Privacy-enhanced CBDCs

No Institute Given

Abstract. Keywords:

1 Related Work

Possible CBDC designs have been extensively explored both by academics and financial institutions. Privacy is one of the significant factors that affects the design choices for CBDCs. While many works state the tradeoff between the privacy of the user and the traceability of transactions by financial regulators, a more nuanced description for a privacy model is needed by first determining the privacy requirements of each stakeholder in the system (*e.g.,* payer, payee, commercial bank, central bank). Then, the required cryptographic tools can be chosen accordingly.

Transaction privacy. Transaction privacy includes hiding the amount transacted as long as it is under a certain threshold. Wüst *et al.* keep the transactions anonymous (payer identity, recipient, identity and the transaction value are kept hidden), as long as the transaction amount is below a certain threshold [12]. In order to determine whether the value is in a certain range, they use zero knowledge proofs. Transactions more than a determined amount should be revealed according to the rules determined by the regulatory authority. Choi *et al.* [8] and Chaum *et al.* [7] also discuss putting a limit for the value of transaction.

Information Asymmetry. Tinn *et al.* utilize intentional asymmetry in their proposed CBDC design [10]. While the identities of the spenders cannot be associated with their purchases, the identities of the receivers are not hidden. The authority can see the identities of receiver.

Allen *et al.* discuss different types of privacy for a CBDC: identity privacy (the fianacial activity cannot be linked to the sender and the receiver) and transaction privacy (value, sender,and recipient of the transaction cannot be learned) [2].

Token money vs account-based money. Several works like [3], [10] draw attention to the differences between account-based (similar to credit or debit card) and token money (like cash). In an account-based system, account holders are known and it is easier for regulators to analyze accounts for ensuring compliance. In a token-based systems, while users have more privacy, as their purchases cannot be tracked, regulation becomes more difficult as purchases cannot be linked to identities. Which model is a more suitable design choice for a CBDC? Armelius *et al.* states that there will not be any difference between a token-based and an account-based CBDC in terms of privacy, as there is a third party (the ledger) involved [4].

Transaction efficiency. Zero-knowledge proofs help the parties validate transactions without disclosing any private information. However long generation times of these proofs creates a concern for CBDCs [2].

Type of blockchain. Some works in the literature ([12], [11]) explore solutions using permissioned blockchains. Corda is used in Phase 2 of Project Jasper [6]. Corda addresses the data privacy concerns by partitioning data among the nodes, so that each node has access to only a part of data. One drawback of this approach is the challenges related to data replication across the network. These systems also introduce a point of failure at every node.

Privacy-preserving KYC. Literature has also explored making regulation procedures privacy-preserving. Biryukov *et al.* propose a privacy-preserving KYC scheme on Ethereum, where banks can perform KYC checks using a smart contract while keeping user information hidden from other parties–only the KYC provider knows the identities [5].

2 Conflict Diagram

Here, we define the main stakeholders and explain the possible conflicts among them. For each conflict pair, we also define possible options to resolve the conflict between each pair. We have three main stakeholders in our diagram:

1. Law enforcement: Their main aim is to prevent crime related to payments.
2. Data holder: They are entities like commercial banks, payment processors and merchants. They want to gather, analyze and monetize the data.
3. Privacy enthusiasts: They are typical users, regulators or privacy advocates. They want to keep their personal data private and they want to avoid intrusive and unnecessary access to their data.

We explain each edge in Figure 1:

2.1 Law enforcement - Data holders

$D \rightarrow L$*:* Data holders have concerns about the cost of maintaining their database for the law enforcement. However, they can benefit from this process if they are financially compensated.

$L \rightarrow D$*:* No concern arising from the law enforcement??

Both commercial banks and the central bank may decide to take some actions to help the law enforcement. Possible options are:

1. They may not take any further action to help the law enforcement.
2. They may follow a model which is similar to the KYC/AML scheme followed by banks today.
3. They can choose to take action somewhere in between the previous options (*e.g.,* less stringent KYC, recording only the transactions over a certain limit). This option can be appealing especially for preventing recording too many transactions unnecessarily, as there is a cost for it.

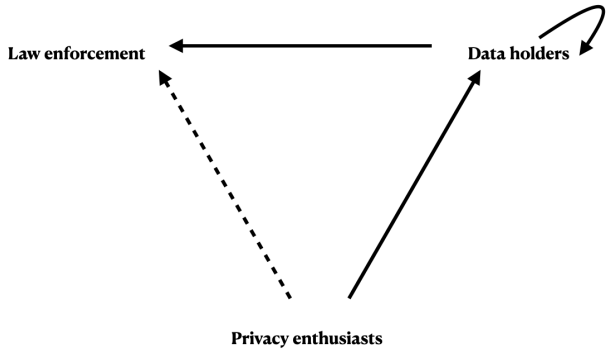

Fig. 1. Conflict Diagram: The possible conflicts that can arise among law enforcement (L), data holders (D) and privacy enthusiasts (P) are captured in this conflict diagram. The conflicts are depicted as arrows between two parties. An arrow initiated from X to Y means that X has concerns about how Y operates.

2.2 Data holders - Privacy Enthusiasts

$D \rightarrow P$: Data holders would like to monetize data. They do not want privacy to hamper their collection and analysis of data.

$P \rightarrow D$: Privacy enthusiasts oppose indirect collection and monetization of their personal information

Possible options:

1. Exceptional access: Data holders have the right to collect all data and analyze them.
2. No access: Data collectors are not allowed to collect and analyze users data.
3. Middle ground: Data collections is subject to a certain set of rules. Different cryptographic tools can be used to enforce these rules and define the conditions under which data collectors are allowed to see the data. Another way to enforce this is by law.

2.3 Privacy Enthusiasts- Law Enforcement

$P \rightarrow L$: Privacy enthusiasts support low crime rates but are concerned about law enforcement mistakes, corruptions and overreach.

$L \rightarrow P$: Law enforcement would like to reach data in the case of an investigation and they do not want the privacy measures to prevent them from doing so.

Possible options:

1. Exceptional access: Law enforcement can reach any data any time they want.
2. No access: Data is kept private and law enforcement cannot demand access.

3. Middle ground: Law enforcement can access data according to certain restrictions. This can be enforced cryptographically. Another solution can be letting users to stay anonymous as long as they transact below a certain limit. All transactions above the limit are not allowed to be anonymous.

2.4 Data holder - Data holder

Different data holders have conflicting interests in terms of data collection. For instance, each bank would like to be the only entity who has access to their data. This type of exclusivity is defined as *horizontal exclusivity*. In contrast, consider the setting where a bank uses Visa network for credit card payments. In this case, the bank has to share its data with Visa. However, the bank is not in direct competition with the Visa network in terms of collection of the data. This type of relation is defined as *vertical exclusivity*.

In another design choice, all competitors may be obliged to share all their data with others in order to prevent monopolization of data. Using a DLT would allow every data holder to see all the data recorded, meaning that there will not be horizontal exclusivity.

Central banks want to choose what to see: they may prefer not be greedy with the data and enforce privacy, so that they will not see everything.

3 Evaluation Framework

	Law enforcement	Privacy enthusiasts		Data holders	
	L → P	P → D	P → L	D → D	D → L
Cash		●	●		
Payment Network	●				
Bitcoin	◐	◐	◐		
Zcash		●	●		
PRcash [12]	●	?	q		
Privacy-preserving KYC [5]			●		

3.1 Stakeholders and conflicts

Law Enforcement Their main aim is to prevent crime related to payments.

$L \rightarrow P$: Law enforcement would like to reach data in the case of an investigation and they do not want the privacy measures to prevent them from doing so.

- **0:** L has no access to data.
- **1:** Even though L does not have full information about transactions, it can still use the data in a meaningful way for its investigations.
- **2:** Privacy does not cause L any problems during investigation. The data may not be hidden and L can reach any time. Even when the data is hidden, L has the right to deanonymize it in order to use it for an investigation.

Privacy Enthusiasts They are typical users, regulators or privacy advocates. They want to keep their personal data private and they want to avoid intrusive and unnecessary access to their data.

$P \rightarrow D$: Privacy enthusiasts oppose indirect collection and monetization of their personal information

- **-2:** D can collect and analyze every data, as data is public.
- **-1:** D can learn information to a certain extent. (*e.g.,* pseudo-anonymity)
- **0:** D cannot collect any data.
- **1:** Certain types of data is hidden, which is enough to address P's concerns. This also does not prevent D from analyzing and collecting the data.
- **2:**

$P \rightarrow L$: Privacy enthusiasts support low crime rates but are concerned about law enforcement mistakes, corruptions and overreach.

- **-2:** L can collect any data.
- **-1:** L has privileged access to data in the case of an investigation.
- **0:** L has no access to data.
- **1:** L can access data based on a condition. For example, transactions over a certain threshold should be deanonymized and L can investigate them.
- **2:**

Data Holders They are entities like commercial banks, payment processors and merchants. They want to gather, analyze and monetize the data.

$D \rightarrow L$: Data holders have concerns about the cost of maintaining their database for the law enforcement. However, they can benefit from this process if they are financially compensated.

- **-2:** D has to handle encrypted data. The cost for D to manage data is high.
- **-1:** D has to maintain data. It is not encrypted, but there is still a cost for managing the records.
- **0:** L does not require any collection of data.
- **1:** L collects data but compensates D for it.
- **2:**

$D \rightarrow D$: Different data holders have conflicting interests in terms of data collection. For instance, each bank would like to be the only entity who has access to their data.

- **-2:**
- **-1:** D can reach other entities' data. It creates competition.
- **0:** Data is not shared.
- **1:**
- **2:**

Notes

Cash: anonymous features of cash, not traceable by L or D.

Visa: D and L can trace and gather data.

Bitcoin: Users remain anonymous as long as they are not associated with the address they use. D can analyze the data to a certain extent.

Zcash: Similar to cash

PRCash: P knows that transactions are anonymous below a certain threshold. Hence, P $\rightarrow$ D and P $\rightarrow$ L conflicts are addressed. L also knows that it can learn the details of a transactions over the threshold.

Privacy-preserving KYC [5] : Solution to make regulation procedures privacy-preserving. P $\rightarrow$ L conflict is addressed.

Tinn et al. [10] : Intentional information asymmetry, identities of receivers are not hidden. The authority can see the identities of receiver. Hence partially addresses the concerns of P.

Choi et al. [8]: Similar to PRcash

Chaum et al. [7]: Similar to PRcash

FedCoin: "Fedcoin is intended as a substitute for cash and, as such, it should preserve the privacy attributes of cash (and possibly improve upon them). The primary issue is that, since the Fed acts as the gateway in and out of Fedcoin, it will have to know the public address of a Fedcoin recipient." As the recipient's address is not hidden P $\rightarrow$ L conflict is addressed partially. As Fedcoin is intended as a substitute for cash, we can assume P $\rightarrow$ D conflict is addressed

CAD-Coin: "With CAD-coin, the central bank again acts as the gateway to conversion from central bank money to CAD-coin, but privacy at conversion is not required. The privacy requirements with CAD-coin instead relate to the needs of the non-central bank participants. In CAD-coin, banks are still identified by a public address, but in order to complete payments requests generated from the real system, which are in terms of a bank's legal name, a bank must know the complete list mapping of bank names to public addresses in the distributed ledger. Therefore, the only way to ensure privacy of the complete transaction record of a bank is to limit each individual bank's access to the distributed ledger itself and to either (i) not involve all parties in transaction validation or (ii) find a way of validating the trades without seeing them, a so called "zero-knowledge validation". [9]

e-krona: Since a permissioned ledger is used, we can assume access to data by D is controlled.

4 Related work grouped according to conflict diagram

4.1 Law enforcement - Data Holders

Biryukov *et al.* propose a privacy-preserving KYC scheme on Ethereum, where banks can perform KYC checks using a smart contract while keeping user information hidden from other parties–only the KYC provider knows the identities [5].

4.2 Data Holders - Privacy Enthusiasts

4.3 Privacy Enthusiasts - Law enforcement

Wüst *et al.* keep the transactions anonymous (payer identity, recipient, identity and the transaction value are kept hidden), as long as the transaction amount is below a certain threshold [12]. In order to determine whether the value is in a certain range, they use zero knowledge proofs. Transactions more than a determined amount should be revealed according to the rules determined by the regulatory authority. Choi *et al.* [8] and Chaum *et al.* [7] also discuss putting a limit for the value of transaction.

Tinn *et al.* utilize intentional asymmetry in their proposed CBDC design [10]. While the identities of the spenders cannot be associated with their purchases, the identities of the receivers are not hidden. The authority can see the identities of receiver.

Allen *et al.* discuss different types of privacy for a CBDC: identity privacy (the financial activity cannot be linked to the sender and the receiver) and transaction privacy (value, sender,and recipient of the transaction cannot be learned) [2].

"Fedcoin is intended as a substitute for cash and, as such, it should preserve the privacy attributes of cash (and possibly improve upon them). The primary issue is that, since the Fed acts as the gateway in and out of Fedcoin, it will have to know the public address of a Fedcoin recipient. With CAD-coin, the central bank again acts as the gateway to conversion from central bank money to CAD-coin, but privacy at conversion is not required. The privacy requirements with CAD-coin instead relate to the needs of the non-central bank participants. In CAD-coin, banks are still identified by a public address, but in order to complete payments requests generated from the real system, which are in terms of a bank's legal name, a bank must know the complete list mapping of bank names to public addresses in the distributed ledger. Therefore, the only way to ensure privacy of the complete transaction record of a bank is to limit each individual bank's access to the distributed ledger itself and to either (i) not involve all parties in transaction validation or (ii) find a way of validating the trades without seeing them, a so called "zero-knowledge validation"." [9]

e-krona uses Corda "For example, the e-krona's DLT network will be private and only accessible for participants approved by the Riksbank." [1]

4.4 Data Holder - Data Holder

References

1. The riksbank's e-krona pilot. Tech. rep., Riksbank (2020)
2. Allen, S., Čapkun, S., Eyal, I., Fanti, G., Ford, B.A., Grimmelmann, J., Juels, A., Kostiainen, K., Meiklejohn, S., Miller, A., et al.: Design choices for central bank digital currency: Policy and technical considerations. Tech. rep., National Bureau of Economic Research (2020)
3. Armelius, H., Claussen, C.A., Hull, I.: On the possibility of a cash-like cbdc. Tech. rep., Sveriges Riksbank Staff memo (2021)
4. Armelius, H., Claussen, C.A., Hull, I.: On the possibility of a cash-like cbdc. Tech. rep., Sveriges Riksbank Staff memo (2021)
5. Biryukov, A., Khovratovich, D., Tikhomirov, S.: Privacy-preserving kyc on ethereum. In: ERCIM Blockchain Workshop (2018)
6. Chapman, J., Garratt, R., Hendry, S., McCormack, A., McMahon, W.: Project jasper: Are Distributed Wholesale Payment Systems Feasible Yet? Financial systems review, Bank of Canada (2017)
7. Chaum, D., Grothoff, C., Moser, T.: How to issue a central bank digital currency. arXiv preprint arXiv:2103.00254 (2021)
8. Choi, K.J., Henry, R., Lehar, A., Reardon, J., Safavi-Naini, R.: A proposal for a canadian cbdc. Available at SSRN 3786426 (2021)
9. Garratt, R.: Cad-coin versus fedcoin. R3 Report **15** (2016)
10. Tinn, K., Dubach, C.: Central bank digital currency with asymmetric privacy. Available at SSRN 3787088 (2021)
11. Veneris, A., Park, A., Long, F., Puri, P.: Central bank digital loonie: Canadian cash for a new global economy. Available at SSRN 3770024 (2021)
12. Wüst, K., Kostiainen, K., Capkun, V., Capkun, S.: Prcash: Fast, private and regulated transactions for digital currencies. In: Financial Cryptography (2018), `https://eprint.iacr.org/2018/412`