# PriCLeSS

## Privacy-Conscious Legally-Sound blockchain Storage

WIDE, Inria Rennes, IRISA, UR1
CIDRE, Inria Rennes, IRISA, UR1
GDD, LS2N, University of Nantes
IODE, University of Rennes 1

## Overall Objectives and Workpackages

**1-Leverage blockchains to provide legal and technical tools to automate and audit operations that access or exploit personal data.**

**2-provide providing legal and technical tools to addresses the challenges posed by distribution and cross-border exchanges**

**3-design an ecosystem of legal and technical tools that can support blockchain-based distributed storage applications, while satisfying privacy and legal requirements**

### WP 1 - Harnessing Blockchain Assets for Privacy Protection

- **Task 1.1:** Privacy Opportunity Analysis.
- **Task 1.2:** From Legal Requirements to Specification.
- **Task 1.3:** Smart Contracts for Legal Compliance.

### WP 2 - Legal Compliance and Scalability through Distribution

- **Task 2.1:** Challenges of Distribution.
- **Task 2.2:** Combining legal specifications and distribution requirements.
- **Task 2.3:** Improving Blockchain storage.

### WP 3 - An Ecosystem to address the Blockchain's shortcomings

- **Task 3.1:** Privacy versus technical characteristics of the Blockchain.
- **Task 3.2:** Enforcing privacy policies.
- **Task 3.3:** Composing data structures into a consistent ancillary ecosystem.

## Blockchain vs GDPR - Tasks 1.1 2.1 3.1

### Five Major Challenges [1, 2]

| | Public permissioned | Public permissionless | Private permissioned |
|---|---|---|---|
| IMMUTABILITY | | | |
| 1st challenge: Irreversibility of DLT ⇒ challenges for data subject rights | Possibility to change content, ledger not immutable, depends on consensus mechanism & number of nodes. 0 + | Very challenging to comply with data protection rules. + + | Possibility to change content, ledger not immutable, depends on consensus mechanism & number of nodes. 0 + |
| DECENTRALIZATION | | | |
| 2nd challenge: Identification of Controllers and Processors | Nodes are identified and authorized to create the ledger, data protection rules are enforceable. 0 | Nodes not identified nor authorized to create the ledger, data protection rules are NOT enforceable. + + | Nodes are identified and authorized to create the ledger, data protection rules are enforceable. 0 |
| 3rd challenge: Transfer of data outside the EU | Restrictions on location can be implemented, data protection rules are enforceable. 0 | No clear solutions for restricting node location, data protection rules are NOT enforceable. + + | Restrictions on location can be implemented, data protection rules are enforceable. 0 |
| 4th challenge: Consent management in a decentralized environment | Reading non-authorized ⇒ difficult to design correct consent management procedure. + | Reading non-authorized ⇒ difficult to design correct consent management procedure. + | As reading is authorized, consent and privacy notice can be managed. 0 |
| AUTOMATION | | | |
| 5th challenge: Automation of decision made with personal data, | Challenging to implement a correct data protection approach. + | Challenging to implement a correct data protection approach. + | Solvable with the correct data protection approach (consent or other legal basis). 0 |

0 **Not a problem**: due to the technological characteristics of the given type of DLT, the challenge does not pose a problem.
\+ **Issue**: the challenge does pose an issue, but it can be easily solved with a legal or a technical solution, without distorting the DLT approach.
\+ + **Big issue**: the challenge does pose an issue, which cannot be easily solved, neither with a legal nor with a technical work-around.

### Identified solutions [3]

| Challenges | | Solutions | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | Not using DLT | Keeping data off-chain in a database, with hash pointers | Encryption of data, deletion of encryption keys | Using private DLTs | Using mutable blockchain-like data structures | Using legal scope of interpretation | Other potential technical solutions |
| Immutability | Right to rectification | Solved | Unclear status of on-chain hash | Data only made inaccessible | Partially solved | Solved | Not Relevant | Not Relevant |
| | Right to erasure | Solved | Solved | Solved | Partially Solved | Solved | May be applied | Not Relevant |
| | Right to object | Solved | Solved | Solved | Partially Solved | Solved | May be applied | Not Relevant |
| | Right to withdraw consent | Solved | Solved | Solved | Partially Solved | Solved | May be applied | Not Relevant |
| Decentralization | Identification of the data controller | Solved | Solved | Solved | Partially solved | | May be applied | |
| | Identification of the data transfers | Solved | Not Relevant | Not Relevant | Partially solved | Not Relevant | May be applied | Sharding |
| | Consent management | Solved | Not Relevant | Not Relevant | Not Relevant | Not Relevant | Not Relevantx | SSI |
| Automation | Right not to be subject to fully automated decisions | Solved | Not Relevant | Not Relevant | Not Relevant | Not Relevant | May be applied | Auditing |

## Redesigning the Blockchain - Tasks 2.2 2.3

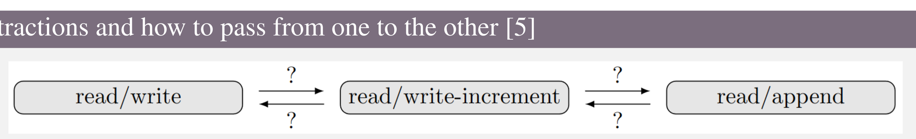
### SplitChain: Resilient-Scalable Sharding [4]

Adaptive elastic sharding, dynamically adpting to load

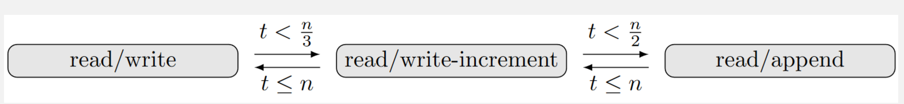
- Proof of Eligibility [13] at a local level
- Each shard managages a separate set of transactions
- Broadcast-based intershard coordination: No inter-shard consensus
- High resistance to attacks
- More details in follow-up poster...

## Shared Memory with Byzantine Actors

### Three abstractions and how to pass from one to the other [5]



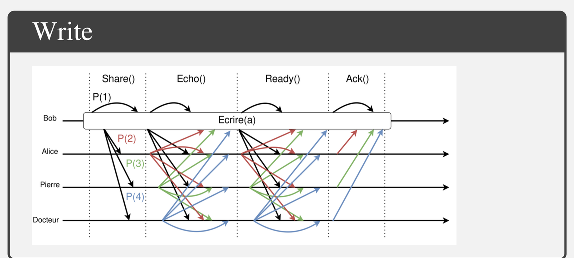

- Implementation of R/W Increment from Send Receive (with $t < \frac{n}{3}$), which implies Read/Write-Increment from Read/Write with a resilience of $t < \frac{n}{3}$.
- We observed that the definition of Read/Write register is included in that of definition of Read/Write-increment.
- We observed that the definition of the Read/Write-increment register is included in the that of the Read/Append register.
- We proved that $t < \frac{n}{3}$ is necessary and sufficient to implement a read/write increment from read/write.
- We proposed an implementation of a Read-append register from a Read/Write-increment register with a resilience of $t < \frac{n}{2}$. We also proved that this is optimal.



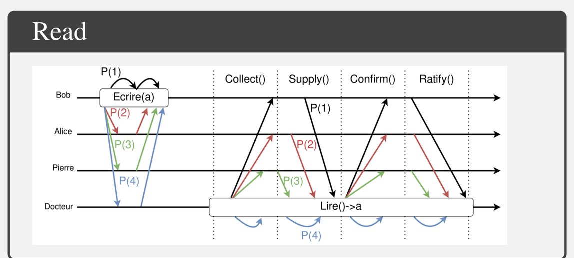

### Privacy-preserving atomic register [6]

- Based on Shamir's secret sharing [14]
- Algorithm based on well known ABD register [15]
- Tolerates up $t < \frac{n}{2}$ Byzantine failures

#### Write




#### Read

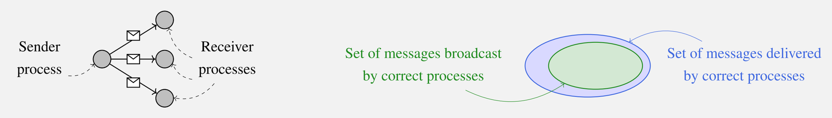



## Broadcast-Based Blockchain Alternatives - Tasks 3.2 3.3

### Large-Scale Consensus Unnecessary for Many Applications

- Money Transfer [16, 17]
- E-voting [7]
- Self-Sovereign Identity [7]

### Reliable Broadcast Abstraction - BRB

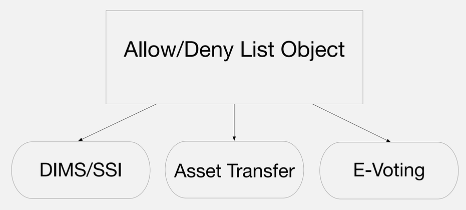



### Allow/Deny List Object [7]

We showed that system wide consensus is unnecessary in a variety of applications

Three operations

- APPEND Add an element to the list
- PROVE Valid if element is in the list
- READ Return list of valid PROVE operations




Main results

- AllowList has consensus number one
- DenyList has consensus number $k$, $k$ being the number of processes that can perform PROVE operations

Application to

- Anonymous Money Transfer
- SSI/DIMS/Verifiable Credentials
- E-voting

### Good-Case Latency of Early-Stopping Byzantine Reliable Broadcast [8]

- Good case latency: Number of rounds needed for the correct processes to brb-deliver a message brb-broadcast by a correct process
- Early stopping: Number of rounds depends on the effective actual number $f$ of Byzantine processes $f = n - c \le t$ (e.g. $\min(t+1, f+2)$) [18]

Main result:

- Novel deterministic algorithm that can brb-deliver a message $m$ in at most $\max(2, t+3-c)$ rounds in good cases

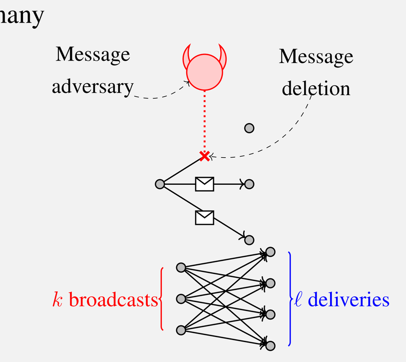
In a nutshell

- During a round: each process adds its signature to the message + signatures chains it receives, and sends them to each process
- Identification of a pattern in a set of messages and a predicate
- At round $R$, a process considers only valid message + signatures chains (those have exactly $R$ different signatures)

### Construct Signature-Free BRB Algorithms under a Message Adversary

Novel Primitive $k2l$-cast $k2\ell$-cast (for $k$-to-$\ell$-cast): modular many-to-many abstraction
($k$ correct processes $k2\ell$-cast) → ($\ell$ correct processes $k2\ell$-deliver)
Operations:

- $k2\ell$_cast$(m, id)$
- $k2\ell$_deliver$(m, id)$ (callback)




Reconstruct existing signature-free BRB algorithms to make them

- MA-tolerant
- shorter and simpler to analyze
- more efficient (they terminate earlier)

#### Bracha

| Threshold | Original version (ECHO phase) | $k2\ell$-cast-based version ($obj_E$) |
|---|---|---|
| Forwarding $q_f$ | $\lfloor \frac{n+t}{2} \rfloor + 1$ | $t+1$ |
| Delivery $q_d$ | $\lfloor \frac{n+t}{2} \rfloor + 1$ | $\lfloor \frac{n+t}{2} \rfloor + 1$ |

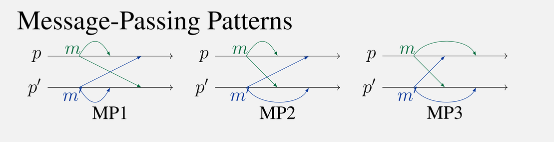
#### Imbs & Raynal

| Threshold | Original version (WITNESS phase) | $k2\ell$-cast-based version ($obj_W$) |
|---|---|---|
| Forwarding $q_f$ | $n - 2t$ | $\lfloor \frac{n+t}{2} \rfloor + 1$ |
| Delivery $q_d$ | $n - t$ | $\lfloor \frac{n+3t}{2} \rfloor + 1$ |

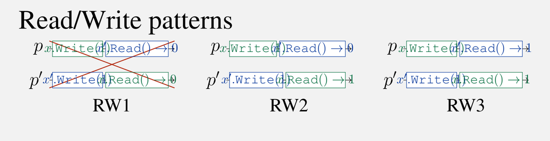
### Mutual Broadcast [9, 10]

Message passing allows interleavings that are forbidden in shared memory.

#### Message-Passing Patterns




#### Read/Write patterns




Mutual Broadcast: novel abstraction that forbids MP1.

- *Validity.* Only mbroadcast messages are mdelivered
- *No-duplication.* Messages are mdelivered at most once
- *Mutual ordering.* For any pair of processes p and p, if p mbroadcasts a message m and p mbroadcasts a message m, it is not possible that p mdelivers m before m and p mdelivers m before m.

In Byzantine case:

- *read-append* instead of *read-write*
- forbid MP1 and MP3

## Outreach

- Brunessen Bertrand and Sandrine Turgis speakers at Colloque L'Europe et les nouvelles technologies, Nanterre, 10/06/2021.
- Blockchain & Privacy Conference (Rennes, 2022) organized by Brunessen Bertrand and Sandrine Turgis, 22 speakers from France, Belgium and Canada. To be published in 2023 with Larcier (editor).
- Brunessen Bertrand and Sandrine Turgis speakers at Blockchain and Privacy International Workshop, Berkman-Klein Center for Internet and Society, Harvard University (Massachussets/Etats-Unis), 22 mai 2023.
- Damien Franchi, talk "Blockchain et Smart Cities : Source denjeux juridiques et techniques du local à linternational", 9/11/2022, Colloquium, Rennes
- Damien Franchi, talk "L'intégration européenne par la recherche d'une identité numérique européenne confrontée aux traitements des données à caractère personnel", 9/05/2023, Bayonne

## Publications

[1] Danaja Fabi Pove et al. "Building Cybersecurity Applications with Blockchain Technology and Smart Contracts". In: ed. by Nour El Madhoun, Ioanna Dionysiou, and Emmanuel Bertin. Springer, 2023. Chap. Data Protection Challenges in Distributed Ledger and Blockchain Technologies: A Combined Legal and Technical Analysis.

[2] Sandrine Turgis. *Blockchain, as a technological tool with strong ambivalences for fundamental rights and especially data protection*. talk. Berkman-Klein Center for Internet and Society, Harvard University (USA). May 2023.

[3] Danaja Fabi Pove et al. "Building Cybersecurity Applications with Blockchain Technology and Smart Contracts". In: ed. by Nour El Madhoun, Ioanna Dionysiou, and Emmanuel Bertin. Springer, 2023. Chap. Solutions to Data Protection Challenges in Distributed Ledger and Blockchain Technologies: A Combined Legal and Technical Approach.

[4] Emmanuelle Anceaume, Davide Frey, and Arthur Rauch. *Sharding in permissionless systems in presence of an adaptive adversary*. Tech. rep. submitted for publication. Sept. 2023.

[5] Vincent Kowalski, Achour Mostéfaoui, and Matthieu Perrin. *Atomic Register Abstractions for Byzantine-Prone Distributed Systems, Extended Version*. Tech. rep. working paper or preprint. Sept. 2023. URL: https://hal.science/hal-04213718.

[6] Quentin Gomes dos Reis et al. "Registre atomique préservant la vie privée tolérant aux byzantins". In: working paper or preprint. Sept. 2023. URL: https://hal.science/hal-04211679.

[7] Davide Frey, Mathieu Gestin, and Michel Raynal. "The Synchronization Power (Consensus Number) of Access-Control Objects: The Case of AllowList and DenyList". In: *DISC 2023*. Oct. 2023.

[8] Timothé Albouy et al. "Good-Case Early-Stopping Latency of Synchronous Byzantine Reliable Broadcast: The Deterministic Case". In: *DISC 2022*. Ed. by Christian Scheideler. Vol. 246. LIPIcs. 2022, 4:1–4:22. ISBN: 978-3-95977-255-6. DOI: 10.4230/LIPIcs.DISC.2022.4. URL: https://drops.dagstuhl.de/opus/volltexte/2022/17195.

[9] Mathilde Déprés et al. "Send/Receive Patterns Versus Read/Write Patterns in Crash-Prone Asynchronous Distributed Systems". In: *Distributed Computing: 37th International Symposium on Distributed Computing, DISC 2023, L'Aquila, Italy, October 9-13, 2023*. 2023.

[10] Mathieu Féry et al. *Causal Mutual Byzantine Broadcast*. Tech. rep. working paper or preprint. Sept. 2023. URL: https://hal.science/hal-04211703.

[11] Timothé Albouy et al. "A Modular Approach to Construct Signature-Free BRB Algorithms under a Message Adversary". In: *OPODIS 2022 - 26th Conference on Principles of Distributed Systems*. Ed. by Eshcar Hillel and Roberto Palmieri. Brussels, Belgium, Dec. 2022, pp. 1–44. URL: https://hal.inria.fr/hal-03906141.

[12] Mathilde Déprés et al. *Send/Receive Patterns versus Read/Write Patterns: the MB-Broadcast Abstraction (Extended Version)*. Tech. rep. working paper or preprint. May 2023. URL: https://hal.science/hal-04087447.

## References

[13] Geoffrey Saunois et al. "Permissionless Consensus based on Proof-of-Eligibility". In: *2020 IEEE 19th International Symposium on Network Computing and Applications (NCA)*. 2020, pp. 1–4. DOI: 10.1109/NCA51143.2020.9306715.

[14] Adi Shamir. "How to Share a Secret". In: *Commun. ACM* 22.11 (Nov. 1979), pp. 612–613. ISSN: 0001-0782. DOI: 10.1145/359168.359176. URL: https://doi.org/10.1145/359168.359176.

[15] Hagit Attiya, Amotz Bar-Noy, and Danny Dolev. "Sharing Memory Robustly in Message-Passing Systems". In: *J. ACM* 42.1 (Jan. 1995), pp. 124–142. ISSN: 0004-5411. DOI: 10.1145/200836.200869. URL: https://doi.org/10.1145/200836.200869.

[16] Alex Auvolat et al. "Money Transfer Made Simple". In: *CoRR* abs/2006.12276 (2020). arXiv: 2006.12276. URL: https://arxiv.org/abs/2006.12276.

[17] Rachid Guerraoui et al. "The Consensus Number of a Cryptocurrency". In: *Proceedings of the 2019 ACM Symposium on Principles of Distributed Computing*. PODC '19. Toronto ON, Canada: Association for Computing Machinery, 2019, pp. 307–316. ISBN: 9781450362177. DOI: 10.1145/3293611.3331589. URL: https://doi.org/10.1145/3293611.3331589.

[18] Ittai Abraham et al. "Good-Case Latency of Byzantine Broadcast: A Complete Categorization". In: *Proceedings of the 2021 ACM Symposium on Principles of Distributed Computing*. PODC'21. Virtual Event, Italy: Association for Computing Machinery, 2021, pp. 331–341. ISBN: 9781450385480. DOI: 10.1145/3465084.3467899. URL: https://doi.org/10.1145/3465084.3467899.