# Towards A Taxonomy of Privacy for Digital Currencies in Regulated Environments

**Privacy and Public Policy Conference 2026**

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

University of Bern
Institute of Computer Science
Cryptology and Data Security Group

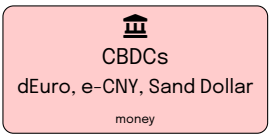
February 9, 2026

# Motivation

# Recent Evolution of Digital Money

## From cryptocurrencies to stablecoins and CBDCs



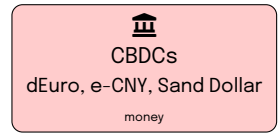



- **Cryptocurrencies:** Sparked a new area of financial technologies (distributed ledgers, decentralized cryptographic protocols) [Nak08; Com15]
- **Stablecoins:** Draw on cryptocurrency advances, aim for stability [DU23; LSSS20]
- **CBDCs:** Central banks increasingly explore novel financial rails [DKM24]

# Recent Evolution of Digital Money

**From cryptocurrencies to stablecoins and CBDCs**






- **Cryptocurrencies:** Sparked a new area of financial technologies (distributed ledgers, decentralized cryptographic protocols) [Nak08; Com15]
- **Stablecoins:** Draw on cryptocurrency advances, aim for stability [DU23; LSSS20]
- **CBDCs:** Central banks increasingly explore novel financial rails [DKM24]

# Recent Evolution of Digital Money

**From cryptocurrencies to stablecoins and CBDCs**

| Cryptocurrencies | Stablecoins | CBDCs |
|---|---|---|
| Bitcoin, Ethereum | USDC, Tether, ~~Libra/Diem~~ | dEuro, e-CNY, Sand Dollar |
| unbacked private money | backed private money | money |

- **Cryptocurrencies:** Sparked a new area of financial technologies (distributed ledgers, decentralized cryptographic protocols) [Nak08; Com15]
- **Stablecoins:** Draw on cryptocurrency advances, aim for stability [DU23; LSSS20]
- **CBDCs:** Central banks increasingly explore novel financial rails [DKM24]

| Either transparent or blocked | Oftentimes lack privacy |
|---|---|

# Recent Evolution of Digital Money

**From cryptocurrencies to stablecoins and CBDCs**

| Cryptocurrencies | Stablecoins | CBDCs |
|---|---|---|
| Bitcoin, Ethereum | USDC, Tether, ~~Libra/Diem~~ | dEuro, e-CNY, Sand Dollar |
| unbacked private money | backed private money | money |

- **Cryptocurrencies:** Sparked a new area of financial technologies (distributed ledgers, decentralized cryptographic protocols) [Nak08; Com15]
- **Stablecoins:** Draw on cryptocurrency advances, aim for stability [DU23; LSSS20]
- **CBDCs:** Central banks increasingly explore novel financial rails [DKM24]

| | | |
|---|---|---|
| Either transparent or blocked | Oftentimes lack privacy | Should be private and regulated |

# The Privacy-Regulation Dilemma

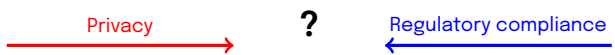
### Citizens Want

- Privacy comparable to cash
- Protection from surveillance
- Financial autonomy
- Price stability

### Regulators Want

- AML/CTF compliance
- Tax enforcement
- Investigative capabilities
- Financial oversight

**Central tension:** How to balance privacy and regulatory compliance?



# Current Approaches Fall Short

⚠ Privacy-preserving cryptocurrencies

**Zcash, Monero:** Absolute privacy → precludes accountability [KAN20]
**Result:** Regulatory bans and exchange delistings [Tre22]

# Current Approaches Fall Short

## ⚠ Privacy-preserving cryptocurrencies

**Zcash, Monero:** Absolute privacy → precludes accountability [KAN20]
**Result:** Regulatory bans and exchange delistings [Tre22]

## ⚠ Most CBDC designs

**Approach:** Little to no built-in privacy mechanisms and oftentimes extensive financial surveillance
**Problem:** Lack robust protections against misuse [CZ25]

# Current Approaches Fall Short

## ⚠ Privacy-preserving cryptocurrencies

**Zcash, Monero:** Absolute privacy → precludes accountability [KAN20]
**Result:** Regulatory bans and exchange delistings [Tre22]

## ⚠ Most CBDC designs

**Approach:** Little to no built-in privacy mechanisms and oftentimes extensive financial surveillance
**Problem:** Lack robust protections against misuse [CZ25]

## ⚠ Traditional view

**Binary treatment:** Privacy fully provided or entirely absent
**Limitation:** Doesn't reflect institutional settings

# Current Approaches Fall Short

## ⚠ Privacy-preserving cryptocurrencies

**Zcash, Monero:** Absolute privacy → precludes accountability [KAN20]
**Result:** Regulatory bans and exchange delistings [Tre22]

## ⚠ Most CBDC designs

**Approach:** Little to no built-in privacy mechanisms and oftentimes extensive financial surveillance
**Problem:** Lack robust protections against misuse [CZ25]

## ⚠ Traditional view

**Binary treatment:** Privacy fully provided or entirely absent
**Limitation:** Doesn't reflect institutional settings

**What is needed:** A framework that treats privacy as configurable

# Our Contribution

**A multidimensional taxonomy**

## Privacy as a configurable space

**Five independent dimensions:**

- **Who:** Identity (anonymous → identified)
- **What:** Information protected (amounts, links, origins)
- **How:** Disclosure control (user consent, protocol, institutional)
- **Why:** Legal basis (statutory, contractual, policy)
- **Where:** Disclosure scope (participants, intermediaries, regulators, public)

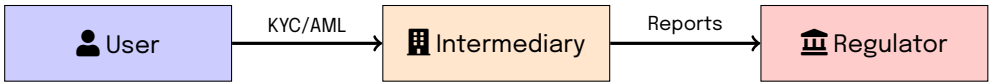
*Each dimension can be independently reasoned about, implemented, and governed*

## Before diving into the taxonomy details...

Let’s establish some background concepts

# Regulatory Approach: Intermediary Oversight

**Traditional banking model extended to cryptocurrencies**




- **Traditional finance:** Banks as choke points for monitoring
- **Cryptocurrency regulation:** VASPs as financial intermediaries [OBC23]
- **Key regulations:** MiCAR (EU), TFR, (FATF Travel Rule) [Fin25]
- **Limitation:** Centralizes control, power asymmetry [KPPO24]

# Technical Privacy Properties

**Four core dimensions of privacy in digital currencies**

## Anonymity (Network-level)

Prevent association between transactions and real-world identity

- Cryptographic addresses
- Tor, Dandelion
- Pseudonymity $\neq$ anonymity

## Unlinkability (Application-level)

Prevent correlation of multiple transactions to same user

- Address rotation
- Stealth addressing
- CoinJoin, Tornado Cash

## Confidentiality (Application-level)

Hide transaction amounts and balances

- Homomorphic commitments
- Range proofs

## Untraceability (Application-level)

Hide which output a transaction spends

- Ring signatures
- Zero-knowledge proofs

# Taxonomy

# Recall: Our Five Dimensions

**Privacy as a configurable space**

**Five independent dimensions:**

- **Who:** Identity (anonymous → identified)
- **What:** Information protected (amounts, links, origins)
- **How:** Disclosure control (user consent, protocol, institutional)
- **Why:** Legal basis (statutory, contractual, policy)
- **Where:** Disclosure scope (participants, intermediaries, regulators, public)

*Now let's explore each dimension in detail*

# Dimension 1: Who (Identity)

**Real-world identity of transacting parties**

**Level 1: Anonymity:** No connection to real-world identity *(Monero [KAN20] over Tor)*

**Level 2: Pseudonymity:** Persistent identifiers, volatile linkage *(Bitcoin [Nak08] addresses)*

**Level 3: Legitimacy:** Anonymous credentials, no direct identity *(BBS+ credentials [BBS04])*

**Level 4: Identified:** Full KYC, identity bound to transactions *(Traditional banking, China's DCEP [Peo21])*

## Observation

Level 1 systems face regulatory hurdles, Level 4 systems meet oversight requirements: trade-off between privacy and accountability

# Dimension 2: What (Transactional Data)

**Layered hierarchy of information protection**

**Level 1: All properties protected:** Confidentiality + unlinkability + untraceability *(Monero [KAN20], Zcash shielded [Ben+14])*

**Level 2: One property violated** *(Early CryptoNote [Sab13]: amounts visible)*

**Level 3: Two properties violated** *(Mimblewimble [Jed16]: some linkability and traceability)*

**Level 4: All information visible,** fully transparent *(Bitcoin [Nak08], traditional banking)*

## Observation

Privacy properties are not binary switches: they form a spectrum that can be calibrated based on regulatory needs and user requirements

# Dimension 3: How (Access Control)

**Governance framework and technical infrastructure**

**Level 1: No disclosure:** Data known only to participants (offline eCash)

**Level 2: User action required:** View keys, selective disclosure (Monero, Zcash [Ben+14])

**Level 3: Stakeholder cooperation:** Banks + regulators collaborate

**Level 4: Full disclosure:** Data accessible by default (Bitcoin, traditional banking)

## Observation

Fundamental design choice: extent to which users retain control over their data, from user autonomy (Level 1-2) to institutional oversight (Level 3-4)

# Dimensions 4 & 5: Why & Where

**Regulatory basis and disclosure scope**

### Why: Regulatory Basis

1. **Legal basis**
   Statutory law, constitutional principles
   *Example: Digital Euro legislation*
2. **Contractual basis**
   Private agreements
   *Example: Permissioned blockchains*
3. **Policy-based**
   Industry standards, compliance frameworks
4. **No normative basis**
   Unrestricted access
   *Example: Bitcoin (technical design)*

### Where: Disclosure Scope

- **Transacting parties**
  Personal financial management
- **Public visibility**
  Anyone can access
  *Example: Bitcoin blockchain*
- **Intermediary access**
  Banks, PSPs, VASPs
  Regulatory compliance role
- **Authority access**
  Regulators, tax authorities
  Legal frameworks (warrants, thresholds)

# Privacy Configurations

# Conditional Disclosure: Privacy Budgets

**Privacy by default with threshold-based disclosure**

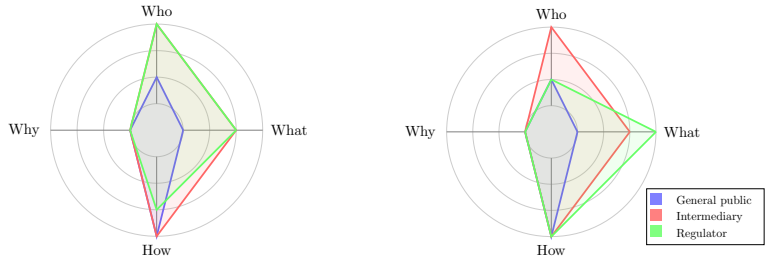



Figure: Below threshold (left): full privacy. Above threshold (right): regulatory disclosure

- **Systems:** PRCash [WKCC19], UTT [Tom+22]
- **Mechanism:** Anonymous credentials with embedded budgets
- **Below budget:** Zero-knowledge proofs, full privacy
- **Above budget:** Transaction details encrypted to regulator

# Mediated Privacy: Threshold Authorities

**Distributed disclosure authority**

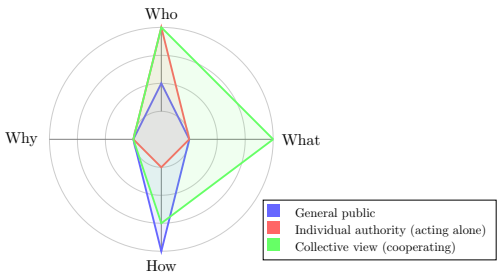



Figure: $(t, n)$ threshold: requires $t$ of $n$ authorities to cooperate

**Mechanism:**

- Decryption key split into $n$ shares
- Any $t$ shares reconstruct key
- Fewer than $t$ reveals nothing

**Benefits:**

- No single actor has unilateral power
- Prevents individual misuse
- Requires coordination for disclosure
- *Examples:* PEReDi [KKS22], UTT [Tom+22]

# Summary

# Key Insights

## Insight 1: Privacy as a tunable configuration space

Binary on/off privacy models fail to address regulatory nuance. Instead, we model privacy as a multi-dimensional **configuration space** with five independent, tunable axes - each adjustable to align with specific compliance, functionality, or risk requirements.

# Key Insights

## Insight 1: Privacy as a tunable configuration space

Binary on/off privacy models fail to address regulatory nuance. Instead, we model privacy as a multi-dimensional **configuration space** with five independent, tunable axes - each adjustable to align with specific compliance, functionality, or risk requirements.

## Insight 2: Selective configurations enable compliance with minimal surveillance

Regulatory compliance does *not* require pervasive transaction tracing. AML/CTF obligations typically demand visibility into amounts and counterparties; not complete historical linkage. **Carefully chosen configurations** can deliver strong privacy while satisfying these targeted requirements.

# Challenged Presumptions

## ✗ Presumption 1: Regulators can only ban privacy coins

**Reality:** Effective oversight can be implemented at key interaction points or by embedding accountability mechanisms directly into protocols.

# Challenged Presumptions

## ✗ Presumption 1: Regulators can only ban privacy coins

**Reality:** Effective oversight can be implemented at key interaction points or by embedding accountability mechanisms directly into protocols.

## ✗ Presumption 2: CBDCs face an insurmountable privacy-functionality trade-off

**Reality:** Conditional disclosure, mediated access controls, and tunable transparency thresholds allow meaningful optimisation across both privacy and regulatory objectives.

# Challenged Presumptions

## ✗ Presumption 1: Regulators can only ban privacy coins

**Reality:** Effective oversight can be implemented at key interaction points or by embedding accountability mechanisms directly into protocols.

## ✗ Presumption 2: CBDCs face an insurmountable privacy-functionality trade-off

**Reality:** Conditional disclosure, mediated access controls, and tunable transparency thresholds allow meaningful optimisation across both privacy and regulatory objectives.

## ✗ Presumption 3: Meeting legal requirements is precluded by technical infeasibility

**Reality:** Proportionality and purpose limitation can be enforced natively within cryptographic protocols, enabling **compliance-by-design** systems.

# Conclusion

## Achieving regulated privacy is a design challenge

**By treating privacy as multidimensional and configurable:**

- Systems can better safeguard user interests
- While simultaneously fulfilling regulatory requirements
- Often without forcing a trade-off between the two
- Instead, integrating both through careful cryptographic design

# Thank you for your attention!

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

University of Bern
Institute of Computer Science
Cryptology and Data Security Group

February 9, 2026

# References I


[BBS04] Dan Boneh et al. “Short Group Signatures”. In: *Advances in Cryptology - CRYPTO 2004, 24th Annual International CryptologyConference, Santa Barbara, California, USA, August 15-19, 2004, Proceedings*. Ed. by Matthew K. Franklin. Vol. 3152. Lecture Notes in Computer Science. Springer, 2004, pp. 41–55. DOI: 10.1007/978-3-540-28628-8_3. URL: https://doi.org/10.1007/978-3-540-28628-8_3 (visited on 09/17/2025).

[Ben+14] 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. DOI: 10.1109/SP.2014.36. URL: https://doi.org/10.1109/SP.2014.36 (visited on 09/17/2025).

[BINSS23] Vitalik Buterin et al. *Blockchain Privacy and Regulatory Compliance: Towards a Practical Equilibrium*. SSRN Working Paper. Available at SSRN: https://ssrn.com/abstract=4563364. 2023. DOI: 10.2139/ssrn.4563364.

# References II


[BIS23] BIS Innovation Hub. *Project Tourbillon - Exploring Privacy, Security and Scalability for CBDCs: Final Report*. Basel, 2023. URL: https://www.bis.org/publ/othp80.pdf.

[CMGS22] David Chaum et al. *Offline eCash 2.0: How to Protect Privacy and Prevent Illegal Activity with a Digital Bearer Instrument*. White paper, version 8-31-22. eCash Foundation. 2022. URL: https://chaum.com/wp-content/uploads/2022/11/Offline_eCash2.0_8-31-22.pdf.

[Com15] Committee on Payments and Market Infrastructures. *Digital currencies*. Tech. rep. Bank for International Settlements, 2015. URL: https://www.bis.org/cpmi/publ/d137.pdf.

[CZ25] Rebecca Clipal and Alejandro Zamora-Pérez. *Economic, financial and monetary developments*. ECB Economic Bulletin 5. ECB, 2025. URL: https://www.ecb.europa.eu/pub/economic-bulletin/html/index.en.html (visited on 09/17/2025).

# References III


[DKM24] Alberto Di Iorio et al. *Embracing Diversity, Advancing Together - Results of the 2023 BIS Survey on Central Bank Digital Currencies and Crypto*. BIS Papers no 147. Basel: Bank for International Settlements, 2024. ISBN: 978-92-9259-770-2. URL: https://www.bis.org/publ/bppdf/bispap147.pdf.

[DU23] Kun Duan and Andrew Urquhart. "The instability of stablecoins". In: *Finance Research Letters* 52 (2023), p. 103573.

[Fin25] 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/Fatf-recommendations/Fatf-recommendations.html.

[Jed16] Tom Elvis Jedusor. *MimbleWimble*. White Paper. 2016. URL: https://docs.beam.mw/Mimblewimble.pdf (visited on 09/17/2025).

# References IV


[KAN20] Kurt M. Koe et al. *Zero to Monero: Second Edition*. 2020. URL: https://www.getmonero.org/library/Zero-to-Monero-2-0-0.pdf (visited on 09/17/2025).

[KKS22] Aggelos Kiayias et al. “PEReDi: Privacy-Enhanced, Regulated and Distributed Central Bank Digital Currencies”. In: *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security, CCS 2022, Los Angeles, CA, USA, November 7-11, 2022*. Ed. by Heng Yin et al. ACM, 2022, pp. 1739–1752. DOI: 10.1145/3548606.3560707. URL: https://doi.org/10.1145/3548606.3560707 (visited on 09/17/2025).

[KPPO24] Pablo Trigo Kramcsák et al. “Untangling Digital Euro’s Personal Data Protection Challenges: An Exploration of Data Processing Activities and Latent Privacy Risks”. 2024. URL: https://www.eba.europa.eu/sites/default/files/2024-12/bb883c9c-1b54-4bb6-b489-aacaedc351b5/session_5_paper_1_andres_chomcyk_penedo.pdf.

# References V


[LSSS20] Alexander Lipton et al. “From tether to Libra: Stablecoins, digital currency and the future of money”. In: *arXiv* (2020). URL: https://arxiv.org/abs/2005.12949 (visited on 09/17/2025).

[Max13] Greg Maxwell. *CoinJoin: Bitcoin Privacy for the Real World*. 2013. URL: https://bitcointalk.org/index.php?topic=279249 (visited on 09/17/2025).

[Nak08] Satoshi Nakamoto. *Bitcoin: A Peer-to-Peer Electronic Cash System*. Whitepaper. 2008. URL: http://bitcoin.org/bitcoin.pdf.

[OBC23] Denise Garcia Ocampo et al. *Crypto, Tokens and DeFi: Navigating the Regulatory Landscape*. FSI Insights on Policy Implementation no 49. Basel: Bank for International Settlements, Financial Stability Institute, 2023. ISBN: 978-92-9259-656-9. URL: https://www.bis.org/fsi/publ/insights49.pdf.

[Peo21] People’s Bank of China. *Digital Currency Electronic Payment (DCEP): China’s Central Bank Digital Currency*. Official central bank digital currency with comprehensive user identification and KYC procedures. 2021. URL: http://www.pbc.gov.cn.

# References VI


[PSS19] Alexey Pertsev et al. *Tornado.Cash Privacy Solution*. Whitepaper. 2019. URL: https://berkeley-defi.github.io/assets/material/Tornado%5C%20Cash%5C%20Whitepaper.pdf.

[Sab13] Nicolas van Saberhagen. *CryptoNote v2.0 (Annotated)*. Monero Research Lab, GetMonero.org. 2013. URL: https://www.getmonero.org/resources/research-lab/pubs/whitepaper_annotated.pdf (visited on 09/17/2025).

[SE24] 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 (visited on 09/17/2025).

[Tom+22] Alin Tomescu et al. *UTT: Decentralized Ecash with Accountable Privacy*. Cryptology ePrint Archive, Paper 2022/452. 2022. URL: https://eprint.iacr.org/2022/452 (visited on 09/17/2025).

# References VII


[Tre22] 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 09/17/2025).

[WKCC19] Karl Wüst et al. “PRCash: Fast, Private and Regulated Transactions for Digital Currencies”. In: *Financial Cryptography and Data Security - 23rd International Conference, FC 2019, Frigate Bay, St. Kitts and Nevis, February 18-22, 2019, Revised Selected Papers*. Ed. by Ian Goldberg and Tyler Moore. Vol. 11598. Lecture Notes in Computer Science. Springer, 2019, pp. 158–178. DOI: 10.1007/978-3-030-32101-7_11. URL: https://doi.org/10.1007/978-3-030-32101-7_11 (visited on 09/17/2025).

# Asymmetric Privacy: Sender vs. Receiver

**Chaumian eCash and Tourbillon project [BIS23]**

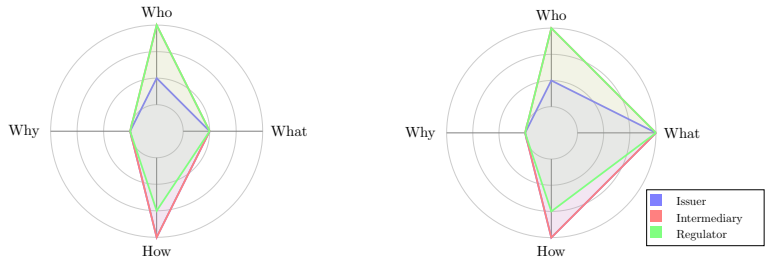



Figure: Sender (left) enjoys untraceability and unlinkability. Receiver (right) has reduced protections

- **Blind signatures** unlink withdrawals from spending
- **Sender:** Strong protection (Level 2 on *What*)
- **Receiver:** Must present coins for deposit (Level 3 on *What*)
- **Result:** Compliance monitoring at receipt points

# Targeted Exposure: View Keys

**Retrospective investigation without blanket surveillance**

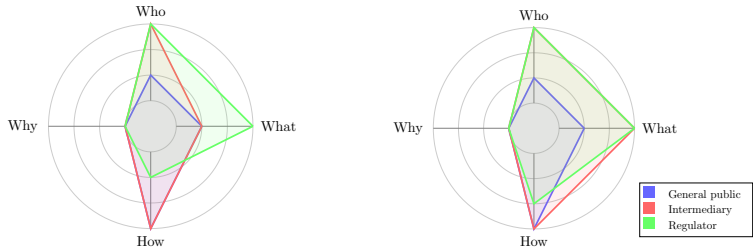



Figure: User cooperation (left) vs. intermediary control (right)

- **Two keypairs:** Spend key (transfer funds) + view key (decrypt values)
- **Governance model 1:** Users hand over view keys under legal mandate
- **Governance model 2:** Intermediaries obtain view keys during KYC
- **Trade-off:** User autonomy vs. regulatory enforceability

# Asymmetric Privacy: Offline vs. Online

**Context-dependent privacy guarantees [CMGS22; SE24]**

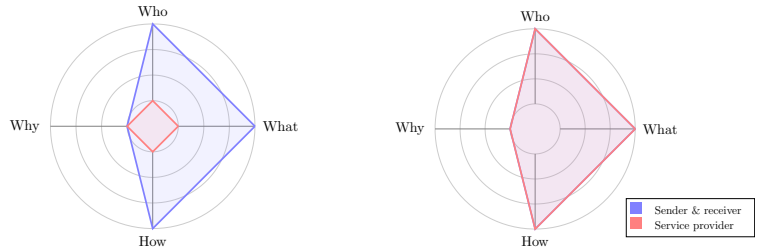



Figure: Offline (left) provides full anonymity. Online (right) requires identification

- **Offline:** Complete anonymity, no institutional disclosure
- **Online:** Full identification, automatic processing
- **Settlement:** Users reconnect, lose anonymity but retain transaction untraceability
- **Physical proximity** limits scale vs. global online networks

# Mediated Privacy: Split Visibility

## Compartmentalized institutional access

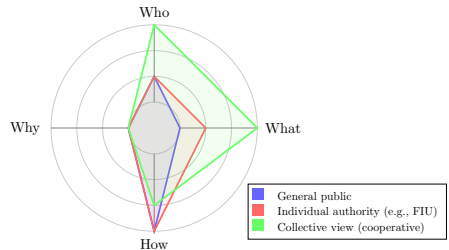



Figure: Different authorities see different fragments; no single complete view

- **FIU:** Observes pseudonymous flows, AML compliance proofs (no identities)
- **IVA:** Maintains KYC mappings (no transaction amounts)
- **Tax authority:** Receives aggregate values (no individual transfers)
- **Result:** Institutional checks and balances, prevents complete surveillance

# Regulating Public Ledgers

## Privacy mechanisms in permissionless systems

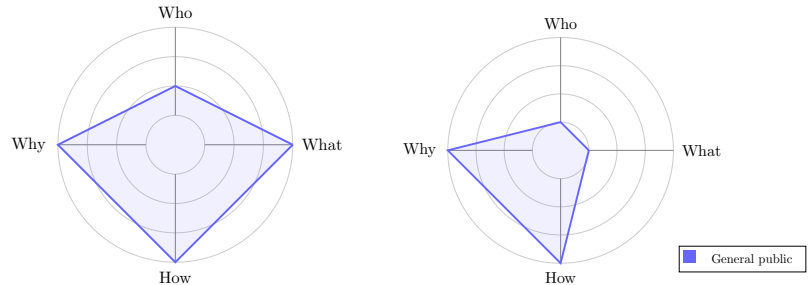



Figure: Bitcoin [Nak08] (left): transparent. Monero [KAN20] (right): privacy-preserving by default

- **Challenge:** No centralized control, prioritize censorship resistance
- **Approaches:** Regulated mixers [Max13] (KYC at access points), compliance proofs for Tornado Cash [PSS19; BINSS23], view key requirements for privacy coins