EXECUTIVE SUMMARY
PRIVACY-ENHANCED PAYMENT SYSTEMS

Authors
Agostino Capponi, Columbia University
Michael Junho Lee, Federal Reserve Bank of New York
Brian Zhu, Columbia University

FEBRUARY 2026

EXECUTIVE SUMMARY

The Global Risk Institute (GRI) has partnered with Columbia University's Center for Digital Finance and Technologies to support actionable research that benefits our members in navigating financial and regulatory risks, especially in an environment where regulatory controls lag technological advancement. Nowhere is this more pronounced than with the development and wide acceptance of digital assets and currency. This paper analyzes the economic design and regulatory implications of payment systems that embed privacy features, such as those found in cryptocurrencies and prospective central bank digital currencies. The authors discuss privacy-enhanced payment systems, exploring the balance between user privacy and the potential for illicit financial activities, while considering regulatory and technological challenges.

The model developed here examines how illicit actors can exploit the provision of privacy (both identity and transaction privacy) for criminal activities. It explores the dual nature of privacy in payments, valued by legitimate users for personal protection, but exploited by bad actors for criminal activity such as money laundering, financial fraud, market manipulation, narcotics trafficking, and cyber crimes. As blockchain based systems become more integrated with traditional financial markets, they allow for a greater facilitation of illicit activity through untraceable transactions. This will have implications for the financial services sector, and regulators.

KEY FINDINGS

While privacy in payments safeguards users' sensitive information, it also creates the opportunity for bad actors to evade detection and law enforcement, generating a fundamental conflict between personal freedom and regulatory control. An optimal system balances the privacy needs of legitimate users with the bad actors' desire to take advantage of the system for criminal activity while avoiding detection.

Optimal System Design: If illicit actors can innovate (improve their methods to evade detection), the optimal payment system is characterized by two rules: (1) require user identity for account creation and (2) offer transaction privacy only for payments below a fixed volume threshold. This limits opportunities for system abuse while still retaining some privacy for legitimate users.

Ranking Payment System: Payment system types are ranked by net social welfare and regulatory risk. Systems that are identity-private and transaction-private (like Monero or ZCash) pose the highest risks under weak enforcement, while systems that require identity but offer limited, well calibrated transaction privacy achieve the best balance.

Policy Implications: The paper advocates for designs that combine identity verification with flow (not just balance) limits and state-contingent privacy. Current approaches to digital cash (e.g., some CBDC pilots) that relax identity requirements or only restrict transaction size may be insufficient.

POLICY RELEVANCE

Currently, the digitalization of economic activity allows for the surveillance and monetization of personal data. As cash payments become increasingly obsolete, both the private and public sectors are looking for ways to enhance the privacy aspect of payments systems in a way that resembles cash payments. Risk professionals, regulators, and system designers will have to come up with the optimal model that balances the privacy utility of legitimate users with the potential attempts of bad actors to exploit the system for illicit activity.

Given the inevitable trade-offs associated with regulatory expectations in privacy-enhanced payment systems, this paper is quite informative for chief risk officers and regulators involved in digital payments, AML compliance, or the strategic planning of financial infrastructures, helping to anticipate these trade-offs.

TAKEAWAY FOR RISK PROFESSIONALS AND REGULATORS.

Financial Crimes: Privacy-enhancing technologies can be used to scale illicit activities for example by structuring and smurfing (breaking down large transactions into smaller ones below the reporting threshold), making regulatory enforcement oversight challenging. This is directly relevant for risk management teams assessing exposure to money laundering and fraud through payment rails.

Regulatory Compliance: The paper's framework highlights how certain privacy features may undermine Anti-money Laundering / Know Your Client efforts. It offers a guide for compliance teams on the comparative risks of different payment regimes and the importance of enforced identity requirements.

System Design and Operational Resilience: As organizations and central banks assess new digital payment infrastructures, the findings help identify how privacy design choices affect system vulnerability to criminal abuse and the sustainability of risk frameworks amidst criminal innovation.

Strategic policy: The findings of the paper could guide CROs in shaping recommendations for digital payments strategy, vendor risk assessment, and engagement with regulators on CBDC and FinTech innovation. Otherwise, heavy emphasis on just privacy features could inadvertently escalate financial crime risk.