CBDC's and Bitcoin: the role of digital money in the modern society and the possible co-existence between two worlds.

Massimo Simbula[1]
msimbula@studiolegalesimbula.com

Abstract

A purely peer-to-peer version of electronic cash. The first 8 words of the well known paper of the unknown Satoshi Nakamoto describes perfectly the sense and the ultimate scope of Bitcoin, a protocol designed to solve the double spending problem of e-money in digital environment through a complex mixture of digital signatures based on cryptography, proof of work system aimed to validate the transactions and, above all, a mechanism of reward granting incentives to the nodes of the network.
Nothing of these elements can be found in most if not all of the other blockchains (a term never used by Satoshi Nakamoto in his paper). However, Distributed ledger technologies (DLTs) are destined to become a transformative feature of financial markets, both in financial products and in the underlying market infrastructure itself. This brief paper investigates the need for a tokenised form of central bank currency (CBDC's) identifying privacy problems that could occur in various CBDC designs.

Paper

According to the European Central Bank a CBDC could be an alternative to euro banknotes and could complement cash by serving as "*an electronic form of money, issued by the Eurosystem, [*that*] would be accessible to all citizens and firms*"[2]. Federal Reserve Bank stated that a CBDC is "*a digital liability of a central bank that is widely available to the general public.*"[3]. The Bank for International Settlements considers a CBDC "*a digital form of central bank money that is different from balances in traditional reserve or settlement accounts*" and that works as "*a digital payment instrument, denominated in the national unit of account, that is a direct liability of the central bank*"[4]. The International Monetary Fund defines a CBDC as "*a new form of money, issued digitally by the central bank and intended to serve as legal tender*"[5]

[1] MASSIMO SIMBULA (Cagliari – Milano) started his activity as legal consultant in 1998. He provided legal assistance to Government, International Organization and Institutions (FMI, World Bank, European Commission, Central Banks) in major international projects, including privatization of state owned companies, cross- border operation, FinTech, Blockchain and Cryptocurrencies. He was foreign in-house lawyer and associate of a major Italian international law firm, covering for more than 6 years activity in EU and US countries. He was also senior internal lawyer of FENDI (LVMH Group) for three years providing legal support for the company in more than 30 countries worldwide. He currently assists Italian accelerators of Digital Startups, Venture Capital with a focus on Blockchain and cryptocurrencies, and many companies operating in the field of Fintech and blockchain services (including Escrow services, DAO, Digital Signature and timestamping on blockchain, NFT etc.). Massimo is arbitrator in disputes relating .IT domain names. He serves as board member in Italian Association www.copernicani.it, in and other association. Massimo Simbula is intensively active in seminars and workshops in Italy and abroad as speaker, related to blockchain, cryptocurrencies and Defi.

[2] European Central Bank, A Digital Euro, https://www.ecb.europa.eu/paym/digital_euro/html/index.en.html (last visited Jul. 28, 2022).

[3] Board of Governors of the Federal Reserve System, Central Bank Digital Currency (CBDC)

[4] Bank for International Settlements, CENTRAL BANK DIGITAL CURRENCIES: FOUNDATIONAL PRINCIPLES AND CORE FEATURES, 3 (2020), https://www.bis.org/publ/othp33.pdf (citing Bank for International Settlements, COMMITTEE ON PAYMENTS AND MARKET INFRASTRUCTURES - MARKETS COMMITTEE: REPORT ON CENTRAL BANK DIGITAL CURRENCIES 4 (2018), https://www.bis.org/cpmi/publ/d174.pdf).

[5] TOMMASO MANCINI-GRIFFOLI, ET AL., CASTING LIGHT ON CENTRAL BANK DIGITAL CURRENCY INTERNATIONAL MONETARY FUND 7 (2018).

CBDCs, in general, can be defined as a new form of money—a digital liability issued and guaranteed by a central bank[6]. But does the world need the CBDC, provided that such "new" digital money has nothing to do with the protocol of Satoshi Nakamoto and does not bring any relevant innovation in the digital environment? As I write this paper, there is not still a well-shaped digital architecture of a CBDC. The only difference of this "new" digital money (apart the exotic name) is that a CBDC is a liability of the central bank, as opposed to commercial banks. But commercial banks, even with all their defects and limits, represent a resilient network based on competition, which may guarantee a limited freedom in terms of censorship, privacy, commercial terms, while a central honey pot controlling any transaction of a digital money, may incur in relevant privacy, cybersecurity and censorship problems.

CBDC is not even a new idea. A similar proposal (but with hard cash), dubbed the "*Chicago Plan*,"[7] was considered by President Franklin Roosevelt during the Great Depression of the 1930s and ultimately rejected.

Fast forward to 2020, with the bills of the US Senate of March 23rd 2020, pompously called "*Take Responsibility for Workers and Families Act*" [8] and "*Financial Protections and Assistance for America's Consumers, States, Businesses, and Vulnerable Populations Act*" the Federal Reserve – the Central Bank US – was trying to create "digital dollars" and digital wallets to directly send citizens $1,000 for each minor and $2,000 for each adult. A new generation Helicopter Money to avoid the friction that would arise in passing through private banks, in order to give immediate support to American families following the serious economic crisis generated by the spread of COVID-19 and also reach those who do not have open bank current accounts. According to this (rejected) bills, the term 'digital dollar' was defined as *"…a balance expressed as a dollar value consisting of digital ledger entries that are recorded as liabilities in the accounts of any Federal Reserve bank; or an electronic unit of value, redeemable by an eligible financial institution (as determined by the Board of Governors of the Federal Reserve System)*".

Even if CBDC may (eventually) be based on cryptography, any cryptographic solution cannot represent a positive innovation in digital payments. On the contrary: cryptography is broadly used in many digital transactions and there is still a central authority acting as custodial of the ledger and, arguably keeping record of such transactions.

The CBDC plan is not without benefits. But there is a risk of definitively fuel the entire financial system with politics and control. Reducing the role of banking intermediaries and payment institutions is not an innovation nor a solution. Furthermore, the absence of a limit on the issuance of a CBDC may quickly lead to hyperinflation. Furthermore, if a central bank decides to issue a CBDC, it should design the CBDC to be privacy-preserving. Four actors are generally involved in processing a payment through a CBDC: the payor, the payee, entities that carry out the payment (in this case, mainly, the central banks, but commercial banks, money service providers, and other authorized entities may be included), and law enforcement agencies. Now, retail payments leave behind a data trail that can be used to construct a detailed picture of an individual's personal life, including travel, financial circumstances, and much more. Similarly, CBDCs acting also as a new form of retail payment method, share the same characteristics. Account data, identity data, and transaction data, separately or collectively, can be used to construct a detailed picture of an individual's personal life. Revealing these data would directly pose a threat to one's safety, dignity, autonomy, and liberty. A central authority recording such data is a hazard considering both forms of political control and potential discrimination or censorship, as well as relevant cybersecurity risks concentrated in the biggest honeypot available in the digital money eco-system.

Conclusion.

The United States and European Union where both founded with a deep skepticism, both principled and practical, of centralized authority. In crafting US and EU system the Founders knew it was better to have competition. We now have financial resilience where banks are able to compete with one another to

---

[6] Jiaying Jiang - University of Florida Levin College of Law UF Law Scholarship Repository - UF LAW FACULTY PUBLICATIONS 2023

[7] https://www.imf.org/external/pubs/ft/wp/2012/wp12202.pdf

[8] https://apps.npr.org/documents/document.html?id=6817441-House-Democrats-Counterproposal-For-Stimulus

provide the best services. A national bank with virtually limitless power and resources is a huge deterrent to the free market and an even larger temptation to autocrats. CBDC's and Bitcoin are a perfect contradiction and CBDC has nothing to do with technological innovation or with a valid alternative to the current digital payment solutions.