

# Privacy in Digital Money from a Technology and Economic Perspective



Published By

Hosted By



in co-operation with the Swiss  
Centre of the BIS Innovation Hub

A Roundtable was held on June 26, 2023, in Zürich as part of the Point Zero Forum. The topic of discussion was “Privacy in Digital Money from a Technology and Economic Perspective.” The Swiss National Bank, in collaboration with the Swiss Centre of the BIS Innovation Hub, hosted the session. Thomas Moser, an Alternate Member of the Governing Board of the Swiss National Bank, served as the moderator. The Roundtable

brought together 13 technologists, economists, officials, and legal experts from various countries.

The Roundtable was conducted under the Chatham House Rule, which ensures that comments are not attributed to individuals. The purpose of this summary is to outline the main themes and important actions that emerged from the discussion.



### Summary of key observations:

- 1. Privacy is a relevant and highly important issue in the context of digital payments:** With the growing prevalence of online financial transactions, safeguarding access to individuals’ personal and financial data assumes utmost importance.
- 2. The technology to provide privacy solutions already exists:** The necessary technology is available to appropriately tackle privacy concerns.
- 3. The public and private sector play both an important role in providing privacy in digital payments:** From an economic view, privacy is essential for trading opportunities and distribution of surplus. Where market incentives are lacking, the public sector needs to intervene through a regulatory framework or consider providing a privacy preserving CBDC.
- 4. Addressing privacy issues requires not only a regulatory framework, but also education:** The challenges of addressing privacy issues go

beyond the lack of incentives or a regulatory framework. Equally crucial is the imperative to enhance the overall educational proficiency of all stakeholders involved in privacy matters.

**5. Achieving proportionality is crucial:**

Balancing privacy considerations requires collaboration between the public and private sectors. A strong regulatory framework is needed to strike a balance between anti-money laundering efforts and privacy concerns, ensuring effective measures against financial crimes while safeguarding individuals' privacy rights.

**6. Sustained dialogues between regulators and professionals hold significant importance:**

The discussions held among economists, cryptographic experts, legal and regulatory professionals and regulators from the public field are of paramount importance as they contribute to the development and advancement of privacy matters in case of digital payments.

**Calls to action:**

This discussion leads to a range of actionable recommendations or initiatives:

- **Privacy is a fundamental and critical consideration in the design of digital money:** Ensuring privacy is an essential aspect of digital currency design, not an afterthought. In the context of a Central Bank Digital Currency (CBDC), any deviation supporting privacy may prove unworkable. As society gradually moves away from physical cash in favour of digital payments, overlooking privacy implications would create a privacy deficit that would be difficult to remedy once digital solutions have been designed without due consideration for privacy.
- **Ensuring privacy is not only essential to maintaining consumer trust, but it also needs to be taken into consideration in data protection regulations:** Individuals are increasingly concerned about the security and confidentiality of their personal information. By prioritising privacy, organisations can foster a sense of trust and confidence among their customers, leading to stronger relationships and loyalty. Privacy is a fundamental aspect of data protection regulations. These regulations are designed to safeguard individuals' personal data and ensure its proper handling, storage, and processing. By incorporating privacy considerations into data protection regulations, organisations can meet legal requirements, mitigate risks, and protect individuals' rights to privacy.
- **Developing a widely accepted form of money that can then be augmented with various desired features as necessary:** The focus should be on incorporating robust privacy technology into electronic money systems. The goal is to establish a highly private form of money that is widely trusted and used. This might involve building a system that ensures limited payment visibility, allowing for the addition of desired features as necessary. Privacy attributes, such as transaction anonymity, mutual identity protection, and verifiable signatures, could be seamlessly integrated into this core privacy-focused solution. By prioritising privacy and promoting the adoption

of such a clean and efficient electronic money system, the needs of the unbanked population could be addressed, and their significant economic challenges could be alleviated.

- **Encourage and facilitate discussions among lawmakers, regulators and experts from different fields across both public and private sectors:** There are fundamental discussions that need to take place, and it will likely take years to reach a point where there is

sufficient clarity to operate a widely accessible means of payment. The discussions held by economists, cryptographic experts, and legal and regulatory professionals is important, as these conversations contribute to the development and progress in this area.



### **Substantive Discussion:**

Detailed deliberations were exchanged during the Roundtable, which are elaborated upon within the framework of five key themes that emerged.

#### **1. Privacy is a relevant and highly important issue in the context of digital payments**

At the outset, it was noted that as online financial transactions become more common, protecting personal

and financial data becomes crucial. Ensuring privacy is essential for maintaining consumer trust and complying with data protection regulations.

Furthermore, the maintenance of the balance between privacy and accountability in financial transactions is important. Accountability should apply not only to individuals using money but also to the government and authorities, ensuring transparency and fairness.

This balance is necessary to prevent financial investigations and anti-money laundering efforts detaching from the regular justice system, which could lead to a lack of accountability to the public.

An approach has emerged from a participant, that privacy could be discussed in three dimensions:

1. *“Privacy is an individual right to autonomy.”*
2. *“Privacy is a personal preference for some individuals.”*
3. *“From an economic perspective, privacy is a factor for achieving fair and efficient trade.”*

On the other hand, it was also mentioned that from an economic perspective (third dimension), trade relies on overcoming information imbalances, and the lack of privacy in payments determines the trading opportunities and the distribution of benefits.

A participant eloquently expressed the following thought:

*“Privacy is a public good, like clean air, and if some people don't protect it, it affects us all.”*

## **2. The technology to provide privacy solutions already exists**

The importance of honouring and preserving privacy in both the present and future, particularly in light of the emergence of quantum computers, was emphasised. Zero knowledge proofs and blind signatures, for example, make it easier and more cost-effective to implement privacy measures.

To put in the words of one of the participants:

*“We have the technology to address privacy in the right way now.”*

Even in regions without formal banking services, mobile phones are prevalent serving as convenient means of access to digital currencies. The potential for utilising digital currencies exists, and it is now about initiating the necessary steps to realise it.

However, it is important to avoid single points of failure or compromise in any system. For instance, entrusting the security of valuable information to a single individual is highly associated with risks. Such a practice is considered bad security practice in any environment. Although implementing robust security measures may come with a cost, it is necessary to ensure the integrity and protection of sensitive data.

Conclusively a participant expressed the following:

*“In response to how much privacy technology can offer, I believe there is no limit.”*

## **3. The public and private sector play both an important role in providing privacy in digital payments**

Both the public and private sectors play crucial roles in ensuring privacy in digital payments. Privacy is essential for enabling trading opportunities and determining the distribution of surplus in transactions. When market incentives alone are insufficient, the

public sector may need to intervene by implementing a regulatory framework or consider a privacy-preserving Central Bank Digital Currency (CBDC). By combining the efforts of both sectors, privacy concerns can be effectively addressed and a secure financial ecosystem can be created. However, striking a balance between privacy rights and effective implementation poses challenges. It requires developing a suitable framework that protects sensitive information while addressing financial crimes like money laundering and fraud. The discussions also highlighted the challenges faced by financial institutions using privacy coins, as regulators may react unfavourably. Ongoing discussions reflect the complexity of this topic and the need for continuous examination and improvement of privacy measures in digital payments.

#### **4. Addressing privacy issues requires not only a regulatory framework, but also education**

Clear standards in the field of privacy will constantly evolve due to the rapid advancements in technology and changing living standards. Policy makers need to continuously adapt frameworks to address these changes. Education is crucial for actors involved in privacy matters, encompassing both professionals and private individuals. Frequently, there is a notable absence of incentives, particularly within the private sector. The need for expertise in creating secure cryptographic solutions and understanding data utilisation is often underestimated. Many individuals are unaware of how their data is being used. However,

access to digital currencies is easily available, and users have a significant responsibility in ensuring the security of their devices and receiving proper education.

One of the participants have summarised this issue as follows:

*“But it’s also another angle that maybe I don’t care about privacy today because I trust everyone around me. But maybe tomorrow there is a different picture because there are different people in charge. [...] and then I changed my mind. But at that point, it would be quite late.”*

#### **5. Achieving proportionality is crucial**

It is crucial to reconcile anti-money laundering (AML) requirements with the protection of individuals’ data, privacy, and confidentiality. Upholding privacy and confidentiality are not merely a matter of compliance, but a fundamental right. Without adequate safeguards, trust and confidence in tokenised money can be compromised. Achieving a good balance between anti-money laundering (AML) efforts and privacy necessitates the development of a robust regulatory framework. This framework should consider the importance of safeguarding individuals’ privacy rights while also ensuring effective measures to combat financial crimes. Striking the right balance involves crafting regulations that enable efficient AML procedures without excessively infringing on privacy. Such a framework should provide clear guidelines and standards to govern the collection, use, and sharing of personal

and financial data, promoting transparency, accountability, and the protection of individual privacy.

#### **6. Sustained dialogues between regulators and professionals hold significant importance**

Questions were raised about how close we are to achieving a legal environment that provides the necessary clarity for various forms of payment and money.

Some participants believe that considerable ground still needs to be covered and highlighted the need to determine who is exposed to which legal requirements. The participants agree that fundamental discussions are required to reach the desired clarity. The importance of continuing dialogues among economic technologists, cryptographic experts, and legal regulators was emphasised.



Key questions shall be posed regarding the preferences of regulators, such as prioritising privacy or investor protection.

There is also a need to define the position and requirements of different stakeholders, including the society, regulators, central banks, and private banks. Stakeholders, i.e., consumers, banking and financial industry, regulators, and central banks, could catalyse and drive the adoption of privacy in digital money. Taking prompt

action is of utmost importance as the potential negative consequences of not addressing the privacy in digital money are significant, while the potential benefits of embracing it are immense.

The overall focus is on understanding the current state, defining goals, and determining the timing of developments in the field of payment systems.



[elevandi.io](https://elevandi.io)