Blockchain – The Chains that Set You Free

In the film, “The Graduate”, the unworldly character Benjamin (played by Dustin Hoffman) is told at the cocktail party that there is one word that he should know and that word is “plastics”. We are not sure in light of plastic’s progress over the last 40 years whether that would have been the best of tips. However in this day and age, someone is more likely to sidle up to you at a party and whisper, over the tinkling of martini glasses, the words, “blockchain or “crypto-currencies”. Not quite as sexy as plastics but definitely more tongue-twisting.

In the Beginning….

… there was Bitcoin…. and it was bad. Well, at least Central Bankers didn’t like it… and neither did Jamie Dimon…. hmmm.. so it must be good..

The first distributed blockchain was conceptualised by an anonymous person or group known as Satoshi Nakamoto, in 2008 and implemented the following year as a core component of the digital currency – BitCoin – where it serves as the public ledger for all transactions. The invention of the blockchain for bitcoin made it the first digital currency to solve the double spending problem without the use of a trusted authority or central server. The BitCoin design has been the inspiration for other crypto-currencies and applications.

Distributed Ledgers

Back in our days of working in Latin America (and Turkey) it was well known that most private companies, and more than a few public companies with family dominated registers, had multiple sets of books. There would be one for the owner (i.e. the CEO), another to show the family shareholders, yet another

to show the tax man and another for regulators and the exchange if the company was publicly listed. All would look quite dramatically different in the numbers they showed.

Blockchains with their distributed ledgers are the very opposite of this. Despite the fact they have multiple copies they are in fact copies of copies and should all be the same. It's the fact that various people hold the same copies that we are supposed to have confidence in their incorruptibility. Indeed the coding is the modern equivalent of indelible ink. Once a transaction is in the ledger it cannot be expunged, and is replicated in all the copies.

The less folksy explanation of a blockchain is that it is a continuously growing list of records, called blocks, which are linked and secured using cryptography. Each block typically contains a hash pointer as a link to a previous block, a timestamp and transaction data. By design, blockchains are inherently resistant to modification of the data.

Therefore a blockchain can serve as "an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way." For use as a distributed ledger, a blockchain is typically managed by a peer-to-peer network collectively adhering to a protocol for validating new blocks. Once recorded, the data in any given block cannot be altered retroactively without the alteration of all subsequent blocks, which needs a collusion of the network majority.

Its enthusiasts would reassure us that blockchains are secure by design and are an example of a distributed computing system with "high Byzantine fault tolerance". Decentralized consensus has therefore been achieved with a blockchain.

So blockchains are now good for more than just recording cryptocurrency transactions. This makes them potentially suitable for the recording of events, medical records, and

other records management activities, such as identity management, transaction processing, documenting provenance, or food traceability. Makes us wonder even about the audit trails on conflict minerals.

Moneyness

It seems appropriate that having founded a research firm based upon Austrian School of Economics, and yet rarely getting to speak of it, that blockchain should bring us the opportunity to quote the school's founder, Carl Menger, on the subject of "moneyness". This concept is oft trotted out by gold's fans to decry *fiat* currencies, which they claim are being debased. The debate now raging is whether crypto-currencies have moneyness or not.

To gauge this we should look at the three key identifiers:

- Medium of exchange (which BitCoin definitely has in a rising number of transactions)
- Store of Value (more a matter of perception than anything else)
- Unit of account (do people value "things" in terms of BitCoin?)

To have moneyness one must meet all three criteria. Even hard core critics would agree the BitCoin, for instance, has the first requirement down. We would argue it has the second by having become the *fiat* currency for the shady netherworlds where people moving large quantities of (drug/gun) money are having to trust in its intrinsic value (if only transitory for as long as they hold the stock of funds in the crypto-currency).

Then there is the unit of account. This is only a heartbeat away. So far BitCoins are valued by what they are worth in other currencies i.e. "so many dollars". But when existing currencies are valued the other way around e.g. how many ringgit can you get for a BitCoin, or cars or property valued

in BitCoin, then cyrpto-currencies come up with three matching fruit in the slot machine and they are off to the races (so to speak).

We awoke to the news this week that the Chicago Mercantile Exchange will shortly begin trading BitCoin futures and this prompted several thoughts. The first being, here comes legitimacy. The second being, the Fed must being having conniptions. The third being: Is this just an attempt by the big banks to get part of the action in manipulating the price of BitCoin (oh, no, not you Jamie Dimon, perish the thought)?

Conclusion

When Jamie Dimon rides in to attack BitCoin one knows that the Powers That Be are getting nervous. Fortunately Jamie is no longer regarded as the 800lb gorilla of the financial space but more of a toothless Rottweiler lapdog of the Central Bankers (to mix a few metaphors) and he has now managed to make himself the subject of chuckles whenever mention is made of crypto-currencies.

When his intervention is combined with Chinese measures to suppress BitCoins (they never control other financial bubbles) then one starts to suspect that the Chinese public (and the broader BitCoin universe of users/holders) may actually be onto something.

On a broader front the war against the public's right to transact is under attack with governments withdrawing large denomination bills and Turkey banning PayPal. The slogan for the masses should be "BitCoin will set you free". However with the CME getting in on the act, one then wonders if the institutionalization of BitCoins isn't going into turbocharged mode before crypto-currencies escape the government's grasp, particularly in the Land of the Free.