Scientific Report on the PriCLeSS Project

Davide Frey and Sandrine Turgis

1 Project overview and objectives

The PriCLeSS project studied how decentralized storage and blockchain technologies can be made privacy-conscious, legally sound, and scalable. Coordinated by Davide Frey and Sandrine Turgis, it brought together distributed computing, blockchain and storage systems, Byzantine fault tolerance, privacy-preserving abstractions, and legal analysis of data protection and fundamental rights. The project started from a concrete tension. Blockchains provide decentralization, auditability, immutability, and resilience to Byzantine failures; yet these same properties can conflict with data minimization, purpose limitation, rectification, erasure, consent, accountability, and the possibility of limiting the circulation of personal data.

PriCLeSS therefore pursued two connected objectives. The first was to identify the legal and technical risks created when distributed ledgers are used to store, coordinate, or certify personal data. The second was to determine whether applications usually implemented on blockchains really require global replication and total ordering, or whether weaker and more localized abstractions can provide the necessary safety properties. This dual objective shaped the whole project: legal constraints were treated as design constraints, and distributed algorithms were evaluated not only for performance and fault tolerance but also for their potential to reduce exposure, replication, and unnecessary synchronization.

2 Scientific contributions

Legal challenges as the starting point. PriCLeSS began from the observation that blockchain architectures are legally ambivalent. Their replication, immutability, transparency, and distributed governance can support integrity and accountability, but they also create tensions with data minimization, purpose limitation, rectification, erasure, consent, and responsibility. The two combined legal and technical chapters on data-protection challenges and solutions for distributed ledgers [1, 2] made this tension the starting point for the project. They showed that compliance cannot be added after the architecture is chosen: decisions about what is stored on chain, what remains off chain, who replicates which data, and which mechanisms allow revocation or correction directly shape the legal status of the system. Sandrine Turgis's 2023 Berkman Klein Center presentation further framed blockchain as a technology with strong ambivalences for fundamental rights and data protection [3].

Reducing exposure: sharding, QAAT, and hidden issuers. The technical work then asked how architectures could reduce exposure while preserving decentralized guarantees. Work on sharding in permissionless systems under an adaptive adversary [4, 5] studied how to avoid full replication without letting an adversary concentrate corrupt nodes in a shard. This connects scalability and privacy: limiting replication can reduce data circulation, but only if the resulting system remains secure against realistic adversaries. QAAT, an asynchronous Byzantine-tolerant asset transfer preprint currently under review, pursued the same objective for cryptocurrency-like systems by combining quasi-anonymity, light local storage, and operation without consensus [6]. SplitChain and QAAT were the main outcomes of Arthur Rauch's PriCLeSS-funded PhD thesis [7]. In parallel, Hidden-Issuer Anonymous Credentials [8] addressed the privacy risk created when a

credential reveals not only its holder but also its issuer. Hiding the issuer is important in identity and access-control settings, where the issuer can itself reveal sensitive information. The work introduced a cryptographic aggregator primitive, which makes it possible to prove set membership without revealing the element and while knowing only a commitment to it. These results illustrate a first PriCLeSS design principle: decentralized systems should expose the minimum amount of information needed for their function.

Weaker synchronization and distributed objects. The next step was to determine whether blockchain applications really need global consensus. The DISC 2023 work on allowlist and denylist objects formalized access control as a distributed object and characterized its synchronization power [9]. The allowlist has consensus number 1 and can be implemented with reliable broadcast. The denylist requires agreement because of its anti-flickering and auditability properties, but only among the processes that can verify membership. This result replaces a binary "blockchain or no blockchain" question with a more precise one: which parties must synchronize for this object to be safe? In the self-sovereign identity setting, this analysis showed that revocation and multi-device support are the operations that require consensus-like coordination, and that even there the agreement can remain localized rather than imposed at the network level.

This question also motivated the PriCLeSS work involving Matthieu Perrin and Achour Mostefaoui on the foundations of distributed objects. With Mathilde Déprés and Michel Raynal, they compared send/receive patterns with read/write patterns in crash-prone asynchronous systems and identified the MB-Broadcast abstraction as a way to express, in message-passing terms, coordination patterns usually captured through shared-memory objects [10, 11]. This contribution is important for PriCLeSS because it gives a language for replacing a ledger by a more precise object specification: instead of assuming a replicated chain, one can ask which communication pattern implements the object and which failures it tolerates. A second line of work, with Vincent Kowalski, studied atomic-register abstractions for Byzantine-prone distributed systems [12]. The register perspective is close to privacy-conscious storage: it separates the logical guarantees expected from a storage object from the heavy machinery of a blockchain, and it makes explicit which safety, liveness, and auditability properties must survive Byzantine behavior. Related technical reports on Causal Mutual Byzantine Broadcast [13] and privacy-preserving Byzantine-tolerant registers [14] extend the same agenda. Together, these results provide alternatives to full ledgers for systems that need auditability and resilience but not universal total ordering.

Broadcast foundations and contention-aware cooperation. Once the project had identified weaker objects, it studied the communication foundations needed to implement them. Byzantine reliable broadcast can replace consensus in several ledger-like applications, including money transfer [15]. PriCLeSS studied reliable broadcast under message adversaries, which model silent churn and the suppression of some messages in addition to Byzantine process failures. This line of work was among the first to use message-adversary reasoning in a fully asynchronous Byzantine setting, thereby connecting peer-to-peer churn with the theory of reliable communication. The project established a tight condition for signature-based Byzantine reliable broadcast with t Byzantine nodes and d suppressed copies of each message, namely $n > 3t + 2d$ [16, 17]; improved communication under message adversaries [18, 19]; introduced a modular signature-free construction based on $k2l$-cast [20]; and optimized good-case early stopping in synchronous Byzantine broadcast [21]. These results have also fed back into work on early stopping, optimistic execution under malicious majorities, and causal ordering properties of reliable broadcast. PriCLeSS also funded Contention-Aware Cooperation (CAC), a novel abstraction published at OPODIS 2025 [22], which lies between reliable broadcast and consensus by adapting cooperation to the actual level of contention in a run. CAC separates the fast-path intuition of optimistic agreement from full consensus: when few processes propose conflicting values, the abstraction can identify and resolve the limited contention while preserving Byzantine fault tolerance. This is especially relevant for PriCLeSS because many privacy-sensitive applications are not continuously contested by all participants. CAC makes

explicit a second PriCLeSS design principle: synchronization should be paid for when conflicts make it necessary, not imposed as a default.

Legal deepening and emerging applications. In parallel, IODE complemented the initial privacy analysis through Damien Franchi's PhD thesis, *Privacy et blockchain : enjeux et encadrement juridique*, prepared at the University of Rennes/IODE under the joint supervision of Brunessen Bertrand and Sandrine Turgis, funded equally by Labex CominLabs and a doctoral contract, and defended on 10 November 2025 [23]. During his thesis, Damien had close interactions with Arthur Rauch, which informed each other's work and made the two doctoral projects a technical/legal dialogue on privacy-conscious blockchain architectures. Damien's thesis studied the articulation between blockchain and privacy, the transformation of legal categories by decentralized technologies, and the conditions under which blockchain mechanisms can be reconciled with European data-protection law. The project also opened a broader ethical line of analysis through work on Layer-2 rollups, which applies ethical risk analysis to operator and governance choices, information asymmetries, and the allocation of risks to users [24]. This work extends the PriCLeSS method beyond data protection alone: it asks who benefits from architectural choices, who controls them, who bears the risk when assumptions fail, and whether users have meaningful information or recourse. Finally, WIDE and IODE are finalizing a joint paper on the privacy implications of blockchain technology in refugee camp management, building on earlier PriCLeSS discussions of blockchain for refugees and humanitarian accountability. This ongoing work brings the project back to one of its core motivations: assessing blockchain not as an abstract infrastructure, but as a socio-technical system whose design choices affect vulnerable people, legal responsibility, and fundamental rights.

3 Interdisciplinary integration, training, and dissemination

PriCLeSS was designed as an interdisciplinary project rather than as a collection of parallel publications. Its scientific progression moved from legal diagnosis to architectural and algorithmic responses, and then back to legal and ethical evaluation of concrete blockchain uses. The technical results identify alternatives to full blockchain infrastructures; the legal work explains why such alternatives matter for rights, accountability, and compliance. For example, the analysis of sharding, hidden issuers, allowlists, denylists, and privacy-preserving registers gives technical form to legal principles such as minimization and proportionality. Conversely, the legal analysis prevented the technical work from treating privacy as a purely cryptographic property: it emphasized governance, qualification of actors, legal responsibility, data-subject rights, and the limits of immutability.

Training and dissemination were major outcomes. The project supported Damien Franchi's doctoral work and created several venues for exchange between computer scientists, legal scholars, and policy-oriented audiences. These included the *Blockchain & Privacy Conference* in Rennes on 13 May 2022, organized by Brunessen Bertrand and Sandrine Turgis; the international workshop *Privacy-Conscious Legally-Sound Blockchain Storage* in Rennes on 9 September 2024, organized by Davide Frey and Sandrine Turgis; and the webinar *Blockchain & Protection de la Privacy* on 23 June 2025, organized by Thomas Cassuto and Sandrine Turgis. The project was also presented at the AFEE congress in Paris Saclay on 10–11 June 2021, at the 2022 Rennes colloquium, at the Berkman Klein Center on 22 May 2023, at CominLabs Days in Rennes on 26 September 2023, and in legal and interdisciplinary workshops including the 2023 PriCLeSS session on blockchain for refugees and the 2024 and 2025 events involving Damien Franchi and Sandrine Turgis.

The edited volume *Blockchain et protection de la Privacy*, published by Larcier in Brussels in 2025 under the direction of Brunessen Bertrand and Sandrine Turgis, provided a systemic legal analysis of blockchain, privacy, European data-protection law, digital sovereignty, disintermediation, and the transformation of legal categories [25]. It treated blockchain not only as a technical tool or a GDPR-compliance problem, but also as a testing ground for contemporary changes in privacy regulation and for the capacity of European law to regulate global, distributed infrastructures.

Written outputs by Brunessen Bertrand, Sandrine Turgis, and Damien Franchi further disseminated these results to legal audiences [26, 27, 28]. International presentations, the Rennes workshops, the Harvard/Berkman-Klein talk, the 2025 edited book, and the follow-up opportunities created by these activities increased the visibility of the Rennes-based collaboration and positioned PriCLeSS within a wider international discussion on blockchain, privacy, data protection, and humanitarian uses of decentralized technologies.

4 Main outcomes and legacy

The main outcome of PriCLeSS is a coherent interdisciplinary argument: the legal challenges of blockchain storage should guide the technical architecture from the beginning. Decentralization need not imply global replication, permanent exposure, or universal total ordering. Many applications require only partial, localized, or conflict-dependent coordination. By moving from data-protection constraints to sharding, privacy-preserving identity, weaker synchronization, broadcast abstractions, and ethical analysis of deployed systems, PriCLeSS produced a framework for designing decentralized systems that are resilient, scalable, and more compatible with data protection.

The project's legacy is therefore both technical and legal. Technically, it contributed sharding analyses, quasi-anonymous asset transfer, hidden-issuer credentials, weaker synchronization results, register abstractions, broadcast algorithms, and CAC. Legally and ethically, it produced doctoral training, book chapters, an edited volume, conference and webinar programs, analysis of Layer-2 rollup risks, and a continuing WIDE-IODE collaboration on blockchain in refugee camp management. The technical outputs also had external impact: HIAC informed subsequent work on issuer-hiding credentials, while the AllowList/DenyList analysis contributed to a broader algorithmic discussion on auditable registers. Together, these results support future work on consensus-free self-sovereign identity, privacy-preserving access control, auditable but non-invasive registers, and decentralized storage systems in which the architecture is designed from the outset around both fault tolerance and legal accountability.

Compact list of main outputs.

1. D. Fabčič Povše et al., Springer, 2023 [1, 2].
2. E. Anceaume, D. Frey, and A. Rauch, SplitChain, sharding technical report and follow-up publications [4, 5].
3. T. Albouy et al., QAAT preprint under review [6].
4. A. Rauch, PhD thesis funded by PriCLeSS, with SplitChain and QAAT as main outcomes [7].
5. D. Bosk, D. Frey, M. Gestin, and G. Piolle, hidden-issuer credentials [8].
6. D. Frey, M. Gestin, and M. Raynal, DISC 2023 [9].
7. M. Déprés, A. Mostefaoui, M. Perrin, and M. Raynal, DISC 2023 [10].
8. M. Déprés et al., MB-Broadcast technical report, 2023 [11].
9. M. Féry et al., Causal Mutual Byzantine Broadcast technical report, 2023 [13].
10. Q. Gomes dos Reis et al., privacy-preserving Byzantine register technical report, 2023 [14].
11. V. Kowalski, A. Mostéfaoui, and M. Perrin, atomic-register technical report, 2023 [12].
12. T. Albouy, D. Frey, M. Raynal, and F. Taïani, DISC 2022 and OPODIS 2022 [21, 20].
13. T. Albouy, D. Frey, M. Gestin, M. Raynal, and F. Taïani, CAC, OPODIS 2025 [22].
14. S. Turgis, Berkman Klein Center presentation, 2023 [3].
15. IODE legal outputs, including D. Franchi's thesis and the 2025 edited book [23, 25].
16. G. Ishmaev, E. Anceaume, D. Frey, and F. Taïani, ethical analysis of L2 rollups [24].
17. WIDE and IODE, paper in preparation on blockchain, privacy, and refugee camp management.

References

[1] D. Fabčič Povše, A. Favenza, D. Frey, Z. Á. Mann, A. Palomares, L. Piatti, and J. Schroers. "Data Protection Challenges in Distributed Ledger Technologies: A Combined Legal and Technical Analysis".

In: *Building Cybersecurity Applications with Blockchain and Smart Contracts*. Springer, 2023, pp. 127–155.

[2] D. Fabčič Povše, A. Favenza, D. Frey, Z. Á. Mann, A. Palomares, L. Piatti, and J. Schroers. "Solutions to Data Protection Challenges in Distributed Ledger and Blockchain Technologies: A Combined Legal and Technical Approach". In: *Building Cybersecurity Applications with Blockchain and Smart Contracts*. Springer, 2023, pp. 153–181.

[3] S. Turgis. *Blockchain, as a Technological Tool with Strong Ambivalences for Fundamental Rights and Especially Data Protection*. Berkman Klein Center for Internet and Society, Harvard University. May 22, 2023.

[4] E. Anceaume, D. Frey, and A. Rauch. *Sharding in Permissionless Systems in Presence of an Adaptive Adversary*. Tech. rep. 2023.

[5] E. Anceaume, D. Frey, and A. Rauch. "Sharding in Permissionless Systems in Presence of an Adaptive Adversary". In: *Networked Systems – 12th International Conference, NETYS 2024*. Vol. 14783. Lecture Notes in Computer Science. Springer, 2024, pp. 1–31.

[6] T. Albouy, E. Anceaume, D. Frey, M. Gestin, A. Rauch, M. Raynal, and F. Taïani. "Asynchronous BFT Asset Transfer: Quasi-Anonymous, Light, and Consensus-Free". Preprint under review. 2024. arXiv: 2405.18072 [cs.DC]. URL: https://arxiv.org/abs/2405.18072.

[7] A. Rauch. "PhD thesis funded by PriCLeSS". PhD thesis. University of Rennes. URL: https://theses.fr/s300188.

[8] D. Bosk, D. Frey, M. Gestin, and G. Piolle. "Hidden Issuer Anonymous Credential". In: *Proceedings on Privacy Enhancing Technologies* 2022 (2022), pp. 571–607. DOI: 10.56553/popets-2022-0123.

[9] D. Frey, M. Gestin, and M. Raynal. "The Synchronization Power (Consensus Number) of Access-Control Objects: The Case of AllowList and DenyList". In: *DISC 2023*. 2023.

[10] M. Déprés, A. Mostefaoui, M. Perrin, and M. Raynal. "Send/Receive Patterns versus Read/Write Patterns in Crash-Prone Asynchronous Distributed Systems". In: *DISC 2023*. 2023.

[11] M. Déprés, A. Mostefaoui, M. Perrin, and M. Raynal. *Send/Receive Patterns versus Read/Write Patterns: The MB-Broadcast Abstraction*. Tech. rep. 2023.

[12] V. Kowalski, A. Mostéfaoui, and M. Perrin. *Atomic Register Abstractions for Byzantine-Prone Distributed Systems*. Tech. rep. 2023.

[13] M. Féry et al. *Causal Mutual Byzantine Broadcast*. Tech. rep. 2023.

[14] Q. Gomes dos Reis et al. *Registre atomique préservant la vie privée tolérant aux byzantins*. Tech. rep. 2023.

[15] A. Auvolat, D. Frey, M. Raynal, and F. Taïani. "Money Transfer Made Simple: A Specification, a Generic Algorithm, and Its Proof". In: *Bulletin of the EATCS* 132 (2020), pp. 21–44.

[16] T. Albouy, D. Frey, M. Raynal, and F. Taïani. "Byzantine-Tolerant Reliable Broadcast in the Presence of Silent Churn". In: *SSS 2021*. Invited paper. 2021.

[17] T. Albouy, D. Frey, M. Raynal, and F. Taïani. "Asynchronous Byzantine Reliable Broadcast with a Message Adversary". In: *Theoretical Computer Science* 978 (2023).

[18] T. Albouy, D. Frey, R. Gelles, C. Hazay, M. Raynal, E. M. Schiller, F. Taïani, and V. Zikas. "Brief Announcement: Towards Optimal Communication Byzantine Reliable Broadcast under a Message Adversary". In: *DISC 2024*. Vol. 319. Leibniz International Proceedings in Informatics (LIPIcs). 2024, 41:1–41:7.

[19] T. Albouy, D. Frey, R. Gelles, C. Hazay, M. Raynal, E. M. Schiller, F. Taïani, and V. Zikas. "Near-Optimal Communication Byzantine Reliable Broadcast under a Message Adversary". In: *OPODIS 2024*. Vol. 324. Leibniz International Proceedings in Informatics (LIPIcs). 2025, 14:1–14:29.

[20] T. Albouy, D. Frey, M. Raynal, and F. Taïani. "A Modular Approach to Construct Signature-Free BRB Algorithms under a Message Adversary". In: *OPODIS 2022*. Vol. 253. Leibniz International Proceedings in Informatics (LIPIcs). 2022.

[21] T. Albouy, D. Frey, M. Raynal, and F. Taïani. "Good-Case Early-Stopping Latency of Synchronous Byzantine Reliable Broadcast: The Deterministic Case". In: *DISC 2022*. Vol. 246. Leibniz International Proceedings in Informatics (LIPIcs). 2022, 4:1–4:22.

[22] T. Albouy, D. Frey, M. Gestin, M. Raynal, and F. Taïani. “Contention-Aware Cooperation”. In: *29th International Conference on Principles of Distributed Systems (OPODIS 2025)*. Vol. 361. Leibniz International Proceedings in Informatics (LIPIcs). Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2025, 9:1–9:25.

[23] D. Franchi. “Privacy et blockchain : enjeux et encadrement juridique”. Co-supervised by Brunessen Bertrand and Sandrine Turgis; defended 10 November 2025. PhD thesis. University of Rennes/IODE, Nov. 10, 2025.

[24] G. Ishmaev, E. Anceaume, D. Frey, and F. Taïani. “Ethical Risk Analysis of L2 Rollups”. Preprint. 2025.

[25] B. Bertrand and S. Turgis, eds. *Blockchain et protection de la Privacy.* Brussels: Larcier, 2025.

[26] B. Bertrand and S. Turgis. “Les paradoxes de la Blockchain et de la Privacy”. In: *Blockchain et protection de la Privacy.* Larcier, 2025.

[27] D. Franchi. *Les enjeux de l’articulation entre Blockchain et Privacy.* Institut Presaje. 2025.

[28] S. Turgis. *Propos introductifs : les paradoxes de la Blockchain pour la Privacy.* Institut Presaje. 2025.