RÉPUBLIQUE FRANÇAISE
Liberté Égalité Fraternité

REDEEM

Resilient, Decentralized and Privacy-Preserving Machine Learning

PROGRAMME DE RECHERCHE
FRANCE 2030
INTELLIGENCE ARTIFICIELLE

CNRS – LIRIS – DRIM Team	**Sonia BEN MOKHTAR**
CEA LIST – Distributed Learning Team	**Cédric GOUY-PAILLER**
Ecole polytechnique – IPP – SIMPAS Team	Aymeric DIEULEVEUT
INRIA – Team MAGNET	Jan RAMON
INRIA – Team ARGO	Kevin SCAMAN
CEA LIST – Distributed Systems Team	Antonella DEL POZZO
CNRS LAMSADE – Miles Team	Rida LARAKI

anr agence nationale de la recherche

Current state of Artificial Intelligence in gobal economy

Value Chain: data and computing power

- Algorithms are widely accessible
- Unequal abilities of economic actors to gather quality data
- Dominant pattern : « unreasonable effectiveness of data »

Fragmented market, largely influenced by a few major actors

- A few actors are gathering huge amount of data
- Unequal access to computing resources
- Highly unequal access to skilled workers able to use computing resources to build on AI

The citizen: producing data, consuming AI

- Users → data → gathered by big actors → AI-based services
- Increasing use of AI at work and in everyday life

Is another approach conceivable?

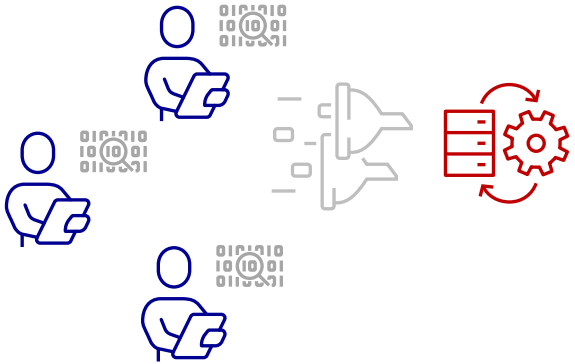
« Europe can develop an AI ecosystem that brings the benefits of the technology to the whole of European society and economy:

- *for citizens […]*
- *for business […]*
- *for services of public interest […] »*

REDEEM ambition: empower citizens, economic actors and public services with capacities regain control over their data and build needed services based on these data in a **trustworthy** manner!

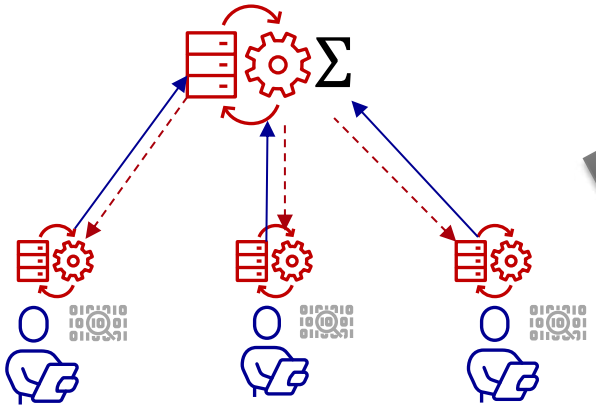
* European Commission (2020). White Paper on Artificial Intelligence: a European approach to excellence and trust. https://commission.europa.eu/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en.

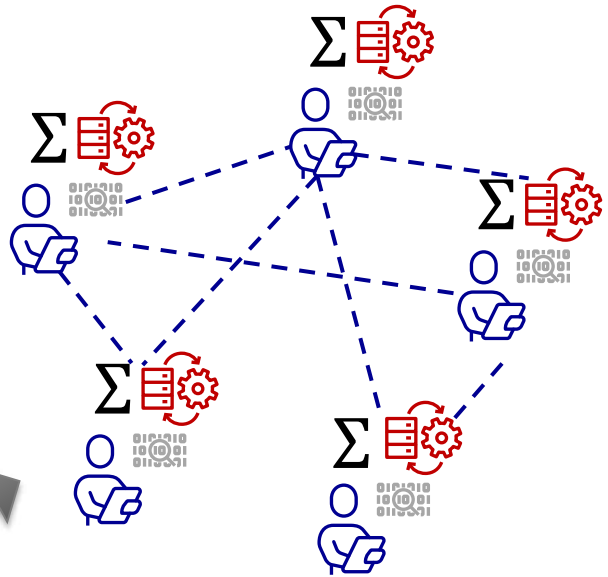
Towards fully decentralized learning



Centralized learning

Federated learning





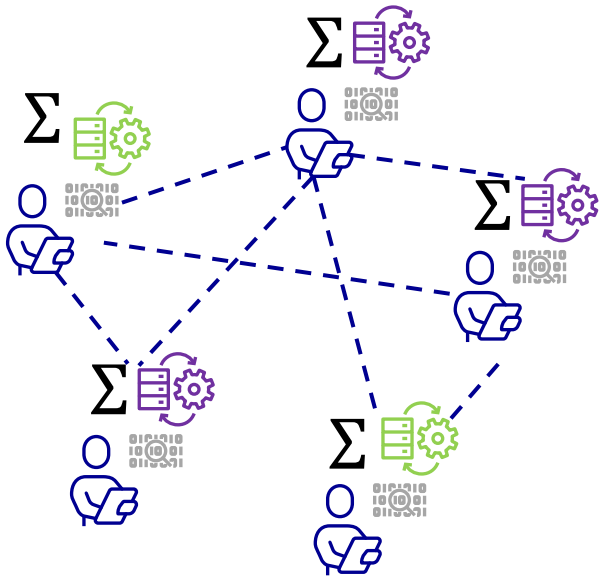
Decentralized learning

Characteristics of Decentralized Learning

- Relies on **direct communication** between data holders.
- Data remains **local**: model parameters are exchanged between participants.
- Allows **asynchrony**: no need for central orchestration.
- **Scalability**: potentially large number of participants.
- **Heterogeneity**: data distribution, computational resources and availability of participants may vary.

Research challenges

- ❑ Distributed optimization theory[1]
- ❑ Data heterogeneity[2, 3]



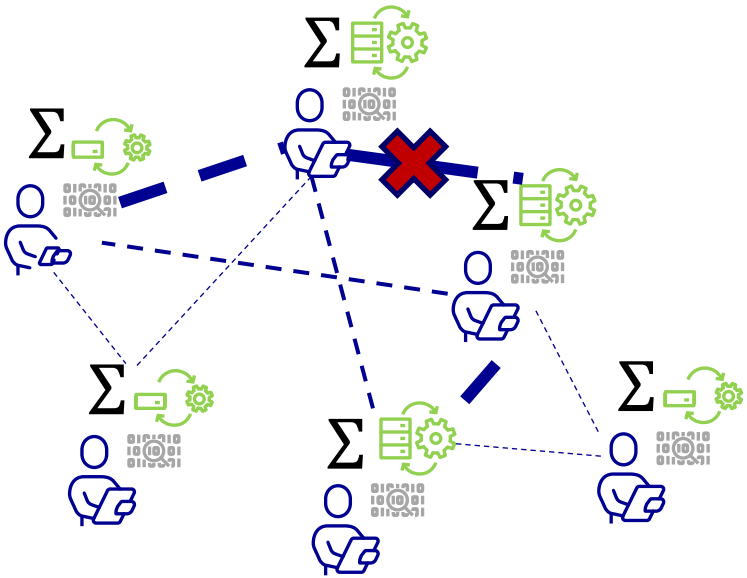
[1] K. Scaman, F. Bach, S. Bubeck, Y. Lee, and L. Massoulié, “Optimal convergence rates for convex distributed optimization in networks,” *J. Mach. Learn. Res.*, vol. 20, pp. 1–31, 2019.

[2] Li, Q., Diao, Y., Chen, Q., and He, B. (2022). Federated learning on non-iid data silos: An experimental study. In 2022 IEEE 38th international conference on data engineering (ICDE) (IEEE), pp. 965–978.

[3] Kairouz, P., McMahan, H.B., Avent, B., Bellet, A., Bennis, M., Bhagoji, A.N., Bonawitz, K., Charles, Z., Cormode, G., and Cummings, R. (2021). Advances and open problems in federated learning. Foundations and trends® in machine learning *14*, 1–210.

Research challenges

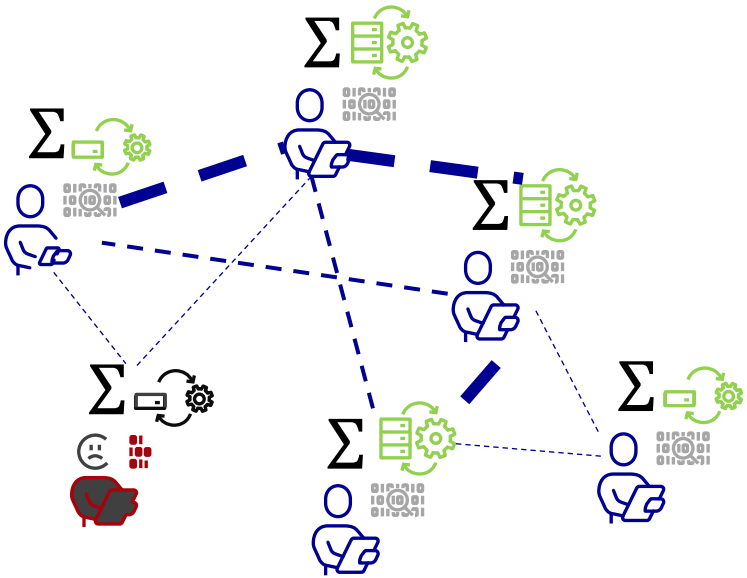
- ❑ Distributed optimization theory
- ❑ Data heterogeneity
- ❑ Network dynamics
- ❑ Device capacity, model size, communication constraints[4]



[4] *C. Philippenko, A. Dieuleveut, Preserved central model for faster bidirectional compression in distributed settings, NeurIPS 2021*

Research challenges

- ❑ Distributed optimization theory
- ❑ Data heterogeneity
- ❑ Network dynamics
- ❑ Device capacity, model size, communication constraints
- ❑ Resilience to attacks[5, 6]
  - Inference attacks from exchanged models
  - Byzantine attacks (*e.g.*, poisoning, backdoor attacks)



[5] C. Sabater, “Efficient and Robust Protocols for Privacy-Preserving Semi-Decentralized Machine Learning,” PhD Thesis, Université de Lille, 2022.

[6] Y. Mao, D. Data, S. Diggavi, and P. Tabuada, “Decentralized Learning Robust to Data Poisoning Attacks,” in *2022 IEEE 61st Conference on Decision and Control (CDC)*, IEEE, 2022, pp. 6788–6793.

Objectives and research directions

Research objective 1 (RO1): Explore algorithmic aspects of decentralized learning in a adversary-free environment

- Explore novel optimization paradigms beyond empirical risk minimization
- Explore novel decentralized algorithms for extremely large models
- Study the impact of gossiping algorithms on the performance of decentralized learning
- Study the impact of network heterogeneity and dynamics on decentralized learning
- Design innovative approaches for personalized learning in decentralized settings

Objectives and research directions

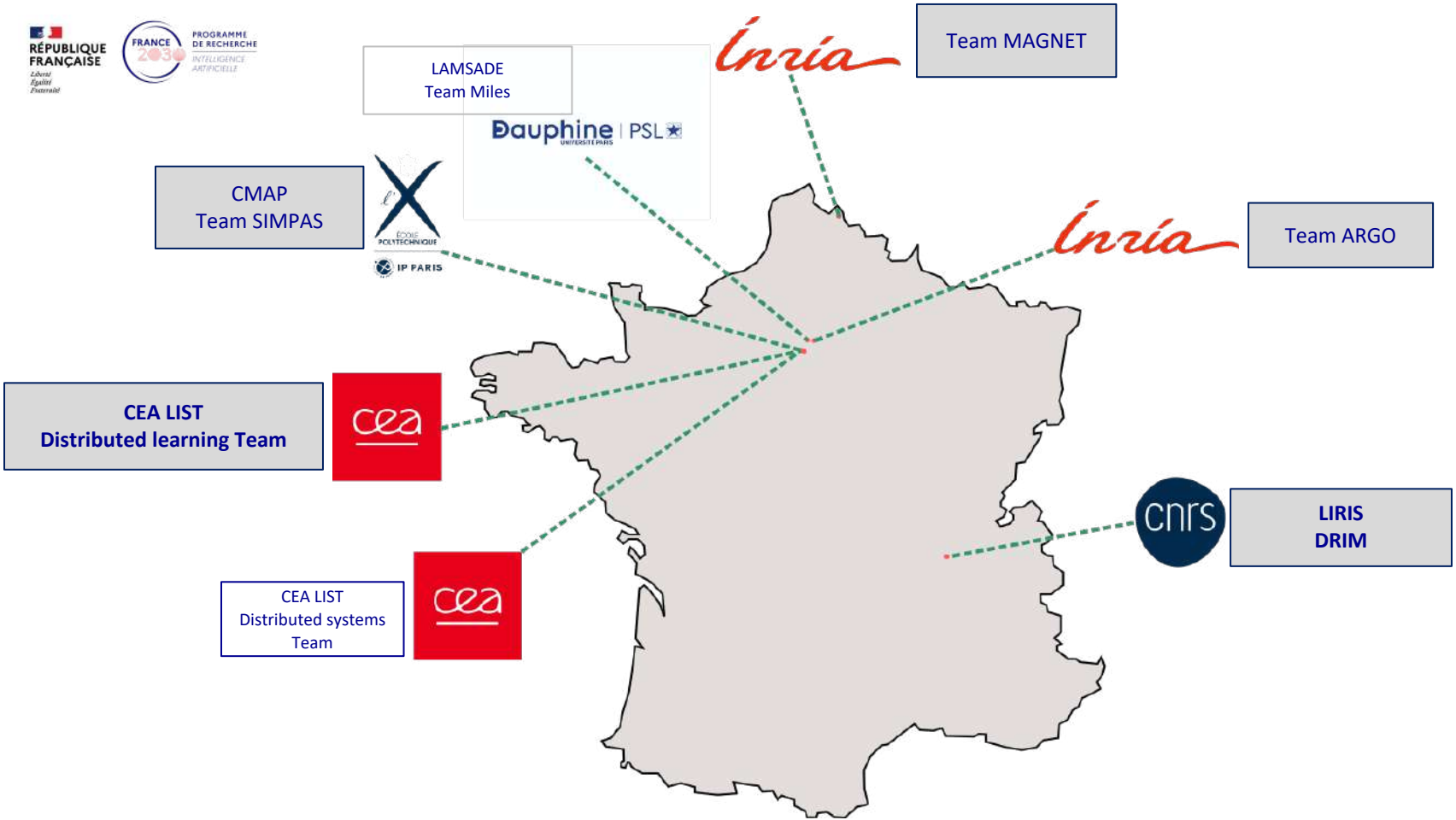
Research objective 2 (RO2): Investigate decentralized learning under attack

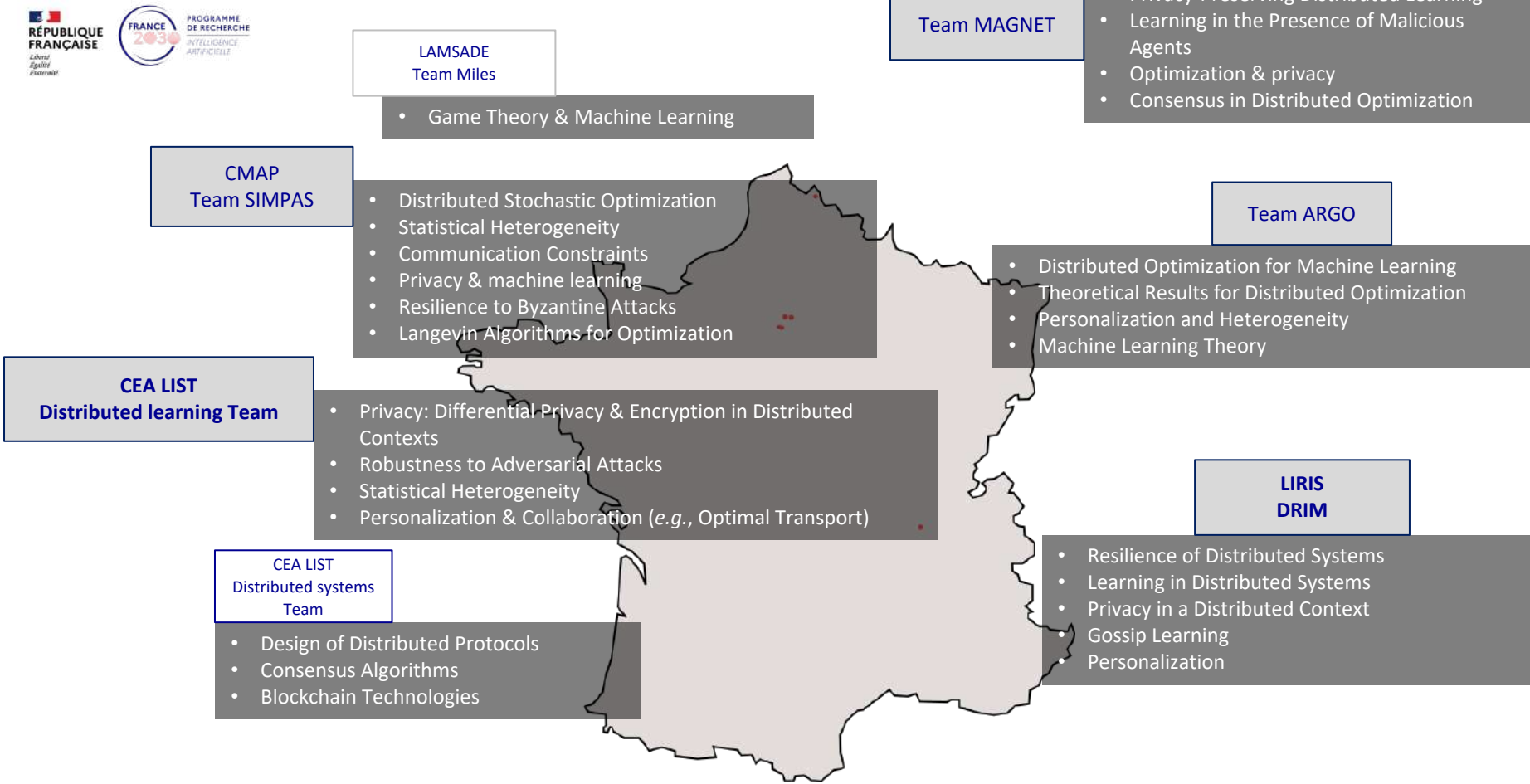
- Privacy attacks and mitigation mechanisms: beyond classical differential privacy (DP)
- Byzantine attacks and mitigation mechanisms: accountability, fault detection, fault tolerance mechanisms, consensus protocols, etc.
- Selfish behaviors and incentives: game theory
- Advanced threats and mitigation mechanisms: colluders, combined threat models, etc.

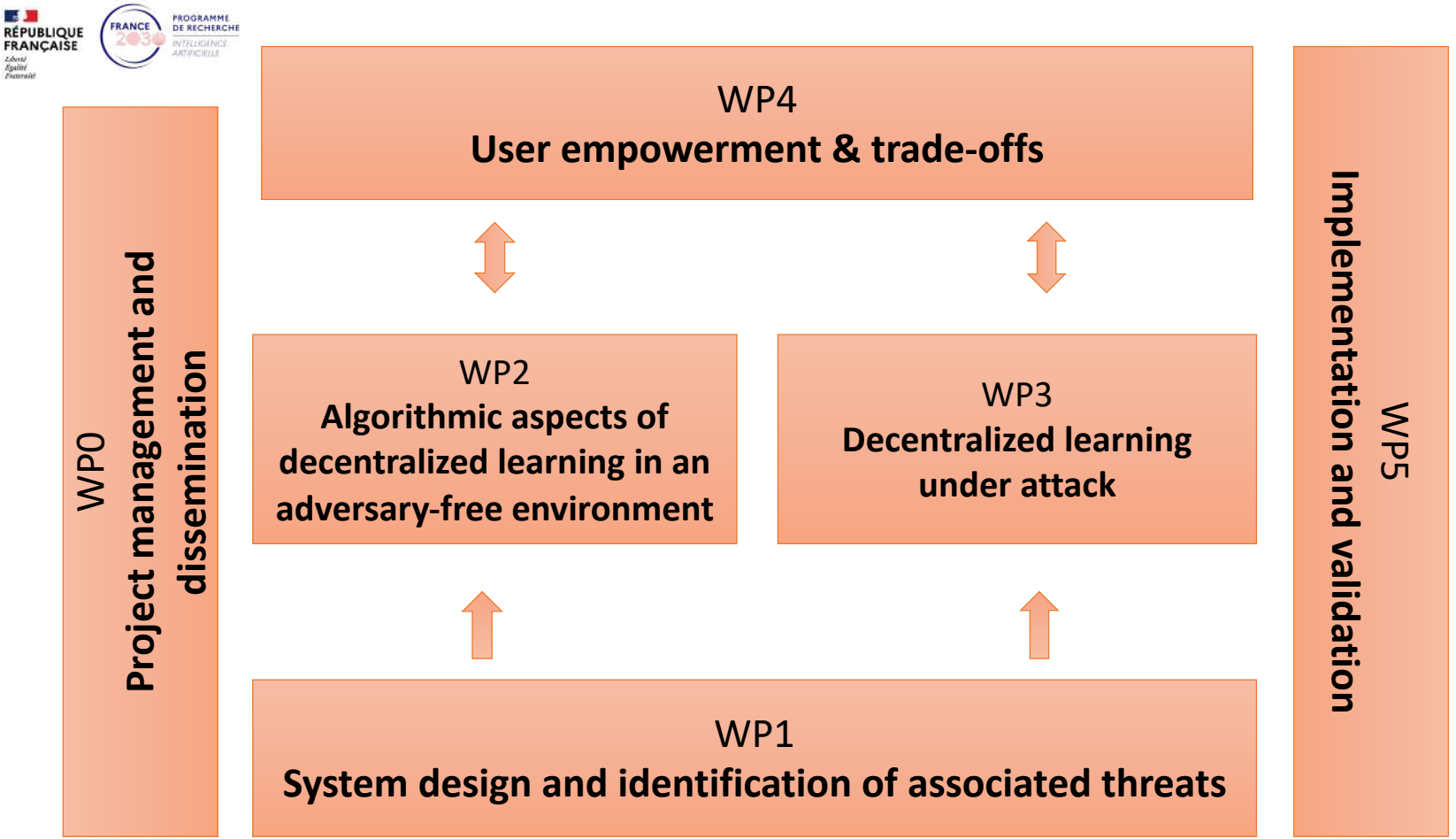
Objectives and research directions

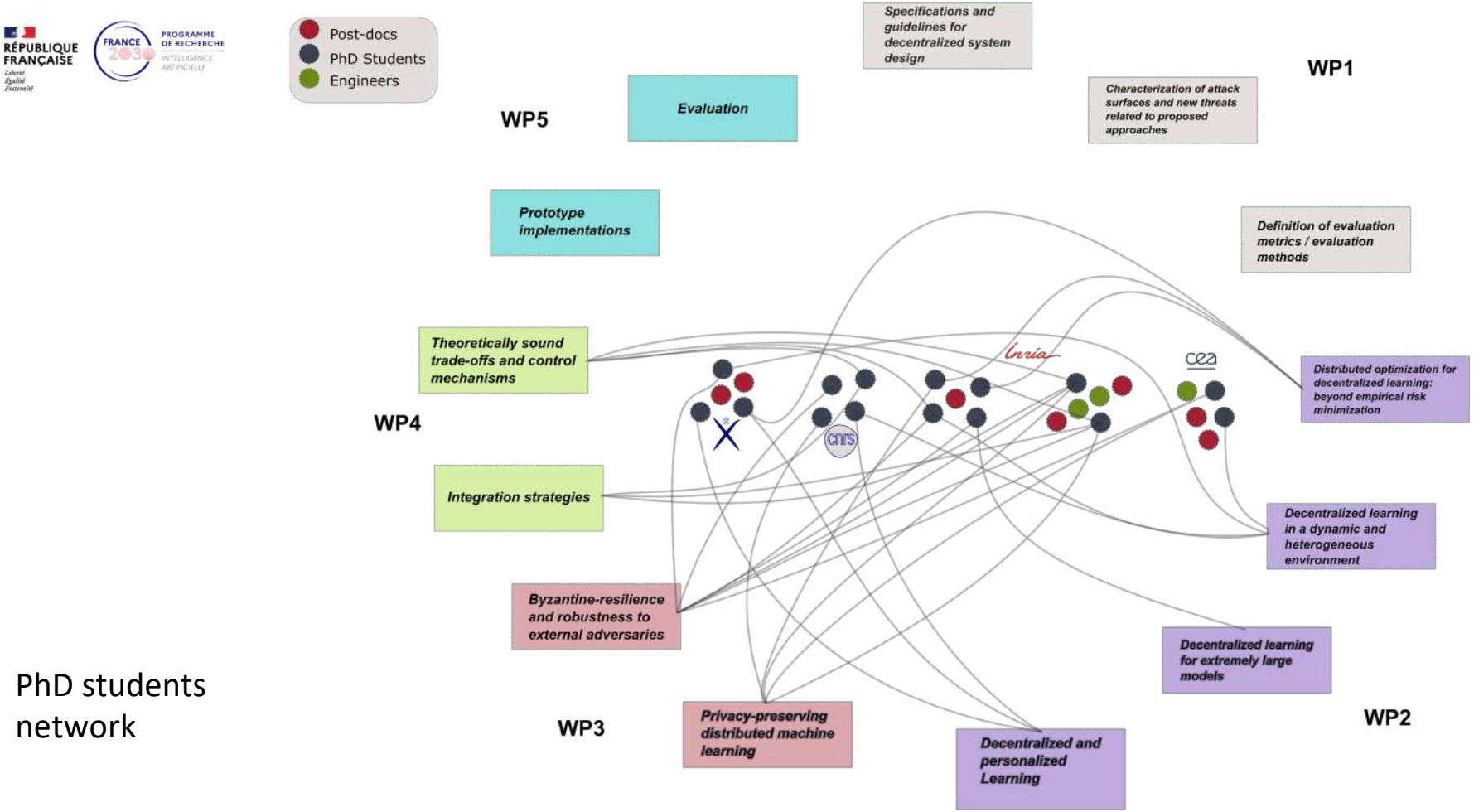
Research objective 3 (RO3): Study performance and resilience trade-offs for decentralized learning in the wild

- The impact of threats investigated in RO2 on algorithms devised in RO1
- The ability of the mitigation mechanisms designed in RO2 to resist these threats and their impact on performance metrics (e.g., model convergence)
- Integration, performance measurement, validation, proofs


Team MAGNET
LAMSADE
Team Miles
Dauphine | PSL
CMAP
Team SIMPAS
Team ARGO
CEA LIST
Distributed learning Team
LIRIS
DRIM
CEA LIST
Distributed systems
Team


LAMSADE
Team Miles
Game Theory & Machine Learning
Team MAGNET
Privacy-Preserving Distributed Learning
Learning in the Presence of Malicious Agents
Optimization & privacy
Consensus in Distributed Optimization
CMAP
Team SIMPAS
Distributed Stochastic Optimization
Statistical Heterogeneity
Communication Constraints
Privacy & machine learning
Resilience to Byzantine Attacks
Langevin Algorithms for Optimization
Team ARGO
Distributed Optimization for Machine Learning
Theoretical Results for Distributed Optimization
Personalization and Heterogeneity
Machine Learning Theory
CEA LIST
Distributed learning Team
Privacy: Differential Privacy & Encryption in Distributed Contexts
Robustness to Adversarial Attacks
Statistical Heterogeneity
Personalization & Collaboration (e.g., Optimal Transport)
LIRIS
DRIM
Resilience of Distributed Systems
Learning in Distributed Systems
Privacy in a Distributed Context
Gossip Learning
Personalization
CEA LIST
Distributed systems
Team
Design of Distributed Protocols
Consensus Algorithms
Blockchain Technologies


WP0
Project management and dissemination
WP4
User empowerment & trade-offs
WP2
Algorithmic aspects of decentralized learning in an adversary-free environment
WP3
Decentralized learning under attack
WP1
System design and identification of associated threats
WP5
Implementation and validation



PhD students network

2nd onsite technical REDEEM meeting.
35 people.
2024-03-21

Targeted results

Develop theoretical and practical foundations for trustworthy decentralized AI

- Research papers in the top international conferences and journals
- Training of young experts in resilient decentralized AI
- 15 PhD students and eq. ~ 20 years post-doctoral researchers directly funded by the project
- Cross-teams theoretical and empirical papers
- Software libraries enabling the rapid prototyping of trustworthy decentralized AI
- Proof of concept and demonstrators
- Articles and outreach to the general public
  - The Conversation, Le Monde/Binaire, ActuIA
- Organization of scientific events
  - *e.g.*, an annual event with the involvement of national and international experts

Anticipated outcomes and future valorization

Leverage effect for European projects

- ERC Grants
- Horizon Europe Projects

Support for the Competitiveness of Economic Actors

- Technology Transfer to SMEs, Intermediate-sized Enterprises, Large Companies
- Exploration of Valorization Models

Regulatory impacts

- Analysis of the Impact of Regulations on a Distributed Model
- Decision Makers Enlightment

Political Impact on Financing Actors

- Public Support to Foster a Model of Pooling Interests for Actors

Empowerment of Moderate-sized Actors (citizens, local communities, SMEs)

- Support for Actors, Associations in Networking Interests and Exploiting REDEEM Components

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

cea cnrs Inria

FRANCE 2030

PROGRAMME DE RECHERCHE

INTELLIGENCE ARTIFICIELLE

Questions?

anr agence nationale de la recherche