Chapter 12
The Privacy Paradox of CBDCs: Navigating the Intricate Balance Between Financial Innovation and Individual Privacy

Guneet Kaur
University of Stirling, UK

ABSTRACT

The advent of central bank digital currencies (CBDCs) has underscored multifaceted privacy concerns identified in literature, particularly in user monitoring and data security. PETs, such as zero-knowledge proofs and homomorphic encryption, emerge as critical in reconciling regulatory compliance with user anonymity. Encryption safeguards CBDC transactions, while multifactor authentication bolsters transaction integrity. Governance structures play a pivotal role in upholding stringent security standards. This discussion navigates through diverse CBDC models and their privacy implications, probing into the intricacies of user monitoring, data breaches, and biometric data protection. Future research should aim to refine PETs, harmonize regulatory frameworks, and fortify biometric data security. The pursuit of robust privacy measures necessitates a delicate equilibrium between technological innovation and regulatory efficacy, fostering trust and compliance amidst the evolving landscape of CBDC privacy concerns.

1. INTRODUCTION

1.1 Overview of Central Bank Digital Currencies (CBDCs)

CBDCs have become a focal point in the global financial landscape, representing a fundamental shift towards digitizing national currencies. A number of factors compelled central banks all over the world to investigate and, in certain cases, test out digital currency initiatives, which has led to a surge in interest in CBDCs (Auer et al., 2023). The exploration of CBDC is primarily driven by the need to adjust to the changing dynamics of the digital economy. In an effort to modernize monetary systems, improve financial inclusion, and promote more effective payment methods, central banks are utilizing technology as digital payment systems become more prevalent and cash usage decreases (Auer et al., 2020). CBDCs

DOI: 10.4018/979-8-3693-1882-9.ch012

have the potential to better meet the changing demands of the digital era by streamlining transactions, cutting expenses, and increasing accessibility to financial services.

The fundamental ideas and control systems of cryptocurrencies and CBDCs differ significantly. Although they both function in the digital sphere, central banks issue and oversee CBDCs, guaranteeing sovereign control and conformity to predetermined monetary policies. Cryptocurrencies such as Bitcoin, on the other hand, function on decentralized networks with no central authority and are frequently praised for their independence from conventional financial institutions (Laboure et al., 2021). The analogy between cryptocurrencies and CBDCs highlights central banks' propensity to capitalize on the benefits of digital currency technology while maintaining regulatory authority. In contrast to cryptocurrencies, CBDCs place a higher priority on stability and conform to established legal and financial frameworks. Their goal is to bring together the stability and regulatory oversight of traditional fiat currencies with the efficiency and innovation of digital currencies.

Additionally, CBDCs have the ability to solve some of the drawbacks of cryptocurrencies, like volatility and regulatory issues. As a regulated digital currency alternative to the current monetary systems, the goal of CBDCs is to incorporate technological advancements while preserving central bank control. Global central banks' investigation of CBDCs is a calculated reaction to shifting financial environments, highlighting the necessity of adjusting to shifting customer tastes and technological breakthroughs. The search for innovation, financial inclusion, and effective payment methods is a driving force behind central banks' navigation of this digital revolution, and it is this quest that is driving the investigation and development of CBDCs as a progressive development in contemporary monetary frameworks.

1.2 Significance of Privacy and Security in CBDC Implementation

To ensure that the public will trust and accept these new forms of money, privacy and security are critical factors in the implementation of CBDCs. Regarding privacy and security, various CBDC design models present a range of opportunities as well as challenges. For CBDCs to be adopted and run successfully, these issues must be resolved. Moreover, the preservation of user privacy and strong security measures become crucial as countries investigate digitizing their currencies, influencing the basic acceptance and trust of these digital forms of money. For a number of reasons, privacy is essential when implementing the CBDC. Primarily, it safeguards transaction confidentiality by preventing unauthorized access to sensitive financial data. Maintaining individual financial autonomy, preventing identity theft, and protecting user information all depend heavily on this confidentiality.

Additionally, privacy preserves money's fungibility — the essential quality that makes one unit interchangeable and indistinguishable from another. In the absence of sufficient privacy safeguards, transaction traceability may result in the "tainting" of funds, which could stigmatize particular currencies and have an impact on their value, acceptance, and circulation. Privacy safeguards are also essential for maintaining citizens' rights. They ensure a certain degree of anonymity in financial transactions, defending people's liberties and insulating them from unauthorized surveillance. Anonymity promotes financial inclusivity and encourages people who are worried about privacy violations to participate in the formal economy.

Finding a balance between privacy protection and security measures is crucial, though. Sturdy security frameworks protect the CBDC system's integrity from online attacks. Multi-factor authentication, encryption, and decentralized ledger technologies—such as blockchain—protect the infrastructure from unwanted changes to transaction records and hacking attempts. Moreover, the intrinsic transparency