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.

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.

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

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.

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

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

A case study: The Building Blocks Project

- Builing Blocks Project
- – Blockchain network for humanitarian assistance
  - UNHCR (United Nations High Commissioner for Refugees)
  - World Food Programme
  - Building Blocks serves 870,000 Rohingya refugees monthly across various programs operating in the worlds largest refugee camp in Coxs Bazar: `https://innovation.wfp.org/project/building-blocks`
- Technical Tradeoffs
  - Permission vs Permissionles
  - Biometrics vs other roots of trust
- Compliance with relevant regulatory frameworks
  - GDPR
  - EIDAS
- Ethical Issues
  - Vulnerable Persons
  - Informed Consent
  - Dignity

Identity Management

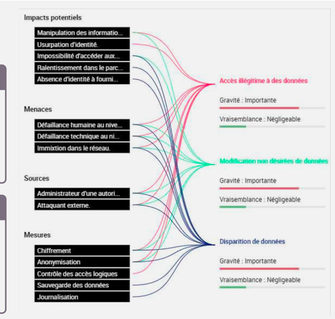
Risk Analysis

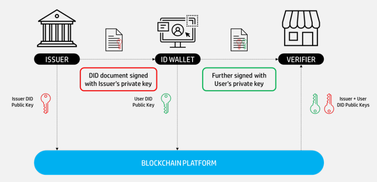
Identify major risks ...

- Unlawful data access
- Unwanted data modification
- Unwanted data deletion

... and their impacts:

- Identity theft
- Inability to access data
- .....



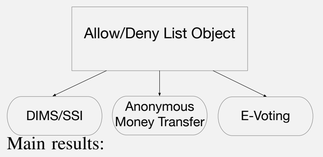


Is Blockchain really neeeded

- Building Blocks offers three main services
  - Identification
  - A basic form of identity management
  - Payment service
- Use case implemented by Building Blocks project does not really need a blockchain
- Actually implemented on a very small private blockchain of a handful of nodes
- Even scaling it up, use cases would not need a blockchain

We showed in 2023 [3]

that system wide consensus is unnecessary in a variety of applications



Three operations:

- APPEND: Adds an element to the list.
- PROVE: Returns valid if element is in the list.
- READ: Returns the 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.

Redesigning the Blockchain - Tasks 2.2 2.3

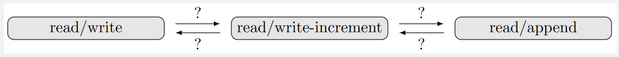
SplitChain: Resilient-Scalable Sharding [16, 17]

Adaptive elastic sharding, dynamically adpting to load.

- Each shard managages a separate set of transactions.
- Broadcast-based intershard coordination: No inter-shard consensus.
- More details on follow-up poster . . .

Shared Memory with Byzantine Actors - Tasks 3.2 3.3

Three abstractions and how to pass from one to the other [12]

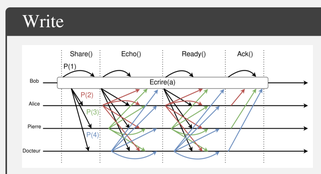


- Implementation of R/W Increment from Send Receive (with $t < \frac{n}{3}$), which implies Read/Write-Increment from Read/Write with a resilience of $t < \frac{n}{3}$.
- The definition of Read/Write register is included in that of definition of Read/Write-increment.
- The definition of the Read/Write-increment 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.

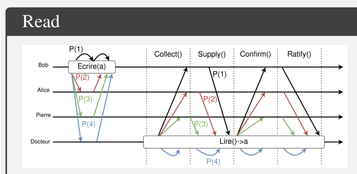
Privacy-preserving atomic register [10, 11]

- Based on Shamir's secret sharing [21].
- Algorithm based on well known ABD register [20].
- Tolerates up $t < \frac{n}{7}$ Byzantine failures.

Write



Read

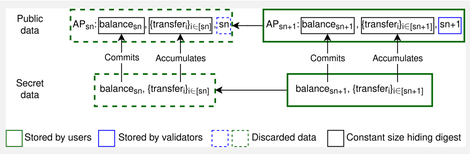


Privacy-preserving atomic register [10, 11]

- Based on Shamir's secret sharing [21].
- Algorithm based on well known ABD register [20].
- Tolerates up $t < \frac{n}{7}$ Byzantine failures.

Broadcast-Based Blockchain Alternatives - Tasks 3.2 3.3

Quasi Anonymous Asset Transfer [15]



Novel asynchronous Byzantine-tolerant asset-transfer system with three noteworthy properties:

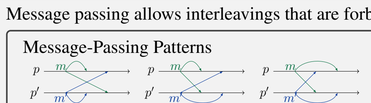
- *Quasi-anonymity:* no information is leaked regarding the receivers and amounts of the asset transfers.
- *Lightness:* The underlying cryptographic schemes are *succinct*(small proofs and fast verification time), and each process only stores its own transfers.
- *Consensus-freedom:* The system does not rely on a total order of asset transfers.

First asset transfer system that simultaneously fulfills all these properties in the presence of asynchrony and Byzantine processes. Modular approach combining a new distributed object called agreement proofs and cryptographic primitives such as commitments, universal accumulators and zero-knowledge proofs.

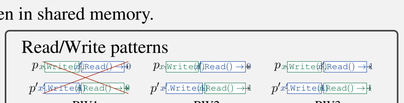
Mutual Broadcast [6, 8]

Message passing allows interleavings that are forbidden in shared memory.

Message-Passing Patterns



Read/Write patterns



Mutual Broadcast: novel abstraction that forbids MP1.

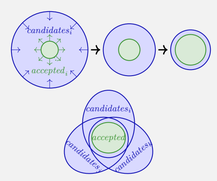
- *Validity:* Only mbroadcast messages are mdelivered.
- *No-duplication:* Messages are mdelivered at most once.
- *Mutual ordering:* For any pair of processes p and p', if p mbroadcasts a message m and p' mbroadcasts a message m', it is not possible that p mdelivers m before m' and p' mdelivers m' before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

In the Byzantine case:

- *Read-append* instead of *read-write*.
- Forbid MP1 and MP3.

Context Adaptive Cooperation [19]

Consensus among k processes (k-consensus) is enough for many applications [3].
But what if we do not know k?



We introduced a novel primitive:
Context-Aware Cooperation (CAC) [19]

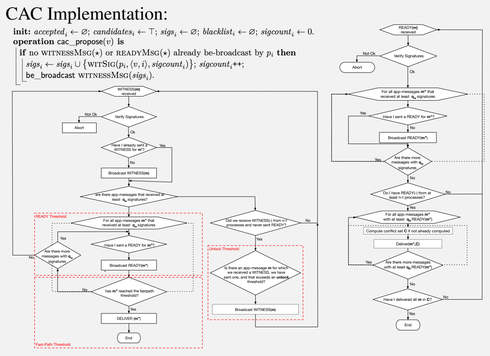
- one operation:
  cac_propose allows a process to propose a value
- two sets: $accepted_i$ and $candidates_i$

CAC Specification

- CAC-Validity. If p_i and p_j are correct, $candidates_i \neq \top$ and $\langle v, j\rangle \in candidates_i$, then p_j cac-proposed value v.
- CAC-Prediction. For any correct process p_i and for any process identity k, if, at some point of p_i's execution, $\langle v, k\rangle \notin candidates_i$, then p_i *never* cac-accepts $\langle v, k\rangle$ (*i.e.*, $\langle v, k\rangle \notin accepted_i$ holds forever).
- CAC-Non-triviality. For any correct process p_i, $accepted_i \neq \varnothing$ implies $candidates_i \neq \top$.
- CAC-Local-termination. If a correct process p_i invokes cac_propose(v), its set $accepted_i$ eventually contains a pair $\langle v', \star\rangle$ (note that v' is not necessarily v).
- CAC-Global-termination. If p_i is a correct process and $\langle v, j\rangle \in accepted_i$, eventually $\langle v, j\rangle \in accepted_k$ at every correct process p_k.

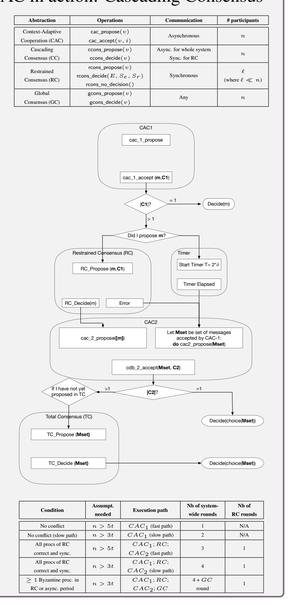
CAC Implementation:

init: $accepted_i \leftarrow \varnothing$; $candidates_i \leftarrow \top$; $sigs_i \leftarrow \varnothing$; $blacklist_i \leftarrow \varnothing$; $sigcount_i \leftarrow 0$.
operation cac_propose(v) **is**
  if no WITNESSMSG$(\star)$ or READYMSG$(\star)$ already be-broadcast by p_i **then**
    $sigs_i \leftarrow sigs_i \cup \{\text{WITNESSTG}(p_i, \langle v, i\rangle, sigcount_i)\}$; $sigcount_i$++;
    be_broadcast WITNESSMSG$(sigs_i)$.



CAC in action: Cascading Consensus

Abstraction	Operations	Communication	# participants
Context-Adaptive Cooperation (CAC)	cac_propose(v) cac_accept(v, i)	Asynchronous	n
Cascading Consensus (CC)	ccons_propose(v) ccons_decide(v)	Async. for whole system Sync. for RC	n
Restrained Consensus (RC)	rcons_propose(v) rcons_decide$(R, \vartheta_R, \beta_{rv})$ rcons_no_decision( )	Synchronous	ℓ (where $\ell \ll n$)
Global Consensus (GC)	gcons_propose(v) gcons_decide(w)	Any	n



Condition	Assumpt. needed	Execution path	Nb of system-wide rounds	Nb of RC rounds
No conflict	$n > 5t$	CAC_1 (fast path)	1	N/A
No conflict (slow path)	$n > 3t$	CAC_1 (slow path)	2	N/A
All procs of RC correct and sync.	$n > 5t$	$CAC_1 \cdot RC_1$ CAC_2 (fast path)	3	1
All procs of RC correct and sync.	$n > 3t$	$CAC_1 \cdot RC_1$ CAC_2 (slow path)	4	1
≥ 1 Byzantine proc. in RC or asynv. period	$n > 3t$	$CAC_1 \cdot RC_1$ $CAC_2 \cdot GC$	$4 + GC$ round	1

Outreach

- PriCLeSS International Workshop in Rennes on September 9, 2024.
- S. Turgis, D. Frey, and D. Franchi speakers at the Workshop on Blockchain & Privacy: International and Comparative Law, University of the French Antilles, 10/11/2023.
- B. Bertrand and S. Turgis organized the Workshop on Blockchain & Privacy: International and Comparative Law, University of the French Antilles, 10/11/2023.
- B. Bertrand and S. Turgis speakers at Colloque L'Europe et les nouvelles technologies, Nanterre, 10/06/2021.
- Blockchain & Privacy Conference (Rennes, 2022) organized by B. Bertrand and S. Turgis, 22 speakers from France, Belgium and Canada. To be published in 2023 with Larcier (editor).
- B. Bertrand and S. Turgis speakers at Blockchain and Privacy International Workshop, Berkman-Klein Center for Internet and Society, Harvard University (Massachussets/Etats-Unis), 22 mai 2023.
- D. Franchi, talk "Blockchain et Smart Cities : Source denjeux juridiques et techniques du local à linternational", 9/11/2022, Colloquium, Rennes.
- D. 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] 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.

[2] 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.

[3] 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.

[4] 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.

[5] 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.

[6] 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.

[7] 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.

[8] Vincent Kowalski, Achour Mostefaoui, and Matthieu Perrin. "Causal Mutual Byzantine Broadcast". In: *Proceedings of the 2024 Workshop on Advanced Tools, Programming Languages, and PLatforms for Implementing and Evaluating algorithms for Distributed systems*. 2024, pp. 1–8.

[9] 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.

[10] Vincent Kowalski et al. "Byzantine-Tolerant Privacy-Preserving Atomic Register". In: *2024: 30th International European Conference on Parallel and Distributed Computing, Madrid, August 26-30, 2024. Proceedings 16*. Springer. 2024.

[11] Vincent Kowalski et al. "Byzantine-Tolerant Privacy-Preserving Atomic Register". In: *2025: 26th International Conference on Distributed Computing and Networking, Hyderabad, January 4-7, 2025. Proceedings 1*. ACM. 2025.

[12] Vincent Kowalski, Achour Mostéfaoui, and Matthieu Perrin. "Atomic Register Abstractions for Byzantine-Prone Distributed Systems". In: *27th International Conference on Principles of Distributed Systems (OPODIS 2023)*. Schloss-Dagstuhl-Leibniz Zentrum für Informatik. 2024.

[13] Sylvain Gay, Achour Mostefaoui, and Matthieu Perrin. "Brief Announcement: No Broadcast Abstraction Characterizes k-Set-Agreement in Message-Passing Systems". In: *Proceedings of the 43rd ACM Symposium on Principles of Distributed Computing*. 2024, pp. 343–346.

[14] Achour Mostefaoui, Matthieu Perrin, and Julien Weibel. "Brief Announcement: Randomized Consensus: Common Coins Are not the Holy Grail!" In: *Proceedings of the 43rd ACM Symposium on Principles of Distributed Computing*. 2024, pp. 36–39.

[15] Timothé Albouy et al. *Asynchronous BFT Asset Transfer: Quasi-Anonymous, Light, and Consensus-Free*. 2024. arXiv: 2405.18072 [cs.DC]. URL: https://arxiv.org/abs/2405.18072.

[16] Emmanuelle Anceaume, Davide Frey, and Arthur Rauch. "Sharding in Permissionless Systems in Presence of an Adaptive Adversary". In: *SIROCCO 2024*. Vietri sul Mare, Italy: Springer-Verlag, 2024, pp. 481–487. ISBN: 978-3-031-60602-1. DOI: 10.1007/978-3-031-60603-8_26. URL: https://doi.org/10.1007/978-3-031-60603-8_26.

[17] Emmanuelle Anceaume, Davide Frey, and Arthur Rauch. "Sharding inäPermissionless Systems inäPresence ofäanäAdaptive Adversary". In: *Networked Systems*. Ed. by Armando Castañeda, Constantin Enea, and Nirupam Gupta. Cham: Springer Nature Switzerland, 2024, pp. 1–31. ISBN: 978-3-031-67321-4.

[18] 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.

[19] Timothé Albouy et al. *Context Adaptive Cooperation*. 2024. arXiv: 2311.08776 [cs.DC]. URL: https://arxiv.org/abs/2311.08776.

References

[20] 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.

[21] 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.

[22] 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.

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

[24] 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.

[25] 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.

[26] Rachid Guerraoui et al. "The consensus number of a cryptocurrency". In: *Distributed Comput.* 35.1 (2022), pp. 1–15.

[27] Saurabh Gupta. *A Non-Consensus Based Decentralized Financial Transaction Processing Model with Support for Efficient Auditing (Master Thesis)*. Arizona State University. 2016.

[28] Alex Auvolat et al. "Money Transfer Made Simple: a Specification, a Generic Algorithm, and its Proof". In: *Bulletin of EATCS* 132 (2020), pp. 22–43.