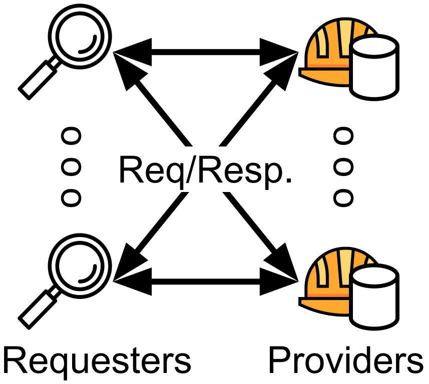
Fair Quality of Service in Adversarial Decentralized Marketplace Mechanisms

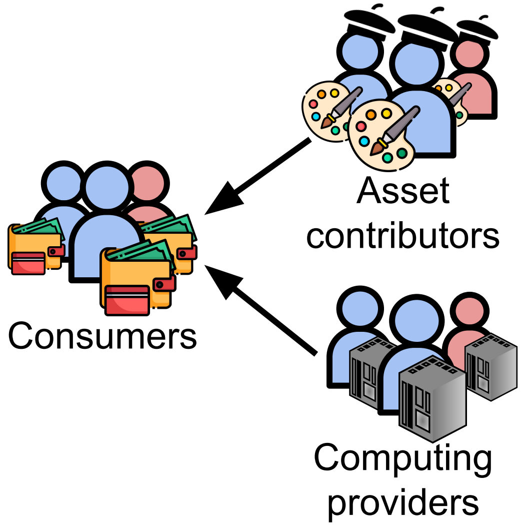
06/05/2024 – Comité de suivi de thèse D3

Matthieu BETTINGER
PhD. student – RedChain-Lab

High-level context – Decentralized marketplaces

Asset / Service Discovery → **Transactions & Match-making** → **Asset / Service Delivery**

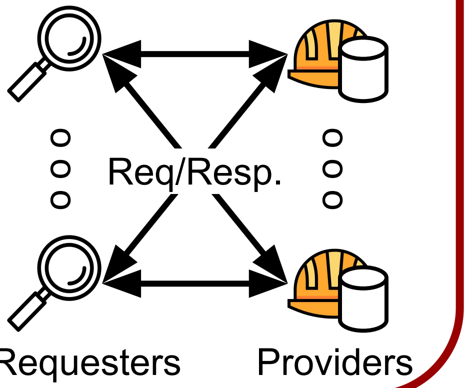




Icons from flaticon.com: Racecar, Market, Money bag – Smashicon, Magnifying glass – ibrandify, Snail, Dollars, Palette – Freepik, Shield – Mayor Icons, Hat – Eucalyp, Wallet – justicon

High-level context – Decentralized marketplaces

Asset / Service Discovery



Req/Resp.

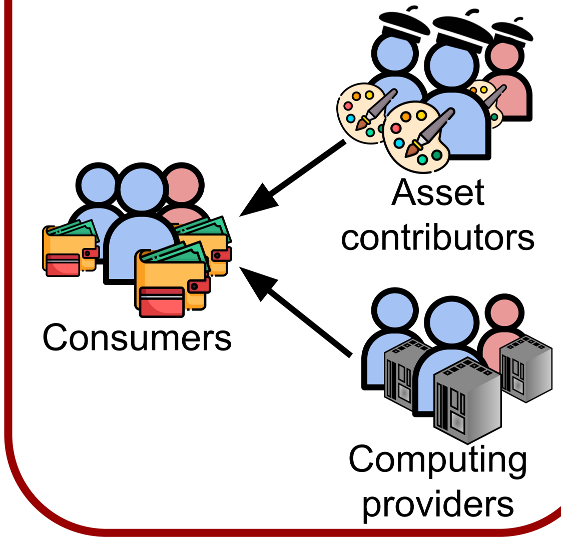
Requesters

Providers

Transactions & Match-making

Market

Asset / Service Delivery



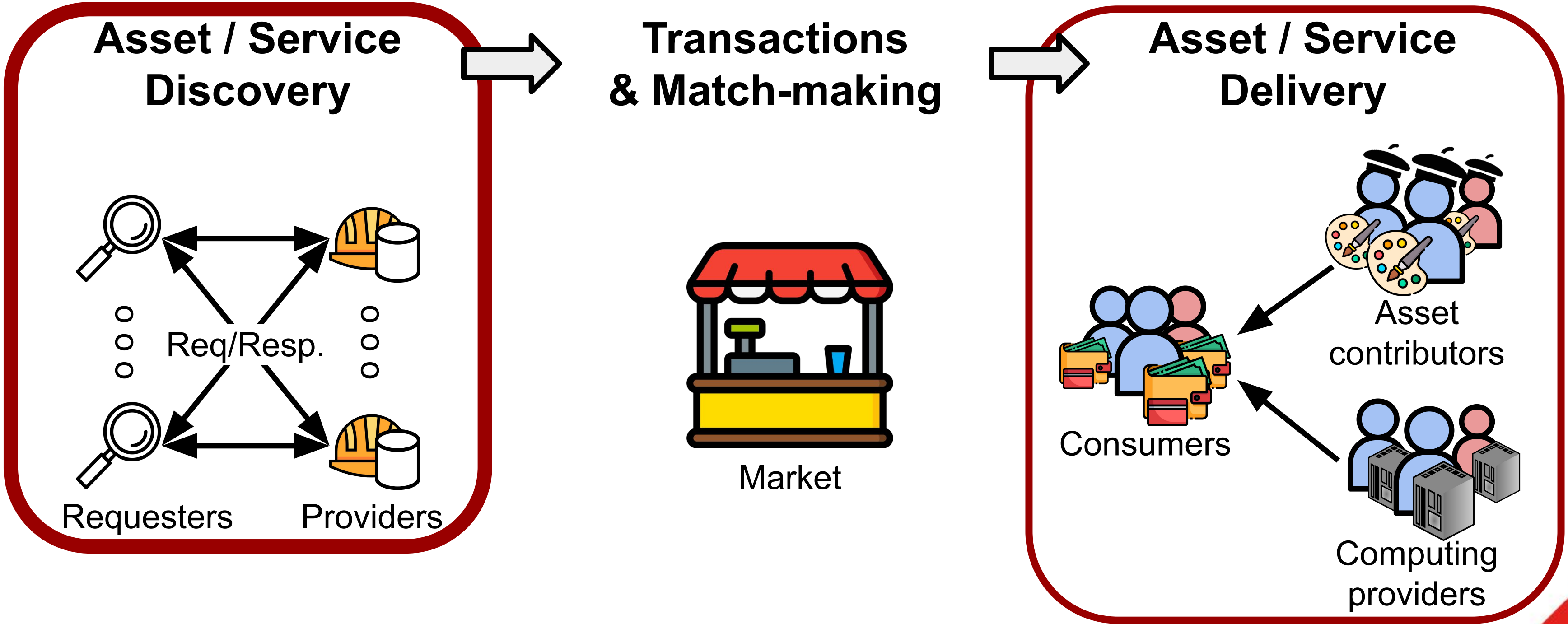
Asset contributors

Consumers

Computing providers

Icons from flaticon.com: Racecar, Market, Money bag – Smashicon, Magnifying glass – ibrandify, Snail, Dollars, Palette – Freepik, Shield – Mayor Icons, Hat – Eucalyp, Wallet – justicon

High-level context – Decentralized marketplaces



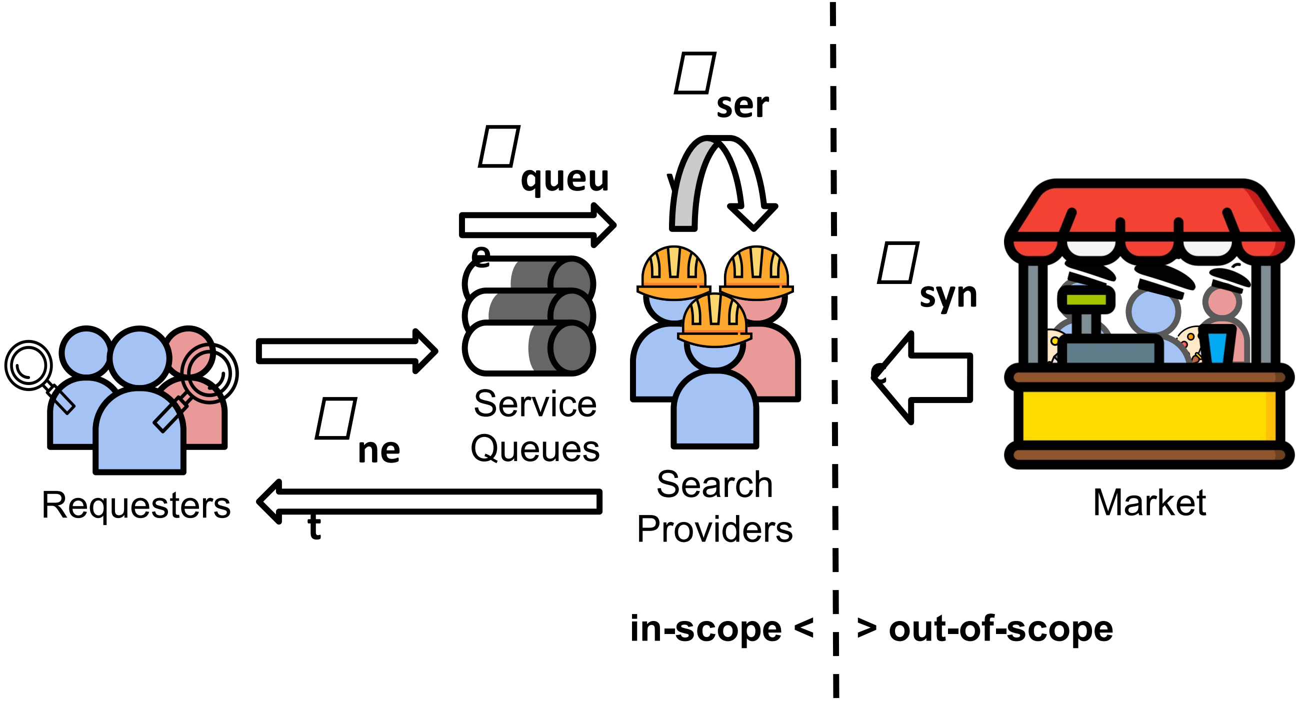
Asset / Service Discovery

Transactions & Match-making

Asset / Service Delivery

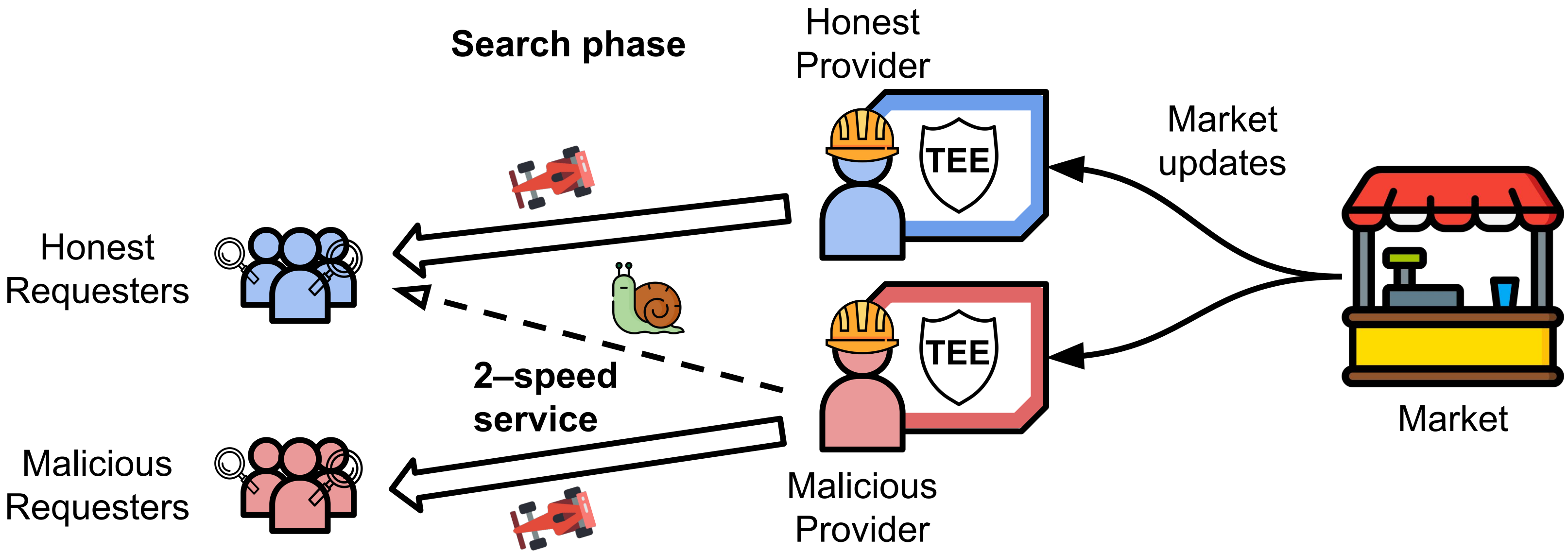
Icons from flaticon.com: Racecar, Market, Money bag – Smashicon, Magnifying glass – ibrandify, Snail, Dollars, Palette – Freepik, Shield – Mayor Icons, Hat – Eucalyp, Wallet – justicon

High-level context – Search/Discovery phase



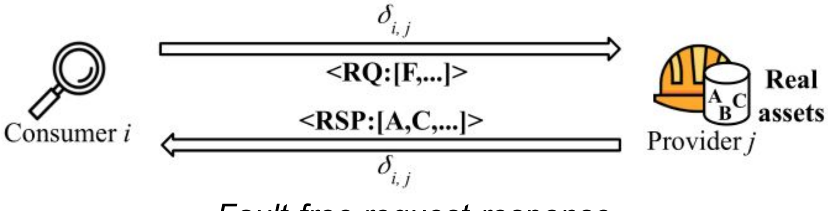
Icons from flaticon.com: Racecar, Market, Money bag – Smashicon, Magnifying glass – ibrandify, Snail, Dollars, Palette – Freepik, Shield – Mayor Icons, Hat – Eucalyp, Wallet – justicon

Contexte du Livrable 1 : ~~FairFetched~~ COoL-TEE

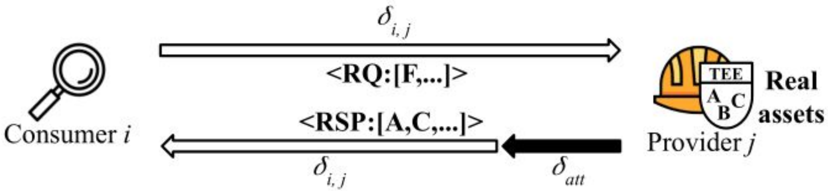


Icons from flaticon.com: Racecar, Market, Money bag – Smashicon, Magnifying glass – ibrandify, Snail, Dollars, Palette – Freepik, Shield – Mayor Icons, Hat – Eucalyp, Wallet – justicon

Contexte du Livrable 1 : COoL-TEE

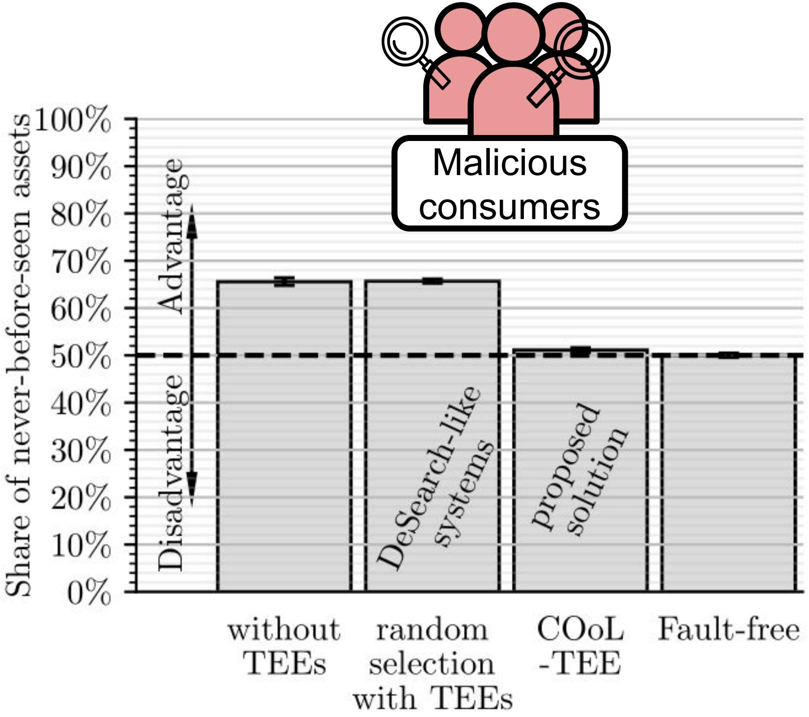


Fault-free request-response



Timing-attacked request-response

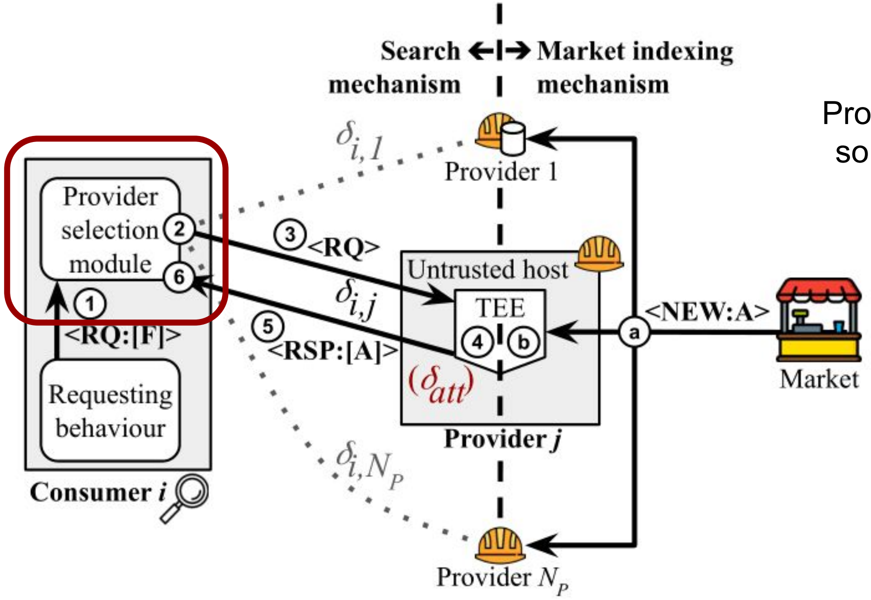
➔ staler response contents



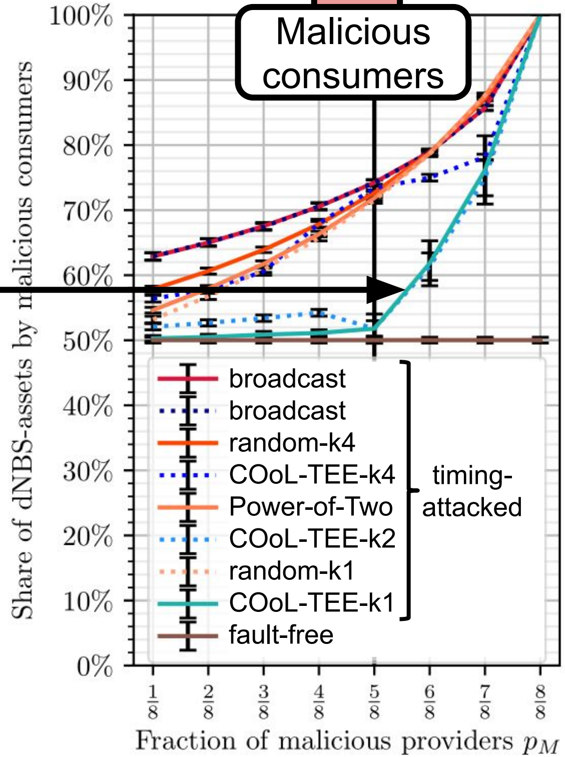
Icons from flaticon.com: Racecar, Market, Money bag – Smashicon, Magnifying glass – ibrandify, Snail, Dollars, Palette – Freepik, Shield – Mayor Icons, Hat – Eucalyp, Wallet – justicon

Contexte du Livrable 1 : COoL-TEE

➔ Client-side Optimization of Latencies + TEEs

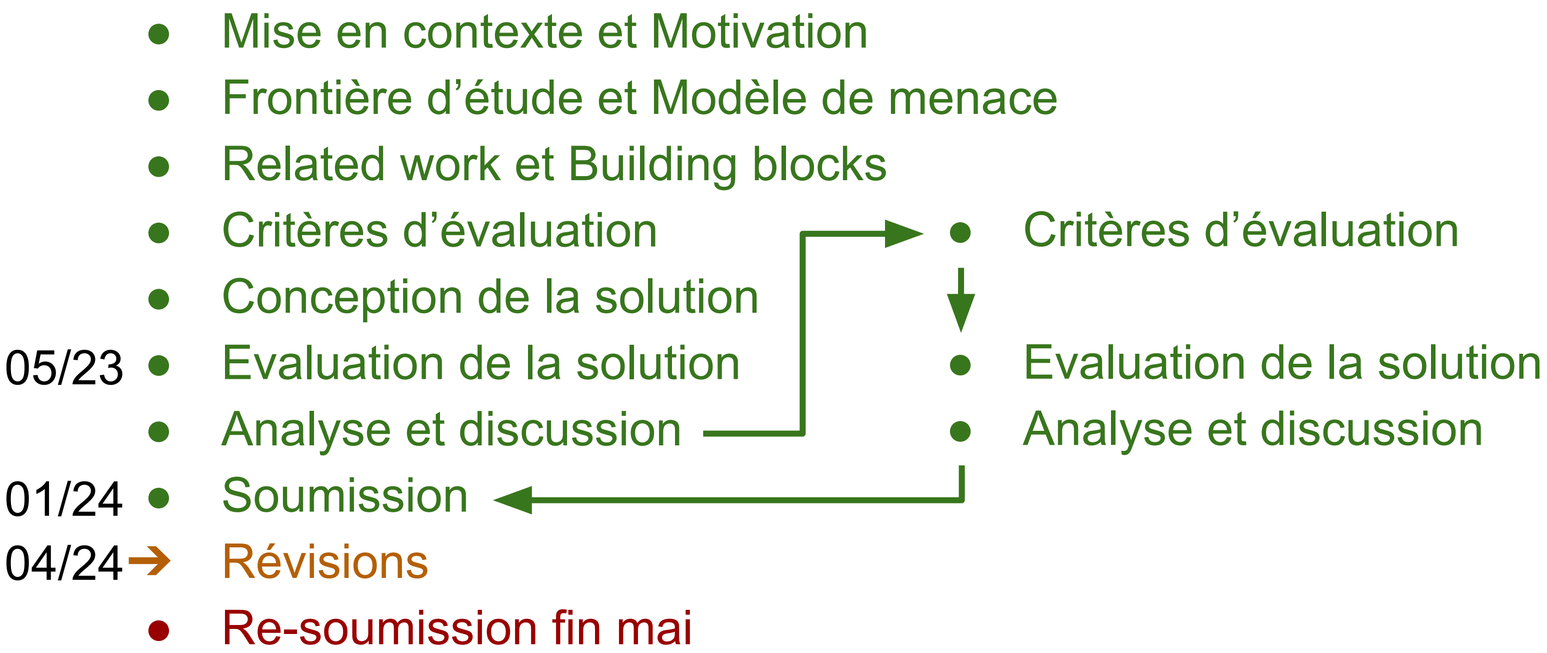


Proposed solution



Icons from flaticon.com: Racecar, Market, Money bag – Smashicon, Magnifying glass – ibrandify, Snail, Dollars, Palette – Freepik, Shield – Mayor Icons, Hat – Eucalyp, Wallet – justicon

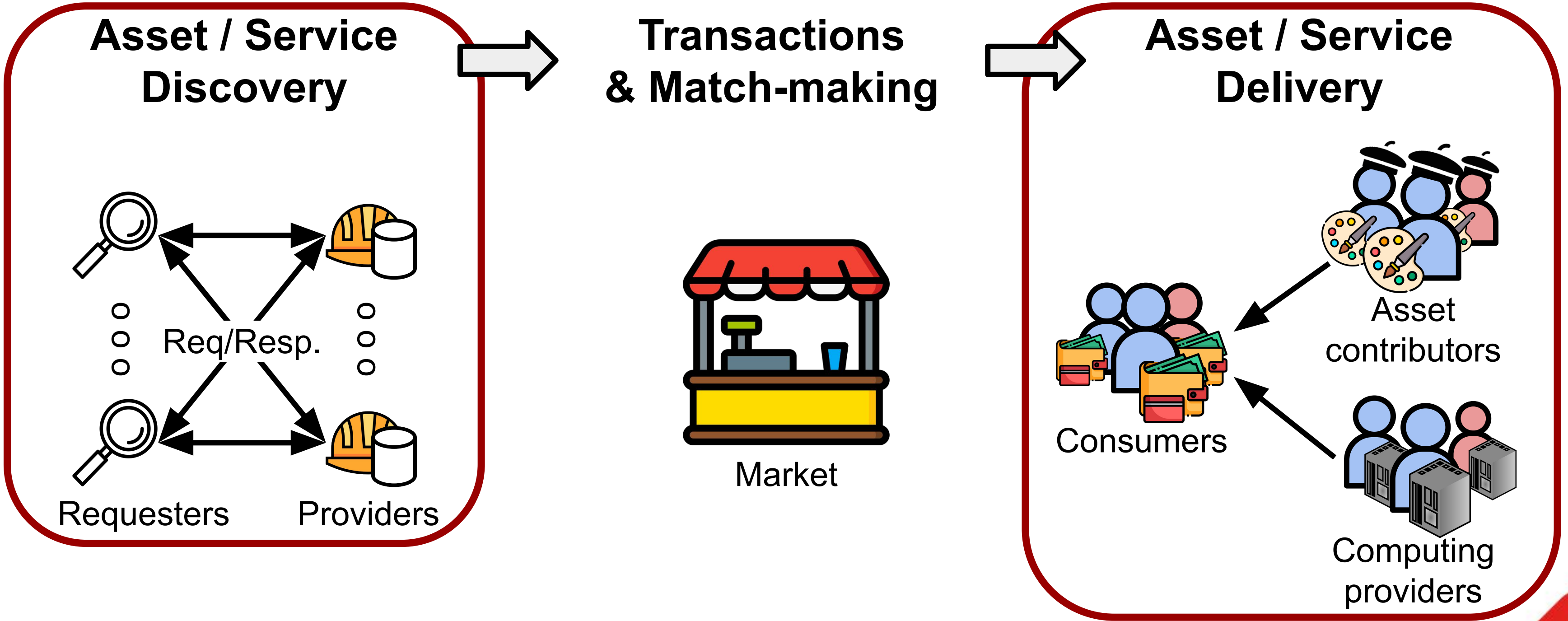
Avancement livrable 1 – Article COoL–TEE



- Mise en contexte et Motivation
- Frontière d’étude et Modèle de menace
- Related work et Building blocks
- Critères d’évaluation
- Conception de la solution
- 05/23 ● Evaluation de la solution
- Analyse et discussion
- 01/24 ● Soumission
- 04/24→ Révisions
- Re-soumission fin mai

- Critères d’évaluation
- Evaluation de la solution
- Analyse et discussion

High-level context – Decentralized marketplaces



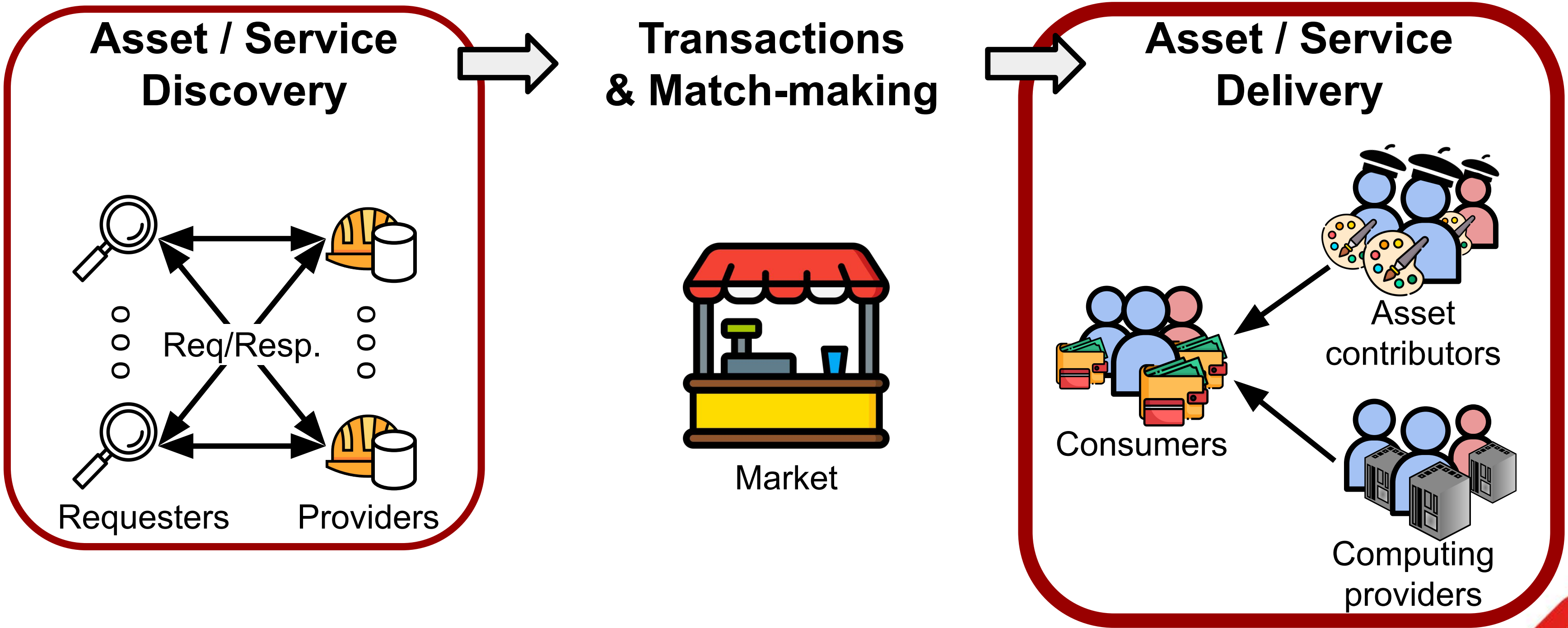
Asset / Service Discovery

Transactions & Match-making

Asset / Service Delivery

Icons from flaticon.com: Racecar, Market, Money bag – Smashicon, Magnifying glass – ibrandify, Snail, Dollars, Palette – Freepik, Shield – Mayor Icons, Hat – Eucalyp, Wallet – justicon

High-level context – Decentralized marketplaces



Asset / Service Discovery

Transactions & Match-making

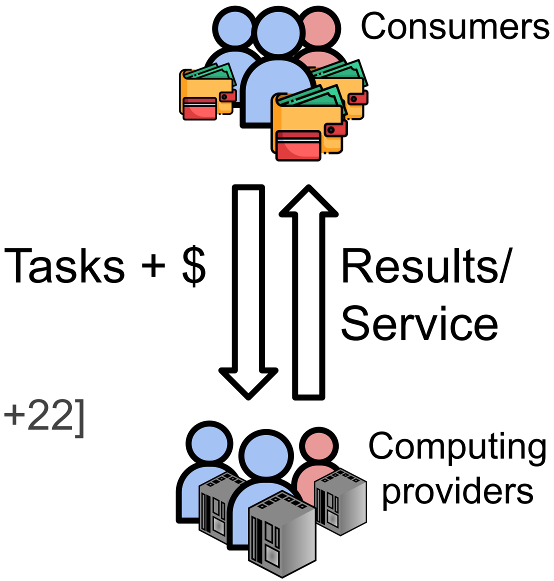
Asset / Service Delivery

Icons from flaticon.com: Racecar, Market, Money bag – Smashicon, Magnifying glass – ibrandify, Snail, Dollars, Palette – Freepik, Shield – Mayor Icons, Hat – Eucalyp, Wallet – justicon

Current work: Service-Level-Indicator measurement with TEEs for Decentralized Computing Marketplaces

- High-level witness-based monitoring lacks granularity & trustworthiness [Abhishek+21, Gonçalves+20, Zhou+18]

- Low-level fine-grained trustworthy measurement TEE building blocks
  - ➔ e.g., elapsed wall-time [Fernandez+23, Hamidy+23], CPU time [Dong+23, Alder+19], storage-time [Zhang+22]
  - ➔ only partial information wrt. SLIs (e.g., availability)



➔ Reinforce outside observations with TEEs, and augment them with the insider point-of-view of Computing Provider TEEs

Icons from flaticon.com: Racecar, Market, Money bag – Smashicon, Magnifying glass – ibrandify, Snail, Dollars, Palette – Freepik, Shield – Mayor Icons, Hat – Eucalyp, Wallet – justicon

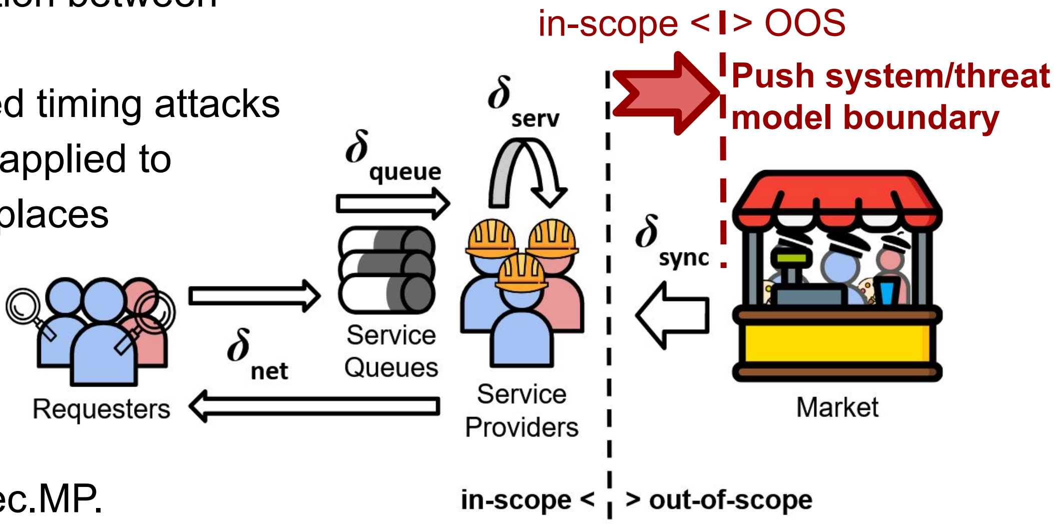
Avancement livrable 2 – Article ServiLI–TEE

- ● Mise en contexte et Motivation
- ● Related work et Building blocks
- ➔ Frontière d’étude et Modèle de menace
- ➔ Critères d’évaluation
- ● Conception de la solution
- ● Evaluation de la solution
- ● Analyse et discussion
- ● Soumission

Future co-supervised work – J.Acker (15/05-10/08)

COoL-TEE extension

- Include provider index updates in threat model
- Naive PubSub introduces correlation between clear-text assets and notifications
  - ➔ Reopens censorship/targeted timing attacks
  - ➔ Privacy-preserving PubSub applied to timing-sensitive Dec.Marketplaces



- Analyze / Evaluate SotA-Privacy-Preserving PubSub applicability to timing-sensitive Dec.MP. e.g., [Keizer+23, Salehi+20, Onica+16]

Icons from flaticon.com: Racecar, Market, Money bag – Smashicon, Magnifying glass – ibrandify, Snail, Dollars, Palette – Freepik, Shield – Mayor Icons, Hat – Eucalyp, Wallet – justicon

Future co-supervised work – H.Mont (03/06-23/09)

Decentralized Computing Marketplace Incentivization

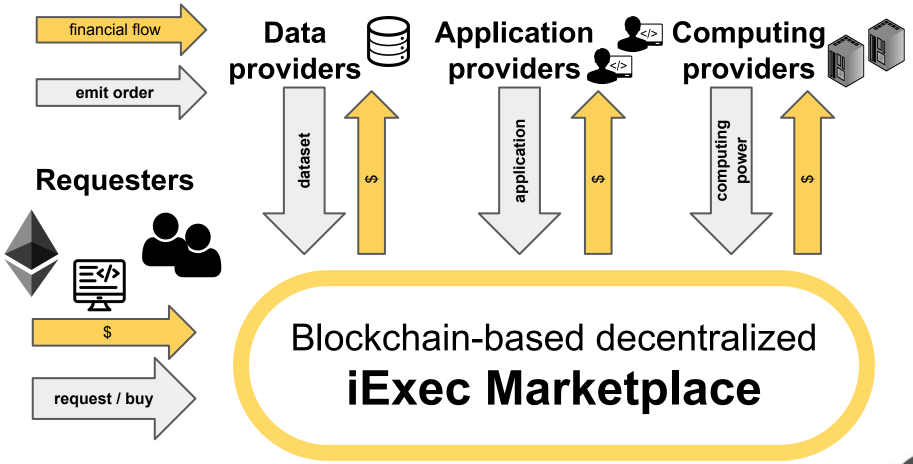
- Multiple stakeholders, but only computing providers are incentivized / can be penalized for bad behaviour
  - e.g., requesting *bound-to-fail* tasks, providing bad-quality data

➔ Characterize attacks by other stakeholders

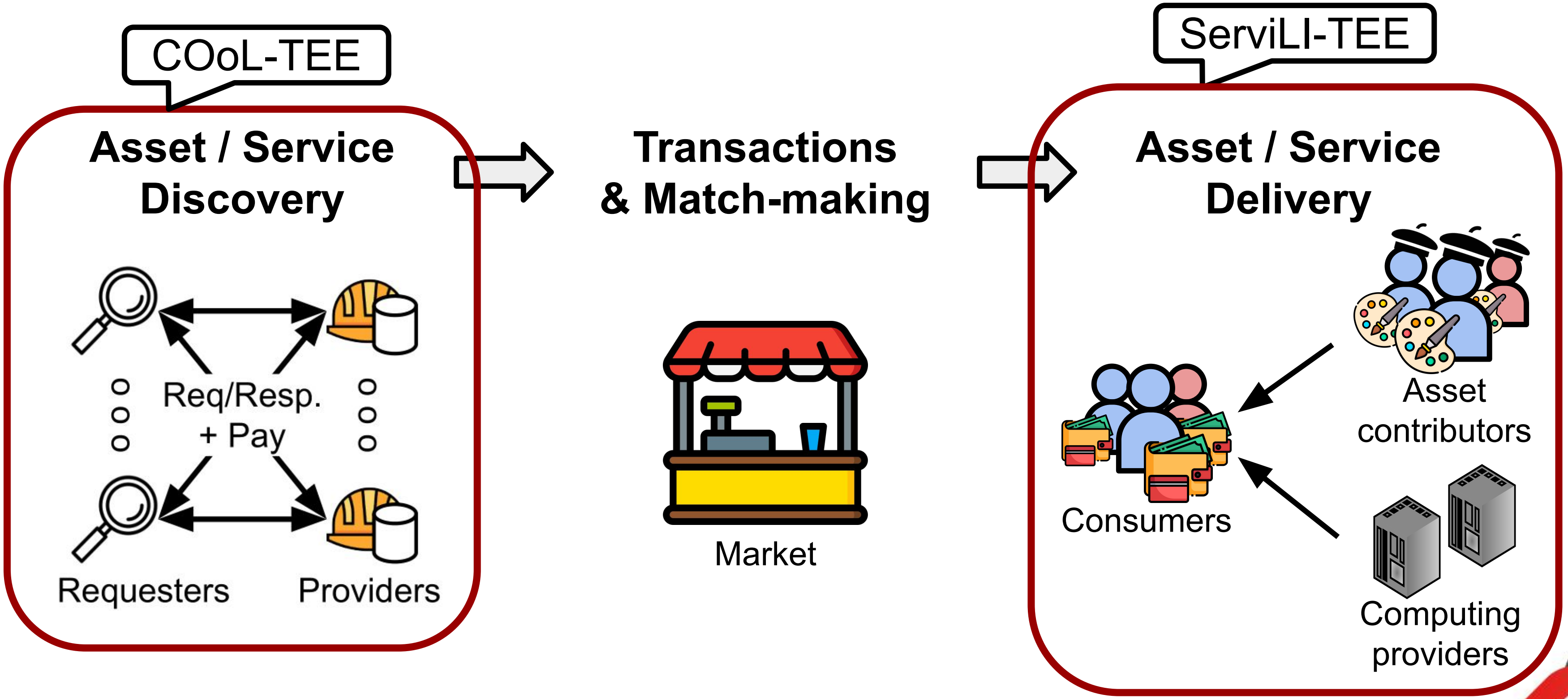
➔ Extend incentivization to prevent attacks

◆ e.g., using game-theoretic, reputation-based mechanisms [Fedak+18, Sarmenta01, Hasan+22]

➔ iExec's Computing Marketplace as a use-case system



Positionnement des travaux



COOoL-TEE

Asset / Service Discovery

Req/Resp. + Pay

Requesters

Providers

Transactions & Match-making

Market

ServiLI-TEE

Asset / Service Delivery

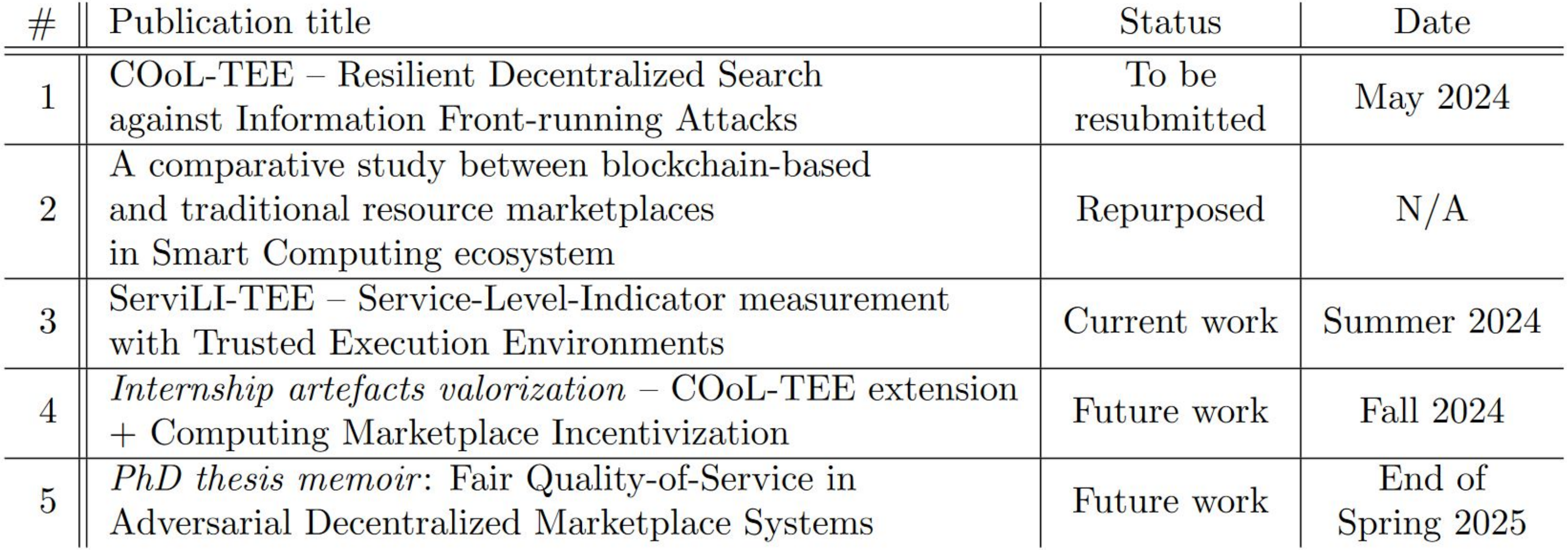
Asset contributors

Consumers

Computing providers

Icons from flaticon.com: Racecar, Market, Money bag – Smashicon, Magnifying glass – ibrandify, Snail, Dollars, Palette – Freepik, Shield – Mayor Icons, Hat – Eucalyp, Wallet – justicon

Calendrier de soumission



#	Publication title	Status	Date
1	COoL-TEE – Resilient Decentralized Search against Information Front-running Attacks	To be resubmitted	May 2024
2	A comparative study between blockchain-based and traditional resource marketplaces in Smart Computing ecosystem	Repurposed	N/A
3	ServiLI-TEE – Service-Level-Indicator measurement with Trusted Execution Environments	Current work	Summer 2024
4	*Internship artefacts valorization* – COoL-TEE extension + Computing Marketplace Incentivization	Future work	Fall 2024
5	*PhD thesis memoir*: Fair Quality-of-Service in Adversarial Decentralized Marketplace Systems	Future work	End of Spring 2025

Table 1: Timeline of (expected) scientific contributions

Organisation et encadrement

- Réunions d’équipe RedChain-Lab hebdomadaires
- Réunions de travail
- Présence 50% LIRIS – 50% iExec

Intégration Laboratoire + Entreprise

- Reading groups mensuels
  + séminaires (e.g., d’équipe à Miribel, wrap-up projet PRIMATE)
  + autres événements
  (e.g., présentation à iExec de J.Passerat-Palmbach sur le front-running)

- Soutenances de thèse

- Événements de mise en place de la stratégie iExec

Interlocuteurs et Contacts externes

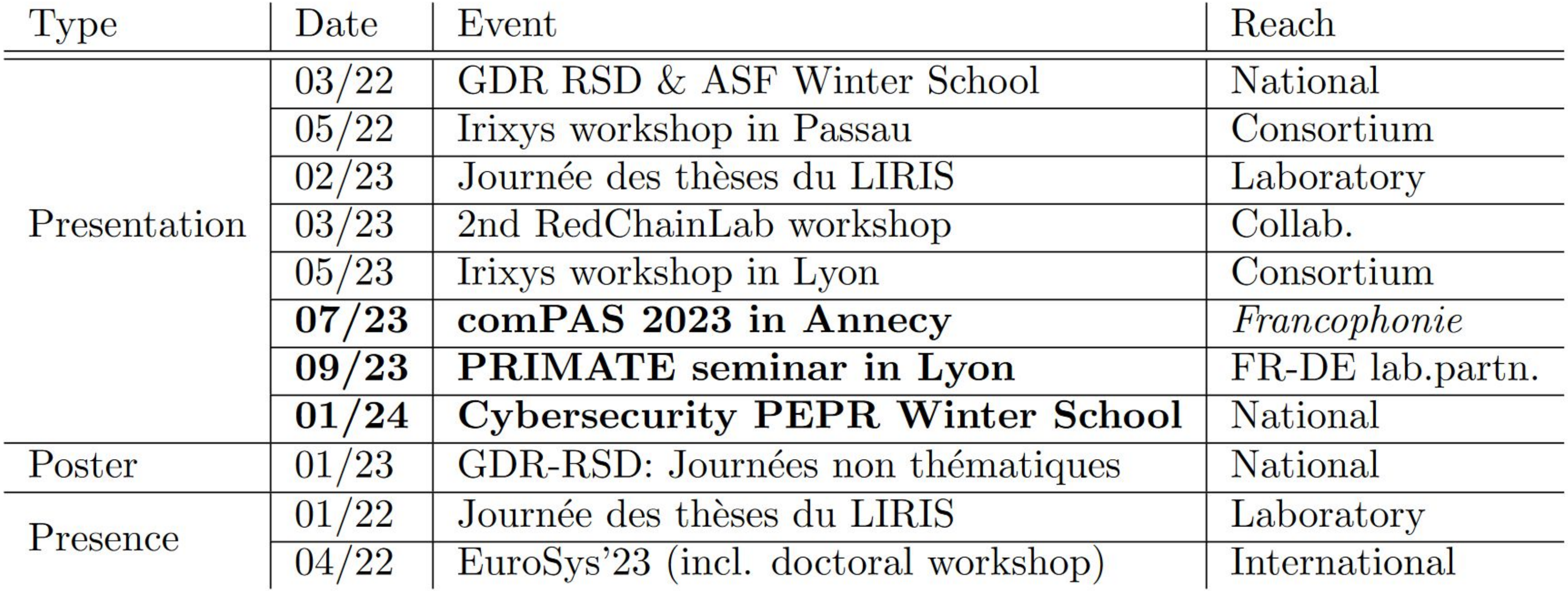
Interlocuteurs:

- Étienne Rivière (UC Louvain)
- Équipe iExec

Contacts:

- **Rüdiger Kapitza (FAU Erlangen-Nürnberg)**
- **Gaël Thomas (Inria Saclay)**
- J. Passerat-Palmbach (Flashbots+IC.London)
- Startups Web3 via iExec

Événements de recherche & Présentations



Type	Date	Event	Reach
Presentation	03/22	GDR RSD & ASF Winter School	National
	05/22	Irixys workshop in Passau	Consortium
	02/23	Journée des thèses du LIRIS	Laboratory
	03/23	2nd RedChainLab workshop	Collab.
	05/23	Irixys workshop in Lyon	Consortium
	07/23	**comPAS 2023 in Annecy**	*Francophonie*
	09/23	**PRIMATE seminar in Lyon**	FR-DE lab.partn.
	01/24	**Cybersecurity PEPR Winter School**	National
Poster	01/23	GDR-RSD: Journées non thématiques	National
Presence	01/22	Journée des thèses du LIRIS	Laboratory
	04/22	EuroSys'23 (incl. doctoral workshop)	International

Conditions matérielles

Locaux:

- Bureau doctorant LIRIS-DRIM
- Bureaux open-space iExec

Matériel:

- Laptop pro. Dell
- UC (SGX-enabled)
- Accès cloud Azure

Formation

Formation scientifique : 65h/30h

Formation à l’Insertion Professionnelle : 32h/30h

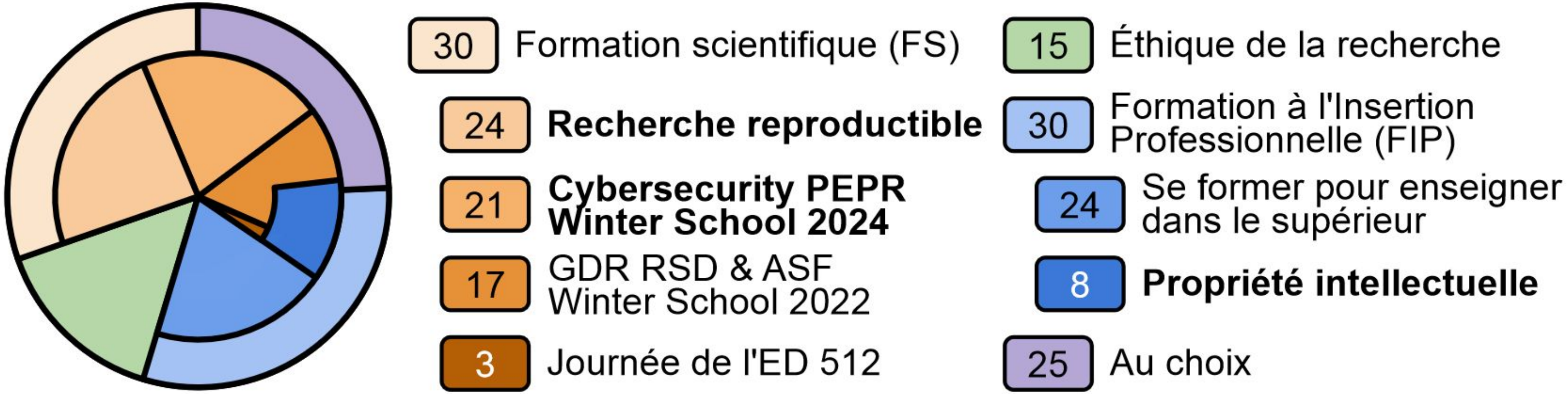


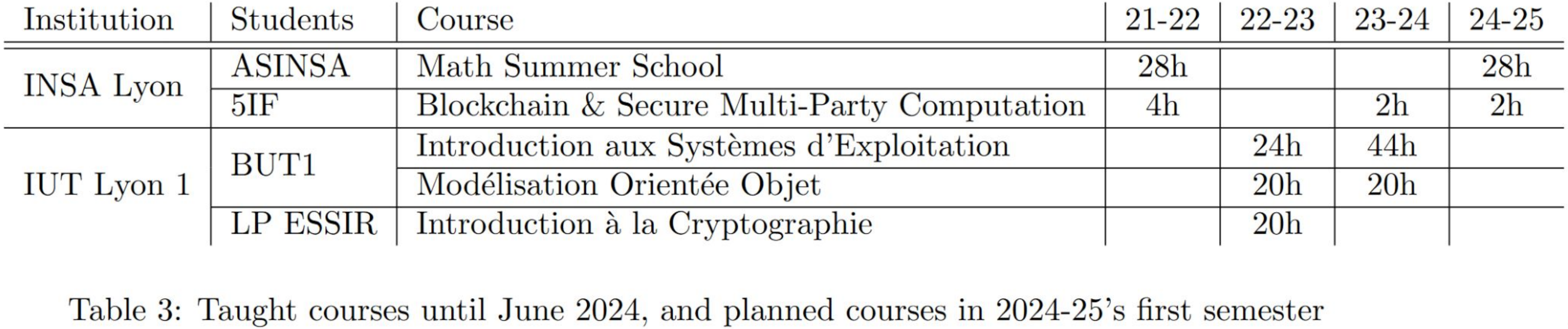
Figure 1: Accomplished training (new in **bold**)

Activités complémentaires

Enseignement:

- Contrat d’ACE à l’IUT Lyon 1 (2022-2024)

Répartition des heures: 146h effectuées + 16h affectées + 30h prévues /192h



Institution	Students	Course	21-22	22-23	23-24	24-25
INSA Lyon	ASINSA	Math Summer School	28h			28h
	5IF	Blockchain & Secure Multi-Party Computation	4h		2h	2h
IUT Lyon 1	BUT1	Introduction aux Systèmes d’Exploitation		24h	44h	
		Modélisation Orientée Objet		20h	20h	
	LP ESSIR	Introduction à la Cryptographie		20h		

Table 3: Taught courses until June 2024, and planned courses in 2024-25’s first semester

Bibliographie

ServiLI-TEE:

G. Fernandez, A. Brito, and C. Fetzer, “Triad: Trusted Timestamps in Untrusted Environments,” in *2023 IEEE International Conference on Cloud Computing Technology and Science (CloudCom)*, Dec. 2023, pp. 169–176. doi: 10.1109/CloudCom59040.2023.00037

C. Dong *et al.*, “T-Counter: Trustworthy and Efficient CPU Resource Measurement Using SGX in the Cloud,” *IEEE Transactions on Dependable and Secure Computing*, vol. 20, no. 1, pp. 867–885, Jan. 2023, doi: 10.1109/TDSC.2022.3145814.

G. M. Hamidy, P. Philippaerts, and W. Joosen, “T3E: A Practical Solution to Trusted Time in Secure Enclaves,” in *Network and System Security*, S. Li, M. Manulis, and A. Miyaji, Eds., in Lecture Notes in Computer Science. Cham: Springer Nature Switzerland, 2023, pp. 305–326. doi: 10.1007/978-3-031-39828-5_17.

F. Alder, N. Asokan, A. Kurnikov, A. Paverd, and M. Steiner, “S-FaaS: Trustworthy and Accountable Function-as-a-Service using Intel SGX,” in *Proceedings of the 2019 ACM SIGSAC Conference on Cloud Computing Security Workshop*, in CCSW’19. New York, NY, USA: Association for Computing Machinery, Nov. 2019, pp. 185–199. doi: 10.1145/3338466.3358916.

Y. Zhang, W. You, S. Jia, L. Liu, Z. Li, and W. Qian, “EnclavePoSt: A Practical Proof of Storage-Time in Cloud via Intel SGX,” *Security and Communication Networks*, vol. 2022, p. e7868502, May 2022, doi: 10.1155/2022/7868502.

P.M Abhishek, Akash Chobari, and D. G. Narayan. 2021. SLA Violation Detection in Multi-Cloud Environment Using Hyperledger Fabric Blockchain. In 2021 IEEE International Conference on Distributed Computing, VLSI, Electrical Circuits and Robotics (DISCOVER) (2021-11). 107–112. https://doi.org/10.1109/DISCOVER52564.2021.9663620

João Paulo de Brito Gonçalves, Roberta Lima Gomes, Rodolfo da Silva Villaca, Esteban Municio, and Johann Marquez-Barja. 2020. A Service Level Agreement Verification System Using Blockchains. In 2020 IEEE 11th International Conference on Software Engineering and Service Science (ICSESS) (2020-10). 541–544. https://doi.org/10.1109/ICSESS49938.2020.9237735

Huan Zhou, Cees de Laat, and Zhiming Zhao. 2018. Trustworthy Cloud Service Level Agreement Enforcement with Blockchain Based Smart Contract. In 2018 IEEE International Conference on Cloud Computing Technology and Science (CloudCom) (2018-12). 255–260. https://doi.org/10.1109/CloudCom2018.2018.00057

J.Acker internship:

N. V. Keizer, O. Ascigil, M. Król, and G. Pavlou, “Ditto: Towards Decentralised Similarity Search for Web3 Services,” in *2023 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPS)*, Athens, Greece: IEEE, Jul. 2023, pp. 66–75. doi: 10.1109/dapps57946.2023.00018.

M. Li *et al.*, “Bringing Decentralized Search to Decentralized Services,” presented at the 15th {USENIX} Symposium on Operating Systems Design and Implementation ({OSDI} 21), 2021, pp. 331–347. Accessed: Feb. 18, 2022. [Online]. Available: https://www.usenix.org/conference/osdi21/presentation/li

P. Agostinho, D. Dias, and L. Veiga, “SmartPubSub: Content-based Pub-Sub on IPFS,” in *2022 IEEE 47th Conference on Local Computer Networks (LCN)*, Sep. 2022, pp. 327–330. doi: 10.1109/LCN53696.2022.9843795.

P. Salehi, K. Zhang, and H.-A. Jacobsen, “On Delivery Guarantees in Distributed Content-Based Publish/Subscribe Systems,” in *Proceedings of the 21st International Middleware Conference*, in Middleware ’20. New York, NY, USA: Association for Computing Machinery, Dec. 2020, pp. 61–73. doi: 10.1145/3423211.3426400.

H.Mont internship:

Gilles Fedak, Wassim Bendella, and Eduardo Alves. iExec : Blockchain-Based Decentralized Cloud Computing. Technical report, http://iex.ec/wp-content/uploads/pdf/iExec-WPv3, 2018.

Luis FG Sarmenta. Sabotage-tolerance mechanisms for volunteer computing systems. In *Proceedings First IEEE/ACM International Symposium on Cluster Computing and the Grid*, pages 337–346. IEEE, 2001.

Gilles Fedak, Cécile Germain, Vincent Neri, and Franck Cappello. Xtremweb : A generic global computing system. In *Proceedings First IEEE/ACM International Symposium on Cluster Computing and the Grid*, pages 582–587. IEEE, 2001.

Omar Hasan, Lionel Brunie, and Elisa Bertino. Privacy-preserving reputation systems based on blockchain and other cryptographic building blocks: A survey. *ACM Computing Surveys (CSUR) 55.2* (2022): 1-37.

Fair Quality of Service in Adversarial Decentralized Marketplace Mechanisms

06/05/2024 – Comité de suivi de thèse D3

Matthieu BETTINGER
PhD. student – RedChain-Lab