

Exploring the Dual Impact of Retail Central Bank Digital Currencies: Efficiency and Privacy Concerns

Massimo Prag

Abstract:

When there are developments or advancements in the financial sector, they prompt reactions and subsequently lead to further changes. When the economy collapsed in 2008, some lost trust in the traditional financial system of debt and lack of transparency. Out of this came Bitcoin in 2009, which was a fully transparent form of currency separate from the government and anti inflationary. Then came rapid digitalization of money and payments. And in response to this, is the CBDC or the Central Bank Digital Currency. CBDCs though still mostly in research and pilot stages will disrupt the current way money works. This paper will explore CBDCs and critique the various privacy concerns that come with it. It will explore its current use and adoption, as well as explore general expected benefits and concerns. This paper takes the stance that this technology is inevitable, but privacy is at stake and there are some solutions to maintain privacy in a data driven world.

Cryptocurrency has been one of the most disruptive technologies of the past twenty or so years. Cryptocurrency is a novel technology that allows people to store, send, and receive value digitally on the blockchain. The blockchain which is the underlying technology for cryptocurrencies is basically a digital ledger that stores transaction data in blocks that contain information from the previous block which is why it's referred to as a chain. All transactions completed and saved to a block cannot be reversed or tampered with. Consensus mechanisms such as proof of work or proof of stake validate every transaction to make sure value is not created out of thin air. What makes blockchain technology so versatile is the fact that transaction data can consist of almost anything from health records to digital assets that represent real world assets. Blockchains are virtually unhackable and more secure than our credit, our debit cards and our bank accounts. Bitcoin has never been hacked, but identities, credit card numbers and bank accounts are stolen every day. That is the power of blockchain.

The first description of blockchain technology was proposed in 1982 by cryptographer David Chaum in his dissertation, "Computer Systems Established, Maintained, and Trusted by Mutually Suspicious Groups." The first working blockchain and cryptocurrency was implemented in 2009 by an entity by the pseudonym Satoshi Nakamoto. This was Bitcoin on its Lightning Network. A whitepaper, or documentation of its design, features, and applications, was released along with it. Bitcoin is pretty much the same as when it was released in 2009 and its infrastructure exists on computers around the world that voluntarily validate transactions and mine new blocks in return for Bitcoin. Since, thousands of cryptocurrencies and blockchains have been released and blockchain technology has evolved. Notable advances include Ethereum and stable coins which are crypto currencies that are pegged to fiat currencies.

One of the most novel advancements in the space has been the retail CBDC or Central Bank Digital Currency. This is basically a digital fiat currency that exists on a blockchain controlled by a central bank. The reality that central banks around the world are trying to manifest is the end of physical cash. Your cash balance would be digital and you would send money between friends, pay for groceries and bills all through a blockchain permissioned and monitored by the government. CBDCs have already been implemented by some countries and are being researched or tested by most according to CBDC Tracker (CBDC Tracker). CBDCs will have many benefits not limited to efficiency and more precise control over monetary policy which will make inflation easier to manage. On the other hand, privacy and user data is something that will need to be safeguarded and protected. While retail CBDC offers substantial benefits in terms of efficiency and monetary policy implementation, they also raise concerns about privacy and trust issues which may limit their adoption and utility.

CBDC will likely be the future of money. Cash will disappear and your balance will be displayed on an app developed by your government where you can send and receive money. Though seemingly dystopian, many countries have fully adopted CBDCs including Jamaica, the Bahamas, Nigeria, and Zimbabwe. Nigeria has seen the largest adoption of its eNaira. Current literature brings up a few general benefits of CBDC adoption. This includes financial inclusion, lower domestic and cross border transaction costs, and effectiveness of monetary policy implementation.

The Federal Reserve lists multiple characteristics of the implementation of a CBDC(Infante). First is the actual distribution and replacement of cash and its effects on reserves. This will generally decide how well monetary policy will be implemented with CBDCs. The Fed depicts five scenarios with the first detailing the disintermediation of banks.

The Federal Reserve states that despite the scenario, it will be able to adjust its main interest rates as it does now. What Central Banks will have to manage is its balance of traditional reserves and CBDCs. Distribution will decide how the balance sheet changes.

According to Ozili CBDCs can tremendously improve financial inclusion when the barrier to acquire such CBDCs is low (Ozili). Meaning the process of CBDC distribution involves little documentation from users and intermediation of central banks is avoided. This scenario of distribution most closely aligns with the bank disintermediation scenario described by the Federal Reserve. The section of society most aided would be previously unbanked citizens.

There is also a good deal of literature that discusses privacy and data issues with CBDCs. First of all the fact that a good deal of privacy will be given up to use CBDC some argue that people will be willing to trade access to private information for convenience and ease of use(Jabbar). The World Economic Forum provides in-depth guidance on privacy in CBDC(Waliczek). Expanding more on the nature of CBDCs, this is an exhaustive list of all potential features, freeze holdings, limit holdings, set expiry dates, set location limits, set spending limits, automatically tax transactions, flag transactions, and implement negative interest rates.

Concerning monetary policy. CBDC allows for precise changes to reserves and the money supply. Central banks will have more data and be better able to act.

There is a reason why about 90% of central banks around the world are researching CBDC technology because they see that digitization is the future and they believe the current system is flawed (CBDC Tracker). Some nations like China want to move away from the dollar as the world reserve currency. Currently according to the BIS, 90% of all forex transactions

involve US dollars(Baranoti). This is why they have the world's largest pilot test which will be mentioned later. Back to the point of digitization as stated, CBDC has many benefits compared to the cash system we have today. It has the potential to increase financial inclusion by giving every citizen access to a bank account. CBDCs also aid in improving social welfare by increasing government revenue. This is done because all transactions can be monitored and all taxable transactions may be taxed. Though this paper argues this is not exactly a benefit, governments see this as a positive as control is their objective.

Moving on to transaction costs. Though liquidity is obviously a concern in cross border transactions, wholesale CBDCs can actually help lower transaction costs. Mbridge, which is being tested by a few central banks including, Hong Kong Monetary Authority, Central Bank of the United Arab Emirates, Digital Currency Institute of the People's Bank of China and Bank of Thailand, made successful transactions between each other over this blockchain without the use of american dollars(“Project MBridge”). In terms of domestic transactions, transactions will naturally be free or close to free since there are no third party intermediaries. It is still not completely clear what position private banks will have in a world of CBDCs.

Privacy and trust is the largest concern when it comes to CBDC. Because this is a novel technology there is still so much to decide and there are not many inherent qualities of CBDC. They can exist on or off a blockchain, as a token or not. All or some transaction information can be shared to central banks, governments, and authorities. What is inherent is the fact that this digital money is issued by the government and if warranted all transactions can be monitored by authorities such as the FBI in the US. Data such as account balance, who you send money to and where your money comes from is very personal and it must be decided who can see it. Also it's unclear how CBDC will affect shadow economies. In the US anyway, the shadow economy is

closing with all cash transactions over \$600 benign deemed taxable. This all stems from the need for control.

There are some solutions that can help improve the privacy of users. First we must realize that CBDC that exist today all exist on permissioned blockchains. To make the distinction, most cryptos today exist on permissionless blockchains meaning, if you have the funds to make a transaction, there is no intermediary to stop you from making that transaction. On a permissioned blockchain there is a control layer where users must have permission to complete transactions despite having the funds. Though this is probably only used in extreme circumstances this is still the nature of a CBDC.

There are various things that can be done. For example there is a technology called zero knowledge proofs which can be used to specify what data is hidden and what data is visible (Waliczek). In mainstream crypto currencies, zero knowledge proofs help validators prove transactions without revealing transaction data. To make the distinction, this mechanism is not used in many cryptos like Bitcoin which are completely transparent and all transaction data is available to the public online.

Other solutions would be recreating the CBDC altogether. I propose we have government debt (money) exist in tokenized form on existing public blockchains such as Ethereum or the Lightning Network. This will limit government oversight of the CBDC and will basically be tokenized government debt. Along with this, only CBDCs on public blockchains will be insured by the FDIC and only government issued tokens can purchase government debt bonds.

The Bahamas was the first country to release its CBDC, the Sand Dollar in 2019. More notable cases of implementation are Nigeria with its eNaira and China with its Digital Yuan. In Nigeria, adoption is almost forced with weekly limits on how much cash citizens can withdraw.

It has improved efficiency by improving transaction speeds and lowering costs for businesses and consumers. In terms of privacy, eNaira is fully monitored by the Central Bank of Nigeria. All transaction data can be viewed by government bodies. China is currently undergoing a large pilot program with about a hundred million users. The technology is currently oversought by The Peoples Bank of China. Though the Digital Yuan offers “controllable anonymity”, anonymity can be breached at any moment and transactions can then be monitored for legal reasons.

Basically the implementation of CBDC will be dependent on laws and hopefully the wishes of the people. How they will be implemented will be a balancing act between anonymity and requirements of regulatory oversight. Combating money laundering terrorism and other financial crimes will always be an honest focus of any functioning government. Control will also be a focus. How a government will choose to design and implement CBDC to tackle either of these focuses will largely underwrite the fundamental function of money in the future.

This paper has provided a light review of some existing literature on CBDC and an examination of the benefits and concerns of this technology. Then moved on to explain why governments are interested in CBDCs. Then provided some theoretical solutions or changes. The implementation of the CBDC is a government response to the disruption that is crypto which actually was meant to allow people to take control of their own finances and promote financial transparency. CBDCs will disrupt the current financial system and most likely end privacy. We can decide how these CBDC will be implemented and only the people can decide its success.

“Central Bank Digital Currency (CBDC) Tracker.” CBDC Tracker, cbdctracker.org/. Accessed

24 Apr. 2024.

Infante, Sebastian, Kyungmin Kim, Anna Orlik, André F. Silva, and Robert J. Tetlow (2022).

“The Macroeconomic Implications of CBDC: A Review of the Literature,”
Finance and Economics Discussion Series 2022-076. Washington: Board of
Governors of the Federal Reserve System,
<https://doi.org/10.17016/FEDS.2022.076>.

Jabbar, Abdul, et al. “Investigating Individual Privacy within CBDC: A Privacy Calculus
Perspective.” Science Direct, 25 Nov. 2022,
[www-sciencedirect-com.ezproxy.neu.edu/science/article/pii/S0275531922002124](http://www-sciencedirect-com.ezproxy.neu.edu/science/article/pii/S0275531922002124#ab0020)
#ab0020.

Maronoti, Bafundi. “Revisiting the International Role of the US Dollar.” The Bank for
International Settlements, 5 Dec. 2022, www.bis.org/publ/qtrpdf/r_qt2212x.htm.

Ozili, Peterson K. "CBDC, Fintech and Cryptocurrency for Financial Inclusion and Financial
Stability." Digital Policy, Regulation and Governance 25.1 (2023): 40-57.
ProQuest. Web. 24 Apr. 2024.

“Project Mbridge: Experimenting with a Multi-Cbdc Platform for Cross-Border Payments.” The
Bank for International Settlements, 31 Oct. 2023,
www.bis.org/about/bisih/topics/cbdc/mcbdc_bridge.htm.

Waliczek, Sandra. "Central Bank Digital Currency Global Interoperability Principles." World

Economic Forum, June 2023,

www.weforum.org/publications/central-bank-digital-currency-global-interoperability-principles/.