Bank For International Settlements Blasts Crypto-Currencies As Fatally Flawed As Money

As currently created, crypto-currencies are serving a purpose of showing what will not work as digital currency, but at the same time, central major banks are intent on creating a replacement that *will* work. By nature, Technocrats will use technology to solve all of their problems, and a cashless global economy obviously begs for some sort of digital currency that is accepted by all. TN Editor

A Bank of International Settlements (BIS) report examines cryptocurrencies in depth. The study, called "Looking Beyond the Hype" investigates whether cryptocurrencies could play any role as money.

Bloomberg, Reuters, and the Bitcoin Exchange guide all have articles on the report but not one of the bothered to link to it.

After a bit of digging, I found the crypto report is part of an upcoming BIS annual report. The BIS pre-released the crypto report today (as chapter 5).

Here's a link to the page that contains a download for two Pre-Released BIS Chapters, one of them is on cryptos. I provide some snips below.

Note: I start with some lengthy snips that explain in detail how blockchain works.

Cryptocurrencies: Looking Beyond the Hype

- Cryptocurrency technology comes with poor efficiency and vast energy use.
- Cryptocurrencies cannot scale with transaction demand, are prone to congestion and greatly fluctuate in value.
- Overall, the decentralised technology of cryptocurrencies, however sophisticated, is a poor substitute for the solid institutional backing of money.
- The underlying technology could have promise in other applications, such as the simplification of administrative processes in the settlement of financial transactions. Still, this remains to be tested.

The Money Flower: A Taxonomy of Money

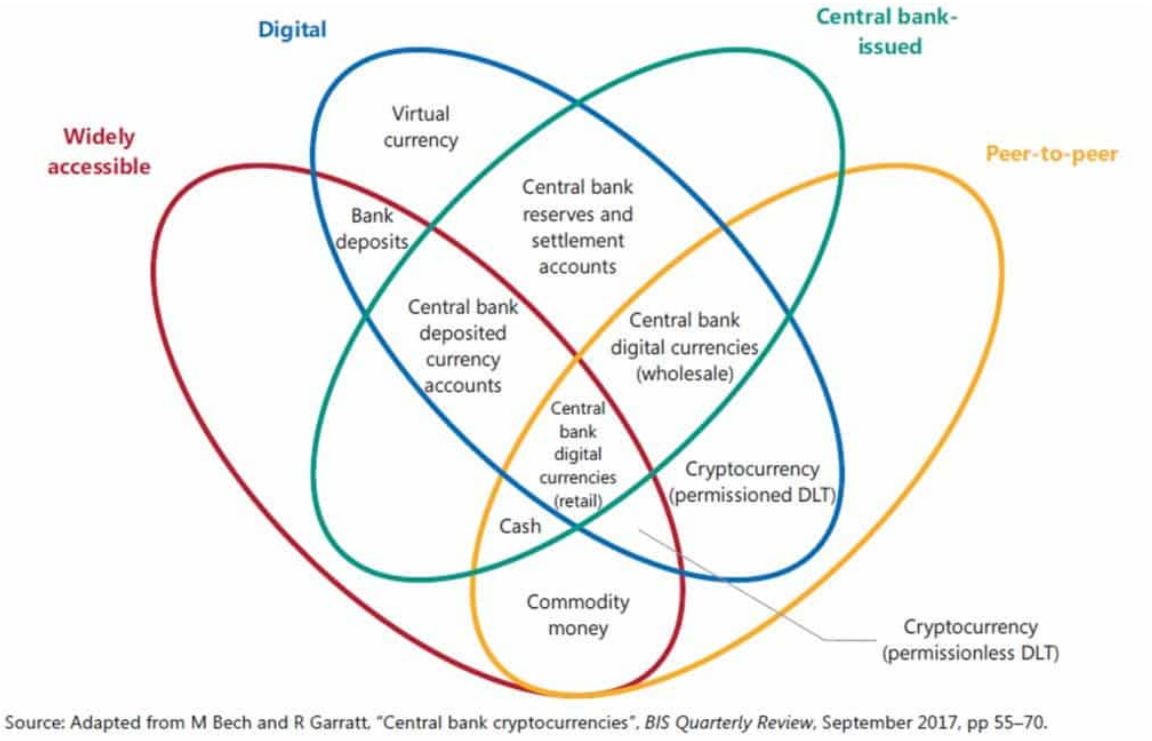

Image: BIS

The money flower distinguishes four key properties of moneys: the issuer, the form, the degree of accessibility and the payment transfer mechanism. The issuer can be a central bank, a bank or nobody, as was the case when money took the form of a commodity. Its form can be physical, eg a metal coin or paper banknote, or digital. It can be widely accessible, like commercial bank deposits, or narrowly so, like central bank reserves. A last property regards the transfer mechanism, which can be either peer-to-peer, or through a central intermediary, as for deposits. Money is typically based on one of two basic technologies: so called "tokens" or accounts. Token-based money, for example banknotes or physical coins, can be exchanged in peer-to-peer settings, but such exchange relies critically on the payee's ability to verify the validity of the payment object – with cash, the worry is counterfeiting. By contrast, systems based on account money depend fundamentally on the ability to verify the identity of the account holder.

Cryptocurrencies: The Elusive Promise of Decentralised Trust

In terms of the money flower taxonomy, cryptocurrencies combine three key features. First, they are digital, aspiring to be a convenient means of

payment and relying on cryptography to prevent counterfeiting and fraudulent transactions. Second, although created privately, they are no one's liability, ie they cannot be redeemed, and their value derives only from the expectation that they will continue to be accepted by others. This makes them akin to a commodity money (although without any intrinsic value in use). And, last, they allow for digital peer-to-peer exchange.

The technological challenge in digital peer-to-peer exchange is the so-called "double-spending problem". Any digital form of money is easily replicable and can thus be fraudulently spent more than once. Digital information can be reproduced more easily than physical banknotes. For digital money, solving the double-spending problem requires, at a minimum, that someone keep a record of all transactions. Prior to cryptocurrencies, the only solution was to have a centralised agent do this and verify all transactions.

Cryptocurrencies overcome the double-spending problem via decentralised record-keeping through what is known as a distributed ledger. The ledger can be regarded as a file (think of a Microsoft Excel worksheet) that starts with an initial distribution of cryptocurrency and records the history of all subsequent transactions. An up-to-date copy of the entire ledger is stored by each user (this is what makes it "distributed"). With a distributed ledger, peer-to-peer exchange of digital money is feasible: each user can directly verify in their copy of the ledger whether a transfer took place and that there was no attempt to double-spend.

While all cryptocurrencies rely on a distributed ledger, they differ in terms of how the ledger is updated. One can distinguish two broad classes, with substantial differences in their operational setup (Graph V.2).

While cryptocurrencies based on permissioned systems differ from conventional money in terms of how transaction records are stored (decentralised versus centralised), they share with it the reliance on specific institutions as the ultimate source of trust.

In a much more radical departure from the prevailing institution-based setup, a second class of cryptocurrencies promises to generate trust in a fully decentralised setting using “permissionless” DLT. The ledger recording transactions can only be changed by a consensus of the participants in the currency: while anybody can participate, nobody has a special key to change the ledger. The concept of permissionless cryptocurrencies was laid out for the case of Bitcoin in a white paper by an anonymous programmer (or group of programmers) under the pseudonym Satoshi Nakamoto, who proposed a currency based on a specific type of distributed ledger, the “blockchain”. The blockchain is a distributed ledger that is updated in groups of transactions called blocks. Blocks are then chained sequentially via the use of cryptography to form the form the blockchain. This concept has been adapted to countless other cryptocurrencies.

Read full story here…