JANUARY 2023

PRIVACY AND CENTRAL BANK DIGITAL CURRENCIES

DIGITAL EURO ASSOCIATION
PUBLIC DIGITAL EURO WORKING GROUP

Privacy and CBDCs
Digital Euro Association
Public Digital Euro Working Group

Chairpersons

Anne-Sophie Gógl
David Tercero-Lucas

Contributors

- Shafiq Amiri
- Cizar Bachir Brahim
- Csaba Gerencsér
- Animesh Ghosh
- Juan Gutiérrez
- Kombe Kaponda
- Conrad Kraft
- Karen Ottoni
- Christian Pfister
- Anthony Ralphs
- Daniel Szego
- Fréderic Tronnier
- Lois Tullo

The views expressed in this paper are the authors' own and do not necessarily reflect the views of their employers or the Digital Euro Association (DEA). The DEA would like to thank its supporting members, whose support was instrumental in making this work possible.

This paper is one in a series of short papers whose aim is broadly informing the public and institutions about particular topics related to CBDCs.

List of abbreviations

AML	Anti-Money Laundering
CBDC	Central Bank Digital Currency
CFT	Combating the Financing of Terrorism
DEA	Digital Euro Association
DLT	Distributed Ledger Technology
ECB	European Central Bank
EDPB	European Data Protection Board
EU	European Union
FATF	Financial Action Task Force
GDPR	General Data Protection Regulation
KYB	Know-Your-Business
KYC	Know-Your-Customer
KYT	Know-Your-Transaction
MNO	Mobile Network Operator
NIST	National Institute of Standards and Technology
PII	Personal Identifiable Information
PKI	Public Key Infrastructure
SSID	Self Sovereign Identity
TEE	Trusted execution environment
TLS	Transport Layer Security
UN	United Nations
WEF	World Economic Forum

Table of Contents

1. Introduction **1**

2. Reasons for Privacy and Degrees of Privacy in CBDCs **2**

2.1 Reasons for Privacy in CBDCs 2

2.2 Privacy in Existing Payment Methods versus CBDCs 2

2.3 Privacy in CBDCs 4

3. CBDC Privacy Stakeholders **5**

4. Technologies **6**

4.1 Trade-off Between Privacy and Security using Technology 6

4.2 Privacy Approaches 6

4.3 Privacy in a Post Quantum World 7

5. Regulation **8**

6. Conclusion **9**

7. Recommendations **10**

References **11**

1. Introduction

Privacy is regarded as a crucial factor in the investigation and development of Central Bank Digital Currencies (CBDC) and is therefore thoroughly researched by monetary authorities, academia, and the private sector. Academic research indicates that CBDC transactions may involve processing significant amounts of identity and transaction-related information (Lee et al., 2021), raising privacy concerns for future users. While there exist countless definitions for privacy, such as "the right to be left alone" (Warren and Brandeis, 1890), in this document, the definition of Nissenbaum (2010) - "the appropriate flow of information" - will be followed.

There is preliminary evidence that suggests that the level of privacy associated with CBDC use will be a key determinant of CBDC adoption and usage. In 2021, the European Central Bank (ECB) issued a report on the public consultation on a digital euro that included 8221 respondents. The report revealed that privacy was the most important feature required by individuals although results varied depending on the country analysed. Nonetheless - on average - privacy was ranked higher than all other features such as security or usability (ECB, 2021). Other central banks have also actively discussed privacy in the development of CBDCs, with a myriad of potential solutions being proposed. For example, the Bank of Canada notes that a decision on the level of privacy that a CBDC might possess is a crucial public policy issue. It adds that a CBDC could be designed to implement a form of privacy rather than cash-like anonymity, allowing it to satisfy anti-money laundering (AML), combating the financing of terrorism (CFT), and other regulations that require disclosure of certain levels of private information (Bank of Canada, 2020). Even the digital yuan - the Chinese CBDC - has included levels of privacy in its pilot and has tiered privacy to balance, transfer and activity limits. It presents five levels, two of which do not require a user's identity, but rather just a phone number or email address. Therefore, there isn't a one-size-fits-all privacy design for CBDCs and there are factors affecting privacy (such as regulation) that extend beyond the central bank's remit or control.

Academic research has also confirmed the importance of privacy for individuals on a hypothetical digital euro in qualitative research with experts and non-experts from Europe (Tronnier and Biker, 2022). The results of the research indicate the crucial role of trust in central banks and the significant negative effect that privacy concerns may have on the intention to adopt and use a CBDC. To mitigate these concerns, technological solutions are currently being discussed and piloted to ensure privacy protection in CBDC payments (Gross et al., 2021; Chaum and Moser, 2022).

In this document, we aim to follow the call of the European Data Protection Board (EDPB, 2022) to shape the public debate on the topic of privacy by providing an overview of privacy in CBDC development and use. To this end, we discuss the possible degrees of privacy in CBDC payments, the relevant actors, technologies, and concerns regarding regulation. The paper concludes with a set of well-considered, actionable recommendations for enhancing privacy in CBDC systems.

2. Reasons for Privacy and Degrees of Privacy in CBDCs

It is imperative to understand why privacy is such a key aspect in CBDC design as well as to assess privacy in existing payment methods such that we may compare this to proposed CBDC models.

2.1 Reasons for Privacy in CBDCs

Privacy is a key consideration for the implementation of CBDCs as it is with any government/public project involving personal or personalized information regarding citizens. The degree of privacy, reasons for it, and prioritization can vary significantly between jurisdictions. It is an essential part of individual autonomy, and many human rights rely on privacy as a core pillar to establish barriers and safeguards from unwarranted interference in people's lives. Privacy provides citizens protection from control and manipulation of power, human dignity, safety and self determination. The increasing digitalization of the economy has made it easier than ever before to acquire data about individuals without their knowledge and infringing their rights to privacy.

Protection of personal information is listed in Article 12 of the United Nations (UN) Universal Declaration of Human Rights (United Nations, 1948) and is reaffirmed as a human right in many other conventions and charters such as the International Covenant on Civil and Political Rights and European Convention on Human Rights. Despite these legal protections, it does not necessarily inhibit the existence or extent of surveillance. In 2021, the United Nations Office of the High Commissioner published a report that detailed how the use of new technologies (artificial intelligence, automated decision-making, machine-learning etc.), affects the enjoyment of the right to privacy and associated rights.

CBDC design and implementation must not increase the exposure or vulnerability of citizen data in favour of speed or efficiency. Doing so would risk violating international laws and conventions and jeopardize the successful adoption of CBDCs. The loss of citizen trust in a CBDC would result in the non-use of the instrument and non-achievement of the policy goals for its implementation.

2.2 Privacy in Existing Payment Methods versus CBDCs

Degrees of privacy vary across existing payment methods. Typically every payment method - with the exception of cash - requires a form of onboarding to utilize. This provides all actors in the payment system with a minimum level of participation and creates a governance and compliance framework. The level of data required and processed varies by transaction and is usually dependent on the transaction type and value. This data might include just account identifiers but could also include other Personal Identifiable Information (PII) to support compliance requirements.

In Table 1, we examine the various payment methods in use today, outlining the minimum data required to utilize each method and compare them with cryptocurrencies and CBDCs.

Activity	Cash	Bank Transfer	Credit / Debit Card	e-Money	Crypto currency	CBDC
Onboarding	None	Account opening and KYC	Account opening and KYC	Account opening and KYC	Pseudo-anonymous, KYC	Account opening and KYC
Point of access	ATMs, other holders of cash	Bank, website, mobile app	ATMs, point of sale (physical & online)	Website / mobile app	Exchanges, wallets	Website / mobile app
Counter-party identification	Anonymous	Bank account & bank code / proxy identifier (e.g. phone number)	Card Number	Proxy identifier (e.g. email address)	Wallet address	Various levels - from complete traceability to full anonymity
Transaction Information	Amount spent	Originator + beneficiary account info, transaction description	Card number (tokenized), purchase information, merchant information, account information for ATM withdrawal	Names & proxy IDs, purchase information	Originating address, destination address, amount transferred, date, time	Dependent on the amount tier
Transaction Monitoring	None	Transaction screening by account servicing institutions, payment schemes	Transaction screening by issuers	Transaction screening by wallet / e-money service	On-chain analysis	Varies - more information than existing payment to cash like

Table 1. Comparison of payment methods and associated data requirements activities
Source: Authors' elaboration

Along with the above requirements for individual transactions, there is often a framework applied by the system operator or state that defines the level of privacy offered in some cases.

2.3 Privacy in CBDCs

Potential models for privacy are dependent on the method of CBDC access and CBDC type.

Some central banks have indicated that onboarding of users is likely to be facilitated by trusted intermediaries, e.g. banks/regulated institutions, telecommunications providers etc., who already have established practices and proficiencies in this regard (EAC, 2022). This in itself will likely require users to provide information to allow the intermediary to KYC (Know your customer) them in accordance with any rules defined by the state.

Once onboarded, consideration will need to be made as to the level of information that is required to be shared. There is certainly potential to offer CBDC users a greater variety of privacy levels than exist in current digital payment methods. There is also the possibility that transaction data - beyond the value movement - is handled off-ledger through a different protocol.

Table 2 summarizes the spectrum of different privacy approaches analysed in this paper. If all transactions and other consumer data are visible to merchants and intermediaries, one would be under the lowest possible level of privacy. On the contrary, if no transaction or other data is visible to intermediaries and merchants, one would achieve the maximum degree of privacy - i.e., full anonymity.

Approach	Summary	Level of privacy
Fully transparent	All transaction and owner data visible.	Low / None
Privacy against merchants	Transaction data is not shared with the merchant but is shared with the CBDC operator.	Low
Transparent to Intermediary	Intermediaries handling the account / transaction can view the data but the originator and beneficiary cannot.	Low
Asymmetric privacy (spender vs. buyer)	Using anonymised tokens to perform the transaction and hide the buyer's identity.	Medium
Privacy for low value payments	Transaction data below a defined amount is hidden / prevented from being accessed.	Medium / High
Privacy under offline functionality	Transaction data associated with offline transactions would be kept off the shared ledger. Only adjustments to balances would be reflected.	Medium / High
Full anonymity	All transaction and owner data is hidden / prevented from being accessed. Commercial Banks and PSPs cannot view a customer's association with a merchant.	Highest

Table 2. Privacy approaches and associated levels of privacy
Source: Authors' elaboration

3. CBDC Privacy Stakeholders

There is a need to ensure a balance between preserving user privacy and compliance with various regulations and policies such as AML/CFT. In order to strike this balance, several stakeholders and participants need to be engaged early in the CBDC journey to get relevant buy-in and allow privacy and trust in the use of a CBDC. These stakeholders include government authorities through the office or ministry of finance, the issuing monetary authorities mainly central banks or reserve banks, financial conduct authorities, financial intelligent centers, commercial banks, payment systems providers, competition and consumer protection agencies, centralized know your customer (KYC) authorities, including Mobile Network Operator (MNO) databases, banking and payments associations, national ID vs functional ID authorities, merchants, payers and most importantly, end-users. Intermediaries can be defined as a party to the relationship between a payee and payer. These could include payment service providers, e-money institutions, and commercial banks, amongst others.

All parties involved in CBDC payments must both receive and provide data in order to fulfill their functions and participate in the CBDC ecosystem. Table 3 summarizes the minimum data required and supplied by the primary stakeholders (end users, central banks, commercial banks, merchants, payment processors, and mobile operators, among others) in the CBDC ecosystem.

Stakeholder	Minimum data required	Minimum data supplied
End users	None	Tiered KYC: Phone Number, Formal ID, National Registration, Drivers License, Passport.
Central Banks	Ledger access (balances)	-
Commercial Banks	Full KYC data	Trading license, Risk-based due diligence.
Merchants	None	Trading License.
Payment Networks (e.g. VISA)	Full KYC data	Trading license, Risk-based due diligence.
Mobile Operator	Full KYC data	Trading license, Risk-based due diligence.

Table 3. Primary CBDC privacy stakeholders in both developed and developing economies
Source: Authors' elaboration

4. Technologies

This section examines the trade-off between privacy and security from a technological perspective and examines the various privacy approaches that central banks may adopt.

4.1 Balancing the Trade-off Between Privacy and Security using Technology

Choosing to prioritize one aspect of privacy can mean sacrificing potential gains in security, a scenario commonly referred to as a trade-off. With the advancement of cryptography, newer systematic and mathematical methods to achieve privacy, confidentiality, and anonymity in a wide range of financial systems and applications are being developed (WEF, 2021). To enhance the robustness of privacy in CBDC implementation, existing technologies require further development to achieve a scalable CBDC system that combines privacy and security. This is one of the main causes of the tension between the cryptocurrency community and the traditional financial world. Fully anonymous/pseudonymous systems cannot satisfy the regulatory requirements of the financial system (which includes know your customer (KYC)/ know your business (KYB)/know your transaction (KYT), AML, and Financial Action Task Force (FATF) travel rules) and cryptocurrency systems keep denying the adoption of the identity concept to protect a user's privacy. However, these two goals (KYC and privacy) are achievable at the same time.

From a technological standpoint, the optimal balance in designing the privacy aspect of digital cash is to have traceability of the sender without disclosing the user's private information. (Cummings et al., 2016). This implies that transactions should primarily be encrypted and anonymous. Some countries may prioritize anonymity for transactions below a certain value, ensuring that the associated data is completely irretrievable. On the other hand, other countries may choose to retain transaction data for all transactions, including low value transactions, making them retrievable only if legally required. It is worth noting that an often-mentioned value proposition of CBDCs is the possibility of completely anonymous payments, where data is not stored or retrievable, a feature that is not currently offered by other digital payment methods.

Self-Sovereign Identity (SSID), a set of technologies that shift control of digital identity from third-party providers to individuals, may offer a solution in the near future (Preukschat and Reed, 2021). In blockchain-based CBDCs (note: at present, not all CBDC implementations are blockchain-based), no personal information can be retrieved from the blockchain without the use of side-chain data. This kind of network separation could be a good balance towards achieving an optimal level of privacy while preventing illegal activity.

4.2 Privacy Approaches

There are many different kinds of privacy approaches. These approaches can however be categorized as follows: software-based approaches, hardware-oriented approaches, and hybrid approaches. The following technologies provide a general spectrum of privacy frameworks, allowing for varied levels of privacy implementation (high, medium, low privacy guarantees). Common software-based privacy approaches include:

- Classical symmetric encryption with a Public Key Infrastructure (PKI) key exchange mechanism (e.g., the Transport Layer Security (TLS) protocol or in the end-to-end encryption of the DC/EP (Turrin, 2021)). Sometimes, a clever key generation for privacy may be used as well (e.g., stealth addresses in Monero (SerHack, 2018)).

- Advanced pseudonymization: ring signatures provide a way to sign a transaction with several private keys, without leaking the explicit owner information, thus providing higher anonymity sets and eventually better privacy (SerHack, 2018).

- Zero knowledge proofs. They provide a way to cryptographically prove a statement without leaking information on the statement itself. As an example, it can be cryptographically guaranteed whether an account has enough balance for a transfer without revealing the exact amount (Bertaccini, 2022).

- Other cryptographic constructions, such as homomorphic encryption, blind signatures, or functional encryption, can provide computation on encrypted data without revealing the data itself.

In the simplest physical privacy design, data exists only where it needs to be visible. This is easiest to realize, for instance, with a message-based CBDC solution. More advanced hardware-based solutions are based on trusted execution environments (TEE) to execute critical privacy-oriented computation on dedicated chips in such a way that data is not made available, not even towards the operators.

Most practical privacy designs combine some of the previously mentioned approaches. For instance, payment channels or roll ups transfer most data or computation outside of a ledger, providing cryptographic data consistency and increased privacy. Other hybrid approaches try to combine classical software-based privacy with physical data separation to provide dedicated optimal solutions for the dual banking system (Chaum et al., 2021).

4.3 Privacy in a Post Quantum World

The infrastructure that secures data and provides users with the required privacy can only be as strong as its weakest link. Developments in quantum information systems are emerging, raising questions related to how quantum computational power can be utilized to overwhelm or break security measures that protect user funds and data. A vulnerability of CBDC can be identified in its infrastructure. Some live CBDC implementations are DLT-based. As the vast majority of existing blockchains rely on elliptic curve cryptography and have their public keys known, a powerful enough quantum computer will be able to derive the private key of an account with at least one outgoing transaction. Although there is no quantum computer capable of breaking blockchains today to carry out “storage” or “transit” attacks, bad actors can employ the “store now, decrypt later” scheme where they would obtain data now, but decrypt it at a later date with quantum capabilities. It is worth considering how privacy achieved through encryption may be affected in a post-quantum world. Transitioning to quantum-secure cryptography may be necessary as leading economies have planned to migrate to quantum-resistant cryptography with National Institute of Standards and Technologies (NIST) spearheading the standardisation mandate. It may be prudent to contemplate the future potential quantum threat in current CBDC design considerations.

5. Regulation

> **Regulation in the context of privacy**
>
> Regulatory bodies have the difficult task of developing a sound framework within which a CBDC system may function. This would require the balancing of data privacy policies and other policy considerations such as AML / CFT / taxation. Regulators are tasked with developing a set of robust CBDC regulations while CBDC technological investigations are undertaken by central banks.

Protection of information privacy is not only desired by users but also compulsory by law as privacy is regarded as a fundamental human right and not just a right granted by a state. This is depicted, as stated in section 2.1, Article 12 of the Universal Declaration of Human Rights by the United Nations (United Nations, 1948) or the Article 17 of International Covenant on Civil and Political Rights which declares that no one shall be subjected to arbitrary or unlawful interference with his privacy.

Data privacy principles must be applied to both the regulator and the subjects of the applicable law. However, the right to the protection of privacy and personal data are not considered to be an absolute right but must be considered in accordance with the principle of proportionality, in relation to its role in society, and in balance with other fundamental rights. Thus, it can be restricted proportionally accordingly by law to provide protection of certain other economic, social rights (e.g. CFT, AML, taxation etc.). Such a proportionate balancing scheme shall be outlined by a Regulatory Body. Regulatory bodies have the difficult task of developing a sound framework within which the implementation and application of a CBDC system may function. In Europe, the EDPB is responsible for ensuring the application of the GDPR, issued a statement on the importance of privacy by-design and by-default principles in the creation of CBDC and called for the avoidance of systematic tracking through CBDC (EDPB, 2022). This could be a guide for other jurisdictions thinking about regulations for CBDC.

To minimize the risk of violation of data privacy regarding a CBDC application, an embedded set of data privacy measures should be executed during the planning, implication, and the execution of a CBDC system.

Examples could be to determine a certain threshold and/or a certain number of transactions per period (or two thresholds, one for each transaction and another for all the transactions during a given lapse of time) which cannot be directly traceable by anyone, including the central bank. Transfers below this threshold would just give rise to the debit of the wallet of the payer and the credit of the wallet of the payee, without any intermediary, not even the central bank, recording the details of the transaction. This would make such transactions analogous to payments in cash. The scope of untraceable transactions should be settled by the law.

6. Conclusion

Ensuring privacy in a CBDC system is not only important for the protection of human rights, but it is also crucial for the successful adoption, usage, and implementation of the digital currency.

The issue of CBDC privacy has become even more important as we witness the division between country and regional governments, their leaders, central banks, and monetary authorities. Each central bank will have a different view and values around privacy but there are some minimum standards that should be respected. All the while, CBDCs are likely to increase cross-jurisdictional data flows.

The implementation of strong encryption methods, strict access controls, regular auditing, and a stringent disciplinary regime for privacy violations can help to ensure the security of a CBDC system. Additionally, establishing robust regulations governing the use of CBDCs can provide further protection for the privacy of individuals.

The tensions between privacy preservation and policy compliance is a longstanding concern that is likely to continue as digital payments and digital money evolve. A well-considered blend of education, policy, and technological prowess is required to strike the right balance between achieving privacy for users, without compromising other policy goals.

7. Recommendations

1. Include strong encryption and security protocols in CBDC design, considering also those utilized in distributed ledger technology to protect the privacy of individuals and their financial information.
2. Obtain early buy-in from key actors in the CBDC ecosystem to ensure they are in agreement and compliant with relevant privacy standards and protocols.
3. Establish clear, transparent and consistent standards for data protection and privacy in CBDCs.
4. Implement robust auditing and monitoring systems to timeously detect and prevent any potential breaches of privacy.
5. Develop an uncompromising disciplinary regime for violations of privacy policies.
6. Work closely with stakeholders and the general public towards factual CBDC education to quell myths related to CBDC privacy.

References

Bank of Canada (2020). Contingency Planning for a Central Bank Digital Currency, *Bank of Canada, https://www.bankofcanada.ca/2020/02/contingency-planning-central-bank-digital-currency/, (site accessed on 11.15.2022).*

Bertaccini, M. (2022). *Cryptography Algorithms: A Guide to Algorithms in Blockchain, Quantum Cryptography, Zero-knowledge Protocols, and Homomorphic Encryption*. Packt Publishing.

Chaum, D., Grothoff, C., and Moser, T. (2021). How to Issue a Central Bank Digital Currency, *SNB Working Papers* (3).

Chaum, D., and Moser, T. (2022). eCash 2.0. Inalienably private and quantum-resistant to counterfeiting, *https://chaum.com/wp-content/uploads/2022/11/eCash_2.0_9-7-22-.pdf* (site accessed on 12.20.2022)

Cummings, R., Ligett, K., Pai, M. M., and Roth, A. (2016). The Strange Case of Privacy in Equilibrium Models. *Proceedings of the 2016 ACM Conference on Economics and Computation. Association for Computer Machinery.*

EAC (2022). Central Bank Digital Currencies: A Solution in Search of a Problem? UK House of Lords, Economics Affairs Committee, *https://publications.parliament.uk/pa/ld5802/ldselect/ldeconaf/131/131.pdf,* (site accessed on 11.23.2022).

ECB. (2019). Exploring Anonymity in Central Bank Digital Currencies, In Focus, (4), 1-10. ECB (2021). Eurosystem Report on the Public Consultation on a Digital Euro. *European Central Bank*, *https://www.ecb.europa.eu/pub/pdf/other/Eurosystem_report_on_the_public_consultation_on_a_digital_euro~539fa8cd8d.en.pdf,* (site accessed on 11.04.2022).

ECB. (2022). Progress on the Investigation Phase of a Digital Euro. *European Central Bank*. *https://www.ecb.europa.eu/paym/digital_euro/investigation/governance/shared/files/ecb.degov220929.en.pdf,* (site accessed on 11.04.2022).

EDBP (2022). Statement 04/2022 on the Design Choices for a Digital Euro From the Privacy and Data Protection Perspective. European Data Protection Board, *https://edpb.europa.eu/system/files/2022-10/edpb_statement_20221010_digital_euro_en.pdf*, (site accessed on 11.07.2022).

Gross, J., Sedlmeir, J., Babel, M., Bechtel, A., Schellinger, B. (2021). Designing a Central Bank Digital Currency with Support for Cash-Like Privacy. Available at SSRN: https://ssrn.com/abstract=3891121

Lee, Y., Son, B., Park, S., Lee, J., and Jang, H. (2021). A Survey on Security and Privacy in Blockchain- Based Central Bank Digital Currencies, *Journal of Internet Services and Information Security*, 11(3), pp. 16–29.

Nissenbaum, H. (2012). *Privacy in Context - Technology, Policy, and the Integrity of Social Life.* Stanford University Press.

Preukschat, A., and Reed, D. (2021). *Self-Sovereign Identity: Decentralized Digital Identity and Verifiable Credentials*, Manning Publications.

Privacy International (2017). What is Privacy? *Privacy International*, https://privacyinternational.org/explainer/56/what-privacy, (site accessed on 11.15..2022).

SerHack (2018). *Mastering Monero: The future of private transactions*, LernoLibro LLC.

Tronnier, F. and Biker, P. (2022). A Framework and Qualitative Evaluation of Privacy Concerns in the Digital Euro. *PACIS 2022 Proceedings*, 63.

Turrin, R. (2021). *Cashless: China's Digital Currency Revolution.* Authority Publishing.

United Nations (1948). The Universal Declaration of Human Rights, *https://www.un.org/en/about-us/universal-declaration-of-human-rights,* (site accessed on 11.14.2022).

United Nations High Commissioner (2021). A/HRC/48/31: The Right to Privacy in the Digital Age. *United Nations High Commissioner for Human Rights Report, https://www.ohchr.org/en/documents/thematic-reports/ahrc4831-right-privacy-digital-age-report-united-nations-high, (site accessed on 11.14.2022).*

Warren, S. D., & Brandeis, L. D. (1890). The Right to Privacy. *Harvard Law Review*, 4(5), 193-220.

WEF. (2021). Privacy and Confidentiality Options for Central Bank Digital Currency, World Economic Forum, White Paper, Digital Currency Governance Consortium White Paper Series.

DIGITAL EURO ASSOCIATION

Digital Euro Association e.V.
Thurn-und-Taxis-Platz 6
60313 Frankfurt am Main

https://www.digital-euro-association.de/

florian.schreiber@digital-euro-association.de

@DigiEuro

Digital Euro Association