www.loria.fr

Loria
Laboratoire lorrain de recherche en informatique et ses applications

# Systèmes collaboratifs de confiance à large échelle

## Journée Mobilité 3.0

Gérald Oster, Equipe-projet COAST

3 juillet 2018

https://twitter.com/Loria_Nancy

gerald.oster@loria.fr

# Thèmes de recherche

- **Systèmes collaboratifs à large échelle sans autorité centrale**
- Confiance et expérience utilisateur
- Cloudware et composition de services

- Applications :
  - Gestion de crise,
  - Ingénierie logicielle,
  - Travail collaborative,
  - Ville intelligente.

Loria

# Collaboration à large échelle

Exemples: Wikis, DVCS, GoogleDocs

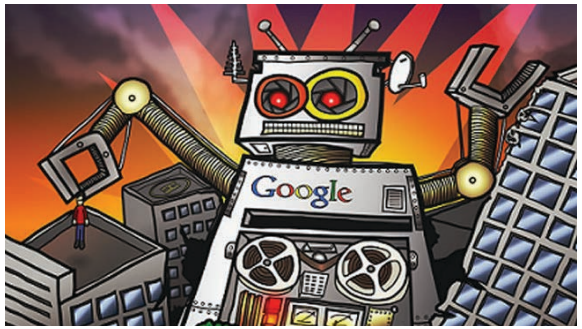
Large échelle : de quelques utilisateurs à des communautés d'utilisateurs

Loria

# Collaboration à large échelle

1 Qui contrôle le serveur ? Qui collaborent ? Comment ?

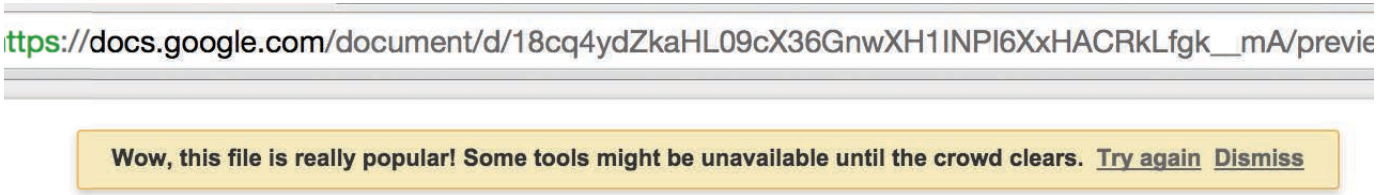
- Centralized control
- Privacy/Trust issues
- Federations





2 Quel passage à l'échelle ?

- Scalability issues (e.g. GoogleDocs 50 users sharing limit)

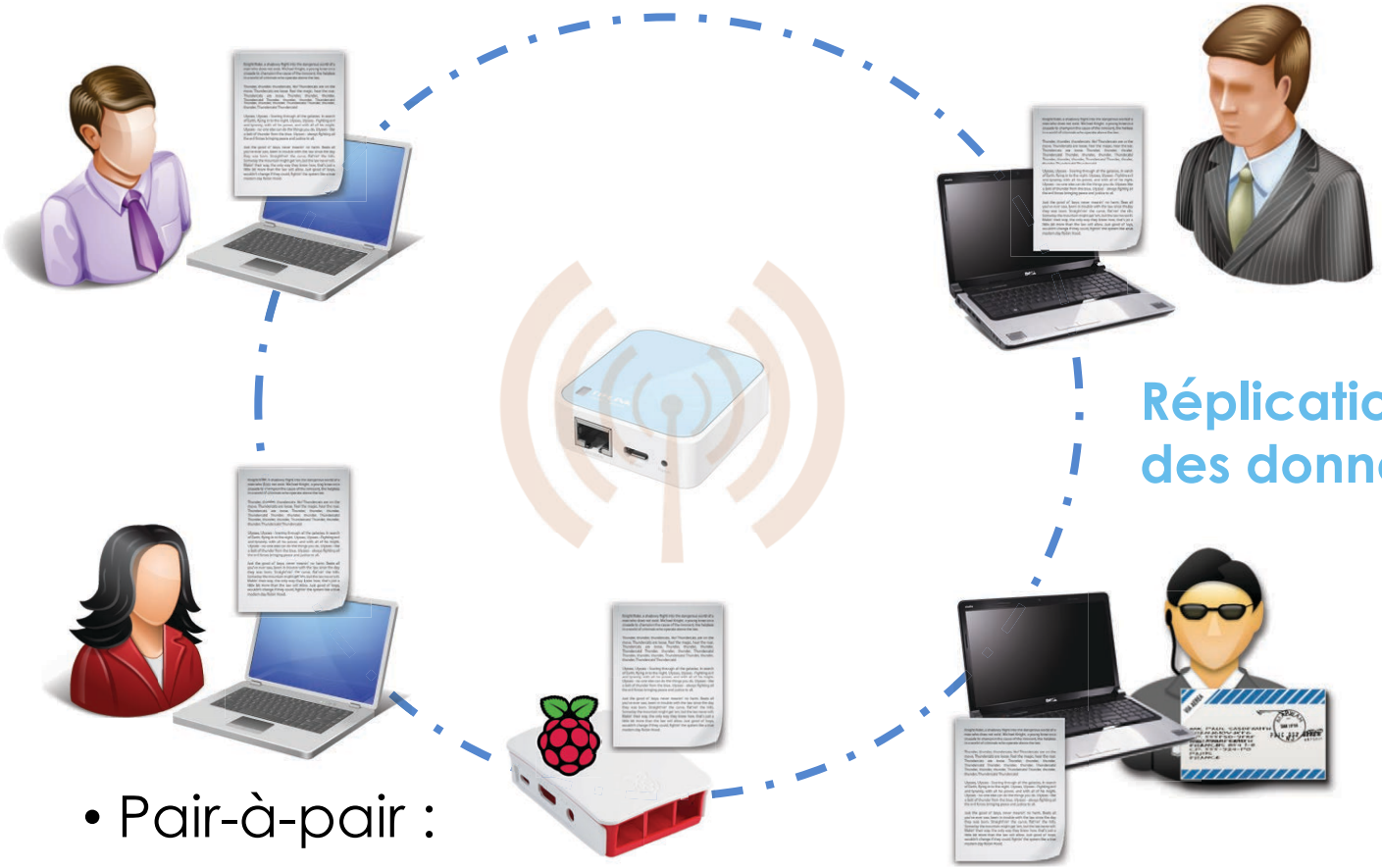



3 Qui paient les coûts ?

- High administration costs (not shared)


Loria

# Collaboration sans serveur central



Réplication optimiste des données

- Pair-à-pair :
  - chacun contrôle la collaboration
  - passe à l'échelle
- Infrastructure réduite
- collaboration utilisateur-machine

Loria

# Problématiques de recherche

1. Comment maintenir la **cohérence de différentes copies de données** en présence de **modification concurrentes** ?

2. Comment garantir le **passage à l'échelle** ?

3. Comment fournir des **mécanismes légers de sécurité** aux services permettant un **accès flexible** et **dynamique** aux ressources partagées ?

4. Comment **évaluer de tels systèmes** collaboratifs ?

Loria

# Problématique de recherche


Comment maintenir la **cohérences des données** répliquées en présence de **modifications concurrentes** ?

Loria

# Réplication Optimiste
## Approche orientée opération

- *n* copies d'un contenu hébergées sur *n* sites
- Un contenu est modifié en appliquant des opérations
- Chaque opération est :
  - générée sur un site(exécution locale), et appliquée immédiatement ;
  - diffusée aux autres sites ;
  - intégrée sur les autres sites (exécution distante).

- Le système est correct si et seulement si les copies sont identiques quand le système est au repos

Loria

# Réplication Optimiste
## Cohérence

- Trade-off entre cohérence et disponibilité
  - Réplication optimiste : autoriser la divergence entre copies
- Cohérence forte à terme
  - Cohérence à terme : « *An update executed at some correct replica eventually executes at all correct replicas* »
  - Convergence forte : « *correct replicas that have executed the same updates have equivalent state* »
- Préservation des intentions (édition collaborative):
  - « *Effect of each operation should be observed on all copies* »

Loria

# Réplication Optimiste
## Types de données sans conflit (CRDT)


- Structure de données
  - Même sémantique (sans concurrence) qu'une structure classique
  - **Conçues pour que ses opérations commutent par construction**
- Register
  - Last-Writer Wins
  - Multi-Value
- Set
  - Grow-Only
  - 2-Phase
  - Observed-Remove
  - Observed-Update-Remove
- Map
- Counter
- Graph
  - Directed
  - Monotonic DAG
  - Edit graph
- **Sequence**

Loria

# Collaboration sans serveur central sécurisée

- Chiffrement de bout-en-bout
- Mécanisme de confiance

Loria

# Collaboration sans serveur central sécurisée

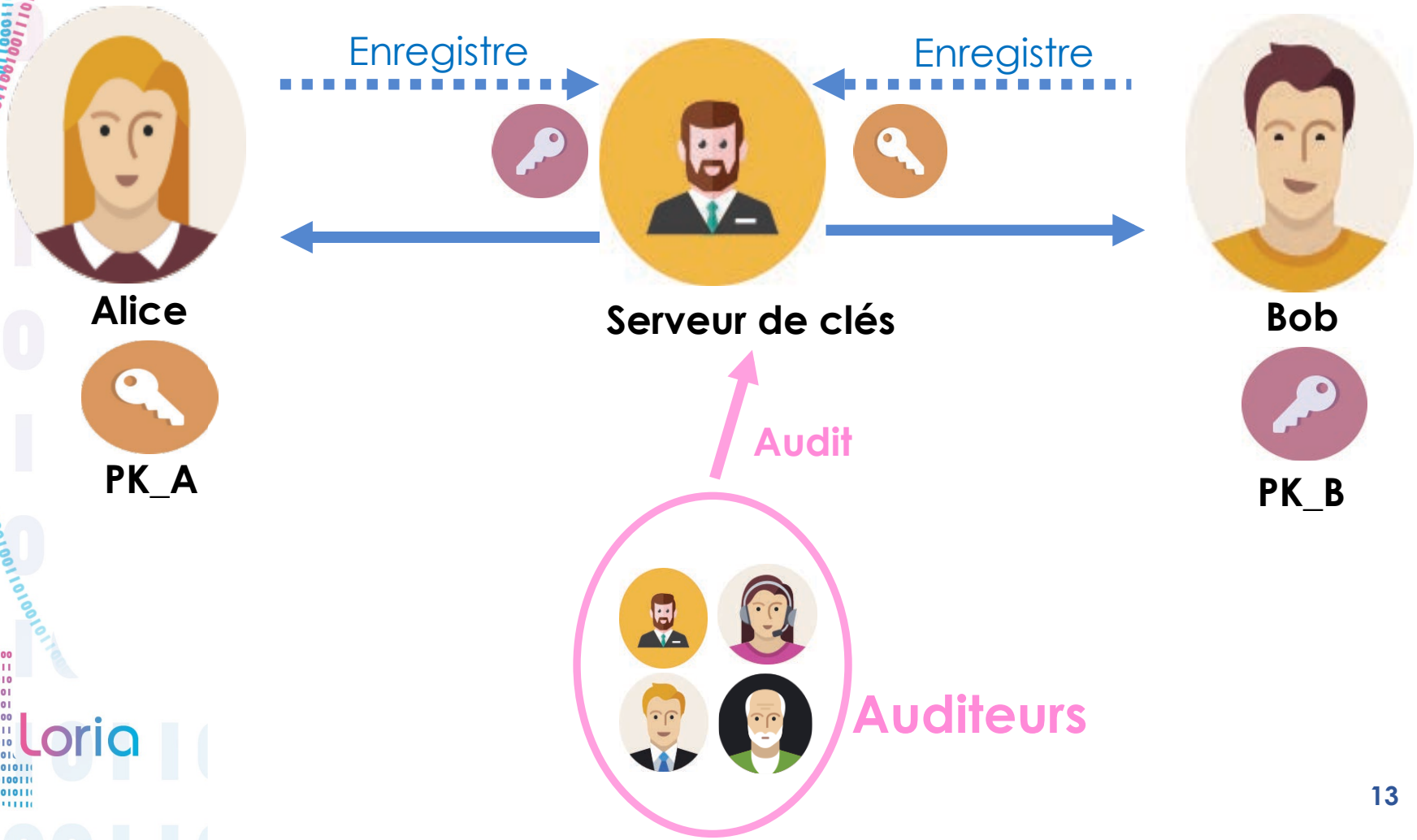
- Concevoir des approches adaptées aux différents modes de collaboration:
  - Autorisant les activités parallèles (édition hors-ligne, collaboration ad-hoc) de multiples sous groups dynamiques

- qui garantissent un chiffrement de bout-en-bout:
  - Comment préserver la **continuité du chiffrement et de la collaboration** ? (ajout, départ, bannissement de collaborateurs)
  - Comment gérer **l'historique de collaboration** *(forward/backward secrecy)* ?
  - Quand faut-il que les **clés de chiffrement** soient **générées**, **renouvelées**, **révoquées** and comment les **partager** ?

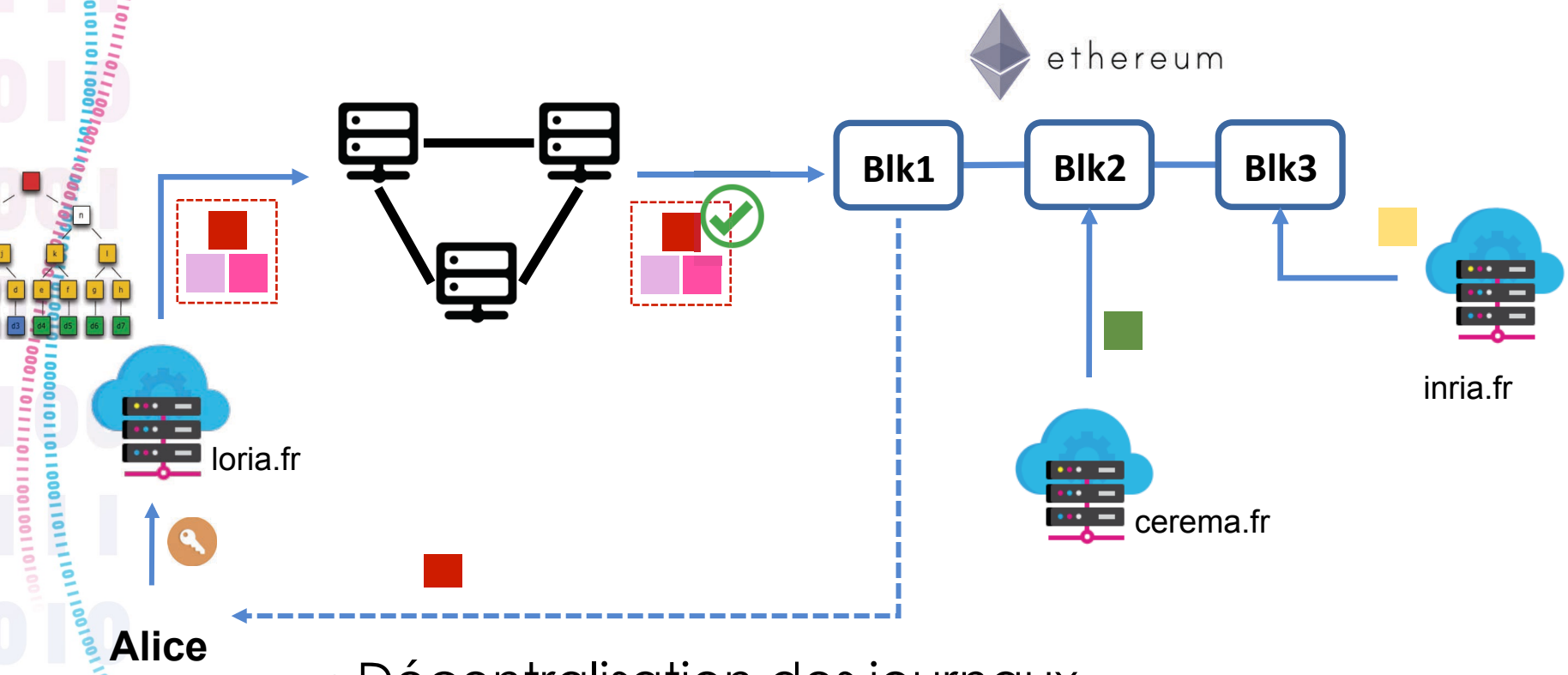
Loria

# Connaître et vérifier l'identité (clefs de chiffrement) d'un tiers ?

Journaux transparents *(transparency logs)*



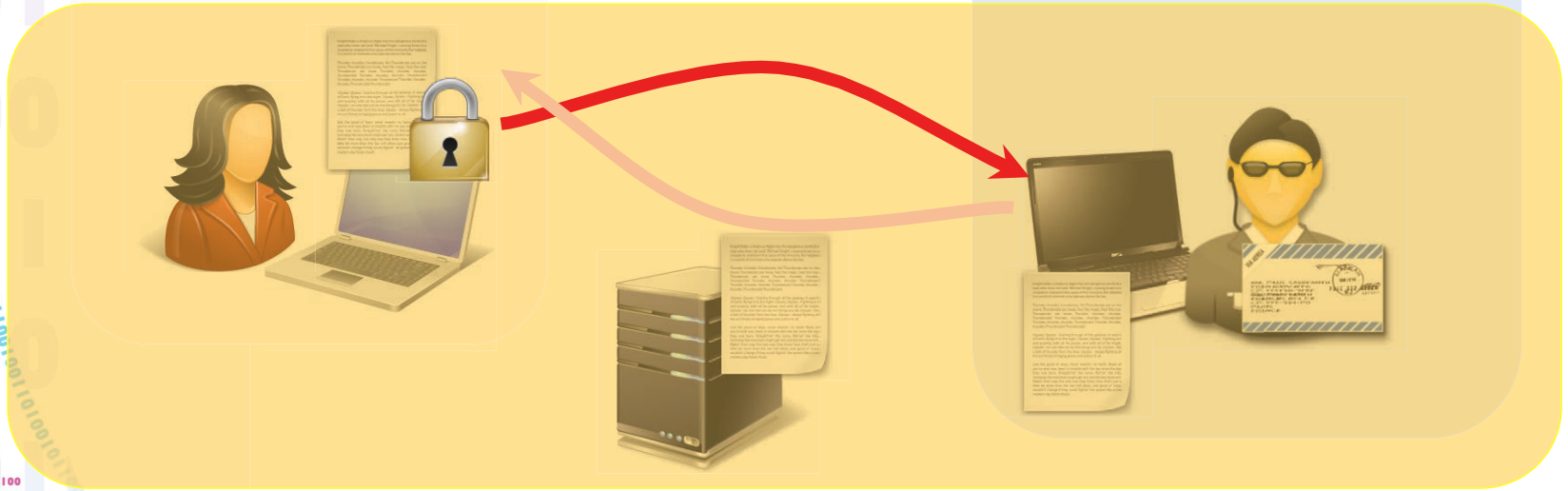
# Audit publique de la cohérence du journal




- Décentralisation des journaux
- Résumé des informations (clés) par arbre de Merkle
- Diffusion publique sur une chaîne de blocs *(blockchain)*

Loria

# Dimension multi-organisationnelle



- Contrôle de la collaboration par les partenaires
- Exemple application : gestion de crises

# OpenPaaS::NG (2014-2018)


bpifrance

cap·digital
Paris Region

Objectives:

*« Develop **a new generation open source platform for collaboration** for enterprises and administration **independently of** big collaboration **services providers** (e.g. Google) »*

Topics: data replication / user studies / secured collaboration

PSPC (Projet Structurant des Pôles de Compétitivité)

- Financed by BPI France / labelised by CapDigital

Partners:

- Linagora (MME, leader), XWiki SAS (SME), Nexedi (SME)
- LIX (DaScim team), LORIA (COAST team)

Period: 48 months / 236 man.years

Budget: 10,7 M€ (total cost: 20,7 M€)

Loria

# ANR STREAMS (2010-2014)



Objectives:

*« design **peer-to-peer solutions** that offer underlying services required **by real-time social web applications** [...]. These solutions are meant to **replace a central authority-based collaboration** with a distributed collaboration that offers support for **decentralisation of services**. »*

Topics: data replication / peer-to-peer collaboration/ trust-based access control

Partners:

- XWiki SAS (SME), Inria, LORIA (COAST / PESTO teams), University of Rennes 1

Period: 42 months

Budget: 450 k€ (total cost: 800 k€)

Loria

# Merci de votre attention

Équipe-projet COAST

https://team.inria.fr/coast/