What consensus mechanism will be used for Central Bank Digital Currencies (CBDCs)?

Vincenzo Vespri[1] and Filippo Zatti[2]

[1] University of Florence
[2] University of Florence & BABEL

In our increasingly digital world, transactions are processed online more frequently, reducing the use of physical money. As a result, central banks around the globe have begun considering the best way to introduce digital fiat currency.

The International Monetary Fund (IMF) defines CBDC as the digital currency issued by central banks [AMO]. According to a recent survey conducted by the Bank for International Settlements [BIS], 80% of central banks are currently working on the development of prototypes for CBDCs. For further details, see [ZH].

Naturally, in the development of CBDCs, central banks have looked to cryptocurrencies as a natural reference for this type of problem. However, there are significant differences between decentralised blockchain-based cryptocurrencies and fiat money, particularly regarding regulatory oversight and required functionality [Z]. Therefore, future digital fiat currencies must do more than copy the model of decentralised cryptocurrencies due to technological differences and related issues. For more information on these differences, please refer to the recent paper [BV].

However, even if the final choice has yet to be made, CBDCs will likely be based on blockchain technology. If this decision is confirmed, one of the most crucial technological aspects during the move towards digital fiat currencies will be selecting the consensus mechanism.

The choice of consensus mechanism depends on whether the blockchain is permissioned or permissionless. Two popular cryptocurrencies, Bitcoin and Ethereum, operate under a permissionless system. This means no central authority controls the network, but cryptocurrencies still face technological challenges like the Buterin trilemma. According to this concept, it is not easy to achieve scalability, security, and decentralisation simultaneously (see [AHM]).

Additionally, the implementation of anonymous blockchain technology is more complex and energy-intensive than permissioned blockchains. However, it is only through this type of blockchain that complete anonymity can be ensured, making cryptocurrencies an ideal payment method similar to cash payments.

Permissioned blockchains are supervised by a central authority, which results in the loss of anonymity but benefits in terms of costs, scalability, security, and simplicity. Central banks are currently exploring the potential of permissioned blockchains.

De Cifris Koine – CIFRIS23 https://doi.org/10.69091/koine/vol-1-W03

However, there are concerns that implementing them may cause Central Bank Digital Currencies (CBDCs) to function like credit cards. The only difference between CBDCs and credit cards is that CBDCs will be issued by a sovereign state, making them more reliable and regulated than private companies. Additionally, automatic services such as paying taxes and utilities could be implemented through smart contracts, making them more efficient. It is feasible to link a wallet to an individual user, enabling tracking of all transactions. However, if central banks adopt a permissioned system, it may be more advantageous for individuals to opt for cash payments rather than digital ones. This is because all transactions made with a permissioned CBDC would be recorded and monitored.

We could have two separate blockchains to address the issue of privacy and cost-effectiveness. One would be permissioned, where all payments to the government or other transactions that do not affect our privacy or taxes would be made. In contrast, the other would be permissionless, allowing us to make untracked payments. The permissionless blockchain would have higher management costs than the permissioned blockchain; hence, a fee comparable to that of credit cards would be charged for its use. Suppose we cannot solve the issues of privacy and non-traceability that led to the introduction of cryptocurrencies by the cypherpunk movement. In that case, we might have to accept the coexistence of CDBC (or fiat digital money) with cryptocurrencies. One solution could be to introduce payment methods only for anonymous payments. It would prevent our purchases from being tracked and our profiles from being created by marketing companies, thus avoiding legal problems that may arise from it.

Instead, we intend to replace cash and cryptocurrencies with CBDC. In that case, we need to ensure that the anonymity of the seller is maintained, which can be achieved by using blockchain permissionless if it is the chosen technology. However, several challenges must be addressed, including ethical, statistical, legal, and technological issues. Using anonymous coins can lead to money laundering and avoidance of taxes to purchase illegal goods and services. On the one hand, using this particular type of coin should be discouraged by monitoring those who purchase it and put it back into circulation, charging high transaction costs, and imposing penalties for those who keep it anonymous for long periods.

On the other hand, it is not advisable to discourage its use because if it costs too much, this type of CBDC will never replace cash or cryptocurrencies. Moreover, the right to privacy and anonymity is fundamental in a digital society like ours. Deleting it is certainly much more dangerous than accepting its connected risks.

References

1. Adrian T., Muhlsein M., Obstfeld M.: Casting light on central bank digital currencies. Staff Discussion Notes 2018 **77**, Paper No. 10.5089/9781484384572.006.A001, 008 (2018).
2. Central bank digital currencies: foundational principles and core features, `https://www.bis.org/publ/othp33.pdf`.
3. Zhang T., Zhigang H.: Blockchain and central bank digital currency ICT express. Volume 8, Issue 2, pp.264-270, (2022).
4. Zatti F.: The economic law of (central bank) digital currency, Law and Financial Markets Review, **77**, Paper No. 10.1080/17521440.2023.2261668, (2013).
5. Bracciali A., Vespri V.: The technological factor in the conception of Central Bank digital currencies, In F. Zatti, R. G. Barresi (eds), Digital Assets and the Law: Fiat Money in the Era of Digital Currency, Routledge **77**, ISBN: 9781032192277, pp. 18-31, (2024).
6.] Altarawneh A., Herschberg T., Medury S., Kandah F., Skjellum A.: Buterin's Scalability Trilemma viewed through a State-change-based Classification for Common Consensus Algorithms. 2020 10th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, **77**, Paper No. 10.1109/CCWC47524.2020.9031204, (2020).
7. Augusto A., Belchoir R., Kocsis I., Gönczy L, Vasconcelos A., Correia M.: CBDC Bridging between Hyperledger Fabric and Permissioned EVM-based Blockchains. IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Dubai, United Arab Emirates, **77** Paper No. 10.1109/ICBC56567.2023.10174953, pp. 1-9, (2023).
8. Zhixiu Y.: On the coexistence of cryptocurrency and fiat money. Review of Economic Dynamics, Volume 49, pp. 147-180, (2023).
9. Beltramini E.: Against technocratic authoritarianism. A short intellectual history of the cypherpunk movement. Internet Histories, 5:2, pp. 101-118, **77** Paper No. 10.1080/24701475.2020.1731249, (2021).
10. Vespri V.: Le anime della matematica. Diarkos, (2023).
11. Hänold S.: Profiling and Automated Decision-Making: Legal Implications and Shortcomings. Corrales, M., Fenwick, M., Forgó, N. (eds) Robotics, AI and the Future of Law. Perspectives in Law, Business and Innovation, Springer, Singapore, **77** Paper No. 10.1007/978-981-13-2874-9_6, (2018).