Programme Interface 2019

Mathématiques de la « blockchain » et applications industrielles

Résumé

La technologie « blockchain » est apparue avec la crypto-monnaie «Bitcoin» en 2008 dont les principes sont décrits dans l'article fondateur de Satoshi Nakamoto (Nakamoto)*. Cette innovation de rupture a été perçue comme une opportunité pour revisiter les relations de confiance dans les services numériques, d'abord dans le secteur financier puis au sein des différents secteurs de l'industrie. Aujourd'hui, le modèle initial a généré une diversité de technologies « blockchain » ainsi qu'une grande variété de cas d'usages qui ne se cantonnent plus aux crypto-monnaies et ouvre de nouveaux sujets d'investigation à la croisée des mathématiques, de l'informatique et de la transformation numérique de la société.*

Pendant les 3 jours de cette session du programme Interface, académiques et industriels se retrouveront pour partager une compréhension commune de ces technologies « blockchain », partant des concepts de base pour aller vers des primitives cryptographiques avancées qui permettent notamment de gérer la confidentialité des données en environnement distribué. L'objectif principal et d'échanger sur des problématiques et techniques mathématiques spécifiques à la gestion de confiance en environnement distribué, en s'appuyant notamment sur des cas d'usages industriels (Identité, énergie, internet des objets,…).

Abstract

The « blockchain» technology appeared with the « Bitcoin » crypto-currency in 2008, whose principles are described in the founding article of Satoshi Nakamoto (Nakamoto). This breakthrough innovation was seen as an opportunity to revisit the relationship of trust in digital services, first in the financial sector and then in different business verticals of the industry. Today, the initial model has generated a diversity of « blockchain » technologies as well as a wide variety of use cases that are no longer confined to cryptocurrencies. This diversity opens up new subjects of investigation at the crossroads of mathematics, computer science and society's digital transformation.

During the 3 days of this session of the Interface program, academics and industry will meet to share a common understanding of these « blockchain » technologies, starting from basic concepts to go to advanced cryptographic primitives that allow to manage the confidentiality of data in particular in a distributed environment. The main objective is to discuss mathematical issues and techniques specific to trust management in a distributed environment, based in particular on industrial use cases (identity, energy, internet of things, etc.).

References

Ecosystem, S. P. (2015). *White paper: Blockchain: Myth or Reality?* https://systematic-paris-region.org/wp-content/uploads/2017/07/Systematic-LB-Blockchain-HD.pdf.

Nakamoto, S. (n.d.). Bitcoin: A Peer-to-Peer Electronic Cash System. *https://bitcoin.org/bitcoin.pdf*.

1. Comité d'organisation, intervenants et participants

1.1 Comité d'organisation

Le comité d'organisation est constitué des personnes suivantes.

- Jacques Patarin (Université de Versailles Saint-Quentin-en-Yvelines)
- Jean-Pierre Tual (Vice-Président du comité Interface)
- Aline Gouget (Gemalto)

1.2 Comité scientifique

Le comité scientifique est constitué des personnes suivantes.

- Daniel Augot (INRIA Saclay et LIX, École polytechnique)
- Julien Bringer (Smart Valor)
- Louis Goubin (Université de Versailles Saint-Quentin-en-Yvelines)
- Louis Granboulan (Airbus)
- Aline Gouget (Gemalto)
- Philippe Jacquet (Nokia)
- Jacques Patarin (Université de Versailles Saint-Quentin-en-Yvelines)

1.3 Audience visée

Académiques et industriels se retrouveront pour discuter et échanger sur le thème des mathématiques de la « blockchain » et ses applications industrielles.

Une introduction générale permettra à un public large de se familiariser avec les concepts de base afin de pouvoir échanger sur des problématiques spécifiques de la gestion de la confiance en environnement distribué et de se familiariser avec des exemples de cas d'usages industriels.

Des notions basiques en sécurité informatique et cryptographie sont souhaitables sans toutefois être nécessaires.

2. Programme prévisionnel

2.1 Journée 1

Matinée **Introduction aux principes mathématiques et technologies de la « blockchain »**

- Présentation : Les technologies « blockchain » ; de quoi parle-t-on ? (Aline Gouget, Gemalto)
- Présentation : Cohabitation de différentes technologies « blockchain » et smart contracts (Julien Bringer, Smart Valor)
- Echanges : Questions & retours sur les principaux sujets d'intérêt

Mots clés : *transaction, signature électronique, protocole de consensus, architecture distribuée, modèles public/privé/hybride, smart contracts, cryptlets*

Après-midi **Cas d'usage : Authentification, Identification**

- Présentation : Contrôle d'accès & « blockchain » (Sophie Dramé-Maigné, Telecom Sud Paris)
- Présentation : Identité digitale & « blockchain » (Laurent Castillo, Gemalto)
- Ateliers : échanges & discussions par petits groupes
- Partage d'information entre les différents ateliers

Mots clés : *authentification, gestion des identités personnelles en environnement distribué, protocoles associés, délégation, cas de l'Internet des Objets.*

2.2 Journée 2

Matinée **Confidentialité des données, Anonymat**

- Présentation : Quelques techniques cryptographiques de gestion de la confidentialité dans des « blockchain » (Daniel Augot, INRIA et Ecole Polytechnique)
- Présentation : Les crypto-monnaies et l'anonymat (Jacques Patarin, UVSQ)

Mots clés : *confidentialité et primitives cryptographiques associées (e.g. ZK-SNARK), crypto-monnaies et anonymisation de transactions, difficultés pratiques et théoriques.*

Après-midi **Cas d'usage : gestion des données**

- Présentation : EDF (à confirmer)
- Ateliers : Intervenants industriels gestionnaires de données - échanges & discussions par petits groupes.
- Partage d'information entre les différents ateliers

Problème clé : *protection des données et cyber-sécurité dans le contexte de la « blockchain » appliqué à des cas d'usages spécifiques.*

2.3 Journée 3

Matinée **La question de la confiance**

- Présentation : La question de la confiance, en particulier dans une « blockchain » et son écosystème ; une formalisation mathématique est-elle possible ? (Louis Granboulan, Airbus)
- Présentation : La « blockchain » en cas de catastrophe cryptographique : quelques scénarios (Louis Goubin, UVSQ)

Mots clés : *modèles de confiance distribuée et formalisation mathématique, cryptanalyse, impact sur les propriétés de sécurité, courbes elliptiques, fonctions de hachage, cryptographie post-quantique, "transition cryptographique".*

Après-midi **Le choix du protocole de consensus**

- Présentation Générale: (Georg Fuchsbauer, ENS)

- Optimisation énergétique de protocoles de consensus, Philippe Jacquet, Nokia)

- Ateliers : introduction sur la sécurité des protocoles de consensus en environnement blockchain publique ou privée, (Aline Gouget) suivie d'échanges & discussions par petits groupes

- Partage d'information entre les différents ateliers

Mots clés : *critères d'optimisation de protocoles de consensus: Proof-of-work, Proof-of-Stake, hard/soft fork, Practical Byzantine Fault Tolerant, Proof-of-Elapsed-Time, problème general du passage à l'échelle.*

Clôture : Session de bilan général entre les participants