Scientific Report on the SplitChain PoC

Davide Frey and Sandrine Turgis

1 Project overview and objectives

The SplitChain PoC was conceived as the proof-of-concept follow-up to PriCLeSS. PriCLeSS had established the central scientific question: how can decentralized storage and blockchain systems be made compatible with privacy, data-protection law, and fundamental rights? SplitChain turned this question into an implementation-oriented research agenda. Its goal was to move from the legal and algorithmic analysis developed in PriCLeSS to a prototype of a blockchain architecture in which data can be stored according to legal, geographical, or administrative constraints without abandoning decentralization and Byzantine resilience.

The starting point is the same tension that motivated PriCLeSS. Public blockchains are global, replicated, append-only infrastructures, whereas legal obligations are often territorial, contextual, and actor-specific. In particular, the GDPR and related European and French legal frameworks require attention to data minimization, purpose limitation, erasure, rectification, consent, and cross-border transfers. A conventional blockchain makes all nodes store all data, possibly across jurisdictions, and therefore offers very little control over where personal data is replicated. SplitChain addresses this problem by designing a sharded blockchain in which the storage of data can be constrained, while the validation of transactions remains decentralized and secure.

2 Scientific and technical contributions

From PriCLeSS to SplitChain. PriCLeSS produced both the legal diagnosis and the technical foundations on which SplitChain builds. The legal chapters on data-protection challenges and solutions for distributed ledgers showed that compliance depends on architectural choices such as on-chain versus off-chain storage, replication, revocation, and governance [1, 2]. The technical work on sharding under adaptive adversaries then provided the core SplitChain result [3, 4]. SplitChain was one of the main outcomes of Arthur Rauch's PriCLeSS-funded PhD thesis, together with QAAT, an asynchronous Byzantine-tolerant asset transfer protocol currently under review [5, 6]. The PoC was designed to turn this body of work into software.

Sharding without a synchronization blockchain. SplitChain is a decentralized state-sharding architecture for account-based blockchains. Its first contribution is to decouple the permanent storage of transactions and associated data from the execution of consensus. Existing sharded blockchains often rely on a global synchronization chain or other heavy coordination mechanisms. SplitChain instead lets shards progress at their own pace and disseminates only the ephemeral information needed by other shards. This design directly serves the privacy and legal objective: data can be assigned to shards according to an allocation policy, including jurisdictional or administrative constraints, while validators are not permanently tied to the data they help validate.

Validator allocation and adaptive security. The main technical difficulty is that sharding reduces replication and therefore makes individual shards easier targets for an adaptive adversary. SplitChain addresses this by using two levels of indirection to allocate validators to consensus committees in random shards. The purpose of this indirection is to make committee composition

difficult to bias while preserving decentralization. SplitChain also organizes inter-shard communication through a hypercube-inspired topology and a Byzantine-tolerant routing mechanism. This allows shards to exchange the information necessary for cross-shard operations without falling back to a global ledger.

Dynamic sharding and load adaptation. SplitChain further supports a dynamic number of shards. When a shard is overloaded, it can split into two shards, each taking over part of the account space. When shards are underloaded, they can merge so that validator resources are not wasted. This adaptive split/merge mechanism is important for two reasons. First, it supports scalability by letting the system follow the workload. Second, it supports security by making the distribution of validation stake more efficient: merging underloaded shards may free enough stake for another shard to split safely.

SplitChain2: legal constraints as placement constraints. The PoC also introduced the implementation objective called SplitChain2 [7]. SplitChain2 augments the original design with the ability to enforce geographical or administrative constraints on data placement. In the PoC narrative, this is the key bridge between the legal and technical parts of the project. The legal problem is not only that blockchains replicate too much data, but that they replicate it without regard to the legal status of the data, the location of the nodes, or the responsibilities of the actors. SplitChain2 translates this problem into a systems objective: the placement of data must be controlled, while the validation process must remain decentralized, randomized, and resilient.

3 Engineering outcomes

SplitChain implementation. The PoC funded an engineering position on "GDPR-Compliant Sharded Blockchain" [7]. Olivier Deloubrier was hired on this fully PoC-funded position to start the implementation of SplitChain. The advertised roadmap moved from state-of-the-art analysis and high-level design to the implementation of an intra-shard consensus algorithm [8] and of a single-shard version of SplitChain. This engineering work is the main practical outcome of the PoC: it transformed the algorithmic design into a software artifact. The PoC was not sufficient to implement the full SplitChain functionality; we therefore plan to continue development by applying for additional funding.

CAC and blockchain-free identity. The PoC also partially funded the engineering position on "Blockchain-Free Self-Sovereign Identity" [9]. Elie Raspaud was hired on this position and implemented Contention-Aware Cooperation (CAC), the PriCLeSS-funded abstraction later published at OPODIS 2025 [10]. The CAC implementation is complete. It will support a systems paper on CAC and will also be used to complete the implementation of a blockchain-free identity management system. This second engineering strand is not a separate topic from SplitChain: both efforts explore the same architectural principle inherited from PriCLeSS, namely that applications should use the weakest coordination mechanism compatible with their safety requirements. SplitChain applies this principle to sharded blockchain storage; CAC and blockchain-free SSI apply it to access-control and identity management [11, 12].

Implementation and transfer perspective. The SplitChain proposal requested 104K euros: 84K euros for the recruited engineer and 20K euros for dissemination, including a workshop to present and disseminate the results [13]. The implementation was expected to support experimentation, performance assessment, and a future systems publication. It was also intended as a basis for longer-term work on decentralized storage and possible technology transfer. The current plan is to continue SplitChain development with future funding, using the PoC implementation as the starting point for a more complete platform and for further validation of the legal and systems assumptions.

4 Interdisciplinary integration and dissemination

The SplitChain PoC preserved the interdisciplinary structure of PriCLeSS. The technical work was carried out by WIDE and CIDRE around distributed systems, sharding, Byzantine resilience, routing, and implementation. The legal work involved IODE researchers and focused on the way blockchain architectures interact with privacy, international and comparative law, digital sovereignty, and humanitarian accountability. This integration reflects the fact that SplitChain does not merely provide scalability. Rather, sharding can become a privacy-conscious and legally relevant architectural mechanism when data placement is treated as a first-class design constraint.

The PoC also funded the 2023 international workshop on *Blockchain & Privacy: International and Comparative Law* organized by Brunessen Bertrand and Sandrine Turgis in Pointe-à-Pitre on 16 November 2023 [14]. Brunessen Bertrand, Sandrine Turgis, and Dayoung Jeong also organized the international workshop *Blockchain, Artificial Intelligence and Digital Sovereignty in Dialogue* at the French Embassy in Seoul, South Korea, on 12 December 2025 [15]. These events extended the legal and interdisciplinary visibility of the project beyond Rennes and helped connect the technical work on privacy-conscious blockchain architectures with comparative law and digital-sovereignty debates.

Several presentations supported this dissemination. At the SplitChain-funded workshop *Blockchain & Privacy: International and Comparative Law*, Brunessen Bertrand and Sandrine Turgis gave an introductory address [16], Damien Franchi presented work on self-sovereign identity and privacy from a compliance perspective [17, 18], Sandrine Turgis presented the ambivalence of blockchain from a fundamental-rights perspective [19], and Davide Frey presented his work on the challenges of applying the GDPR to blockchain systems and the associated possible solutions [20, 1, 2]. At the 2025 Seoul workshop, Brunessen Bertrand addressed operational data ethics, Damien Franchi discussed convergences between blockchain and artificial intelligence for data traceability, and Sandrine Turgis presented blockchain for humanitarian accountability [21, 22, 23]. This international visibility also led to further invitations abroad, including at the Institute for Technology and Society of Rio de Janeiro and at the Universidad de Lima [24].

5 Main outcomes and legacy

The SplitChain PoC produced four main outcomes. First, it consolidated SplitChain as the technical continuation of PriCLeSS: a sharded blockchain architecture designed to reduce replication, preserve Byzantine security, and make legally constrained data placement possible. Second, it moved the work from theory toward implementation by funding the engineering effort that started the SplitChain prototype. Third, it strengthened the low-synchronization line of work by partially funding the engineering effort that completed the CAC implementation and supports future work on blockchain-free identity management. Finally, it supported dissemination of scientific results to a large community of computer-science and legal scholars.

The scientific legacy of the PoC is therefore broader than a single prototype. It links several strands of the PriCLeSS agenda: sharding as a way to reduce exposure, QAAT as quasi-anonymous and light asset transfer, CAC as contention-dependent cooperation, and legal analysis as the framework that explains why these technical choices matter. The project also created a concrete bridge between doctoral research, engineering, and international legal dissemination. Its next step is to continue development and validation of SplitChain with future funding, while using the CAC implementation to prepare a systems paper and to complete a blockchain-free identity management platform.

Compact list of main outputs.

1. SplitChain PoC proposal and implementation roadmap [13].
2. E. Anceaume, D. Frey, and A. Rauch, SplitChain technical report and follow-up publications [3, 4].
3. T. Albouy et al., QAAT preprint under review [5].

4. A. Rauch, PhD thesis funded by PriCLeSS, with SplitChain and QAAT as main outcomes [6].
5. Olivier Deloubrier's PoC-funded engineering work on SplitChain/SplitChain2 [7].
6. Elie Raspaud's partially PoC-funded implementation of CAC and blockchain-free SSI components [9].
7. T. Albouy, D. Frey, M. Gestin, M. Raynal, and F. Taïani, CAC, OPODIS 2025 [10].
8. D. Frey, M. Gestin, and M. Raynal, synchronization power of access-control objects [11].
9. IODE SplitChain-specific events and international visibility [14, 15, 24].

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] E. Anceaume, D. Frey, and A. Rauch. "Sharding in Permissionless Systems in Presence of an Adaptive Adversary". In: *SIROCCO*. Brief announcement. 2024.

[4] 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.

[5] 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.

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

[7] Inria. *GDPR-Compliant Sharded Blockchain*. Engineering position offer no. 2023-06904. 2023.

[8] G. Saunois, F. Robin, E. Anceaume, and B. Sericola. "Permissionless Consensus Based on Proof-of-Eligibility". In: *NCA 2020 – 19th IEEE International Symposium on Network Computing and Applications*. 2020. URL: https://hal.archives-ouvertes.fr/hal-03043681.

[9] Inria. *Blockchain-Free Self-Sovereign Identity*. Engineering position offer no. 2023-06905. 2023.

[10] 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.

[11] 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.

[12] 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.

[13] D. Frey and S. Turgis. *PriCLeSS-PoC: Privacy-Conscious Legally-Sound Blockchain Storage Proof-of-Concept*. CominLabs PoC proposal. 2023.

[14] B. Bertrand and S. Turgis. *Blockchain & Privacy: International and Comparative Law*. International workshop, Pointe-à-Pitre, Guadeloupe. Nov. 16, 2023.

[15] B. Bertrand, S. Turgis, and D. Jeong. *Blockchain, Artificial Intelligence and Digital Sovereignty in Dialogue*. International workshop, French Embassy, Seoul, South Korea. Dec. 12, 2025.

[16] B. Bertrand and S. Turgis. *Rapport introductif*. International workshop *Blockchain & Privacy: International and Comparative Law*, Pointe-à-Pitre, Guadeloupe. Nov. 16, 2023.

[17] D. Franchi. *Self-Sovereign Identity and Privacy: For a More Compliant Approach on the Blockchain?* International workshop *Blockchain & Privacy: International and Comparative Law*, Pointe-à-Pitre, Guadeloupe. Nov. 16, 2023.

[18] 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.

[19] S. Turgis. *The Ambivalence of Blockchain from a Fundamental Rights Perspective*. International workshop *Blockchain & Privacy: International and Comparative Law*, Pointe-à-Pitre, Guadeloupe. Nov. 16, 2023.

[20] D. Frey. *Blockchain and GDPR: Challenges and Technical Solutions*. International workshop *Blockchain & Privacy: International and Comparative Law*, Pointe-à-Pitre, Guadeloupe. Nov. 16, 2023.

[21] B. Bertrand. *Vers une éthique opérationnelle de la donnée*. International workshop *Blockchain, Artificial Intelligence and Digital Sovereignty in Dialogue*, French Embassy, Seoul, South Korea. Dec. 12, 2025.

[22] D. Franchi. *Convergences Blockchain et IA pour la traçabilité des données*. International workshop *Blockchain, Artificial Intelligence and Digital Sovereignty in Dialogue*, French Embassy, Seoul, South Korea. Dec. 12, 2025.

[23] S. Turgis. *Blockchain for Humanitarian Accountability / Blockchain et action humanitaire responsable*. International workshop *Blockchain, Artificial Intelligence and Digital Sovereignty in Dialogue*, French Embassy, Seoul, South Korea. Dec. 12, 2025.

[24] B. Bertrand and S. Turgis. *International invitations following SplitChain-related blockchain and privacy work*. Invitations to the Institute for Technology and Society of Rio de Janeiro and the Universidad de Lima. 2025.