TOWARDS A TAXONOMY OF PRIVACY FOR DIGITAL CURRENCIES IN REGULATED ENVIRONMENTS

François-Xavier Wicht, Christian Sillaber, Mirjam Eggen, Christian Cachin

University of Bern, Institute of Computer Science
University of Bern, Institute for Civil Law

Digital currencies raise a fundamental tension between individual privacy and regulatory oversight, particularly for anti-money laundering (AML) and counter-terrorism financing (CTF) compliance. While privacy-preserving cryptocurrencies prove that strong privacy is technically achievable without intermediaries [2], these same features have prompted regulatory concerns and prohibitions in some jurisdictions [6]. The debate is most acute for central bank digital currencies (CBDCs) and stablecoins, where recent advances in financial technology have reframed the question: it is no longer whether privacy is technically feasible, but how much privacy should be permitted under regulatory supervision [1].

Answering this question requires bridging a fundamental divide: technical and regulatory communities understand privacy differently. Cryptography researchers often treat privacy as binary—a system is either private or it is not—enabling formal analysis but overlooking the nuanced, context-dependent requirements of regulation. In contrast, regulatory frameworks rely on intermediaries for privacy oversight, obligating banks, exchanges, and virtual asset service providers (VASPs) to implement identity verification, transaction monitoring, and record-keeping.

Recent regulatory initiatives, including the European Union's Markets in Crypto-Assets Regulation (MiCAR), the Transfer of Funds Regulation (TFR), and the Financial Action Task Force (FATF) Recommendation 16 ("Travel Rule") [3], extend this intermediary-based paradigm to digital assets. However, when applied to state-operated CBDCs, this approach raises significant concerns, as enhanced central surveillance capabilities risk eroding fundamental privacy rights.

This paper proposes a multidimensional taxonomy to bridge these divergent perspectives. Rather than treating privacy as a monolithic property to be maximized or constrained, the taxonomy decomposes it into five analytically distinct dimensions, each of which can be independently configured:

1. *Who*: The identities of the transacting parties, which may range from completely anonymous or pseudonymous users to fully identified individuals or institutions.
2. *What*: The categories of transactional or personal data protected, such as transaction amounts, linkages between transactions, sources or destinations of funds, and account balances.
3. *How*: The methods and mechanisms used to control disclosure and access, including user consent, system-wide protocol design, and institutional permissions or restrictions.
4. *Where*: The entities or domains to which information may be disclosed, which could be limited to specific participants, intermediaries, regulators, or extended to the general public.
5. *Why*: The rationale or basis for allowing disclosure, such as legal requirements, contractual agreements, supervisory mandates, or other regulatory justifications.

This framework departs from traditional cryptographic privacy models, which address protocol-level objectives (confidentiality, unlinkability, untraceability) but omit institutional questions of who may access what information under which circumstances. The taxonomy provides a shared vocabulary for system architects and policymakers to discuss privacy features required or permissible for digital currency systems in varying regulatory contexts.

Applying this taxonomy highlights a persistent disconnect between regulatory and technical strategies. Regulators rely on institutional oversight at entry and exit points [5], while cryptographic research pursues end-to-end privacy guarantees [7]. Recent proposals seek compromise by integrating cryptographic primitives and accountability features, such as view keys or conditional tracing, while avoiding mass surveillance [4].

The taxonomy surfaces several recurring design patterns, including: *asymmetric privacy* (granting different privacy guarantees to different roles), *conditional disclosure* (ensuring privacy by default, with predefined exceptions), *mediated privacy* (applying distributed or collaborative controls over data release), *targeted exposure* (enabling investigatory access with proper authorization), and *regulatory privacy mechanisms* (embedding compliance directly into technical protocols). Each pattern comes with its own balance of privacy protection, regulatory effectiveness, and governance complexity.

Three key insights follow. First, privacy in digital currency systems is not binary but modular and multi-dimensional, resisting the false dichotomy between total privacy and total surveillance. This invites nuanced policy responses specifying which privacy dimensions may be adjusted and when. Second, regulatory compliance does not require universal traceability: AML obligations call for investigating specific suspicious transactions rather than indiscriminate monitoring. Selective disclosure mechanisms could satisfy regulatory imperatives while safeguarding routine privacy. Third, practical adoption of privacy-preserving yet accountable architectures for CBDCs depends not only on technical soundness but also on institutional alignment, legal compatibility, and political consensus.

Critical challenges remain. Jurisdictional conflicts raise technical and governance hurdles that cryptography alone cannot address. Privacy-preserving solutions for systemic risk monitoring and regulatory reporting remain nascent. Developing investigative tools that limit access to authorized use while preventing mass surveillance is challenging. Fundamental questions about AML/CTF regime efficacy persist, as rigorous evidence of their effectiveness and surveillance impact remains scarce.

This taxonomy serves as an analytical tool, not a prescriptive solution. It clarifies the design space, highlights trade-offs, and fosters dialogue between technological and regulatory communities. Realizing its benefits requires stakeholders to move beyond entrenched positions and engage with the proposition that privacy and regulatory compliance can be reconciled. Ultimately, the question is not only what is technically feasible, but what level of financial surveillance societies are willing to endorse.

References

[1] Raphael Auer et al. *Privacy-enhancing technologies for digital payments: mapping the landscape*. BIS Working Papers 1242. Bank for International Settlements, 2025. URL: https://www.bis.org/publ/work1242.htm.

[2] Eli Ben-Sasson et al. "Zerocash: Decentralized Anonymous Payments from Bitcoin". In: *2014 IEEE Symposium on Security and Privacy, SP 2014, Berkeley, CA, USA, May 18-21, 2014*. IEEE Computer Society, 2014, pp. 459–474. URL: https://doi.org/10.1109/SP.2014.36.

[3] Financial Action Task Force (FATF). *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations*. Updated June 2025. Paris, France, 2025. URL: https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html.

[4] Christina Garman, Matthew Green, and Ian Miers. "Accountable Privacy for Decentralized Anonymous Payments". In: *Financial Cryptography and Data Security - 20th International Conference, FC 2016, Christ Church, Barbados, February 22-26, 2016*. Ed. by Jens Grossklags and Bart Preneel. Vol. 9603. Lecture Notes in Computer Science. Springer, 2016, pp. 81–98. URL: https://doi.org/10.1007/978-3-662-54970-4_5.

[5] Christian Sillaber and Mirjam Eggen. "Privacy in payments: What a CBDC can do better than commercial bank money". In: *ZBB* 4 (2024), pp. 267–276. URL: https://doi.org/10.15375/zbb-2024-0401.

[6] U.S. Department of the Treasury. *U.S. Treasury Sanctions Notorious Virtual Currency*. Aug. 2022. URL: https://home.treasury.gov/news/press-releases/jy0916 (visited on 12/10/2025).

[7] François-Xavier Wicht et al. "A Transaction-Level Model for Blockchain Privacy". In: *Financial Cryptography and Data Security - 28th International Conference, FC 2024, Willemstad, Curaçao, March 4-8, 2024*. Ed. by Jeremy Clark and Elaine Shi. Vol. 14745. Lecture Notes in Computer Science. Springer, 2024, pp. 293–310. URL: https://doi.org/10.1007/978-3-031-78679-2_16.