The Need for a Dependable, Private Commodity Exchange Mechanism

By Jonathan Carriel

an introduction to

BEDROCK
Digitized Bullion System

BedrockDBS.com

April 27, 2025

Table of Contents

World exchange mechanisms are collapsing

The world's exchange mechanisms are collapsing because it is obvious that the world reserve currency is overextended beyond all repair. Since World War 2, virtually all national fiat currencies have been evaluated in relation to the US Dollar. At the time, the US was a creditor nation that clearly possessed the bulk of the world's gold supply, and external central banks were permitted to draw upon it. For a quarter-century, the US used its privileged position in fiscally irresponsible ways, slowly deteriorating the dollar's bedrock value. In 1971, the US effectively admitted it could no longer redeem demands for bullion, and the Dollar would henceforth "float" – its base to be understood as the productivity and credit of the US economy. And the rest of the world's governments went along with this.

After half a century of floating, the US Dollar can purchase only a small fraction of what it could in 1971. Currencies that are related to it have inflated even more. The upshot has been the complete destruction of global saving, the source of all future productivity and progress.

Meanwhile, in the midst of increasingly frequent global crises, the world's money managers are preoccupied with sanctioning and embargoing each other, with cutting off entire populations from critical exchange methods such as SWIFT.

Individual privacy is under heavy attack

Individualism is succumbing to collective *identity politics*. Freedom of speech is being eroded in the name of *political correctness* and the supposed prevention of *hate crime*.

Private property is, as always, the scapegoat of elitists who believe in the perfect equality of everyone underneath them. Freedom of trade is circumscribed by ever-increasing regulations – all in the name of the public good. The bureaucratic attitude toward private transactions is that every exchange is *guilty until proven innocent*.

On the global scale, genuine free trade would be easy to arrange: goods and services are exchanged without imposts irrespective of national borders. Free trade *agreements*, by contrast, are meticulously detailed restrictions on exchange, created for the benefit of various pressure groups and painstakingly balanced against others – all at the expense of the general public.

Promising Developments in Preserving Privacy

Increasingly, over the past generation, a new *technology of privacy* has been developed that can now shield many areas of human life, and promises much more.

The technology has been boosted by public alarm over notorious government surveillance activities and, especially, criminal identity theft. These depredations have produced a glimmer of awareness of every person's need for privacy, which should someday translate into increased general consumer demand for applications that default to privacy.

Encoded secret messaging has been around since ancient times, but *public-key cryptography* is new. It is *impervious* to everyone unwilling to spend an enormous fortune attempting to break it. And best of all, it has become an *automatic* default of a growing number of computer systems, instantly sparing consumers their bewildering complexity.

The TOR Project's network of decentralized internet access is a major accomplishment, despite t its utility being hampered by its requirement to use special software.

The most aware of today's system developers have been diligently at work, making constant – on—going – on-going – improvements.

There is reason to hope that absolute privacy can be restored, not just for communications, but for private transactions.

These are true modern breakthroughs, very important new tools in the struggle for human freedom. Never before has an enormous and growing percentage of the world's population possessed reliable technological means of evading authoritarian oversight. If they can manage the currently necessary "learning curve," people can break around restrictions, rather than facing them head on.

The cryptocurrency effort to solve the free exchange problem

The ingenious creation of Bitcoin and its supporting blockchain technology has already allowed millions to evade logjams in value transfers. It has enabled fast, mostly secure

international moves and permitted people's life savings to escape protectionist currency restrictions and rampant hyperinflation.

Blockchains have supported a new infrastructure of "trustless" contractual interactions which, being driven by open-source computer programs, do not require faith in unknown people or businesses. This will expedite the pace of all global commerce.

An extensive cryptocurrency support ecosystem has been developed: public information sources, computer and smartphone applications, open exchanges, private wallets, marketing, and education.

Unfortunately, a counter-revolution by the authoritarians has suborned many private financial institutions into tracking their customers – officially to prevent criminal violence but more realistically to surveil overtaxed citizens and prevent their attempts to escape confiscation.

However, the simple existence of new "currencies" independent of national fiat currencies has also drawn the attention of millions to the inadequacies of the latter. Public awareness of genuine problems with politically-mandated money systems has skyrocketed, thanks to the crypto world.

Why recent solution attempts are insufficient

Cryptography *is* the best answer to privacy of communications. And promisingly, future development should make it "friendlier," and make it standard, not a special application requiring extra effort. Continuing increases in internet speed and reductions in expense – following the still-operative *Moore's Law* – will open encrypted communications to ever more people around the world. The decentralization of the internet epitomized by TOR and cryptocurrencies should become easier and more familiar over time.

The cryptocurrencies that are currently available, however, are never going to be the ultimate solution to the problem of free private exchange. They are transitional. Like fiat money, they may be temporarily useful to pass funds while their individual value holds, but they lack some of the fundamental requirements of an exchange mechanism. These requirements were explained by Aristotle two thousand years ago.

- An exchange mechanism must be **durable**, not perishable. Cryptos *do* pass this requirement, given the permanence of each transaction on the blockchain.

- An exchange mechanism must be **divisible** – able to be partitioned without loss of value. Here, cryptocurrencies surpass anything the ancient philosopher may have dreamed about.
- It must be **convenient**, easily portable. This is *a work in progress* for cryptocurrencies. Resorting to a cell-phone or a full computer is not as easy as pulling out coins, paper bills, or a plastic card. Crypto's programmers are laboring mightily to change this – and eventually will succeed.
- An exchange mechanism must be **recognizable** by all parties. In any particular locale, national coins and bills are instantly understood (even though no one knows exactly what they represent). Cryptocurrencies, however, face an *invisibility hurdle*: how does anyone recognize an electron at a store counter? How can non-professionals tell the difference between crypto A and crypto B? This is one of the factors that has limited the acceptance of cryptos – and may be a permanent barrier.
- Most importantly, Aristotle asserted that an exchange mechanism must be **intrinsically valuable**. Whatever changes hands for a good or service needs to be valued *in its own right*, because it's a sophisticated form of barter. If the medium has no intrinsic value in the marketplace, the recipient would find no use for it. (Though fiat money has no intrinsic value, it's legally-required, and heavily discounted. Its conventional acceptance in its polity allows it to pass … for a time.)
    - This is an impossible challenge for today's cryptocurrencies. No matter that their systems limit the total number of their tokens; no matter that some tokens do represent payment for services rendered and, in rare circumstances, some are accepted by speculators for actual goods. The public understandably cannot – and never will – be able to answer the question, *What is it?*
- And that obviates the final desideratum: the exchange mechanism must be useful as a **store of value**. If a medium is durable and has intrinsic value, it can be *saved for future use*. The more confident a holder feels about the future value of the medium, the greater the ease with which he or she will accept it today.
    - To hold value over lifetimes, the mechanism must also be **scarce**. It must be known to be rare in nature, and difficult to produce.
- A further objection to today's cryptocurrencies is that they suffer from *collective* inflation. However strictly any particular token is constrained, the proliferation of

cryptos leads to ever more tokens chasing finite societal values – the same problem for which fiat money is rightly condemned.

A potential solution: Merge ancient truths with modern technology

A usable exchange mechanism must be anchored in a **commodity**. Only a homogeneous, recognizable good can possibly satisfy all the requirements of a truly acceptable exchange mechanism. Given that commodities are the bedrock products upon which all manufactured goods depend, they offer assurance of fungible current value and future value.

- Bedrock's premise is that the modern technologies of encryption and blockchains will permit a commodity to be employed as an everyday exchange mechanism, in addition to its function as a basic economic component. To ensure this, the commodity must be vaulted *before* it is digitally divided.
- It cannot be "based on" or "backed by" the commodity, it must verifiably *be* the commodity itself. Public confidence will depend on a one-to-one correlation of the commodity established in the vault and the "tokens" that will represent it.
- Free exchanges must also be *completely* free of government surveillance, as well as criminal interference. Prevention of fraudulent impersonation can and should be managed privately, and the presumption of firms and customers should default to the presumption of innocence regarding all transactions.

How could this be established? **Bedrock** has an outline of an exchange mechanism that will require a great deal of work to bring into being. But we also have to say that we currently see no existing or potential alternative.

Please investigate and consider our Whitepaper.