Owner Credit / Wealth Coin

Perry Kundert

2018-02-16 17:51:00

A secure, distributed method for creating dynamically stable monetary systems, where each unit is defined/created by the ownership of real wealth.

After another tragic flirtation with central planning, at the beginning of the 21st century the global fiat credit system imploded. PDF / Text

Now that the dollar is in full-on decline as the world's de-facto reserve currency, other even less friendly authorities are lining up to take its place.

Do you really, *really* want to do this all again?

Contents

1 Dynamically Stable Currencies

Central planners have proven themselves unworthy of "managing" currencies, probably due to the fact that these groups are composed of people, and people are subject to greed. Therefore, it is necessary to establish currencies which have a value that is mathematically related to the intrinsic value of physical, widely traded commodities. Just as units of temperature are related in some widely known way to physical heat and cold, units of currency would be related to the rising and falling true "value" of a basket of commodities (KWh of electrical power, Kilograms of gold, Tonnes of cereal grains, live chickens, whatever).

The function of banks, traditionally the "creators" of credit (often by proxy for a central bank), would be relegated to the menial role of "aggregators" of credit – credit would be created by those who create the actual underlying wealth.

Finally, the value of the unit of currency would be held dynamically stable, by varying a credit factor K (the amount of credit created per unit of wealth), as the price of the basket of commodities increases and decreases (inflates and deflates). In an economy where the underlying commodities are heavily traded, the value of the basket could be priced on a literally sub-second basis, and the credit factor K updated continuously in sub-second real-time (using an industrial process-control feedback damping control algorithm called a PID control loop).

As a result, several good things would happen:

1. The creation and ownership of wealth – by individuals – would be immediately convertible to credit in a currency, proportional to the credit factor K. The value of the unit of currency is held, dynamically and immutably, equivalent to the value of the basket of commodities defining the currency.

    - New credit would be created proportionally to the creation of new wealth, and by the ebb and flow of liquid credit within the economy; as prices decline (deflation), K increases, allowing new credit to be created, to purchase the under-priced wealth. As prices increase (inflate), the inverse occurs (encouraging the selling of wealth for credit which is stored up or used to redeem previously pledged wealth), driving excess liquidity from the economy.
    - All factors influencing the value of the currency (commodity prices, inflation/deflation, credit factor K) are transparent, allowing the individual creators of wealth to issue/redeem credit for their own benefit – not the central planners' benefit!
    - Units of credit can be stored and passed down to future generations, without loss of value, allowing multigenerational wealth transfer – something that has been made impossible by the usury-based central bank monetary systems.

2. All currencies would all be freely tradable, and frictionlessly convertible at current market rates, as defined by the price of the underlying commodity basket.

- Attempts to "corner the market" on commodities by artificially increasing or decreasing their price would bring the wealth of the entire economy to bear on the attack; as K is increased/decreased in response, the wealth owners in the economy could use their individual and collective credit to literally suck the wealth out of the attacker, transferring it to the wealth owners, and eliminating the attack. Or, they could simply transfer their credit, immediately and frictionlessly to a different currency, leaving the attacker holding his own worthless, manipulated currency.

3. Credit could be used – spent, traded, given, stored, lent – without usury. Of course, it could be lent at interest if the owner of the credit wishes (eg. to companies, strangers).

4. All transactions in a currency are universally visible and completely anonymous.

   - Every transaction is provably between the owners of two valid credit accounts, and the credit system is in accounting balance before and after every transaction (no credit created it lost, until it is redeemed by un-pledging the wealth by which it was created).
   - Every transaction is anonymous and cryptographically secured (but either party may choose to prove and/or reveal their part in a transaction.)

And, best of all:

1. No "central planners" would ever again be able to hold its citizens hostage to a Fiat currency (which it can create and spend first, in effect robbing its citizens via the indirect tax called Inflation). Denizens like Robert Mugabe and the heads of central banks would be powerless against the sheer defensive force of wealth created and wielded by their own citizens.

   - The constant drain of wealth from the economy toward the central and commercial banks caused by the payment of interest on credit creation would be eliminated.

2 Owner Credit

In 2008 (before Bitcoin had been introduced), I wrote a prototype for a currency basket denominated value-stable mutual credit cryptocurrency:

`https://github.com/pjkundert/ownercredit`

Around 2018, I put down some thoughts on the concepts underpinning a decentralized, dynamically stable wealth-backed currency system, that is immune from debasement attempts by bankers and other undesirables:

Wealth Coin

3 Prior Art

I want to acknowledge prior art that I've discovered in this field.

3.1 Sweetbridge Liquidity Protocol (circa 2018)

The Sweetbridge project proposed in their whitepaper Sweetbridge Liquidity Protocol (link) a system to attach locked collateral assets (called Vaults), to activate Sweetcoin and generate interest-free loans of Bridgecoin.

While the project's ERC-20 token appears to have ceased to be viable, the design is very interesting, and contains some components that are necessary to implement wealth-backed monetary systems. However, some challenging design decisions may have interfered with its viability:

Most challenging, I think, was its requirement for a legal authority (liens and contracts) over the assets attached to the vaults which allowed forced sales, if the amount "borrowed" exceeds the value of the assets in the vault.

Some missing components in their design were:

1. Fixed issuance vs. Mutual Credit. Issuing ERC-20 tokens to various stakeholders, and then trying to attract assets to uphold the valuation of these tokens is (in my opinion) not viable. Dynamically issuing balances based on the attachment of attested wealth (and nothing else!) is viable, but requires smart contracts that are not expressible in EVM (eg. Solidity) code.

2. Using USD as value stability reference vs. a basket of commodities. The value reference (eg. the Buck) must represent commodities that underpin the economy serving the society using the monetary unit. All assets trade in their market currency, but their system-facing value (ie. in Bucks) is represented in terms of that basket. It fluctuates constantly, as the asset, the asset's market currency, and the currency vs.

the monetary unit (eg. the Buck's) basket of commodities fluctuates. But all this is trackable on a second-by-second basis.

3. Forced asset sales vs. automatic borrowing and insurance contracts. Integrating forced sales of assets (via liens, contract execution, bailiff seizures, auctions, ...) is not really practical, IMHO. However, when the valuation of an asset fluctuates and a Mutual Credit account goes into arrears, the (already paid for) borrowing smart contract and if necessary the (already paid for) insurance smart contract can automatically take effect and make the monetary system whole. No execution of liens and legal recourse required! Of course, the decentralized insurance system is funded by ordinary investors, and underwritten by real re-insurers who **do** hold the liens and legal contracts to the assets used as collateral! These people can (at the glacial speed of the legal system) take recourse and attempt to recover their losses through normal systems, completely unrelated to the operation or integrity of the wealth-backed monetary system. This radically simplifies the operation and integrity of the system, as proposed by Wealth Coin.

But overall, their effort is very mathematically impressive! It is, I believe, much closer to being viable than they may now believe (given their initial foray).

I believe Scott Nelson et.al. deserve to be heard for their great work, and their design is a great step toward a viable system. They are among the very few, I believe, who have deeply thought through the requirements and implications of what is actually required to implement a wealth-backed cryptocurrency system.

3.2 Sweetbridge Transparent yet Private Currency (circa 2021)

A detailed treatise (link) on an approach to transparent (client mutual identity verification) yet private (quorum of participants required for decryption of transaction details) and auditable (assets backing tokens comply with legal requirements) cryptocurrency money.

3.2.1 Innovative Approach to Asset-Backed Tokens

Sweetbridge proposes a mechanism for minting tokens based on attestation of assets. This approach addresses a crucial aspect of cryptocurrency: ensuring that digital tokens represent real-world value.

Money that works as a proxy for something else must be considered a reliable representation for that thing. Attestation is one way for this to occur, which requires (at least):

- Trustworthy verification of asset ownership
- Accurate valuation of the underlying assets
- Regular audits to ensure continued asset backing
- Mechanisms to prevent double-spending or over-issuance of tokens

3.2.2 Balancing Transparency and Privacy

The Sweetbridge protocol aims to strike a delicate balance between transparency and privacy, which is crucial for widespread adoption of cryptocurrency:

- Transparent Identity Verification: Client mutual identity verification ensures that participants in the system are known entities, reducing the risk of fraudulent activities.
- Private Transaction Details: By requiring a quorum of participants for decryption of transaction details, the system maintains user privacy while still allowing for necessary audits.
- Auditable Asset Backing: The system ensures that assets backing tokens comply with legal requirements, providing a layer of trust and regulatory compliance.

3.2.3 Interest Free Capital? Oops...

A primary goal is to free up trapped assets held by individuals and corporations:

> From the economic standpoint, BRC will operate as a fully collateralized value-stable currency and adhere to strict accounting standards that govern assets classified as cash equivalents. Sweetbridge-licensed entities will provide liquidity and collateralization mechanisms necessary for such classification. The BRC protocol allows the value trapped in any asset to be converted into a new asset class that can be treated as a cash equivalent. This process can be used with any asset that has a market for

> price discovery and is accomplished without selling the valued asset.

This is indeed an admirable goal. Presumably, this would allow people to gain *interest-free* access to capital, as ***cash equivalents***.

If people and organizations can take **existing** property and opt for *interest-free* ***cash equivalent***, would they not decide to retire interest-bearing debt instruments with the proceeds? After all: free cash flow! Yes indeed, they would do so – *at scale.*

Interesting things happen in Usury-based Fiat monetary systems when the deposits created through debt contracts are retired at scale. More on that in a second... But first:

3.2.4 KYC & AML, FTW!

The primary mechanisms proposed for identity and attestation are to utilize approved regulatory bodies. Seems to make sense!

But, this raises the burning question: if such bodies *were* effective at their tasks, why would the amount of financial fraud and human trafficking occurring under their watchful care and authority exceed multiple Trillions of dollars per year?

It could be convincingly argued that nobody could *accidentally* be that bad, and it therefore must be intentional. But, even granting them the benefit of the doubt; if they **are** as spectacularly, unbelievably and lethally incompetent as the evidence seems to suggest:

Why would one willingly base the integrity of a *new* system on that broken foundation of trust?

3.2.5 The Inevitable Results: Controlled Demolition

Unfortunately, it is unlikely that existing financial authorities would *knowingly*:

1. *Improve* the KYC/AML results they provide to Sweetbridge, in order to yield a **more** valid (*less* corrupt) currency-equivalent system than their *own* native currency, or

2. *Continue* to allow operation of such an alternative cash-equivalent *if* it proves itself able to compete with the native currency, because: *mass*

> *retirement* of interest-bearing debt *must inevitably lead* to the implosion of Usery-based Fiat currency (since new money **must** be continually issued at exponentially increasing rates to pay for the compounding interest cost of existing debt underlying the current monetary base).

Thus, the proposed approach (from their summary):

> The BRC protocol is designed to first and foremost serve the needs of regulators and those entities for which regulatory compliance is essential.

is (in my opinion) *not viable from first principles.*

Any *successful* attempt would be short lived, as the native monetary system's authorities and beneficiaries simply **cannot abide** a successful competitor – and has *all* the necessary authority, financial capability and incentive to ***ensure*** such a competitor cannot continue to exist!

3.2.6 So, How *Can* It Be Done?

The *idea* of baking valid identity and attestation into a cryptocurrency, and combining it with:

- Cryptographic proofs of validity (zk-SNARK, etc.), and
- Publicly auditability (Homomorphic encryption of all balance calculations and public multi-party auditing of backing assets), with
- Decentralized proofs of identities (countersinging of agent identities to establish verified community relationships)

is entirely possible and can usefully accomplish what I believe may be real, viable goals:

- An account is associated with an entity known by and verified as trustworthy by known *communities* (*not* necessarily regulated or approved),
- Balances are backed by attested wealth, countersigned by pseudorandomly allocated attestators with cryptographically proven, long-term correctness in underwriting each type of wealth/asset (*not* necessary regulated or approved),
- Insurance has been purchased to cover loss of assets and failure to perform, which is automatically triggered on decentralized verification of such an event. Legal authority to recover assets is in place with the re-insurers, so they can recover their losses, outside of the jurisdiction of the monetary system.

3.2.7 Summary

Overall, Scott Nelson et.al. have made valiant and well-considered efforts to architect a system that could, potentially, operate within and be acceptable to the global Usery-based Fiat monetary system.

The ideas are sound, though, if implemented using fully decentralized:

- Identity and community membership proofs,

- Attestation of attached wealth and backup borrowing lines,

- Insurance to automatically make good the monetary system, with legal recourse for losses offline in each jurisdiction where the asset is held.

- Denominated in units equivalent in value to a broadly traded basked of commodities.

The next generation in decentralized agency, attestation, privacy and auditability provided by "Unenclosable Carriers" like Holochain and their associated global-scale DHT storage and distributed WASM-based full application sized "smart contracts" and integrity validation code renders such attempts to appease (evidently) integrity-hostile arbitrary authorities obsolete.