2024-05-28

# Privacy Considerations in CBDC Systems

By Joachim Samuelsson, CEO, Crunchfish

Published also by Central Bank Payments News, May 2024

**Privacy is an area that has not been explored deeply for CBDC systems, yet it is key for public adoption of digital currencies. In this whitepaper, Crunchfish CEO Joachim Samuelsson outlines practical considerations for how privacy may be implemented in CBDC systems and presents an innovation that balances the public's need for privacy with regulatory requirements for transactional traceability.**[1]

Increased payments digitalization has undoubtedly had numerous benefits for millions of people across the world. The adoption of faster and more convenient digital payment services (e.g., mobile wallets, real-time payments) has unlocked new economic opportunities and served as an engine for financial innovation in many societies. At the same time, it has led to the gradual displacement of cash, the most anonymous form of payment that exists today.

Cash is not only preferred by criminals; individuals may have a legitimate need for greater anonymity around the types of transactions they make given their personal situation or because they lack the typical documentation required to use other types of digital payment methods.[2] This raises numerous questions regarding how to best safeguard user privacy in a world that is increasingly digitalized. The demand for alternative digital payment instruments with cash-like privacy features is one of the most compelling reasons for the development of central bank digital currencies (CBDCs). In a public consultation that the European Central Bank carried out in April 2021, a plurality of respondents considered "transaction confidentiality" to be the most important parameter in the design of the digital euro.[3]

Enhancing the privacy features of existing payment methods, such as real-time payments, also has numerous advantages. For example, it can help prevent the unauthorized use of consumer data in the event of a cyber-attack or data breach and can help mitigate the commercial exploitation of data without user consent. This is important as many studies

[1] This whitepaper is a revised version of the whitepaper Privacy Considerations in the series Enabling Offline Payments in an Online World by Lipis Advisors, sponsored by Crunchfish. https://www.crunchfish.com/wp-content/uploads/2023/05/Lipis_WP3_Crunchfish_Enabling-offline-payments_FINAL.pdf

[2] https://www.bankofcanada.ca/2023/02/staff-analytical-note-2023-2/

[3] https://www.ecb.europa.eu/pub/pdf/other/Eurosystem_report_on_the_public_consultation_on_a_digital_euro~539fa8cd8d.en.pdf

have shown that privacy concerns can have a significant impact on users' willingness to use or adopt digital payment methods or services.[4]

Over recent years, both the private and public sectors have responded to increased digitalization with new tools and strategies for safeguarding user privacy. Encryption and tokenization have become important tools for protecting user data; they serve the function of securing data that is transmitted during payment processing, thereby making it less vulnerable to criminal or commercial exploitation in the event of a cyber-attack or data breach. Tokenization has become very popular in the cards space, where tokens (a unique string of numbers or characters) are used to substitute the cardholder's Primary Account Number (PAN).[5] Services such as Apple Pay, Samsung Pay, and Google Pay, etc., use tokenization for online and (contactless) in-store transactions. The fact that the PAN is not transmitted during the transaction reduces the risk that criminals, merchants, and/or other third parties will be able to successfully exploit sensitive data if it is hacked or stolen. Using encryption during payment processing offers the same types of benefits, though the data transformation that occurs is reversible using a corresponding encryption key.[6]

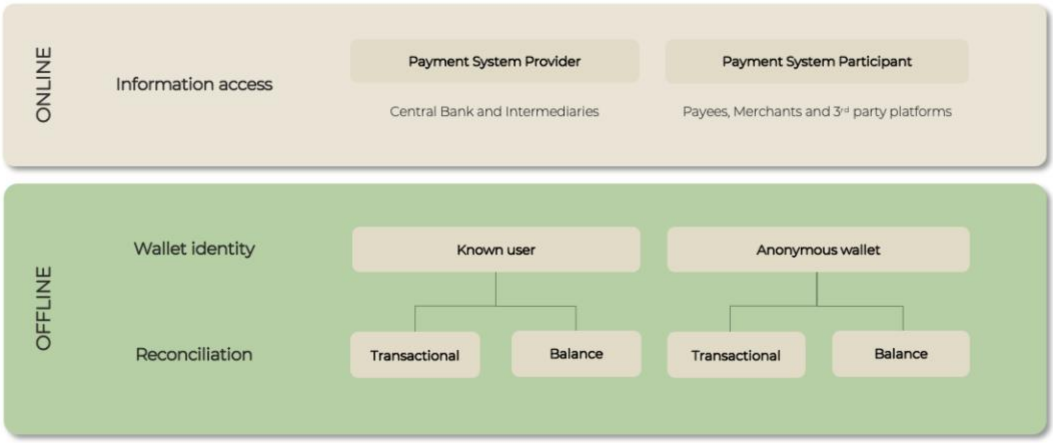
Alongside the adoption of these technologies, the development of data privacy legislation aimed at strengthening legal protections for individuals has emerged across the globe. According to UNCTAD, 137 out of 194 countries tracked have legislation in place aimed at protecting user data.[7] Examples include the General Data Protection Regulation (GDPR) in the EU, Lei Geral de Proteçao de Dados (LGPD) in Brazil, and Thailand's Personal Data Protection Act (PDPA), to name a few. These types of legislative initiatives are another important tool in mitigating against criminal and commercial exploitation of user data and ultimately ensuring trust and adoption of digital payments.

While the use of tokenization and encryption combined with better legal protections for consumers can help increase the security of user data in the hands of merchants, their benefits are limited to certain types of payments and use cases. For CBDCs, however, it is important to have anonymity in relation to the payment providers (e.g., system operator, intermediaries such as banks and payment service providers) as well. This underscores the need for new tools and solutions for enhancing the privacy options of existing payment instruments through innovations such as offline payments.

[4] https://ieeexplore.ieee.org/abstract/document/6339927
[5] https://www.pwc.in/industries/financial-services/fintech/dp/tokenization.html
[6] https://csrc.nist.gov/glossary/term/encryption
[7] https://unctad.org/page/data-protection-and-privacy-legislation-worldwide

## Offline Functionality as a Privacy-Enhancing Tool

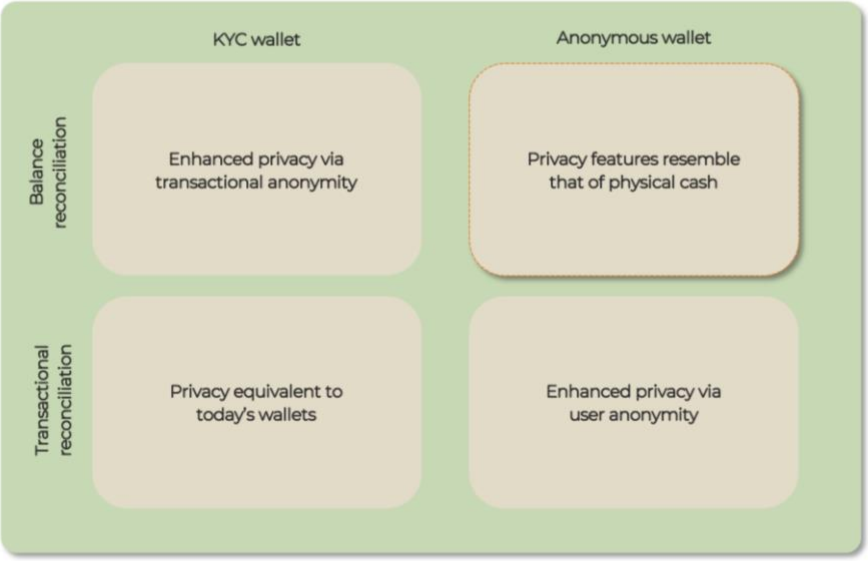
There are various options available to system operators, central banks, and regulators regarding the privacy features of offline payment systems. They may differ according to who has access to the information, whether the identity of the wallet holder is known, and what kind of data is reconciled with the online ledger. For example, do providers (system operator, payment service provider, etc.) and/or participants (merchants, beneficiary, and other third parties privy to a transaction) have access to the information? Is the identity of the wallet holder anonymous or is KYC required? What type of data is shared with the online ledger, i.e., transaction data vs. balance adjustments? These considerations are summarized in the visual below.



*Privacy considerations for offline payment system design*

With transactional reconciliation, offline transaction data is fully shared with the system operator once connectivity with the online ledger occurs. Even though the transaction data is shared fully with the system operator, the time delay between when the offline transaction occurs and when it is shared with the system operator offers some additional privacy for the transaction. In contrast, balance reconciliation is where offline transaction data is kept off the shared online ledger, though adjustments to balances would be reflected once reconciliation with the online ledger occurs. This therefore offers greater privacy with respect to the transaction data but still a degree of transparency for the system operator.

The 2x2 matrix below shows how the privacy features of different offline payment implementations can offer different levels of privacy depending on the choice of wallet design and the nature of reconciliation with the online ledger.



| | KYC wallet | Anonymous wallet |
|---|---|---|
| Balance reconciliation | Enhanced privacy via transactional anonymity | Privacy features resemble that of physical cash |
| Transactional reconciliation | Privacy equivalent to today's wallets | Enhanced privacy via user anonymity |

*Privacy features of different offline implementations*

It should also be noted that there is also the possibility of no reconciliation with the online ledger for each of the previous cases. In a fully offline model, neither offline transaction data nor adjustments to balances are reconciled with the online ledger or a third party. This would allow for completely anonymous payments, with cash-like user privacy. However, fully anonymous offline payments would pose numerous challenges from a compliance perspective, as even CBDCs would still need to comply with existing KYC/AML regulations. This could potentially be mitigated through the introduction of third-party service providers that could offer funding and defunding services for offline CBDC wallets. Such a model could enable greater anonymity for the user and their transactions.

**Design Considerations for Enhancing the Privacy of Offline Payment Systems**
Our analysis in the previous section illustrates the unique and novel aspects of using offline functionality to enable privacy. Specifically, it can enable a model through which the system operator or payment service provider has a more limited ability to observe users' transactional data. This can be done by restricting the type of data that is shared with the online ledger at the time of reconciliation to include only balance adjustments rather than transaction-level data. However, from the perspective of the system operator,

achieving greater levels of privacy for offline payments inevitably results in trade-offs, such as greater operational complexity and higher costs resulting from the increased amount of data that must be secured.[8] This underscores the need for smart design choices that maximize efficiency and scalability.

There are a range of design choices that can support the various privacy implementations available for offline payments. In the first two white papers in the whitepaper series Enabling Offline Payments in an Online World,[9] the three most relevant aspects of offline payment system design were outlined: the online payment rail (account-based or token-based), security protocol (native layer-1 or non-native layer-2), and trusted environment (hardware or software-based). In this section, how the choice of security protocol can impact the privacy features of offline payments is discussed.

The purpose of the offline security protocol is to preserve the integrity of the payer as well as the offline payment data to prevent double-spending and protect sensitive data.[10] A native layer-1 security protocol for offline payment systems is defined as one that uses the same security protocol as the underlying online payment rail; in contrast, a native layer-2 security protocol uses as a separate scheme from the online rail.

The choice of security protocol is a highly relevant design choice that will impact the privacy features of the offline payment system. In building an offline payment system designed to complement an account-based online rail, for example, a layer-1 offline protocol may limit privacy from the system operator as offline transactions would be subjected to the same degree of transparency as the online transactions. In contrast, offline payments based on a non-native layer-2 protocol would allow for greater privacy for users given that the security protocol is separate from the online payment scheme. In this instance, the level of privacy would be comparable to withdrawing money from an ATM; the sender signs out funds through the debiting of a locally held offline balance. Only adjustments to balances are reflected on the online ledger.

### Balancing Enhanced Privacy with the Need for Regulatory Transparency and KYC

While it is certain that offline functionality can offer some enhanced privacy benefits depending on the type of implementation, it must also be balanced against other needs, such as the need to mitigate against fraud risks.[11] Typically, stricter frameworks for KYC can be associated with lower privacy levels while higher levels of privacy can be associated with less strict KYC requirements. In nearly all markets, this trade-off is

[8] https://www.bankofcanada.ca/2020/06/staff-analytical-note-2020-9/#:~:text=Privacy%20in%20a%20CBDC%20goes,requires%20consultation%20with%20external%20parties.

[9] https://www.crunchfish.com/offline-payments-online-world/

[10] https://www.crunchfish.com/wp-content/uploads/2023/03/Lipis_WP2_Crunchfish_Enabling-offline-payments_FINAL_.pdf

[11] https://www.crunchfish.com/wp-content/uploads/2023/05/Lipis_WP2_Crunchfish_Enabling-offline-payments_v5.pdf

determined by the need to comply with existing regulations covering KYC as well as other areas such as Anti-Money Laundering (AML) and Counter-Terrorism Financing (CTF), which usually involve collecting and verifying information about the identity of the parties involved in a transaction.

While privacy features can help protect the confidentiality of this information, it does not negate the need to comply with the existing legal framework, particularly for real-time payment systems. In the debate around the appropriate degree of privacy for CBDCs, regulators and payment system operators around the world have been inclined toward tiered KYC models with restrictions to prevent criminal exploitation and misuse, which is also likely to apply for offline use. For instance, an offline wallet may be subject to caps on the value of holdings or limits can be imposed on the number of consecutive offline transactions that can occur without connecting to the online ledger. Different limits for different levels of KYC compliance could also allow for some privacy flexibility, with fully KYC-compliant wallets providing the least restrictions on holdings and services.

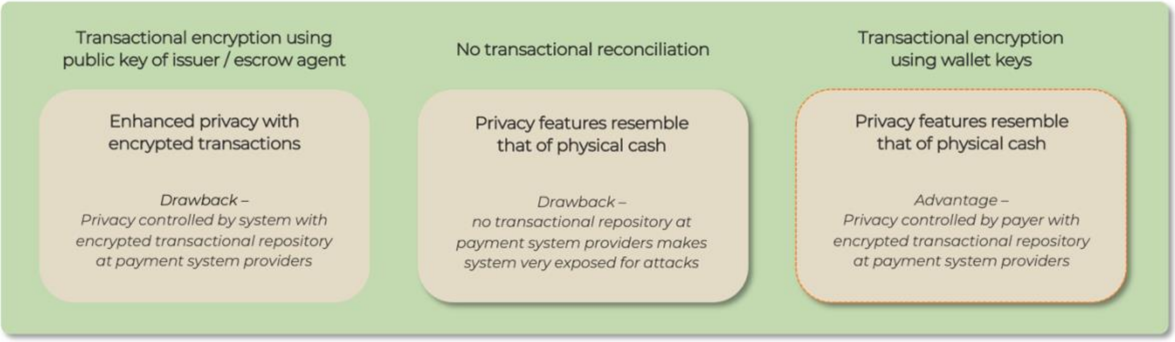
Exploring new forms of privacy for CBDCs may also require reassessing the existing legal frameworks. In the case of a digital euro, the European Data Protection Board (EDPB) recommended developing a specific legal framework for the digital euro that would address data protection and AML/CFT aspects, having deemed that the current legal framework on electronic payments does not seem to be appropriate for a tool like the digital euro, which is likely to have different characteristics from other means of electronic payments.[12] Additionally, balance reconciliation for offline payments may offer an attractive middle ground within existing regulatory frameworks as well by providing some confidentiality around transactional data while still providing a degree of transparency to the system operator and other involved parties.

There are several implementation options in CBDC systems with balance reconciliation to allow for private transactions less than a specified amount. One way would be to simply debit the balance of the payer and credit the balances of the payee and allow them to defund their wallets considering the present balance without sending up the transactional data to the central ledger at all. Such an implementation system would be blind to attacks as transactions below the privacy limit would never be invisible to the system.

An alternative approach that has been suggested is to rely on balance reconciliation, but the payer encrypts the transactional data that may trace the transaction back to the payer with the public key of the issuer. This means that the transaction is private in

[12] https://www.edpb.europa.eu/system/files/2022-10/edpb_statement_20221010_digital_euro_en.pdf

relation to the merchant as well as the system if the transactional data is not decrypted. In this way, the private transactions are encrypted when they are registered in the online ledgers of the payer and the payee, allowing the system to decrypt them with the issuer's private key in case there is a suspected attack. The drawback of this approach is that the payer is not in control of the decision to decrypt its transaction and the decryption would happen without the payer even knowing about it.



Transactional encryption using public key of issuer / escrow agent

Enhanced privacy with encrypted transactions

*Drawback – Privacy controlled by system with encrypted transactional repository at payment system providers*

No transactional reconciliation

Privacy features resemble that of physical cash

*Drawback – no transactional repository at payment system providers makes system very exposed for attacks*

Transactional encryption using wallet keys

Privacy features resemble that of physical cash

*Advantage – Privacy controlled by payer with encrypted transactional repository at payment system providers*

*Balance reconciliation with different ways of concealing transactions*

Crunchfish has recently implemented and patented a novel approach with balance reconciliation. Private transactions are encrypted and sent to the backend, but where the keys used for the transaction are wallet keys,[13] in contrast to prior art using public keys controlled by either the issuer or an escrow agent. In this way the payer is in full control of the privacy of their transactions even if all private transactions are sent to the online ledger encrypted. In this innovative way, regulatory requirements for transactional traceability are balanced with requirements for privacy where the payer is in full control of the encrypted transactional data for amounts below defined thresholds, defined by the issuer and the regulator. If the issuer suspects an attack by the payer, the issuer can contact the payer for permission to decrypt the data. In case the payer is not willing to grant access, the issuer may decide to lock the wallet or disallow any more private transactions.

At the Central Bank Payment Conference[14] in Kuala Lumpur on June 10-12, Crunchfish CEO Joachim Samuelsson will present technical ways to guarantee true privacy in CBDC systems and discuss security and scalability issues for hardware- and software-based CBDC mobile wallets.

[13] https://www.crunchfish.com/crunchfish-provides-and-patents-digital-cash-privacy/
[14] https://currencyresearch.com/the-central-bank-payments-conference/

**About Crunchfish**
*Crunchfish is a deep tech company developing a device-agnostic generic trusted client application platform for offline payments, tokenized card payments as well as other mobile client / server systems. Crunchfish has been listed on Nasdaq First North Growth Market since 2016, with headquarters in Malmö, Sweden and with a subsidiary in India.*

**About the author**
*Joachim Samuelsson is CEO at Crunchfish AB since 2020 and has been a board member since 2012. Joachim is a technology pioneer and a serial entrepreneur since 1996 with successful engagements in ComOpt AB, Actix Ltd and Biomain AB. He worked at Ericsson during 1989–1996. He holds many patents in digital payments and mobile application technology. Master of Science 1988 in Industrial Engineering and Management at Linköping University, Sweden. Born in 1965.*