**Scoping Note for GPI Crypto-Currency Work**

**Introduction**

There is increasing activity, both discussion and actions, in relation to the establishment and use of crypto-currencies (DCs), both central bank and private DCs. The research discussion (and action) has significantly been within the central banking fraternity (including BIS), banking sector research departments, and more widely via private sector interests, companies, consultants, and some think tanks. The activity will continue to accelerate. There is an opportunity for an appropriate think-tank to move ahead of the field. GPI could be that organisation: it fits well with our profile and portfolio. Bruegel have produced one piece of research, so we would need to go beyond that research, perhaps developing a more policy-oriented approach, taking account of the various contribution, BIS, ECB, BoE, RIKS, etc.

I have done a fair amount of research, as has Chris Luenen, and other GPI Fellows could become involved. The themes we would develop are the four briefly outlined below. I am not suggesting that we pursue all four at the same time, but sequentially, though observing the linkages. The intention would be to develop a GPI expertise on DCs. Our developed expertise, embedded in our first published thematic report, could be widely advertised. We might then seek significant financial support, grants, for our further work. (It would be useful, of course, if we could also to try to obtain some seed funding for the first piece of work, from outside funding organisations, such as the Madison Group).

I suggest that Themes 1 and 2 would provide the basis for our initial work, though there will be some overlap with the two other themes, especially Theme 3. This focus closely matches our two recent forays in the central banking research and policy area, the Federal Central Banks Report and the ECB Mandate report.

The information set out below represents a reasonable coverage of the issues. Inevitably, given the speed at which events are moving in this field (and my own limitations), *it is neither comprehensive nor deep enough to do justice to the topic*.

**Theme 1: Central Bank Digital Currencies and Implications**

A number of central banks have either conducted research and piloting of crypto-currencies/digital currencies (DCs). The two most advanced are China and the Bahamas. Both CBs have issued DC “tokens”[[1]](#endnote-1) delivered into pay wallets on smartphones. The value is 1:1 with the accepted national currency.

It should be noted that the function of the CB token serves three of the functions required of money, namely: as a medium of exchange, as a deferred standard of money, and importantly, as the tokens are issued by the CB, an accepted unit of account. The one function that the token does not necessarily seek provide is being a store of value, though it would be possible.

It is also important to note that, though private crypto currencies have been developed, ostensibly using block chain technology (see below[[2]](#endnote-2)), this is not the preferred route of CBs. There are a variety of reasons for this route not being selected, with the intensive energy cost probably pre-eminent among them. China’s rapid deployment of its DC may be partly motivated to curb the large amount of Bitcoin mining in the country, which threatens, at the margin, its intended reduction of energy usage. It is estimated that Bitcoin mining in China, probably accounts for around 5% of its electricity generation carbon emissions.

Mastercard, Visa, PayPal and others are moving to become closely involved with digital currencies - and in the case of Mastercard, the Bahamas CBDC - essentially to offer wider payment transactions settlement. It is highly unlikely that Bitcoin will, or can, be used in this way. Facebook’s Diem, though not yet launched, will potentially provide a quintessentially transactions currency (see below)[[3]](#endnote-3).

CBDCs may adopt - perhaps are likely to adopt - a form of distributed ledger technology network. This type of DLT[[4]](#endnote-4) system would be likely to see the CB having centralised control over what is entered on the ledgers and who has access to the network using it. The CB could then authorise a consortium to control the propagation and verification of transactions. Such a structure is patently different from the Bitcoin structure, a so-called *public* blockchain system, where participation is unrestricted. Instead, the identity management of pseudonymous agents is through “proof of work”, secured by the hash-mining process (See note on hash-mining below).

Such a CBDC system would be similar to those used by Etherium and other private DCs, insofar as distributed ledger technology would be used. The difference would be that the CB would be the trusted “fat controller”, rather than a consortium of wealthy private individuals or corporates.

N.B. *Interestingly, the choice presented above, between state control versus corporate control, is the more general choice that all populations and countries will face this century in a variety of areas.*

One of the positive reasons for CB digital currencies is that they enable monetary policy to have a more direct impact on the spending of the general public than the current preferred alternative of large-scale asset purchases, CE and QE. However, there are both merits and demerits in relation to CBDCs

For instance, the use of CBDCs will also have an impact on the use of banks by the public deposits and the financial intermediation function still performed by banks for both personal and for business customers, notwithstanding the modern monetary context whereby loans create deposits and central bank reserves.

Moreover, central CB control would involve the CB in considerable computerised data management. The volume of electronic transactions would vastly exceed the volume current passing through the existing wholesale banking, RTGS (real-time gross settlement systems). This centralised control via a core ledger is the model suggested by the BoE as a *possible* route. Although, if this mode of CB operational control were adopted, it a would be possible for DLT to permit multiple other firms to provide computing capacity, and so avoid the CB having to operate the complete infrastructure.

What is clear from the outset is that any CB considering implementation of a DC would need to ensure four key features: scalability, confidentiality, resilience, and security. For instance, it is unlikely that anonymity would be provided given the need to retain anti-money laundering protection.

**Theme 2: Transactions, Digital Tokens, Stablecoins, and the Decline of Cash**

One of the motivations for CB proceeding to DCs has been the continuing decline in the use of cash in developed economies, and prospectively in a number of developing countries where demographic factors and the ready availability of smartphones strengthen the case.

The gradual replacement of cash by tokens seems inevitable, though both would continue to exist for some considerable time. Nor need there be any requirement to force the pace of utilisation between CB tokens and cash in any country. It is anticipated that there will be a generational divide and the younger, tech-savvy generations will adapt to using tokens relatively rapidly, given their intensive use of smartphones.

Another motivation for the CBs to move forward rapidly in the medium of exchange, transactions area is the forthcoming launch of Facebook’s Diem DC, an updated and modified version of the initially-launched (and withdrawn) Libra offering. The Diem is going to be tied to the dollar. Amazon is apparently developing its own DC. Diem, and presumably the Amazon variant, are looking to become a medium of exchange, transactions product, unlike Bitcoin.

The problem arises that the large-scale use – say at country of even international levels – of commercial DCs is unrealised and hence untested. Bitcoin operates with a relatively restricted network of participants and is unsuited to becoming a vehicle for widespread payment transactions. As the Swedish Riks CB report makes clear, scalability has raised a variety of problems for private cryptocurrencies (stablecoins). Notably, to make sure authentication is maintained. Insofar as the *limited* distributed ledger, independent network structure is used it appears feasible to protect the authenticity of the CB issuance of the tokens, at least if the participants are online. The technology has to ensure that the tokens, once used, are destroyed. Bitcoin dealt with this via pseudonymised accounts, the specific Bitcoin network structure, and distributed consensus achieved via “proof of work”.

**Theme 3: Digital Currencies, Regulation, and the Banking Sector**

The advent of Libra woke up central banks and governments to the need for regulatory action in relation to private DCs. Hitherto, they had been relaxed about Bitcoin, which despite the speculative activity surrounding it, especially in the relatively early stages of its development This lack of concern was related to Bitcoin’s aim to be a store of value, similar to gold. Moreover, though the value of the dollar may affect the value of Bitcoin, the reverse is not the case. Although, given the acquisition of Bitcoin by the corporate treasuries of various major investment companies (such as Morgan Stanley) and other major corporates (such as Tesla), its value is increasing in comparison with other dollar-denominated assets.

Despite is $1 trillion valuation it is not clear that in the longer-run, even as an asset class it will dominate. Essentially, it is an illiquid asset whose tradability is therefore limited. There is a fixed limit to the amount of Bitcoin – the underlying algorithm sets the limit as 21million tokens that can be created via data mining, and the current supply is 18.7 million, relatively close to that limit. (*See note on Bitcoin below*)[[5]](#endnote-5)

Currently, the banking sector has been relatively relaxed about private DCs, and CBDCs have not yet emerged, except in China (which has to be treated *sui generis*, given the involvement of the state with the banking sector) and the Bahamas (which is motivated by including excluded groups. The CB is working with Mastercard).

I suspect that to protect their own DCs, CB’s and governments will impose strict conditions on private DC transactions. The protection of the banking sector will be another stimulus to regulatory action. This year will see EU regulation published. In early 2020, the EU proposed a single regulation for all crypto-assets *not* falling under existing regulations (MiFIDII). The so-called Markets in Crypto-Assets Regulation (MiCAR) is expected to come into effect by the end of this year.

**Theme 4: Digital Currencies and the Global Currency Environment**

By market value in terms of the value of the currency in circulation Bitcoin at $I trillion. rates well above the pound sterling, but lower than the Euro and only half the value of the dollar in circulation. However, in terms of numbers of transactions Bitcoin averages about 0.5 billion a day. The comparable figure for the US dollar is around 6 trillion a day (BIS 2019).

Suggestions that Bitcoin is a candidate for becoming a global currency are wide of the mark. Bitcoin will survive, as a store of value and a limited asset class, but it will not become a global digital currency. Others - Facebook’s Diem - may seek to become a global network for private financial transactions, a kind of “value-web” as Coinbase has suggested. However, unlike the www it will need to be regulated. We do need a digital global currency, but this needs to be a substitute for SDRs, though with complete global backing. We are some way off that desideratum, though sometime this century it will be reached.

A further question relates to the interaction of CB digital currencies and private DCs, and whether this will stabilise or create instability in the global currency environment. Currently, and in the view of some CBs, this certainly appears a possibility, if left unregulated, as it expands globally.

**Conclusion**

The note indicates the potential areas of interest to GPI in relation to developing our expertise and reputation in the area of DCs, both central bank and the private company development of DCs used for payment transactions.

There are, currently, conflicting opinions on the desirability and practicality of CBDCs, especially in the projected use of DLT. In this conflicted situation, with both research and experimentation accelerating, we may be able to “get ahead of the curve”, save for a relatively few other think-tanks.

Clearly, a significant measure of research will be required, and perhaps the recruitment of some expertise from outside the core group of Fellows. However, there is a close ‘fit’ with our recent other work in the central banking and monetary policy areas, and our wider expertise, so the initiative seems appropriate.

**Michael Lloyd**

1. *Tokens are the terminology used for CBDC systems, as opposed to the use of stablecoins for private systems, essentially they are both electronic cash* [↑](#endnote-ref-1)
2. *The term blockchain is used synonymously with distributed ledger technology (DLT). Blockchain certainly uses a DLT, though has extra features which protect Bitcoin from external attack and enable a specific form of network consensus. It is preferable to restrict the use of blockchain to define the Bitcoin structure and some other, including Etherium1.0. DLT can then be used to discuss other private cryptocurrencies and those CBs who are considering a decentralised structure/system of DCs.*  [↑](#endnote-ref-2)
3. *Various private cryptocurrencies want to achieve scalability in order to be able to offer wide payment transactions systems. Etherium2.0 and Facebook’s Diem are two contenders. Scalability was simply not possible with the blockchain technology used by Bitcoin. Hence, the use of distributed ledger systems and some form a of network consensus voting to replace “proof of work” by “proof of stake”. Etherium 2.0 for instance is abandoning proof of work and moving to achieving the distributed consensus via “proof of stake”. Hence, instead of miners there will be “validators”. The validators use a portion of their Ether stablecoins as a permanent stake in the network. The validators then bet on the next blocks to be added to the chain, and gain a reward proportional to their stake, if successful. There is a system for selecting validators. (There are a number of sources on the web, of varying quality, who can be consulted for more detail).*

   *We do not know yet what network consensus system will be used by Facebook for Diem. An issue for GPI is rather the impact of the circulation of an increasing number of stablecoins, within national and global payment systems, and how this might be regulated and/or subject to intervention by the establishment of CBDCs.* [↑](#endnote-ref-3)
4. *A DLT system exhibits a certain set of characteristics. These are: shared record-keeping, multi-party consensus on a shared set of records, independent validation of records by each participant, evidence of non-consensual changes to records, demonstration of resistance to external interference. These characteristics will be established in a framework that will have three broad layers: agreed protocols, the network operation, and the data in the records. Essentially the underlying objective is to achieve* ***trust and reliance*** *in the system.* [↑](#endnote-ref-4)
5. *Given the nature of Bitcoin’s blockchain variant, the way to obtain Bitcoins and to become recognised, albeit pseudonymously, as a validated participant in the network, is to add a new block to the chain, linked by a hash to a previous block. In effect, this process further extends the distributed ledger, at least until the fixed limit is reached. This process of hash-mining is rewarded when successful by an allocation of a (gradually decreasing) number of Bitcoins. “Hash mining” requires considerable computer skill, effort, and power, and the expenditure of electrical energy.*  [↑](#endnote-ref-5)