[61] by Alan Blinder, Former Vice-Chairman of the Federal Reserve, in relation to government-administered Deposit Insurance ("DI"), complete with a reference to the "100 year flood" as beloved by such apologists as the "six-sigma event".

> "DI contributes to stability principally by mitigating or preventing bank runs. As a side benefit, effective deposit insurance also protects small depositors from loss if their banks fail. But we would argue that protecting the small depositor is an incidental benefit, not the main social purpose of DI."

Every brand of real money entails an Issuer that carries all Base Money issued and outstanding as balance sheet liabilities, offset by earmarked assets affording it the wherewithal to buy back and extinguish any or all of the money[62]. A reduction in demand for a particular Currency can (eventually) be offset by a reduction in the quantity in circulation. In the case of a currency board model, any deviation in exchange

[60] 'Reform of Deposit Insurance – a Report to the FDIC', Mar 2001, A. Blinder, R. Wescott

[61] 'The mess that is deposit insurance', Aug 2010, F. Salmon quoting N. Taleb: "In other words, it would allow the super-rich to scam taxpayers by getting free government sponsored insurance. Yes, scam taxpayers. Legally. With the help of former civil servants who have an insider edge."

[62] The current situation for national central banks in the Eurosystem may be an exception due to peculiarities of the TARGET2 mechanism, a clearing house that never clears. For example, 46% of the assets on the balance sheet of the Bundesbank consist of claims on the TARGET2 system. These are assets for which no market exists or could exist.

value from that of the designated outside money creates self-correcting arbitrage opportunities and the adjustment is almost immediate.

With an unbacked cryptocurrency, obviously, there is no mechanism for reduction of the quantity in circulation. A decrease in overall demand for such play money leads directly to a decrease in its exchange rate relative to real money.

With anything less than full backing, regardless of any algorithm, the possibility always exists of a sudden loss of confidence of a magnitude that burns through trading balances of third parties electively making a market, perhaps so abruptly as to cause them to default on their obligations. It is then that holders of the money pay attention to the fact that the issuer lacks the means to buy back all (or perhaps any) of the money.

When such an event occurs, it is always unexpected and all are astounded by such an unpredictable/ leptokurtotic tail event.

In contrast, while the consultative document expresses concerns of possible illiquidity or fire sales of backing assets impairing the ability of an entity such as Libra to meet redemption obligations in a timely manner, were it to indeed, as specified, maintain a stronger balance sheet than any bank, this would neutralize any tipping point or cascade type phenomenon, attenuating rather than amplifying such panic impulses. A private sector issuer of money with a bullet proof balance sheet is more likely to survive a financial system collapse than are most banks and all entities relying on an algorithmic stabilization mechanism.

Appendix 3: "is this thing counterfeit or legitimate?"

In relation to the question "is this thing counterfeit or legitimate?", long before cryptocurrencies and noise about "token-based money", widely used Shopping Cart Interfaces such as the one developed/deployed by e-gold.com (very much an "account-based system") provided a merchant with notification of received payment which could be validated by cryptographic means enabling sufficient confidence that correct and final payment had been received as to warrant automatic release of goods/services for electronic or physical delivery. A simple example excerpted from the 2004 specification for this notification:

> "Example of V2_HASH
>
> Assume input from merchant using e-gold account 123456 of: **`PAYMENT_ID = AB-123`**
>
> Has an alternate passphrase of "ohboyi'msogood1". [(Only) the MD5 hash of which was on file in the e-gold account records for that merchant]. This merchant receives a payment via the e-gold® shopping cart for $300.00 USD worth of gold from e-gold account 456789. The values returned from the e-gold® system to the merchant via his STATUS_URL input are:

```
PAYMENT_ID = AB-123
PAYEE_ACCOUNT = 123456
PAYMENT_AMOUNT = 300.00
PAYMENT_UNITS = 1
PAYMENT_METAL_ID = 1
PAYMENT_BATCH_NUM = 789012
PAYER_ACCOUNT = 456789
ACTUAL_PAYMENT_OUNCES = 2.000000
```

```
USD_PER_OUNCE = 600.00
FEEWEIGHT = 0.000833
TIMESTAMPGMT = 876543210
```

> First we compute the MD5 hash of the merchant's alternate passphrase. It is: **67C305DCE49D430D540FCB3D6D2E13B0** [Again, only the hashed value of this "alternate passphrase" was actually stored in the e-gold database]. We can now build our concatenated string to hash for a comparison with the V2_HASH returned from e-gold®. The concatenated string is:
> AB-123:123456:300.00:1:1:789012:456789:67C305DCE49D430D540FCB3D6D2E13B0:2.000000:
> 600.00:0.000833:876543210
>
> When we perform an MD5 hash on this string we get:
> **7F8FAF7DB12315BC2B4B06E163F78D31**
> And that is the expected value that should arrive in the V2_HASH field from e-gold."

Voila! A token "7F8FAF7DB12315BC2B4B06E163F78D31" from an overtly "account-based system" required and sufficient for "the payee to be satisfied with the validity of the payment".

This same general logic, hashing a concatenation of (the values of) a bunch of different fields, including (for each transaction) the payment amount and the coordinates of the recipient, is used for generating payment instructions (tokens!) in essentially all so-called "token-based" systems. Whether or not to employ asymmetric cryptographic technology such as using a private key controlled by the payer to digitally sign (or sign and encrypt) the payment instruction has no bearing on the fact that it is still just a payment instruction that, if it meets system rules and requirements, will result in decrementing the money balance of the payer and an increment of that of the designated recipient (notwithstanding that, with Bitcoin and similar systems, directing a payment to an otherwise valid address, control of which has been lost, can result in value irrevocably lost in the ether).

Appendix 4: Misuse of "Fiat"

The term "fiat" appears 15 times in the document, 14 as "fiat currency" or currencies, once as "fiat money". In every case it is used in obedience with the usage the crypto community favors, as a synonym or shorthand for 'government-issued money'. This emphasis could be claimed to derive from many centuries of usage of the word "fiat" in legal contexts that involved (government or court) decree. But fiat money really means money that, on the discretionary vs. rules-based axis, lies toward the pole of *arbitrary* (i.e. discretionary) policies. There have been, and there continue to be, multiple instances of government-issued money that it would be inaccurate to describe as "fiat". And, as noted below, some of the most fiat media of exchange ever to see the light of day have been 'pre-mined' cryptocurrencies.

This f-word, reminiscent of another much more infamous label, was first used as a pejorative term. Its first usage as an adjective pertaining to money appears to have been in 1816 as the English economy was in the throes of the whipsaw effects—severe boom-inducing inflation, followed by ruinous deflation—caused when the Bank of England suspended gold convertibility to finance the Napoleonic wars and later restored it. Prior to this episode, there was a long history of government involvement in the arrangements governing the British Pound but no one felt moved to apply this f-word.

First known: C. R. Prinsep, "An Essay on Money" [In response to "Proposals for an Economical and Secure Currency; with Observations on the Profits of the Bank of England, etc." By David Ricardo esq. London 1816] in The Edinburgh Review or Critical Journal, Volume 62, December 1818, p.80.

"While it is the power of the Directors of the Bank of England to increase or diminish the amount of currency in the country at their pleasure, no person can form any probable estimate of the value of his property at any period but a little remote. The estate that is purchased today, and reckoned a good bargain, may, by the Bank's limiting its discounts, or withdrawing its notes from circulation, be rendered, in a very short time, not worth half the sum paid for it: And, on the contrary, if the Directors were more liberal in granting discounts, and increased the number of their notes in circulation, either by lending to the State or to individuals, the estate might speedily become worth double the money, that is, double the paper it had been sold for. This artificial and unnatural system, renders the *money value* of all the property in the empire, on the views and opinions—the whims and caprices—of *twenty-four* individuals. It is their fiat alone which makes transaction good, and another bad. They hold the scale of value, and change its graduation as they hold proper."

The root of the problem, per Prinsep, was the "at their pleasure" and "whims and caprices" aspect.

In the second known published usage (1820), an author styling himself as VINDEX, exercised by the same episode of monetary mayhem, took pains to emphasize the "arbitrary" nature of such "fiat" manipulations.

The Pamphleteer; "Observations on the present National Distress".

Having spoken of a hypothetical prince who "had debased and reduced his coin or current medium" in order to reduce his outstanding debt, later, "when all sort of money transactions had been accommodated to the new measure of value…this **arbitrary** prince, by his **arbitrary** fiat" restores the coin or currency to its original purity and intrinsic value. [Emphasis added]

The word pair "fiat money" did not appear in print until 1879 though, once it did appear, the term began to appear in multiple publications. The context was another disruptive monetary episode arising from suspension and restoration of gold convertibility, this time in the US. The US government, in a replay of the monetary manipulations that funded the Napoleonic wars, and a prelude to the monetary machinations of World War I, had financed its 1860's civil war by debasing the money supply, issuing irredeemable greenbacks. Subsequently, in 1875 Congress moved to restore convertibility, and the prospect of the deflationary consequences resumption would entail was deeply polarizing.

The official organ of the American Bankers' Association (established in 1875), "The Banker's Magazine" Volume 33, 1879 applied the term fiat money as shorthand for irredeemable money. An article "Fiat Money in England" held forth that "The theory of a Government redeemable currency, not protected by a deposit of coin, dollar for dollar, is a delusion, and that of an irredeemable fiat money a dangerous experiment".

Similarly, Congress at the epicenter of the dispute, embraced the term. "The Report and Accompanying Documents of the National Monetary Commission organized under the Joint Resolution of August 15, 1876", aired the "Views of the metallic school", contrasting them with "Views of the Paper, or Fiat Money School".

Such usage of the term “fiat money”, to denote irredeemable money, the value of which is a function of arbitrary discretionary determinations, was universal until about a decade ago when the ‘cool kids’ found it expedient as a label for all government-issued money. By emphasizing the coercive or authoritarian[63] connotations of the term, rather than the arbitrary aspects epitomized by irredeemability, the desired effect—of selectively applying a pejorative term to government issued money, thereby casting cryptocurrencies as a positive alternative—was achieved.

But the fact is that a number of government-issued brands of money—those issued in accordance with a currency board model—are rules-based and redeemable, while the most egregiously fiat (arbitrary, irredeemable) would-be media of exchange to ever be pawned off on the public have in fact been unbacked cryptocurrencies. Ripple, for example, created an arbitrary number of unbacked tokens, 100 billion of them—consisting strictly of numbers, with no earmarked portfolio of assets for anchoring them to any particular value, and with no obligation to buy them back at any price—and sold them to the public. Tens of billions of them, raking in over a billion USD in real money.

My recommendation is that you reject this usage of the term “fiat” as shorthand for government-issued money and, if used at all, apply it instead to money that is issued on an arbitrary, discretionary, irredeemable basis.

[63] Prior to the 1870’s there seems to have been only one outlier. In 1843, Sir Travers Twiss, in a lecture “On Money and Currency”, did apply the term “fiat” to emphasize the coercive role of state authority. Contrasting a bank note to paper money stamped with the imprimatur of the state, he held forth: “the former is strictly so much credit; the latter professes to be so much value: the former rests on general confidence, the latter on the fiat or authority of the state.” But Twiss was a jurist and monetary economics was not his field.

Appendix 5: Definitions

The following list of proposed definitions does not include a new label for securities or other financial assets other than Money since they already have serviceable definitions for which it is not necessary to append modifiers relating to whether they are in digital or “crypto” form.

Base Money means **Money**, for which a **Monetary Authority** is directly liable, serving as the medium in which like-denominated **Broad Money** is payable.

Broad Money means **Monetary Liabilities** of a **Person** other than a **Monetary Authority** which are payable on demand or at maturity in like-denominated **Base Money**.

A **Deposit** (noun) means a liability of a **Person** (e.g. a bank) payable on demand or at maturity, offered without legal requirement of prospectus and used as a means of funding an asset portfolio which may include remunerative assets, gains or losses from which inure to the benefit or detriment of the **Person** for whom/which the deposit constitutes a liability. A **Deposit** also means the corresponding asset of the depositor.

Digital Base Money means **Base Money** instantiated in digital form.

Issuance (of **Money**) means the act or process of creating **Base Money**.

Legal Person (or **Juristic Person**) means an entity other than a **Natural Person** recognized by law as the subject of rights and duties.

Monetary Authority means a **Person** responsible for the **Issuance** of the **Base Money** of a particular brand of **Money** and provision of a mechanism for settling transfers of that **Base Money**.

Monetary Liability is a subset of the accounting primitive “liability” that specifically refers to **Money** that has been **Issued** by the **Person** for whom/which it constitutes a liability and remains outstanding.

Money is a branded liability of a **Person**, or physical tokens the value of which derive from the materials of which they are composed, created to serve as a medium of exchange, quantities of which are denominated and expressed in particular units designated as specific to that brand of **money**. For its owner or beneficial owner, **Money** is a current asset.

Natural Person means a human being.

Person means a Natural Person or a Legal Person.

Privately-issued Money means Money the Base Money of which is Issued under the auspices of a Private-Sector Monetary Authority.

Private-Sector Monetary Authority means a **Monetary Authority** for which a **Person** or **Persons** other than a government is responsible.