BANCA D'ITALIA
EUROSISTEMA

Mercati, infrastrutture, sistemi di pagamento

(Markets, Infrastructures, Payment Systems)

Privacy-Enhancing Technologies and Auditability in Digital Payment Systems

by Matteo Nardelli, Francesco De Sclavis and Michela Iezzi

September 2026

Number 93

BANCA D'ITALIA
EUROSISTEMA

Mercati, infrastrutture, sistemi di pagamento

(Markets, Infrastructures, Payment Systems)

Privacy-Enhancing Technologies and Auditability in Digital Payment Systems

by Matteo Nardelli, Francesco De Sclavis and Michela Iezzi

Number 93 – September 2026

The papers published in the 'Markets, Infrastructures, Payment Systems' series provide information and analysis on aspects regarding the institutional duties of Banca d'Italia in relation to the monitoring of financial markets and payment systems and the development and management of the corresponding infrastructures in order to foster a better understanding of these issues and stimulate discussion among institutions, economic actors and citizens.

The views expressed in the papers are those of the authors and do not necessarily reflect those of Banca d'Italia.

The series is available online at www.bancaditalia.it.

Printed copies can be requested from the Paolo Baffi Library: richieste.pubblicazioni@bancaditalia.it.

ISSN 2724-6418 (online)
ISSN 2724-640X (print)

Banca d'Italia
Via Nazionale, 91 - 00184 Rome - Italy
+39 06 47921

Designed and printing by the Printing and Publishing Division of Banca d'Italia

PRIVACY-ENHANCING TECHNOLOGIES AND AUDITABILITY IN DIGITAL PAYMENT SYSTEMS

by Matteo Nardelli*, Francesco De Sclavis* and Michela Iezzi*

Abstract

As digital payment systems evolve, protecting privacy has become one of the main design challenges. On the one hand, digital transactions should protect users from unwarranted monitoring and data misuse. On the other, regulatory compliance requires mechanisms for oversight, traceability, and accountability. Balancing these objectives is particularly complex in institutional payment infrastructures, where public trust and regulatory responsibilities must coexist. This paper provides an overview of privacy-enhancing technologies (PETs) for digital payment systems, with particular attention to both decentralized architectures and centrally managed infrastructures. The paper also presents the main privacy goals – such as anonymity, confidentiality, and unlinkability – and the cryptographic tools used to achieve them, including blind signatures, commitments, and zero-knowledge proofs. Finally, the paper examines the auditability mechanisms that enable selective oversight without fully compromising user privacy, and highlights the main design trade-offs and architectural choices.

Keywords: Digital payment systems; privacy-enhancing technologies; auditability; selective disclosure.

Sintesi

Con l'evoluzione dei sistemi di pagamento digitali, la tutela della privacy è diventata una delle principali sfide progettuali. Da un lato, le transazioni digitali dovrebbero proteggere gli utenti da forme di monitoraggio ingiustificato e dall'uso improprio dei dati; dall'altro, il rispetto delle regole richiede meccanismi di controllo, tracciabilità e attribuzione delle responsabilità. Bilanciare questi obiettivi è particolarmente complesso nel caso delle infrastrutture di pagamento istituzionali, nelle quali devono coesistere fiducia del pubblico e responsabilità regolamentari. Il lavoro offre una panoramica delle tecnologie per la tutela della privacy nei sistemi di pagamento digitali, con particolare attenzione sia alle architetture decentralizzate sia alle infrastrutture gestite centralmente. Presenta inoltre i principali obiettivi di privacy, tra cui anonimato, riservatezza e non collegabilità, e gli strumenti crittografici impiegati per conseguirli, incluse firme cieche, commitment e prove a conoscenza zero. Esamina infine i meccanismi di verificabilità che consentono controlli selettivi senza compromettere del tutto la privacy degli utenti, evidenziando i principali compromessi progettuali e le scelte architetturali.

* Directorate General for Information Technology, Banca d'Italia.

CONTENTS

1 Introduction[1]

The rapid growth of digital payment systems—from decentralized crypto-assets to centrally managed digital payment infrastructures—has renewed interest in how to balance privacy with accountability. In this work, the term *digital payment systems* is used in a broad sense to refer to infrastructures for digital value transfer, including decentralized crypto-asset networks, centrally managed systems operated by public or regulated institutions, and hybrid architectures combining institutional oversight with cryptographic privacy mechanisms. These systems rely on cryptographic techniques and, in many designs, distributed consensus to provide secure and programmable value transfer. Crypto-asset systems, like Bitcoin (Nakamoto, 2008) and Ethereum (Buterin *et al.*, 2013), have shown that it is technically possible to transfer value without relying on traditional intermediaries. In parallel, public institutions are exploring new forms of digital payment infrastructures to modernize payment systems, increase financial inclusion, and ensure monetary and financial stability in a digital age (e.g., BIS Innovation Hub, 2023; BIS Innovation Hub and Bank of England, 2023; Lovejoy *et al.*, 2023; Torres Vives *et al.*, 2024). These developments raise critical questions about user privacy, institutional control, and legal compliance (e.g., Auer *et al.*, 2025; Herskind *et al.*, 2020). The challenge is not just technical: public trust in digital payment systems depends on balancing privacy expectations with fraud prevention, governance constraints, and regulatory accountability. Privacy in digital payment systems should not be viewed as an absolute or binary property, but as a *design requirement* shaped by architectural and cryptographic choices. In the European legal framework, this perspective is also connected to the principle of data protection by design and by default set out in Article 25 of the General Data Protection Regulation (GDPR) (European Parliament, 2016), which requires appropriate technical and organizational measures to implement data-protection principles, such as data minimization, into the design and operation of processing systems. In this sense, *privacy-by-design* should be understood as both an architectural principle and a way to align technical design with broader data-protection expectations: privacy guarantees should be considered from the earliest stages of system design, rather than added afterwards. Different system designs embed different assumptions about who can

[1]The authors would like to thank Marco Benedetti, Romina Gabbiadini, Giuseppe Galano, Sara Giammusso, Lorenzo Gobbi, Antonio Muci, Fabiana Rossi, and Eugenio Rubera for their insightful discussions and for their valuable feedback throughout the development of this work.

access transaction data, under which conditions, and with what degree of granularity. As a result, technical design decisions directly shape the balance between user privacy, regulatory oversight, and institutional trust.

In response, a new field of privacy-preserving digital payments has emerged, leveraging Privacy-Enhancing Technologies (PETs)—tools that allow transaction details to be hidden or selectively revealed. The literature has proposed several approaches, including mixing protocols (e.g., Maxwell, 2013; Ruffing and Moreno-Sanchez, 2017; Ziegeldorf *et al.*, 2018), confidential transactions (e.g., Baudet *et al.*, 2023; Bünz *et al.*, 2020; Guan *et al.*, 2022), and privacy-native digital payment solutions (e.g., Kiayias *et al.*, 2022; Noether *et al.*, 2016; Tomescu *et al.*, 2022; Wüst *et al.*, 2022). They implement various properties of privacy, including anonymity, confidentiality, and unlinkability. At the same time, compliance with Anti-Money Laundering (AML) and Combating the Financing of Terrorism (CFT) regulations requires mechanisms for auditability and selective disclosure. Such rules require financial systems to support the prevention, detection, and investigation of illicit activity; recent frameworks on crypto-assets and digital operational resilience further stress the importance of governance, risk management, and operational robustness in digital financial infrastructures. This paper does not provide a legal analysis of these frameworks. Rather, it uses them as background constraints that help explain why privacy-preserving payment systems cannot be evaluated only in terms of cryptographic privacy, but must also be considered in relation to auditability, accountability, and operational feasibility. To reconcile these goals, recent work has explored cryptographic tools such as Zero-Knowledge Proofs (ZKPs), threshold encryption, and homomorphic commitments.

For public institutions and system designers, these technological developments are becoming increasingly relevant. The design of modern digital payment systems requires not only policy and economic choices, but also an understanding of the technical mechanisms that make privacy and oversight possible. Several PETs have been studied and stress-tested in decentralized crypto-asset systems from a technical perspective; however, the policy and governance constraints of institutional payment systems introduce different requirements and trade-offs. In this context, a clear understanding of the underlying *technological trade-offs* is essential to avoid conflating policy objectives with specific implementation choices. Seemingly abstract design decisions—such as the choice between account-based and token-based models, or between encrypted and commitment-based representations—can have concrete implications for

compliance, supervision, and user trust. This paper does not aim to prescribe specific system architectures or regulatory choices. Rather, it offers a high-level map of the technological options and trade-offs that shape privacy-preserving digital payment systems.[2] In particular, the paper reviews the main privacy goals relevant to digital payment system design, including sender and receiver anonymity, transaction confidentiality, and unlinkability, and discusses the technical tools used to achieve them. Then, it examines how auditability mechanisms can enable authorized entities to verify compliance with rules without necessarily undermining privacy guarantees. By doing so, it seeks to offer central banking experts, policymakers, operators, technologists, and interested readers a clearer picture of the available options and their limitations, which may be useful when reasoning about existing systems, their constraints, and possible future digital payment infrastructures.

The paper is organized as follows. Section 2 introduces the concept of privacy in digital payment systems and presents the main PETs used to implement privacy-preserving solutions. Section 3 traces the evolution of such systems across three generations, from early ecash to modern designs that integrate privacy with auditability requirements. Section 4 examines how value can be represented in account-based and token-based models. Section 5 analyzes the key privacy properties, including anonymity, confidentiality, and unlinkability, together with their trade-offs. Section 6 focuses on auditability and accountability mechanisms, which are critical for regulatory compliance. Section 7 summarizes the main findings and design trade-offs. Section 8 reviews related surveys to position this work within the broader literature. Finally, Section 9 concludes by reflecting on the main challenges and policy-relevant considerations.

2 Background

2.1 Primer on Privacy

In the context of digital payment systems, the term *privacy* refers to the ability of individuals and organizations to control what others know about their financial activity. This includes

[2]This paper builds upon the broader technical survey by the authors Nardelli *et al.* (2026). The two contributions differ in scope, audience, and purpose. The technical survey provides a detailed technical systematization of privacy-preserving digital payment systems, covering cryptographic primitives, protocol architectures, value representation models, and system-level design choices. The present article adopts a higher-level and policy-oriented perspective, aimed at making the main technological options and trade-offs accessible to a broader readership and at translating the technical design space into a conceptual map for institutional and policy-oriented discussions.

who they are, who they transact with, how much they send or receive, and when or how often they do so. Privacy is a broad and multi-layered concept that can be understood differently depending on the analytical perspective adopted, whether institutional or technical.

From a business or institutional standpoint, privacy in digital payments is about protecting sensitive financial data while maintaining compliance, trust, and operational integrity. User trust is crucial. People are more likely to use digital money if they feel confident that their data will not be misused, sold, or exposed to unauthorized parties. Privacy helps maintain that trust. Businesses rely on privacy to keep their financial strategies confidential—such as vendor relationships, supply chain payments, or mergers and acquisitions activities. Leaking such data can harm competitiveness. Nonetheless, privacy must coexist with legal and regulatory responsibilities, including AML and CFT obligations, tax enforcement, consumer protection, and broader requirements related to governance and operational resilience. Systems need to be *private but not opaque* to authorized entities. One of the frequently discussed objectives of digital currencies is to approximate some privacy characteristics traditionally associated with cash. This is especially important for small everyday payments and financial inclusion. Auer *et al.* (2025) frame this balance through the lens of soft and hard privacy. *Soft privacy* relies on institutional rules, contracts, or legal frameworks. For instance, a bank may pledge not to share transaction records unless required by law. The guarantee comes from trust in institutions and governance, but it can be fragile if institutions fail or misuse their power. *Hard privacy* embeds protections directly into the technology. For example, a digital payment system could use cryptography to hide transaction amounts, ensuring that even intermediaries cannot access sensitive data. Here, privacy comes from mathematical guarantees, not trust in human behavior. Auer *et al.* (2025) introduce a similar distinction also for auditability. *Soft auditability* relies on discretionary oversight, such as regulators requesting records during an audit. Conversely, *hard auditability* is automatically enforced by the system. For example, a digital currency could automatically enforce and attest (via cryptographic proofs) compliance predicates (e.g., limits, eligibility), revealing only the minimum information required by the rules. A promising privacy-preserving digital payment system should combine soft and hard approaches: cryptographic protections establish baseline guarantees, while institutional governance defines lawful and accountable exceptions, an equilibrium further discussed in Section 6 through the lens of auditability and selective disclosure.

From a technical point of view, privacy is not a single feature, but a collection of composable design goals and protective mechanisms that can be embedded into the architecture of a digital payment system. These are not visible to the user, but they define how the system handles data under the hood. In the following, the most important technical facets implementing the notion of privacy are introduced. They capture complementary dimensions of privacy in digital payment systems.

Anonymity Anonymity refers to the ability to perform a transaction (e.g., a payment) without revealing the identity of the parties involved. Sender anonymity protects the payer's identity.[3] Receiver anonymity protects the recipient's identity. For example, a user can make a payment that cannot be traced back to him personally.

Confidentiality Confidentiality ensures that the details of a transaction, e.g., the amount transferred or the parties involved, are hidden from third parties, even if the transaction is recorded on a public ledger. For example, this ensures that the amount of money transferred is known only to the sender and receiver, not to the public or intermediaries.

Unlinkability Unlinkability means that different payments cannot be connected to the same user. Even if transactions are publicly visible, an observer cannot tell whether two payments were made by the same person.

Auditability Auditability is the ability of authorized entities to verify that transactions comply with rules, either in real-time or retroactively, without necessarily revealing all user or transaction details. For example, a regulator can confirm that a transaction stayed within legal limits, even if he cannot see the exact amount or the parties unless specific conditions are met. Auditability can be supported by mechanisms such as revocable anonymity, which allow transactions to be traced only under well-defined legal conditions without making tracing the default system behavior.

Accountability Closely related to auditability, accountability refers instead to the system's ability to link actions to real-world identities when necessary, such as in the case of fraud, legal investigations, or AML/CFT enforcement. It typically requires registration or identity-binding mechanisms. Ultimately, it ensures that users can be held responsible for their actions, especially in the case of fraud or abuse.

[3] A closely related notion is *untraceability*, which emphasizes that a specific transaction cannot be attributed to a unique sender with certainty. While anonymity hides identities, untraceability focuses on attribution.

In designing digital payment systems, central banks and policymakers face a key challenge: *How much privacy is enough, and for whom?* A fully private system may protect individuals' freedom but hinder enforcement of financial laws. A fully transparent one may support oversight but compromise civil liberties and user trust. The goal is to build a system that is *private by default*, but auditable when necessary—with clear rules, strong protections, and trustworthy institutions (e.g., Auer *et al.*, 2025). This is where PETs come into play: a collection of cryptographic tools and methods that help achieve this balance. In practice, these tools operate at different layers of a payment system, from value representation to compliance verification. The next section introduces these technologies and explains how they are used in practice. Throughout the paper, privacy properties are discussed across two complementary levels. At the *cryptographic level*, properties such as anonymity, confidentiality, or unlinkability describe what can be inferred from the cryptographic protocol itself. At the *system level*, the same properties also depend on architectural choices, operational metadata (e.g., timing, address reuse, denominations), and governance mechanisms. Unless explicitly stated otherwise, references to privacy goals should be understood as emerging from the combined design of cryptographic techniques and system architecture.

2.2 Privacy-Enhancing Technologies

PETs are a set of tools from cryptography and computer science that can *(i)* protect transaction data (e.g., amounts), *(ii)* reduce linkability between identifiers and real users, and *(iii)* enable selective disclosure and compliance verification.[4] This section introduces a selection of commonly referenced PETs that are used in privacy-preserving digital payment systems. For a policy-oriented reader, the key point is not only how these mechanisms work at the cryptographic level, but which institutional functions they may support. Some PETs hide transaction data from unauthorized parties, others reduce the possibility of linking transactions to the same user, while others enable selective disclosure or compliance verification under predefined conditions. For formal definitions of the underlying cryptographic primitives used in PETs, the reader can refer to standard textbooks (e.g., Boneh and Shoup, 2020; Katz and Lindell, 2007; Paar and Pelzl, 2009). Table 1 summarizes the key properties of the PETs presented in

[4]In this work, the term PETs refers specifically to cryptographic techniques and protocols used to protect transaction privacy in digital payment systems. The paper does not consider PETs designed for privacy-preserving data analytics, such as differential privacy, federated learning, or related approaches.

this section. The table should be read as a qualitative guide rather than as a benchmark. Its purpose is to help identify which privacy goals different PETs may support (e.g., confidentiality, unlinkability, selective disclosure, or compliance verification) and which trust assumptions and operational costs they typically introduce.[5]

2.2.1 Encryption. Encryption schemes are often the first layer of privacy protection in digital payment systems, allowing transaction data (or identities) to remain confidential even when stored or transmitted.

Identity-based Encryption. Identity-based Encryption (IBE) schemes (Shamir, 1985) are public-key encryption schemes in which the public key is a string that uniquely identifies a user (e.g., an email). The corresponding private keys for decryption are derived from a master secret by a dedicated key-generation authority (often called a Private Key Generator), which introduces a trust assumption at the cryptographic level. If this role is assigned to a single entity, the system concentrates significant power in that authority, since compromise or misuse of the master secret may affect the confidentiality of users' keys. Distributed protocols can mitigate this concentration by requiring multiple parties to cooperate, but the key-escrow property remains an inherent trade-off in IBE. IBE can be used to simplify key management, recovery, and access control within an organization.

Threshold Encryption. Threshold encryption allows data to be encrypted in such a way that it can only be decrypted when a predefined quorum of participants agrees to reveal it. Threshold encryption can help maintain privacy while removing single points of failure.

Homomorphic Encryption. Homomorphic encryption schemes (Rivest *et al.*, 1978) allow computing additions, multiplications, or both, without revealing the plaintext. Operations can be performed directly on ciphertexts such that the result corresponds to the encryption of the

[5]The listed PETs span different abstraction layers, ranging from cryptographic primitives and encryption schemes to signature families and full protocol constructions. Therefore, the comparison is indicative rather than exhaustive. The computational-cost categories are qualitative and should not be interpreted as benchmark results. *Low* refers to mechanisms whose core operations are typically lightweight in payment-system workflows. *Medium* refers to mechanisms that introduce additional cryptographic operations, interaction, or quorum-related overhead. *High* refers to mechanisms whose cost may become operationally significant because of proof generation, ciphertext computation, large proofs, or complex setup and verification procedures. Actual costs depend on parameters, implementation, hardware, batching, and the surrounding system architecture.

Table 1. Qualitative comparison of main PETs for privacy-preserving payments. Costs indicate typical operational overhead; figures are from different evaluation settings and not directly comparable.

PET	Main Privacy Goal	Main Trust Dependency	Computational Cost
Identity-Based Encryption	Confidential communication using identity strings as public keys	Trusted private key generator	Medium[α]
Threshold Encryption	Confidentiality with decryption requiring cooperation of a quorum	Quorum of decryption authorities	Medium–High[β]
Homomorphic Encryption	Computation over encrypted data without revealing plaintexts	Holders of the decryption key	High[γ]
Commitments	Hide a value while binding the committer to it	No trusted party	Very low
Homomorphic Commitments	Verifiable aggregation of hidden values	Public parameters without a known trapdoor	Low–Medium[δ]
Blind Signatures	Unlink signature issuance from later spending	Issuing authority or signer quorum	Low
Randomizable Signatures	Unlink different presentations of the same signed information	Original issuer or signer quorum	Low–Medium
Ring and Group Signatures	Signer anonymity within an anonymity set	None (ring); designated opener (group)	Medium[ϵ]
Threshold Signatures	Distribute authorization among multiple parties	Quorum of signers	Medium[ζ]
ZKPs	Prove properties of hidden data without revealing the witness	Scheme-dependent setup; transparent alternatives exist	Medium–High[η,θ,ι]
One-time Addresses	Receiver unlinkability through fresh destination keys	No additional trusted party	Low[κ]

[α] *Identity-based encryption:* Pairing-based IBE relies on relatively costly cryptographic operations. In Cheng *et al.* (2025), one pairing took ≈ 1 ms; complete encryption require additional operations.

[β] *Threshold encryption:* Decryption requires combining a quorum of partial decryptions and Lagrange interpolation (e.g., Kiayias *et al.* (2022)).

[γ] *Homomorphic encryption:* Costs depend strongly on the scheme, multiplicative depth, and batching; bootstrapping, when required, is typically a dominant operation (Cheon *et al.*, 2024; Gentry, 2009).

[δ] *Homomorphic commitments:* Pedersen commitments are lightweight: creation uses two scalar multiplications and one group addition; aggregation uses only group additions (Bünz *et al.*, 2018; Pedersen, 1992).

[ϵ] *Ring signatures:* MLSAG has linear signature size and verification cost; Triptych reduces signature size to logarithmic in the anonymity set (Noether and Goodell, 2020; Noether *et al.*, 2016).

[ζ] *Threshold signatures:* FROST produces a signature in two signing rounds by aggregating shares from a threshold of participants (Connolly *et al.*, 2024).

[η] *zk-SNARKs:* Groth (2016) proofs contain three group elements and verification uses three pairings. In the evaluation by Ernstberger *et al.* (2024), verification remained within 5 ms, while proving depended strongly on the circuit and implementation.

[θ] *STARKs:* Winterfell reports 110–152 KB proofs, 1.2–20.5 s proving, and 4.4–5.9 ms verification on an 8-core 2.4 GHz Intel i9 (Meta Platforms, Inc., 2025).

[ι] *Bulletproofs:* For a hidden value represented with 64 bits, Bulletproofs+ produces a 576 B proof that the value lies within a valid range, compared with 688 B for the original Bulletproofs. Multiple range checks can be combined without the proof size increasing proportionally (Bünz *et al.*, 2018; Chung *et al.*, 2022).

[κ] *One-time addresses:* Generating a fresh destination key is lightweight, but recipient discovery may require scanning candidate outputs (e.g., Noether *et al.* (2016)).

operation applied to the plaintexts. This allows computation to be delegated to a third party while maintaining confidentiality.

2.2.2 Commitments. While encryption protects the content of data, commitments provide a complementary approach by allowing values to remain hidden while still supporting verifiable operations. Commitments are among the simplest building blocks for protecting data in payment systems, allowing values to remain hidden while still enabling verification and controlled disclosure.

Commitments. Formally, a commitment scheme is a cryptographic primitive that lets someone commit to a value in a way that he cannot change it later. The scheme consists of two phases: (i) *commit phase*, where a commitment is made to a value v, but the value is kept secret from third parties; (ii) *opening phase*, where the committed value v is revealed. Intuitively, commitments can be compared to placing a value in a sealed envelope: a simple example is a hash-based commitment, where a hash of the value (usually combined with randomness) acts as a binding reference without revealing the underlying data. A commitment is *hiding* if an adversary cannot distinguish which of two values corresponds to the commit; it is *binding* if the committer cannot generate the same commit from two different values. In payment systems, commitments are relevant because they allow values to be represented without exposing them in clear. For example, a system may commit to a transaction amount and later prove that the amount is positive, within an allowed range, or consistent with the sender's balance, without disclosing the exact value. This makes commitments a basic building block for confidentiality and data minimization in digital payment infrastructures.

Homomorphic commitments. Homomorphic commitments, such as Pedersen (Pedersen, 1992) or ElGamal-style constructions (Elgamal, 1985), allow operations (e.g., addition, multiplication) to be performed directly on committed values without revealing them. For instance, Pedersen commitments make it possible to check simple arithmetic relations over hidden amounts. In simplified terms, combining two commitments can correspond to committing to the sum of the two underlying values, without revealing those values. This property illustrates how computations can be carried out on hidden data. From a policy perspective, this is relevant

because some rules can be verified on concealed transaction amounts, reducing the need to expose raw payment data to all system participants.

2.2.3 Anonymity-enhanced Signatures. Beyond hiding transaction data, some PETs focus on protecting user identities during authorization and spending, often by extending traditional digital signatures with anonymity properties.

Blind Signatures. Blind signatures (Chaum, 1983) are a form of digital signature in which the signer produces a valid signature on a message without learning its content: before signing, the message is *blinded*, i.e., transformed through a random element that makes it unrecognizable. Once the contents of the signed message are unblinded, they can be publicly verified as usual.

Randomizable Signatures. Randomizable signatures allow a previously generated signature to be transformed into a fresh valid signature. Under the security assumptions of the scheme, this can prevent different presentations of the same signed credential from being linked through the signature alone.

Group Signatures. Group signature schemes (Chaum and van Heyst, 1991) enable any member of a designated group to generate a valid signature without revealing who signed (ensuring anonymity). A verifier uses a group public key to confirm that a valid signature was produced by some group member. Many group signature constructions also aim to provide *unlinkability*, meaning that it is difficult to determine whether two different signatures were produced by the same user, although the exact guarantees depend on the specific scheme and anonymity definition (Perera *et al.*, 2022). Some group signature constructions also include a designated opening authority (often called a group manager) that can reveal the signer's identity under predefined conditions, making anonymity revocable rather than permanent. This introduces a trust assumption at the system level.

Ring Signatures. Ring signatures (Rivest *et al.*, 2001) are similar to group signatures, as they hide the signer's identity behind a group. Unlike many group-signature schemes, standard ring signatures have no designated opening authority. A valid signature shows that one member of the ring signed, without identifying which one. A verifier needs the whole list of public

keys to verify the validity of the signature. Effective anonymity nevertheless depends on the construction, decoy selection, and available metadata.

Threshold Signatures. Threshold signatures are a type of signature that can be jointly produced by a committee of signers. A t-of-n signature scheme requires at least t signers out of a total of n participants to produce a valid signature.

2.2.4 Key Protocols. Finally, some PETs operate at the protocol level, enabling advanced privacy properties such as verifiable correctness, selective disclosure, or unlinkable address generation without revealing sensitive information.

Zero-knowledge Proofs. A ZKP is a protocol enabling one party (the prover) to demonstrate to another party (the verifier) that a statement is true, without disclosing any information beyond the validity of the statement itself. A dishonest prover can convince the verifier of a false statement only with negligible probability (*soundness*). Importantly, the proof guarantees that the statement is correctly verified with respect to predefined rules, not that external claims made by the prover are inherently true. In a payment context, this can be used to prove that a transaction satisfies a rule without revealing the underlying private data. For example, suppose that a system must check that a payment amount v is below a predefined threshold L, without revealing the exact amount to all system participants. The payer can hide v inside a cryptographic commitment $C = \mathrm{Com}(v; r)$, where r is fresh randomness, and provide a ZKP showing that the committed value satisfies $0 \leq v \leq L$. The verifier learns that the threshold rule is respected, but does not learn v. More generally, similar techniques can be used to prove sufficient funds, token validity, or other policy conditions without disclosing the account balance, token identity, or identifying information. Conversely, an honest prover can always convince the verifier when the statement is true (*completeness*). ZKPs can be either *interactive*, requiring the parties to exchange messages, or Non-Interactive Zero-Knowledge (NIZK), when the verifier is convinced through a single message. Non-interactive proofs are especially relevant for payment systems because they can be attached directly to a transaction and verified without requiring an additional back-and-forth interaction between payer, payee, and verifier. Various NIZK protocols have been designed, including Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge (zk-SNARKs) (Bitansky *et al.*, 2012), Bulletproofs (Bünz *et al.*, 2018),

and Zero-Knowledge Scalable Transparent Arguments of Knowledge (zk-STARKs) (Ben-Sasson *et al.*, 2019). Some NIZK proof systems, notably preprocessing zk-SNARKs such as Groth (2016), require an initial setup ceremony to generate and distribute common parameters, whereas *transparent* systems avoid this requirement. For payment-system design, the main differences among these proof systems concern operational trade-offs such as proof size, verification time, proving cost, setup assumptions, and transparency. These aspects affect scalability, implementation complexity, and the degree of trust required in the system setup. The popular Groth16 construction for zk-SNARKs (Groth, 2016) is optimized for performance but requires a trusted setup.[6] Bulletproofs are optimized for range proofs, namely proofs that a hidden value lies within an allowed interval, and do not require trusted setup. In payment systems, this is relevant when a system must verify that a committed amount is non-negative or below a predefined threshold without revealing the amount itself. Zk-STARKs are transparent proof systems, meaning that they do not require a trusted setup. Compared with succinct zk-SNARKs, they typically produce larger proofs but rely on weaker setup assumptions. Recent surveys on ZKPs can be found, e.g., in Christ *et al.* (2024); El-Hajj and Oude Roelink (2024).

One-time Addresses. At the protocol level, stealth addresses (or one-time addresses) improve receiver privacy by deriving a fresh destination public key for each payment from the recipient's public information and sender-chosen randomness. Fresh destination keys make it more difficult for observers to link two payments to the same recipient, while the recipient can detect and spend outputs addressed to him.

3 Generations of Privacy-preserving Digital Payment Systems

Three generations of privacy-preserving digital payment systems can be identified, as summarized in Figure 1.[7] The first generation consists of solutions designed for centralized infrastructures, where the primary objective was to protect sender anonymity. The second generation arose with the advent of decentralized crypto-assets, which enabled peer-to-peer value transfer without intermediaries and shifted the focus toward unlinkability and stronger anonymity

[6] In practice, parameters are generated via publicly auditable multi-party computation ceremonies, and security holds as long as at least one participant is honest and destroys the corresponding secret randomness.

[7] These generations emerge from the classification proposed by Nardelli *et al.* (2026). They reflect research trends rather than a linear progression in real-world deployments; different systems may adopt features from more than one generation.

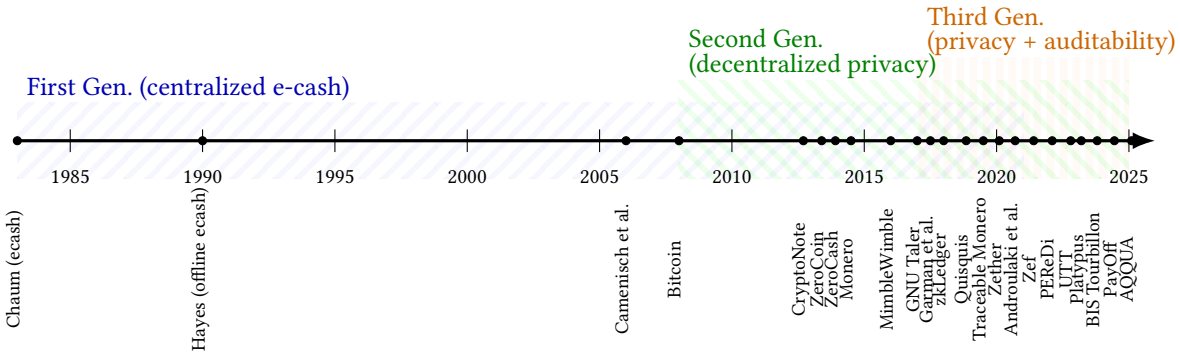

Fig. 1. Conceptual evolution of privacy-preserving digital payment systems across three generations. The figure shows selected representative systems and research lines, without aiming to provide an exhaustive classification of all proposals in the literature. The classification is conceptual rather than strictly chronological: individual systems may combine features from multiple generations, and the boundaries between categories should be read as indicative.

properties. The third generation builds on these advances by introducing mechanisms that reconcile strong privacy guarantees with auditability and regulatory compliance. This shift is particularly relevant for institutional and regulated digital payment systems, where privacy guarantees must coexist with compliance, governance, and oversight requirements.

First Generation. The *first generation* focuses on the design of digital payment systems leveraging digital signatures and a centralized authority (i.e., the issuing bank) (Chaum, 1983). The central problem is to guarantee sender anonymity even though the user must interact with a trusted issuer (e.g., a bank) to obtain valid tokens for subsequent payments. Chaum (1983) proposes one of the first attempts to construct a digital payment system, commonly referred to as *ecash*. Later, several works improved ecash with different features, including support for different coin denominations, partial spending, token transferability, offline spending, and auditability (e.g., Bauer *et al.*, 2021; Camenisch *et al.*, 2006; Dold, 2019; Hayes, 1990).

Second Generation. The *second generation* of works emerged with the introduction of Bitcoin (Nakamoto, 2008). Bitcoin and, later, Ethereum (Buterin *et al.*, 2013) propose public and permissionless blockchains, meaning that the ledger contains transactions visible to everyone and anyone can participate in the process of updating the public ledger by following a specific (validation and consensus) protocol. Being public, these blockchains use addresses (acting

as pseudonyms) to exchange money in a pseudo-anonymous manner, as addresses are not directly tied to user identities. The second generation of solutions mainly focuses on improving unlinkability, anonymity, and confidentiality (e.g., Androulaki *et al.*, 2013; Baudet *et al.*, 2023; Fauzi *et al.*, 2019; Friolo *et al.*, 2024; Herrera-Joancomartí, 2015; Meiklejohn *et al.*, 2013; Miers *et al.*, 2013; Van Saberhagen, 2013). Overall, this second generation of approaches can be classified into three main categories: privacy-native protocols, mixing protocols, and off-ledger solutions.

- Changing the protocol of existing blockchains is hard, as it involves forks. Therefore, *privacy-native protocols* define (mostly) alternative payment systems with improved confidentiality, anonymity, and unlinkability features (e.g., Ben Sasson *et al.*, 2014; Noether *et al.*, 2016; Van Saberhagen, 2013).
- Mixing protocols propose supplementary services for permissionless blockchains aimed at coordinating sets of users to create transactions (or transaction sequences) that obscure input-output relationships (e.g., Bissias *et al.*, 2014; Bonneau *et al.*, 2014; Maxwell, 2013; Qin *et al.*, 2023; Ruffing and Moreno-Sanchez, 2017; Seres *et al.*, 2019; Valenta and Rowan, 2015; Wang *et al.*, 2023; Ziegeldorf *et al.*, 2018). Mixing protocols aim to break the link between sender and receiver, thus reducing the possibility of linking blockchain addresses together (i.e., they enhance transaction unlinkability).
- Off-ledger solutions process part of the payment activity outside the base ledger and later settle or anchor the result on it, reducing the need to record every operation on the shared ledger (e.g., Baudet *et al.*, 2023; Qin *et al.*, 2023). This approach may reduce on-chain metadata, but does not automatically provide cryptographic privacy unless combined with additional techniques.

Third Generation. While protecting the privacy and anonymity of payers and payees remains essential, the *third generation* of privacy-preserving digital payment systems introduces mechanisms that balance these guarantees with auditability and regulatory compliance (e.g., Androulaki *et al.*, 2020; Garman *et al.*, 2017; Kiayias *et al.*, 2022; Li *et al.*, 2021; Papadoulis *et al.*, 2024; Sarencheh *et al.*, 2025; Tomescu *et al.*, 2022; Wüst *et al.*, 2019; Wüst *et al.*, 2022). These approaches are particularly motivated by regulatory and compliance requirements, including AML and CFT. Auditability refers to the system's ability to track, verify, or selectively disclose

information about transactions, without fully compromising user privacy. This capability enables the enforcement of specific policies that apply to users, coins, or transaction behaviors over time. To achieve this, modern privacy-preserving systems integrate mechanisms such as revocable anonymity, trapdoor-based decryption, and ZKPs for correctness and compliance.

4 Value Representation

Different approaches have been proposed to represent funds and value transfers in modern digital payment systems. This section classifies them into account-based and token-based, and presents how different approaches improve privacy-related features of the two types of ledgers.

4.1 Account-based

Account-based ledgers associate a balance with each account address, which is debited or credited by transactions. This approach simplifies state management and enables simple definitions of policies based on cumulative balances. Nonetheless, it requires safeguards against replay and double-spending attacks, often implemented by storing a sequence number (or *nonce*) in each account and updating it with every transaction. Since the balance of an account is explicitly represented, obtaining anonymity and unlinkability is challenging, especially in systems where users cannot freely generate multiple addresses (e.g., Guan *et al.*, 2022). Privacy-preserving account-based solutions replace plain-text balances with commitments, achieving *confidentiality* of balances and transactions (e.g., Baudet *et al.*, 2023; Fauzi *et al.*, 2019; Guan *et al.*, 2022). Liu *et al.* (2022) propose an account-based digital payment system with sender and receiver anonymity but with no unlinkability. The system follows a two-tier model where the central authority can identify users via encrypted identifiers, while intermediaries cannot. To guarantee anonymity while ensuring *unlinkability*, most of the approaches change users' account address at each transaction and use an authenticator to prove correctness. The authenticator can be, e.g., a digital signature (e.g., Kiayias *et al.*, 2022) or a ZKP (e.g., Fauzi *et al.*, 2019; Wüst *et al.*, 2022). For example, in PEReDi (Kiayias *et al.* (2022)), account states must be (blindly) signed by a quorum of maintainers, and since each transaction reveals prior account snapshots to construct new authenticators, randomized signatures are used to prevent linkability. Conversely, Platypus (Wüst *et al.* (2022)) relies on ZKPs. Quisquis (Fauzi *et al.*

(2019)) uses updatable public keys to update accounts (and their associated address) with each transaction. The account-based model lends itself well to *auditability*, as it allows simple definition of policies on holding limits (e.g., Gross *et al.*, 2021; Papadoulis *et al.*, 2024; Wüst *et al.*, 2022) or spending and receiving limits (e.g., Papadoulis *et al.*, 2024); these mechanisms are discussed more broadly in Section 6.

4.2 Token-based

Token-based ledgers do not maintain explicit balances per address, but instead track individual tokens. The user's balance can be derived from the sum of all owned tokens. This model can facilitate privacy because balances need not be explicitly materialized, although transaction-linkage analysis may still reconstruct them. It also introduces management complexity, particularly when users distribute their coins across multiple addresses. There are two main types of token structures: Chaumian tokens and unspent tokens. Although both represent digital value, they differ in structure, spending mechanisms, privacy guarantees, and centralization.

Chaumian tokens (Chaum, 1983) use blind signatures and were first deployed in centralized, bank-issued electronic cash schemes. When issuing a token, the bank blindly signs a random value provided by the payer, allowing the payer to later unblind it for spending. Blind signatures prevent the bank from linking withdrawals to subsequent transactions. These tokens rely on a trusted authority to issue and verify their validity. Some implementations introduce expiration to limit circulation (e.g., Dold, 2019; Lovejoy *et al.*, 2023). Research on electronic cash also influenced decentralized privacy-preserving systems such as Zerocoin (Miers *et al.*, 2013), Zerocash (Ben Sasson *et al.*, 2014), and Monero (Noether *et al.*, 2016). In permissionless settings, these systems replace a central issuer with publicly verifiable ledgers and combinations of cryptographic mechanisms, including ZKPs, commitments, ring signatures, and serial-number, nullifier, or key-image mechanisms.

Unspent tokens, introduced in Bitcoin (Nakamoto, 2008), represent transaction outputs that can be used as inputs for future transactions, which in turn create new unspent tokens. They are inherently traceable unless PETs are used. Unspent tokens are created as transaction outputs; only newly issued units arise through the protocol's issuance mechanism. Their core attributes include an identifier, value (or its commitment), and ownership information. Ledger validation

and consensus prevent double spending, while the public record can complicate privacy. Privacy-focused crypto-asset systems employ stealth addresses, ring signatures, confidential transactions, and ZKPs to *obscure* transaction details and *unlink* payments (e.g., Ben Sasson *et al.*, 2014; Noether *et al.*, 2016; Poelstra, 2016). Tokens can also include auxiliary data to support *policy* enforcement (e.g., Xue *et al.*, 2023). For example, Xue *et al.* (2023) include information to prove in Zero-Knowledge (ZK) that the total amount of the crypto-assets transferred and the transaction frequency in a time period are limited.

4.2.1 Preventing Double Spending. Two main approaches to double spending protection emerge: deposit-time checks and publicly verifiable ledgers. In centralized systems relying on Chaumian tokens, token validity is checked at deposit time, i.e., when the recipient interacts with the bank to deposit the token (e.g., Tomescu *et al.*, 2022). Conversely, public ledgers use validation rules and the recorded spent or unspent state to prevent reuse of an output (e.g., Nakamoto, 2008). Privacy-preserving systems may instead publish serial numbers, nullifiers, or key images to identify repeated spending without revealing the underlying token. ZKPs or signatures can additionally prove authorization and value conservation (e.g., Ben Sasson *et al.*, 2014; Noether *et al.*, 2016).

5 Privacy Features

This section presents the key technical solutions used to obtain the different privacy goals. Privacy in digital payments is often defined through different sub-properties focusing on anonymity of participants, value confidentiality, and unlinkability (e.g., Almashaqbeh and Solomon, 2022; Genkin *et al.*, 2018).

5.1 Sender Anonymity

Sender anonymity means protecting the identity of the person who initiates a digital payment, so that others (including intermediaries or observers) cannot trace who sent the money. Different systems protect the sender's identity in different ways. Some rely on cryptographic signature schemes that blind the sender's identity. Others use mathematical proofs to hide it while proving that the payment is valid. Others provide controlled transparency, where a trusted party can intervene for auditability purposes under predefined conditions.

Blind Signatures. This technique lets an issuing authority (e.g., a central authority in institutional payment settings) approve a digital token representing a unit of value without seeing its details. Specifically, the issuer cannot link that token back to the person who requested it. In a blind signature protocol, the user first hides (i.e., blinds) the content of a token before sending it to the issuer for approval. The issuer signs the blinded token without learning its details; later, the user removes the blinding factor and obtains a valid signature that cannot be linked to the original request. Chaum (1983) introduces *blind signatures* precisely to break the link between the signing request and the later spending of a token. To obtain revocable anonymity and reveal the sender on double spending, Hayes (1990) introduces a *one-time blind signature* scheme. UnTraceable Transactions (UTT) (Tomescu *et al.*, 2022) realizes blind signatures using *randomizable signatures*, which allow signatures to be altered using fresh randomness without compromising their validity. All these schemes rely on a central issuer, who can represent a single point of failure. This can be mitigated, e.g., by using *threshold blind signatures*, where a quorum of authorities must cooperate to create a valid blind signature (e.g., Androulaki *et al.*, 2020; Kiayias *et al.*, 2022).

Group Signatures. Group signatures allow anyone in a predefined group to sign a transaction anonymously. With this technique, a designated opening authority (sometimes called a group manager) sets up the anonymity set and can, optionally, uncover the sender's identity under predefined conditions. This introduces an additional accountability mechanism. For example, in Zhang *et al.* (2019), a trusted centralized entity sets up the anonymity set and can, optionally, uncover the sender's identity for inspection.

Ring Signatures. Ring signatures offer a similar form of anonymity, but without a trusted opening authority. With this technique, the signer forms a ring from his public key and a set of decoy public keys. The resulting signature proves that one corresponding secret key was used, without identifying which one. In systems such as Monero, ring signatures are applied to a set of possible inputs so that observers cannot readily determine which input belongs to the actual spender. This approach is used in privacy-focused crypto-asset systems like CryptoNote (Van Saberhagen, 2013) and Monero (Noether *et al.*, 2016). The privacy protection is limited by the number of decoys in the ring: larger groups provide better privacy, though they can increase the size of the transaction. Moreover, the effective anonymity set may be

smaller than the nominal ring size when decoy selection, timing patterns, or transaction history allow observers to distinguish likely real inputs from decoys. For instance, empirical analyses of Monero have shown that some earlier protocol choices and decoy-selection strategies were vulnerable to traceability heuristics (Möser *et al.*, 2018), illustrating that practical anonymity depends not only on the cryptographic primitive, but also on implementation choices and usage patterns.

ZKPs and Commitments. Spending an unspent token requires proving authorization without necessarily revealing which token is being spent. In Zerocash-style systems, a coin is represented by a commitment, and spending publishes a serial number or nullifier together with a ZKP that the coin is valid and unspent. In account-based systems, sender's anonymity is harder to maintain because account balances are usually visible. To solve this, some proposals hide the account balance inside a commitment and use ZKPs to verify that the transaction is correct. For example, Gross *et al.* (2021) build on Zerocash by committing to account states and invalidating the previous states when accounts are updated. The authors suggest using Merkle trees[8] to prove that a transaction proposal refers to an existing commitment in the ledger without pointing to (and thus revealing) it. Platypus (Wüst *et al.*, 2022) uses a model where payer and payee exchange with the central bank commitments to their updated accounts as well as the transaction amount, with two additional ZKPs proving the update's validity. Conversely, PEReDi (Kiayias *et al.*, 2022) achieves sender anonymity through anonymous channels, an encrypted ledger, and a threshold signature scheme. Solidus (Cecchetti *et al.*, 2017) uses banks as proxies; therefore, transactions are not explicitly exchanged between users but among their respective banks.

5.2 Receiver Anonymity

Receiver anonymity can be achieved through several PETs, including one-time destination keys (or stealth addresses), encrypted addresses, and commitment-based outputs. These mechanisms can be integrated into both decentralized crypto-asset systems and centrally managed digital payment infrastructures.

[8] A Merkle tree is a hash-based data structure that summarizes a set of elements through a single root value and supports short membership proofs. In privacy-preserving payment systems, it can be combined with ZKPs to show that a committed value belongs to the ledger without revealing which value is being used.

Obtaining receiver anonymity with Chaumian tokens is challenging, as the payee must interact with the bank to deposit the received tokens. One-time destination keys are a general cryptographic mechanism that can be adopted in different payment architectures; privacy-focused crypto-asset systems provide well-known implementations of this approach. In CryptoNote (Van Saberhagen, 2013), the sender generates a *one-time destination key* by combining a random number with the receiver's public key. As a drawback, the receiver has to scan incoming transactions using his private key, reconstruct the corresponding one-time destination public key from each transaction, and check whether the payment was intended for him. A similar approach is also used in Monero (Noether *et al.*, 2016) (and in derived systems such as Elfadul *et al.* (2024); Li *et al.* (2021)), where it is referred to as *stealth addresses*. Alternatively, UTT (Tomescu *et al.*, 2022) ensures receiver's anonymity using *homomorphic commitments*: a coin is a commitment to a tuple containing the owner's identifier, a serial number issued by the central bank, and its value. To make a payment, the sender creates a transaction including the receiver's identity commitment, which can later be aggregated by an issuing authority (e.g., a central authority in institutional payment systems) to issue new coins for the recipient without learning his identity.

In the unspent token-based ledger Zerocash (Ben Sasson *et al.*, 2014), the sender includes an *encrypted version of the recipient's address* in the transaction (using asymmetric encryption). Also in this case, each user has to scan the ledger, decrypt transactions, and identify those intended for him. Another approach, used in MimbleWimble (Poelstra, 2016), performs transactions between *commitments* rather than addresses. By using commitments as outputs, coins behave as self-contained cryptographic objects controlled by secret blinding factors, the knowledge of which (along with the knowledge of the coin value) would enable spending the funds. This supports confidentiality and reduces linkability, but does not by itself guarantee anonymity at the system or network layer.

Account-based approaches typically achieve receiver anonymity using mechanisms similar to those employed for sender anonymity. This is done by *updating account state commitments* and employing ZKPs to verify correctness without revealing the receiver's identity.

5.3 Transaction Value Confidentiality

Two main approaches emerge from the literature to conceal transaction details: commitments and public key encryption. To prove correctness without compromising confidentiality, these approaches are usually combined with ZKPs.

Commitments. As introduced in Section 2.2.2, commitments allow values to remain hidden while still supporting verification. Confidential Transactions[9] use *Pedersen commitments* to hide transaction amounts while allowing the ledger to verify value conservation. Monero adopted and extended this technique by combining it with ring signatures for sender's anonymity (Noether *et al.*, 2016). Zerocash (Ben Sasson *et al.*, 2014) uses ZKPs to achieve full transaction privacy: a cryptographic commitment is made to a new coin; then, a ZKP ensures transaction validity without exposing sensitive data. Commitment-based schemes are widely adopted to obtain transaction value confidentiality, especially because their homomorphic versions allow commitments to be combined without leaking sensitive data. To prevent users from creating negative or overflowing amounts, ZK range proofs show that a committed value is non-negative and lies within a valid range.

Public Key Encryption. In PEReDi (Kiayias *et al.*, 2022), senders and receivers update their accounts by submitting *encrypted transaction information* to several maintainers who operate a distributed ledger. Transactions are encrypted using threshold encryption, which requires a quorum of maintainers to cooperate to revoke confidentiality and decrypt transaction details. Using encryption instead of commitments allows revocation capabilities and facilitates the implementation of auditability and tracing mechanisms. In future payment systems, threshold cryptography may support governance objectives such as distributed control over issuance, multi-party authorization of audit or tracing operations, resilience against insider risk, and separation of duties across institutional actors, even when full decentralization is not desired. This is relevant in regulated payment settings because disclosure or tracing powers need not be assigned to a single authority: they can instead be distributed across multiple designated actors, possibly including operational entities, supervisory bodies, or independent audit functions.

[9] https://elementsproject.org/features/confidential-transactions/investigation

From this perspective, threshold mechanisms provide a technical way to implement multi-stakeholder governance arrangements, where sensitive actions require cooperation among several parties rather than unilateral access by one actor.

A few solutions implement privacy-preserving payment systems using smart contracts on public blockchains. For example, Zether represents account balances as ElGamal ciphertexts and attaches NIZK proofs so that state updates can be verified without exposing balances or transfer amounts (e.g., Bünz *et al.*, 2020).

5.4 Linkability and Unlinkability

Unlinkability ensures that transactions cannot be correlated or traced back to the same user. Obtaining unlinkability in public ledgers is challenging as linking between addresses in crypto-asset systems stems from different patterns (e.g., Lu *et al.*, 2022; Zhong and Mueen, 2024). A non-exhaustive list of patterns and heuristics to link addresses is the following.

- *Common input ownership heuristic*: If multiple addresses appear as inputs in a single transaction, they are likely controlled by the same entity;
- *Change address*: In a transaction with two outputs, one is the payment, the other one may be the change returned to the sender;
- *Address reuse*: Using the same address for multiple transactions makes it easy to link payments to the same user[10];
- *Temporal analysis*: If transactions occur in rapid succession or at predictable intervals, they may be linked to the same entity;
- *Clustering analysis*: Wallet-specific behavior, such as round numbers, fee patterns, or recurring spending habits, can help group addresses;
- *Dust attack analysis*: Small amounts of crypto-assets are sent to many addresses to track their movements; if the dust is later spent with other funds, it may reveal links between addresses.

Existing countermeasures primarily aim to obscure input-output relations within transactions through mixing protocols and address reuse prevention. Mixing protocols disrupt common ownership heuristics and help mitigate change address attacks. Address-changing techniques

[10]This works because addresses are pseudonymous but not private.

generate new sender or receiver addresses for each transaction to prevent linkability. Additionally, ensuring network anonymity helps further obscure user identities. To counter dust attacks, the simplest defense is to ignore dust transactions, preventing adversaries from establishing links between addresses. The remainder of the section reviews mixing protocols and approaches adopted in privacy-native payment systems.

Mixing Protocols. Mixing protocols are specifically designed to work on existing blockchains and improve unlinkability in public ledgers (Maxwell, 2013). The naïve approach to mixing uses a centralized service that collects transactions and publishes a single large transaction with multiple inputs and outputs. This obscures which inputs correspond to which outputs, thereby reducing linkability between sender and receiver.

Different mixing protocols exist with different trade-offs in terms of complexity, efficacy, trust, and usability. In centralized solutions, a third party (often called *mixer* or *tumbler*) provides the mixing service for a fee. While such designs are simple and support large anonymity sets, they introduce risks such as availability, theft, and potential privacy breaches. Therefore, different trust models have been proposed to mitigate these concerns (e.g., Bonneau *et al.*, 2014; Heilman *et al.*, 2016; Valenta and Rowan, 2015). For instance, Mixcoin (Bonneau *et al.*, 2014) offers a signed warranty enabling customers to prove that the mixer has misbehaved; TumbleBit (Heilman *et al.*, 2016) prevents coin theft using an on-chain escrow and ZKPs. Decentralized mixers remove the need for a trusted party by using cryptographic protocols, smart contracts that enforce mixing rules on-chain, or peer-to-peer coordination, enhancing security and censorship resistance, but often incurring higher complexity, requiring user coordination, and typically supporting smaller anonymity sets. Notable examples include CoinShuffle++ (Ruffing *et al.*, 2016) and ValueShuffle (Ruffing and Moreno-Sanchez, 2017)—which further conceals transaction value.

Although improving unlinkability, mixing protocols are still vulnerable to transaction graph analysis to some extent. For example, if the mixing process does not involve adequate randomization or if there are patterns in the amounts or timing of transactions, likely connections can be identified, even after several rounds of mixing. Also, if a participant does not properly

anonymize the change, it can be traced back to the sender. To maximize privacy, participants need to combine mixing protocols with other privacy-preserving techniques and follow practices such as avoiding address reuse and carefully managing change outputs.

Integrated Solutions. Privacy-preserving crypto-asset systems leverage a variety of strategies to improve unlinkability, focusing primarily on address-changing, transaction mixing, and the use of ZKPs. One-time destination addresses (or *stealth addresses*) help obtain recipient unlinkability exploiting the idea of changing address for each transaction involving a user. Specifically, different protocols propose approaches to update the recipient address with limited or no interaction with the payee (e.g., Fauzi *et al.*, 2019; Noether *et al.*, 2016). For strong transaction privacy, *ZKPs* offer a powerful solution (e.g., Ben Sasson *et al.*, 2014). They allow transactions to prove their validity without revealing the underlying private data. In these systems, public transactions may contain commitments, nullifiers, and ciphertexts together with validity proofs, rather than explicit sender–receiver links. Among ZK-based approaches, the *commitments and nullifiers* strategy (e.g., Tomescu *et al.*, 2022) is particularly interesting: a coin contains a commitment to its serial number, and spending the coin involves publishing a pseudo-random value derived from the coin serial number (namely, a nullifier[11]). This ensures unlinkability to the original coin, while marking it as spent.

6 Auditability

Full privacy often conflicts with compliance: if transactions are completely opaque, regulators have no oversight (Ballaschk and Paulick, 2021). *Auditability* means being able to check and verify that digital transactions follow the rules without necessarily revealing all private details. It plays a crucial role in the third generation of privacy-preserving digital payment systems, especially in institutional and regulated payment settings. Importantly, auditability need not be limited to inspecting individual transactions: it can also verify compliance with rules over time, such as cumulative limits, frequency constraints, or behavioral patterns. The concept of auditability is closely related to that of *policy*, which refers to the rules enforced by the protocol

[11] A *nullifier* is a privacy-preserving marker of spent value. It allows the system to recognize that a token has already been used, and therefore to prevent double spending, without revealing which specific token or user is behind the transaction. In policy terms, nullifiers illustrate how a system can enforce correctness rules while limiting the exposure of identifying or transaction-level information.

(and configured by system operators) to govern behaviors (e.g., to restrict who can transact and under what conditions). These rules are meant to prevent unwanted behavior before it happens. Auditability, instead, allows checking what actually happened after the fact. It helps regulators or auditors review transactions, spot suspicious activity, or ensure that limits were respected while still protecting user privacy where possible. Finally, *accountability* adds another layer, enabling a user's actions to be connected to his real identity, e.g., through trusted authorities and Know Your Customer (KYC) procedures. While auditability concerns the ability to verify that rules have been followed, accountability concerns the conditions under which actions can be linked back to identifiable users. In institutional settings, both properties depend on how informational powers are allocated among different actors. Issuing authorities, regulated intermediaries, supervisors, public authorities, or other designated entities may have different powers to verify compliance, request disclosure, or recover identity information, depending on the system design. For this reason, auditability and accountability mechanisms should specify not only *what* can be verified or revealed, but also *who* can trigger verification, disclosure, or identification, under which conditions, and with which procedural or technical safeguards. A key design challenge is that such mechanisms may inadvertently reveal additional information through operational patterns, e.g., metadata, timing, or selective disclosure processes. For this reason, they must be carefully engineered to limit unintended information leakage while preserving their regulatory function.

From an institutional perspective, auditability is therefore not only a technical feature, but also a governance choice. Different mechanisms allocate different informational powers to different actors: some allow users to prove compliance without revealing private data; others enable intermediaries, supervisors, or designated authorities to obtain selected information under predefined conditions; still others distribute disclosure powers across multiple parties to reduce reliance on a single trusted actor. Against this background, we identify the following approaches that enable or support auditability: anonymity budget, operating limits, revocable anonymity and user tracing, coin tracing, and verification without disclosure. These approaches can be seen as different policy knobs: some limit privacy quantitatively, others enable conditional disclosure, and others support compliance verification without revealing sensitive data.

6.1 Anonymity Budget

An *anonymity budget* limits the participant's ability to perform anonymous payments. Each transaction consumes a portion of this budget. Once it is exhausted, further private payments may be blocked or require additional authorization (e.g., Tomescu *et al.*, 2022; Wüst *et al.*, 2019). For example, PRCash (Wüst *et al.*, 2019) restricts the total amount of anonymous payments a user can *receive* within a time window (or epoch). UTT (Tomescu *et al.*, 2022) employs the anonymity budget to balance privacy with accountability for *spending* operations. Beyond the allocated budget, transactions may either lose privacy or require auditing. In UTT, the anonymity budget is represented by a special non-spendable token that must be included in each anonymous but accountable transaction. By adjusting its size and duration, authorities can regulate the flow of anonymous funds. Budgets can be defined on spending, receiving, or net flows depending on the threat model and policy goal. A typical use case is to allow stronger privacy for low-value or low-risk payments, while requiring additional checks, reduced anonymity, or auditability once cumulative amounts exceed predefined limits.

6.2 Operating Limits

Operating limits indicate constraints beyond which transactions cannot be carried out. Examples of operating limits may include caps on transaction amounts, limits on cumulative spending, or constraints on usage frequency. Such mechanisms illustrate how technical design choices can support policy objectives while remaining subject to legal and institutional considerations. In practice, limits may apply to a single transaction, a user's overall balance, the amount of funds sent or received, or the number of transactions within a time window. Compliance with such limits can be proven in zero-knowledge. A central idea is the enforcement of a *per-transaction spending limit*, whereby a transaction becomes invalid if it exceeds the defined limit, unless it is signed by an authorized party (e.g., Garman *et al.*, 2017). Another proposal involves maintaining a *per-user counter* incremented with each outgoing transaction. The system can then reject transactions if the user's counter is above a predefined threshold. AQQUA (Papadoulis *et al.*, 2024) uses *multiple counters* per account, which are publicly stored as three commitments: one to the account balance, and two to the cumulative amounts sent and received. During an audit, the authority selects a user by his public key and requests the opening of two historical account state snapshots for each of the selected user's accounts.

These openings allow the authority to inspect whether the user complies with specific policies. After the audit, the user randomizes his accounts, thereby reducing subsequent linkability.

6.3 Revocable Anonymity

Revocable anonymity refers to a privacy model in which users remain anonymous by default, but their identity can be revealed under predefined conditions. Some contributions use special *digital signatures* that reveal the sender's identity if he double spends (e.g., Hayes, 1990). Other approaches *encrypt* user-related information within the transaction, in special *tags*, making them accessible only to tracing authorities with decryption capabilities (e.g., Garman *et al.*, 2017; Kiayias *et al.*, 2022; Li *et al.*, 2021). This is often referred to as the *trapdoor* approach, where decryption is enabled through a private key or other privileged information. Many systems also rely on registration authorities that link real-world identities to cryptographic keys, making traced identities resolvable (e.g., Liu *et al.*, 2022; Zhang *et al.*, 2019). For example, Liu *et al.* (2022) consider a setting in which each transaction includes the user's identity encrypted under the public key of a designated authority. In a more general setting, Garman *et al.* (2017) propose a tracing mechanism where each user receives a *unique encryption key*: if the user is being traced, the key is a randomized version of the authority's key; otherwise, it is derived from a null key. Users cannot tell which type of key they received. Xue *et al.* (2023) encode the payer's identity in each transaction using the regulator's key and the transaction's epoch identifier. The epoch identifier enables temporal scoping, which limits the impact of key compromise and can enable granular tracing (e.g., to investigate suspicious behavior in a particular time window).

A few works assign *long-term public identifiers or keys* to users, from which one-time keys are derived for individual transactions. User-tracing mechanisms aim to link these one-time keys to the corresponding long-term public identifier. For example, Traceable Monero (Li *et al.*, 2021) introduces a method for generating one-time key pairs for *payees*, where each one-time address is associated with a tag. This tag can be decrypted by the tracing authority to recover the payee's long-term public key. The tag is designed to support both *backward and forward tracing*: it can identify both the accounts that sent funds to the current account and the subsequent accounts that receive funds originating from it.

The ability of tracing authorities to decrypt tracing data places a high trust burden on a *centralized entity*. From a governance perspective, this means that access to sensitive payment information depends on how disclosure powers are assigned, constrained, and audited. To mitigate concentration of power, Yu *et al.* (2024) require collaboration between *two distinct authorities* to detect correlations among a batch of transactions—specifically, those originating from the same user. Conversely, PEReDi (Kiayias *et al.*, 2022; Sarencheh *et al.*, 2022) proposes distributing the decryption power across multiple parties, requiring them to cooperate and reach a *quorum* in order to access private information. Conceptually, this can support multi-stakeholder governance models in which sensitive disclosure or tracing operations require cooperation among several designated entities, rather than unilateral access by a single authority. The concrete allocation of these roles would depend on the legal and institutional framework.

6.4 Coin Tracing

Garman *et al.* (2017) propose an approach to trace certain coins, avoiding extensive transaction auditing. In particular, the scheme enables tracing by marking specific coins as traceable, i.e., *tainted coins*[12]. When such a coin is spent, all resulting output coins also become traceable. To implement this, each coin contains a fresh *encryption key*, and tracing data for the outputs is encrypted under the input coin's key and under the authority's public key to prevent the sender from performing unauthorized tracing. To limit cascade tracing and collusion risk (i.e., when a user and the authority jointly trace non-tainted coins), exchanges are allowed to verifiably remove tracing using a public dummy key.

6.5 Verification without Disclosure

Verification without disclosure (or privacy-preserving verification) allows a party to confirm compliance with a policy without directly accessing the underlying private data. These mechanisms rely on cryptographic proofs (usually NIZK) to show that hidden data satisfies specific constraints (e.g., Ma *et al.*, 2021; Narula *et al.*, 2018; Wüst *et al.*, 2022). At the cryptographic level, the proof is designed to reveal no more than the validity of the stated claim (although

[12] A tainted coin is a traceable digital asset, which could be linked to illicit or suspicious activity, often flagged for enhanced scrutiny or restricted use.

the surrounding system may still expose metadata). This property is particularly relevant for supervisory purposes, as it allows authorized entities to verify that predefined rules or behavioral constraints are respected without requiring direct access to individual transaction data. For example, Platypus (Wüst *et al.*, 2022) defines account states with opaque *auxiliary data* to support custom policy checks. Zether (Bünz *et al.*, 2020) implements confidential transactions in Ethereum, using NIZKs to verify properties like non-negative balances.

7 Design Trade-offs and Takeaways

The previous sections show that privacy-preserving digital payment systems cannot be evaluated by looking at a single privacy goal or a single cryptographic mechanism in isolation. Anonymity, confidentiality, unlinkability, auditability, and accountability interact with one another, and the mechanisms used to support them introduce different assumptions about trust, governance, performance, and system architecture. For this reason, the choice of a PET is not a linear decision path, but a design exercise that depends on the payment model, the actors involved, the expected usage patterns, and the institutional or operational constraints of the system.

There is a rapidly evolving landscape of privacy goals in digital payment systems. While early systems primarily targeted anonymity and unlinkability through address obfuscation and mixing techniques, more recent designs emphasize stronger notions of confidentiality and auditability. These properties are supported by advanced cryptographic tools such as ZKPs, homomorphic commitments, and threshold encryption. However, no single protocol fully satisfies all privacy and compliance objectives; instead, systems occupy different points in a broader design space shaped by cryptographic choices, ledger architecture, institutional roles, and policy priorities.

In general, achieving comprehensive privacy requires combining multiple techniques, each with specific trade-offs. Blind signatures are lightweight and provide cash-like unlinkability between issuance and spending at the cryptographic layer. However, practical systems may still require additional measures, such as denomination handling, network anonymity, batching, or metadata minimization, to mitigate linkability arising outside the core cryptographic protocol. Ring signatures offer sender anonymity through decoy sets, but the effective anonymity

depends on ring size, decoy selection, usage patterns, and transaction metadata. Increasing the anonymity set can also affect transaction size, verification cost, and latency.

Commitments and encryption-based techniques address confidentiality, but they do not solve all privacy goals on their own. Commitments can hide transaction amounts while still enabling correctness checks, especially when combined with range proofs or other ZKPs. Encryption and threshold encryption can support selective auditability or conditional disclosure, but require careful governance of decryption capabilities, key shares, and quorum rules. Thus, the same mechanism that protects transaction data may also introduce new questions about who can authorize disclosure, how such powers are constrained, and how misuse or unintended information leakage is prevented.

ZKPs are among the most flexible tools because they allow a system to verify statements about hidden data. They can support checks on balances, transaction limits, token validity, or other policy conditions without revealing the underlying information. At the same time, they introduce non-trivial engineering trade-offs. The concrete overhead depends on the proof system, implementation, parameters, and hardware. Succinct proof systems such as zk-SNARKs provide compact proofs and fast verification, but may require trusted setup and non-trivial proving costs. Transparent systems such as zk-STARKs avoid trusted setup but typically produce larger proofs. Bulletproofs are often used for range proofs and avoid trusted setup, but verification can be more expensive. These differences matter for scalability and operational feasibility, especially when proofs must be generated or verified at high volume.

Therefore, the main takeaway is that no single PET is universally preferable to another. Rather, privacy-preserving digital payment systems require a layered design in which cryptographic mechanisms, ledger structure, governance arrangements, and usage assumptions are considered together. Threshold cryptography may support distributed governance models, ZKPs may enable compliance verification without exposing transaction data, and commitments may support confidential balances under institutional oversight. Their suitability ultimately depends on the architecture, threat model, transaction patterns, operational requirements, and policy objectives of the payment system.

8 Overview of Related Work

A large body of literature has explored privacy-preserving digital payment systems, motivated by both technological challenges and the societal implications of financial surveillance. This section provides references to key surveys covering privacy in both decentralized crypto-asset systems and institutional digital payment infrastructures.

Privacy in Crypto-asset Systems. Genkin *et al.* (2018) offered a broad and accessible overview of techniques for anonymity in decentralized crypto-asset systems, while emphasizing the absence of a unified definition of privacy, which hinders fair comparisons between systems. More recent surveys have attempted to formalize anonymity notions. For instance, Amarasinghe *et al.* (2019) developed a taxonomy of anonymity features (including anonymity, confidentiality, unlinkability, untraceability, and deniability). Feng *et al.* (2019) offered a layered classification of privacy-preserving mechanisms, from network-level obfuscation to cryptographic primitives. Similarly, Peng *et al.* (2021) identified PETs and illustrated how various protocols integrate them. Unlike the preceding surveys, Almashaqbeh and Solomon (2022) focus primarily on privacy in blockchain computation (i.e., smart contracts), but do not consider accountability requirements in payment systems.

Privacy in Institutional Digital Payment Systems. A distinct body of work addresses privacy in institutional and regulated digital payment systems, driven by the need to balance individual privacy with oversight and compliance requirements. Auer *et al.* (2025) distinguish between *soft privacy*, based on access controls and trust in intermediaries, and *hard privacy*, grounded in cryptographic techniques. While they offer a high-level classification and conceptual framework, their discussion emphasizes policy and architectural perspectives, leaving a more detailed comparison of cryptographic techniques beyond their primary scope. Darbha and Arora (Bank of Canada)[13] and Pocher and Veneris (2022) examine PETs from a compliance and governance perspective. These works provide architectural blueprints but offer limited analysis of the underlying cryptographic mechanisms.

Recent applied research initiatives further explore how PETs may be integrated into emerging digital payment infrastructures. For example, collaborations between central banks and

[13] https://www.bankofcanada.ca/2020/06/staff-analytical-note-2020-9/

research laboratories, such as the Bank of England study on enhancing the privacy of a potential digital pound (Torres Vives *et al.*, 2024), investigate how techniques including ZKPs, pseudonymization, and secure multiparty computation can support privacy while addressing regulatory constraints. Other initiatives, such as Project Hamilton (Lovejoy *et al.*, 2023) and projects within the BIS Innovation Hub, address architectural and system-level aspects of emerging digital payment infrastructures, while privacy-preserving cryptographic mechanisms are treated at different levels of detail depending on the scope of each initiative. As a result, much of this literature focuses on policy and infrastructure trade-offs rather than low-level protocol analysis.

This work provides a high-level structured overview of cryptographic primitives, protocols, and system architectures across both decentralized and institutional digital payment systems.

9 Conclusion: No Silver Bullet but Informed Choices

Designing digital payment systems that protect user privacy while supporting legal and institutional oversight is not only a technical challenge, but also a strategic and societal choice. As institutions explore new forms of digital money, they face a complex balancing act: preserving the confidentiality and freedom that users expect from cash, while ensuring that the system remains secure, auditable, and compliant with financial regulations.

From this perspective, privacy in digital payments should be understood not as an isolated technical feature, but as the outcome of policy choices embedded in system design. Decisions about which transaction data remain hidden, under what conditions information can be revealed, and which entities are authorized to perform audits are ultimately translated into architectural and cryptographic mechanisms.

PETs offer a diverse and evolving toolkit to support this balance. Whether through blind signatures, ZKPs, anonymous addresses, or selective disclosure mechanisms, these technologies can provide different levels of anonymity, confidentiality, and unlinkability—tailored to the policy goals of each jurisdiction. At the same time, mechanisms for auditability and accountability help define how oversight powers are allocated and constrained, allowing digital payment systems to support public trust and regulatory scrutiny without necessarily turning privacy into full transparency. Crucially, these technologies do not eliminate the need for governance and institutional trust, but rather reshape how oversight and trust are implemented.

By enabling selective, conditional, and verifiable disclosure, PETs expand the design space available to system designers and public authorities beyond purely opaque or fully transparent models. In this sense, PETs can help align technical design with data-protection principles, such as data minimization and privacy-by-design, while also supporting compliance-oriented functions, such as conditional traceability, accountable disclosure, and targeted auditability. This, in turn, means that privacy and oversight requirements can be considered explicitly at the architectural level, rather than enforced solely through *ex-post* controls.

However, there is *no one-size-fits-all solution*: each design involves trade-offs between user protection, institutional control, technical complexity, and operational cost. As a result, evaluating privacy-preserving payment systems requires moving beyond binary classifications and instead assessing how different design choices align with specific regulatory objectives, risk tolerances, and usage contexts.

This paper builds on the broader technical survey by the authors (Nardelli *et al.*, 2026), but serves a different purpose. While the survey provides a comprehensive technical analysis of cryptographic primitives, protocol architectures, value representation models, and system-level design choices, the present article offers a higher-level and policy-oriented synthesis. Its contribution is to translate the technical design space of privacy-preserving digital payment systems into a conceptual map of the trade-offs among privacy, auditability, accountability, governance, and operational feasibility. A clear understanding of these technological options and their limitations is therefore essential for informed discussions on the evolution of digital payment infrastructures.

List of Acronyms

AML	Anti-Money Laundering.
CFT	Combating the Financing of Terrorism.
GDPR	General Data Protection Regulation.
IBE	Identity-based Encryption.
KYC	Know Your Customer.
NIZK	Non-Interactive Zero-Knowledge.
PET	Privacy-Enhancing Technology.
ZK	Zero-Knowledge.
zk-SNARK	Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge.
zk-STARK	Zero-Knowledge Scalable Transparent Arguments of Knowledge.
ZKP	Zero-Knowledge Proof.

References

Almashaqbeh G. and R. Solomon (2022), SoK: Privacy-Preserving Computing in the Blockchain Era, In *Proceedings of the 2022 IEEE 7th European Symposium on Security and Privacy (EuroS&P)*, pp. 124–139, New York City, US, IEEE.

Amarasinghe N., X. Boyen, and M. McKague (2019), A Survey of Anonymity of Cryptocurrencies, In *Proceeding of the Australasian Computer Science Week Multiconference*, ACSW '19, New York, NY, USA, ACM.

Androulaki E., J. Camenisch, A.D. Caro, M. Dubovitskaya, K. Elkhiyaoui, and B. Tackmann (2020), Privacy-preserving auditable token payments in a permissioned blockchain system, In *Proceedings of the 2nd ACM Conference on Advances in Financial Technologies*, AFT '20, p. 255–267, New York, NY, USA, ACM.

Androulaki E., G.O. Karame, M. Roeschlin, T. Scherer, and S. Capkun (2013), Evaluating User Privacy in Bitcoin, In Sadeghi A.R., editor, *Financial Cryptography and Data Security (FC)*, pp. 34–51, Springer.

Auer R., R. Böhme, J. Clark, and D. Demirag (2025), Privacy-enhancing technologies for digital payments: mapping the landscape, "BIS: Working Papers", p. 23.

Ballaschk D. and J. Paulick (2021), The public, the private and the secret: Thoughts on privacy in central bank digital currencies, "Journal of Payments Strategy & Systems", 15, 3, pp. 277–286.

Baudet M., A. Sonnino, M. Kelkar, and G. Danezis (2023), Zef: Low-latency, Scalable, Private Payments, In *Proceedings of the 22nd Workshop on Privacy in the Electronic Society*, WPES '23, p. 1–16, New York, NY, USA, ACM.

Bauer B., G. Fuchsbauer, and C. Qian (2021), Transferable E-Cash: A Cleaner Model and the First Practical Instantiation, In Garay J.A., editor, *Public-Key Cryptography – PKC 2021*, pp. 559–590, Springer.

Ben-Sasson E., I. Bentov, Y. Horesh, and M. Riabzev (2019), Scalable Zero Knowledge with No Trusted Setup, In Boldyreva A. and D. Micciancio, editors, *CRYPTO*, pp. 701–732, Springer.

Ben Sasson E., A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, and M. Virza (2014), Zerocash: Decentralized Anonymous Payments from Bitcoin, In *Proceedings of the 2014 IEEE Symposium on Security and Privacy*, pp. 459–474.

BIS Innovation Hub (2023), Project Tourbillon: Exploring privacy, security and scalability for CBDCs, Technical report, BIS.

BIS Innovation Hub and Bank of England (2023), Project Rosalind: Building API Prototypes for Retail CBDC Ecosystem Innovation, Technical report, Bank for International Settlements Innovation Hub and Bank of England.

Bissias G., A.P. Ozisik, B.N. Levine, and M. Liberatore (2014), Sybil-Resistant Mixing for Bitcoin, In *Proceedings of the 13th Workshop on Privacy in the Electronic Society*, WPES '14, p. 149–158, New York, NY, USA, ACM.

Bitansky N., R. Canetti, A. Chiesa, and E. Tromer (2012), From extractable collision resistance to succinct non-interactive arguments of knowledge, and back again, In *Proceedings of ITCS'12*, p. 326–349, ACM.

Boneh D. and V. Shoup (2020), A graduate course in applied cryptography, "Draft 0.5", p. 14.

Bonneau J., A. Narayanan, A. Miller, J. Clark, J.A. Kroll, and E.W. Felten (2014), Mixcoin: Anonymity for Bitcoin with Accountable Mixes, In Christin N. and R. Safavi-Naini, editors, *Financial Cryptography and Data Security*, pp. 486–504, Berlin, Heidelberg, Springer.

Bünz B., S. Agrawal, M. Zamani, and D. Boneh (2020), Zether: Towards Privacy in a Smart Contract World, In Bonneau J. and N. Heninger, editors, *Proceedings of FC'20*, pp. 423–443, Cham, Springer.

Bünz B., J. Bootle, D. Boneh, A. Poelstra, P. Wuille, and G. Maxwell (2018), Bulletproofs: Short Proofs for Confidential Transactions and More, In *Proceedings of the 2018 IEEE Symposium on Security and Privacy (SP)*, pp. 315–334.

Buterin V. et al. (2013), Ethereum white paper, https://ethereum.org/it/whitepaper/.

Camenisch J., S. Hohenberger, and A. Lysyanskaya (2006), Balancing Accountability and Privacy Using E-Cash (Ext. Abstr.), In De Prisco R. and M. Yung, editors, *Security and Cryptography for Networks*, pp. 141–155, Berlin,

Heidelberg, Springer.
Cecchetti E., F. Zhang, Y. Ji, A. Kosba, A. Juels, and E. Shi (2017), Solidus: Confidential Distributed Ledger Transactions via PVORM, In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, CCS '17, p. 701–717, New York, NY, USA, ACM.
Chaum D. (1983), Blind Signatures for Untraceable Payments, In Chaum D., R.L. Rivest, and A.T. Sherman, editors, *Advances in Cryptology*, pp. 199–203, Boston, MA, Springer.
Chaum D. and E. van Heyst (1991), Group Signatures, In Davies D.W., editor, *Proceedings of EUROCRYPT'91*, pp. 257–265, Berlin, Heidelberg, Springer.
Cheng H., G. Fotiadis, J. Großschädl, and D. Page (2025), Fast AVX-512 Implementation of the Optimal Ate Pairing on BLS12-381, IACR ePrint 2025/1283.
Cheon S., Y. Lee, D. Kim, J.M. Lee, S. Jung, T. Kim, D. Lee, and H. Kim (2024), DaCapo: Automatic Bootstrapping Management for Efficient Fully Homomorphic Encryption, In *33rd USENIX Security Symposium (USENIX Security 24)*, pp. 6993–7010, USENIX Association.
Christ M., F. Baldimtsi, K.K. Chalkias, D. Maram, A. Roy, and J. Wang (2024), SoK: Zero-Knowledge Range Proofs, Crypt. IACR 2024/430.
Chung H., K. Han, C. Ju, M. Kim, and J.H. Seo (2022), Bulletproofs+: Shorter Proofs for a Privacy-Enhanced Distributed Ledger, "IEEE Access", 10, pp. 42081–42096.
Connolly D., C. Komlo, I. Goldberg, and C.A. Wood (2024), The Flexible Round-Optimized Schnorr Threshold (FROST) Protocol for Two-Round Schnorr Signatures, RFC 9591.
Dold F. (2019), *The GNU Taler system: practical and provably secure electronic payments*, PhD thesis, Université de Rennes.
El-Hajj M. and B. Oude Roelink (2024), Evaluating the Efficiency of zk-SNARK, zk-STARK, and Bulletproof in Real-World Scenarios: A Benchmark Study, "Information (Switzerland)", 15, 8, p. 463.
Elfadul I., L. Wu, R. Elhabob, and A. Elkhalil (2024), A privacy and compliance in regulated anonymous payment system based on blockchain, "Journal of Ambient Intelligence and Humanized Computing", 15, 8, pp. 3141–3157.
Elgamal T. (1985), A public key cryptosystem and a signature scheme based on discrete logarithms, "IEEE Transactions on Information Theory", 31, 4, pp. 469–472.
Ernstberger J., S. Chaliasos, G. Kadianakis, S. Steinhorst, P. Jovanovic, A. Gervais, B. Livshits, and M. Orrʻu (2024), zk-Bench: A Toolset for Comparative Evaluation and Performance Benchmarking of SNARKs, In *Security and Cryptography for Networks*, volume 14973 of *Lecture Notes in Computer Science*, pp. 46–72, Springer.
European Parliament (2016), Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, General Data Protection Regulation, Article 25, Data protection by design and by default.
Fauzi P., S. Meiklejohn, R. Mercer, and C. Orlandi (2019), Quisquis: A New Design for Anonymous Cryptocurrencies, In Galbraith S.D. and S. Moriai, editors, *Advances in Cryptology – ASIACRYPT 2019*, pp. 649–678, Cham, Springer.
Feng Q., D. He, S. Zeadally, M.K. Khan, and N. Kumar (2019), A survey on privacy protection in blockchain system, "Journal of Network and Computer Applications", 126, pp. 45–58.
Friolo D., G. Goodell, D. Toliver, and H.D. Nakib (2024), Private Electronic Payments with Self-Custody and Zero-Knowledge Verified Reissuance.
Garman C., M. Green, and I. Miers (2017), Accountable Privacy for Decentralized Anonymous Payments, In Grossklags J. and B. Preneel, editors, *Financial Cryptography and Data Security*, pp. 81–98, Berlin, Heidelberg, Springer.
Genkin D., D. Papadopoulos, and C. Papamanthou (2018), Privacy in decentralized cryptocurrencies, "Commun. ACM", 61, 6, p. 78–88.
Gentry C. (2009), Fully homomorphic encryption using ideal lattices, In *Proceedings of the 41st Annual ACM Symposium on Theory of Computing*, STOC '09, p. 169–178, New York, NY, USA, ACM.

Gross J., J. Sedlmeir, M. Babel, A. Bechtel, and B. Schellinger (2021), Designing a central bank digital currency with support for cash-like privacy, "Available at SSRN 3891121".

Groth J. (2016), On the Size of Pairing-Based Non-interactive Arguments, In Fischlin M. and J.S. Coron, editors, *Advances in Cryptology – EUROCRYPT 2016*, pp. 305–326, Berlin, Heidelberg, Springer.

Guan Z., Z. Wan, Y. Yang, Y. Zhou, and B. Huang (2022), BlockMaze: An Efficient Privacy-Preserving Account-Model Blockchain Based on zk-SNARKs, "IEEE Transactions on Dependable and Secure Computing", 19, 3, pp. 1446–1463.

Hayes B. (1990), Anonymous one-time signatures and flexible untraceable electronic cash, In Seberry J. and J. Pieprzyk, editors, *Advances in Cryptology — AUSCRYPT '90*, pp. 294–305, Berlin, Heidelberg, Springer.

Heilman E., L. Alshenibr, F. Baldimtsi, A. Scafuro, and S. Goldberg (2016), TumbleBit: An Untrusted Bitcoin-Compatible Anonymous Payment Hub, Crypt. IACR 2016/575.

Herrera-Joancomartí J. (2015), Research and Challenges on Bitcoin Anonymity, In Garcia-Alfaro J., J. Herrera-Joancomartí, E. Lupu, J. Posegga, A. Aldini, F. Martinelli, and N. Suri, editors, *Data Privacy Management, Autonomous Spontaneous Security, and Security Assurance*, pp. 3–16, Springer.

Herskind L., P. Katsikouli, and N. Dragoni (2020), Privacy and Cryptocurrencies-A Systematic Literature Review, "IEEE Access", 8, pp. 54044–54059.

Katz J. and Y. Lindell (2007), *Introduction to modern cryptography: principles and protocols*, Chapman and hall/CRC.

Kiayias A., M. Kohlweiss, and A. Sarencheh (2022), PEReDi: Privacy-Enhanced, Regulated and Distributed Central Bank Digital Currencies, In *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security*, CCS '22, p. 1739–1752, New York, NY, USA, ACM.

Li Y., G. Yang, W. Susilo, Y. Yu, M.H. Au, and D. Liu (2021), Traceable Monero: Anonymous Cryptocurrency with Enhanced Accountability, "IEEE Transactions on Dependable and Secure Computing", 18, 2, pp. 679–691.

Liu Y., J. Ni, and M. Zulkernine (2022), AT-CBDC: Achieving Anonymity and Traceability in Central Bank Digital Currency, In *Proceedings of the 2022 IEEE International Conference on Communications*, pp. 4402–4407.

Lovejoy J., M. Virza, C. Fields, K. Karwaski, A. Brownworth, and N. Narula (2023), Hamilton: A High-Performance Transaction Processor for Central Bank Digital Currencies, In *Proceedings of the 20th USENIX Symposium on Networked Systems Design and Implementation (NSDI 23)*, pp. 901–915, Boston, MA, USENIX.

Lu Q., X. Xu, H.D. Bandara, S. Chen, and L. Zhu (2022), Patterns for Blockchain-Based Payment Applications, In *Proceedings of the 26th European Conference on Pattern Languages of Programs*, EuroPLoP '21, New York, NY, USA, ACM.

Ma S., Y. Deng, D. He, J. Zhang, and X. Xie (2021), An Efficient NIZK Scheme for Privacy-Preserving Transactions Over Account-Model Blockchain, "IEEE Transactions on Dependable and Secure Computing", 18, 2, pp. 641–651.

Maxwell G. (2013), CoinJoin: Bitcoin privacy for the real world, https://bitcointalk.org/index.php?topic=279249.0.

Meiklejohn S., M. Pomarole, G. Jordan, K. Levchenko, D. McCoy, G.M. Voelker, and S. Savage (2013), A fistful of bitcoins: characterizing payments among men with no names, In *Proceedings IMC'13*, p. 127–140, ACM.

Meta Platforms, Inc. (2025), Winterfell: A STARK Prover and Verifier for Arbitrary Computations, Software repository, Accessed: 2026-09-08.

Miers I., C. Garman, M. Green, and A.D. Rubin (2013), Zerocoin: Anonymous Distributed E-Cash from Bitcoin, In *Proceedings of the 2013 IEEE Symposium on Security and Privacy*, pp. 397–411.

Möser M., K. Soska, E. Heilman, K. Lee, H. Heffan, S. Srivastava, K. Hogan, J. Hennessey, A. Miller, A. Narayanan, and N. Christin (2018), An Empirical Analysis of Traceability in the Monero Blockchain.

Nakamoto S. (2008), Bitcoin: A peer-to-peer electronic cash system, "Satoshi Nakamoto".

Nardelli M., F. De Sclavis, and M. Iezzi (2026), A Hitchhiker's Guide to Privacy-Preserving Digital Payment Systems: A Survey on Anonymity, Confidentiality, and Auditability, "Distrib. Ledger Technol.".

Narula N., W. Vasquez, and M. Virza (2018), zkLedger: Privacy-Preserving Auditing for Distributed Ledgers, In *Proceedings of the 15th USENIX Symposium on Networked Systems Design and Implementation (NSDI 18)*, pp.

65–80, Renton, WA, USENIX.
Noether S. and B. Goodell (2020), Triptych: Logarithmic-Sized Linkable Ring Signatures with Applications, IACR ePrint 2020/018.
Noether S., A. Mackenzie, et al. (2016), Ring confidential transactions, "Ledger", 1, pp. 1–18.
Paar C. and J. Pelzl (2009), A Textbook for Students and Practitioners, "Understanding Cryptography, Springer".
Papadoulis G., D. Balla, P. Grontas, and A. Pagourtzis (2024), AQQUA: Augmenting Quisquis with Auditability, IACR ePrint 2024/1181.
Pedersen T.P. (1992), Non-Interactive and Information-Theoretic Secure Verifiable Secret Sharing, In Feigenbaum J., editor, *Advances in Cryptology — CRYPTO '91*, pp. 129–140, Berlin, Heidelberg, Springer.
Peng L., W. Feng, Z. Yan, Y. Li, X. Zhou, and S. Shimizu (2021), Privacy preservation in permissionless blockchain: A survey, "Digital Communications and Networks", 7, 3, pp. 295–307.
Perera M.N.S., T. Nakamura, M. Hashimoto, H. Yokoyama, C.M. Cheng, and K. Sakurai (2022), A Survey on Group Signatures and Ring Signatures: Traceability vs. Anonymity, "Cryptography", 6, 1.
Pocher N. and A. Veneris (2022), Privacy and Transparency in CBDCs: A Regulation-by-Design AML/CFT Scheme, "IEEE Transactions on Network and Service Management", 19, 2, pp. 1776–1788.
Poelstra A. (2016), Mimblewimble, Technical report, The University of Rostock.
Qin X., S. Pan, A. Mirzaei, Z. Sui, O. Ersoy, A. Sakzad, M.F. Esgin, J.K. Liu, J. Yu, and T.H. Yuen (2023), BlindHub: Bitcoin-Compatible Privacy-Preserving Payment Channel Hubs Supporting Variable Amounts, In *Proceedings of the 2023 IEEE Symposium on Security and Privacy (SP)*, pp. 2462–2480.
Rivest R.L., L. Adleman, and M.L. Dertouzos (1978), On Data Banks and Privacy Homomorphisms, In *Foundations of Secure Computation*, pp. 169–179, Academic Press.
Rivest R.L., A. Shamir, and Y. Tauman (2001), How to Leak a Secret, In Boyd C., editor, *Advances in Cryptology — ASIACRYPT 2001*, pp. 552–565, Berlin, Heidelberg, Springer.
Ruffing T. and P. Moreno-Sanchez (2017), ValueShuffle: Mixing Confidential Transactions for Comprehensive Transaction Privacy in Bitcoin, In Brenner M., K. Rohloff, J. Bonneau, A. Miller, P.Y. Ryan, V. Teague, A. Bracciali, M. Sala, F. Pintore, and M. Jakobsson, editors, *Financial Cryptography and Data Security*, pp. 133–154, Cham, Springer.
Ruffing T., P. Moreno-Sanchez, and A. Kate (2016), P2P Mixing and Unlinkable Bitcoin Transactions, IACR ePrint 2016/824.
Sarencheh A., A. Kiayias, and M. Kohlweiss (2022), PEReDi: Privacy-Enhanced, Regulated and Distributed Central Bank Digital Currencies, IACR ePrint 2022/974.
Sarencheh A., A. Kiayias, and M. Kohlweiss (2025), PARScoin: A Privacy-preserving, Auditable, and Regulation-friendly Stablecoin, In Kohlweiss M., R. Di Pietro, and A. Beresford, editors, *Proceedings of CNS'25*, pp. 289–313, Singapore, Springer Nature Singapore.
Seres I.A., D.A. Nagy, C. Buckland, and P. Burcsi (2019), MixEth: efficient, trustless coin mixing service for Ethereum, IACR ePrint 2019/341.
Shamir A. (1985), Identity-Based Cryptosystems and Signature Schemes, In Blakley G.R. and D. Chaum, editors, *Advances in Cryptology – CRYPTO'84*, pp. 47–53, Berlin, Heidelberg, Springer.
Tomescu A., A. Bhat, B. Applebaum, I. Abraham, G. Gueta, B. Pinkas, and A. Yanai (2022), UTT: Decentralized Ecash with Accountable Privacy, IACR ePrint 2022/452.
Torres Vives G., M. Virza, R. Youngblom, F.C. Calabia, N. Vaughan, Z. Said, C. Mundakkal, and S. Mullings (2024), Enhancing the Privacy of a Digital Pound, https://www.dci.mit.edu/projects/enhancing-the-privacy-of-a-digital-pound, MIT Digital Currency Initiative and Bank of England research project.
Valenta L. and B. Rowan (2015), Blindcoin: Blinded, Accountable Mixes for Bitcoin, In Brenner M., N. Christin, B. Johnson, and K. Rohloff, editors, *Financial Cryptography and Data Security*, pp. 112–126, Springer.
Van Saberhagen N. (2013), CryptoNote v 2.0, https://cryptonote.org/whitepaper.pdf.

Wang Z., M. Cirkovic, D.V. Le, W. Knottenbelt, and C. Cachin (2023), Pay Less for Your Privacy: Towards Cost-Effective On-Chain Mixers, IACR ePrint 2023/1222.

Wüst K., K. Kostiainen, V. Čapkun, and S. Čapkun (2019), PRCash: Fast, Private and Regulated Transactions for Digital Currencies, In Goldberg I. and T. Moore, editors, *Financial Cryptography and Data Security*, pp. 158–178, Cham, Springer.

Wüst K., K. Kostiainen, N. Delius, and S. Capkun (2022), Platypus: A Central Bank Digital Currency with Unlinkable Transactions and Privacy-Preserving Regulation, In *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security*, CCS '22, p. 2947–2960, New York, NY, USA, ACM.

Xue L., D. Liu, J. Ni, X. Lin, and X.S. Shen (2023), Enabling Regulatory Compliance and Enforcement in Decentralized Anonymous Payment, "IEEE Transactions on Dependable and Secure Computing", 20, 2, pp. 931–943.

Yu Q., S. Liao, L. Wang, Y. Yu, L. Zhang, and Y. Zhao (2024), A regulated anonymous cryptocurrency with batch linkability, "Computer Standards & Interfaces", 87, p. 103770.

Zhang L., H. Li, Y. Li, Y. Yu, M.H. Au, and B. Wang (2019), An efficient linkable group signature for payer tracing in anonymous cryptocurrencies, "Future Generation Computer Systems", 101, pp. 29–38.

Zhong S. and A. Mueen (2024), BitLINK: Temporal Linkage of Address Clusters in Bitcoin Blockchain, In *Proceedings of the 30th ACM SIGKDD Conference on Knowledge Discovery and Data Mining*, KDD '24, p. 4583–4594, New York, NY, USA, ACM.

Ziegeldorf J.H., R. Matzutt, M. Henze, F. Grossmann, and K. Wehrle (2018), Secure and anonymous decentralized Bitcoin mixing, "Future Generation Computer Systems", 80, pp. 448–466.

Recently published papers in the 'Markets, Infrastructures, Payment Systems' series

n. 53 The Bank of Italy's statistical model for the credit assessment of non-financial firms, *by Simone Narizzano, Marco Orlandi and Antonio Scalia*

n. 54 The revision of PSD2 and the interplay with MiCAR in the rules governing payment services: evolution or revolution?, *by Mattia Suardi*

n. 55 Rating the Raters. A Central Bank Perspective, *by Francesco Columba, Federica Orsini and Stefano Tranquillo*

n. 56 A general framework to assess the smooth implementation of monetary policy: an application to the introduction of the digital euro, *by Annalisa De Nicola and Michelina Lo Russo*

n. 57 The German and Italian Government Bond Markets: The Role of Banks versus Non-Banks. A joint study by Banca d'Italia and Bundesbank, *by Puriya Abbassi, Michele Leonardo Bianchi, Daniela Della Gatta, Raffaele Gallo, Hanna Gohlke, Daniel Krause, Arianna Miglietta, Luca Moller, Jens Orben, Onofrio Panzarino, Dario Ruzzi, Willy Scherrieble and Michael Schmidt*

n. 58 Chat Bankman-Fried? An Exploration of LLM Alignment in Finance, *by Claudia Biancotti, Carolina Camassa, Andrea Coletta, Oliver Giudice and Aldo Glielmo*

n. 59 Modelling transition risk-adjusted probability of default, *by Manuel Cugliari, Alessandra Iannamorelli and Federica Vassalli*

n. 60 The use of Banca d'Italia's credit assessment system for Italian non-financial firms within the Eurosystem's collateral framework, *by Stefano Di Virgilio, Alessandra Iannamorelli, Francesco Monterisi and Simone Narizzano*

n. 61 Fintech Classification Methodology, *by Alessandro Lentini, Daniela Elena Munteanu and Fabrizio Zennaro*

n. 62 The Rise of Climate Risks: Evidence from Expected Default Frequencies for Firms, *by Matilde Faralli and Francesco Ruggiero*

n. 63 Exploratory survey of the Italian market for cybersecurity testing services, *by Anna Barcheri, Luca Bastianelli, Tommaso Curcio, Luca De Angelis, Paolo De Joannon, Gianluca Ralli and Diego Ruggeri*

n. 64 A practical implementation of a quantum-safe PKI in a payment systems environment, *by Luca Buccella and Stefano Massi*

n. 65 Stewardship Policies. A Survey of the Main Issues, *by Marco Fanari, Enrico Bernardini, Elisabetta Cecchet, Francesco Columba, Johnny Di Giampaolo, Gabriele Fraboni, Donatella La Licata, Simone Letta, Gianluca Mango and Roberta Occhilupo*

n. 66 Is there an equity greenium in the euro area?, *by Marco Fanari, Marianna Caccavaio, Davide Di Zio, Simone Letta and Ciriaco Milano*

n. 67 Open Banking in Italy: A Comprehensive Report, *by Carlo Cafarotti and Ravenio Parrini*

n. 68 Report on the payment attitudes of consumers in Italy: results from ECB SPACE 2024 survey, *by Gabriele Coletti, Marialucia Longo, Laura Painelli, Emanuele Pimpini and Giorgia Rocco*

n. 69 A solution for cross-border and cross-currency interoperability of instant payment systems, *by Domenico Di Giulio, Vitangelo Lasorella, Pietro Tiberi*

n. 70 Do firms care about climate change risks? Survey evidence from Italy, *by Francesca Colletti, Francesco Columba, Manuel Cugliari, Alessandra Iannamorelli, Paolo Parlamento and Laura Tozzi*

n. 71 Demand and supply of Italian government bonds during the exit from expansionary monetary policy, *by Fabio Capasso, Francesco Musto, Michele Pagano, Onofrio Panzarino, Alfonso Puorro and Vittorio Siracusa*

n. 72 Statistics on tokenized financial instruments: A challenge for central banks, *by Riccardo Colantonio, Massimo Coletta, Riccardo Renzi*

n. 73 Credit Risk Assessment with Stacked Machine Learning, *by Francesco Columba, Manuel Cugliari, Stefano Di Virgilio*

n. 74 What if Ether Goes to Zero? How Market Risk Becomes Infrastructure Risk in Crypto, *by Claudia Biancotti*

n. 75 The Cyber Risk of Non-Financial Firms, *by Francesco Columba, Manuel Cugliari, Marco Orlandi, Federica Vassalli*

n. 76 Sustainability and financial innovation: The emerging role of Fintech for Good (F4G), *by Alessandro Lentini and Daniela Elena Munteanu*

n. 77 Hydrogeological and credit risk: the Italian firms' physical risk-adjusted probability of default, *by Manuel Cugliari, Simone Narizzano and Federica Vassalli*

n. 78 Liquidity Optimization in Gross Settlement Systems with Quantum Reordering: Application to TARGET2, *by Valerio Astuti, Adriano Baldeschi, Luca Bastianelli, Giuseppe Bruno, Ajit Desai, Danica Marsden and Riccardo Russo*

n. 79 The expert assessment within Banca d'Italia's in-house credit assessment system, *by Lorenzo Esposito, Massimo Guglielmi, Francesco Monterisi, Simone Narizzano and Marco Orlandi*

n. 80 Digital payments and economic performance: evidence from Italy, *by Guerino Ardizzi, Niccolò Lippi Boncambi, Cristina Demma and Alberto Leorati*

n. 81 The euro-area repo market: structure, participants and interlinkages, *by Lorenzo Caverni, Annalisa De Nicola and Mattia Persico*

n. 82 Siamese Networks for AI-powered Automated Banknote Quality Control, *by Salvatore Gentile, Andrea Luciani, Sabina Marchetti, Domenico Pansini and Marco Viticoli*

n. 83 Private Equity and Innovation in the Euro Area, *by Emanuele Degani, Simone Letta and Tommaso Perez*

n. 84 Social and Governance Factors in Default Risk Assessment, *by Manuel Cugliari, Stefano Di Virgilio, Enrico Foscolo and Alessandra Iannamorelli*

n. 85 Household Allocation of the Next Generation of Digital Money, *by Marcello Pericoli*

n. 86 Are Stablecoins Efficient for Remittances? Evidence from a Mystery Shopping Exercise by Banca d'Italia, *by Alberto Di Iorio, Enrica Di Stefano, Michele Mascioli and Giorgio Trebeschi*

n. 87 Who uses 'Buy Now, Pay Later' in Italy? Evidence from Household Survey Data, *by Daniele Figoli and Serena Palazzo*

n. 88 Fee-cap Models for Payment Instruments: a Policy Perspective, *by Nicola Branzoli, Stefano Pietrosanti and Alessia Vita*

n. 89 Send me money ASAP: Fast Payment Systems and the Cost of Remittances, *by Marco Brandi, Alberto Di Iorio and Andrea Nobili*

n. 90 Hedging at speed in sovereign bond markets, *by Onofrio Panzarino and Antonio Perrella*

n. 91 Sentiment analysis with large language models for credit risk assessment, *by Manuel Cugliari and Giulio Gariano*

n. 92 The Architecture of Cross-Border Finance: Fifty Years of Evolution from National Segmentation to Fragmented Globalization, *by Cristina Di Luigi and Antonio Perrella*