

---

## 先端技術セミナー

---

日時： 9月5日(水) 16:50~18:20

場所： 北海道大学 工学部棟 オープンホール

演題： 「ブロックチェーン技術とその技術的背景」

講師： 田中 圭介 氏 (東京工業大学 情報理工学院 教授)

デファゴ クサヴィエ 氏 (東京工業大学 情報理工学院 教授)

### 講演概要：

#### Part 1: ブロックチェーンの概要

ビットコイン等の暗号通貨、および、暗号通貨を支えるブロックチェーン技術の概要を紹介し、ブロックチェーンの技術的背景について解説した後、ブロックチェーン技術とはなにかについて説明します。そこでは、ブロックチェーン技術で用いられる重要な構成要素である暗号技術についても述べるとともに、ブロックチェーンが動作するための重要な概念であるインセンティブについても述べます。さらに、ブロックチェーン技術の適用可能性についても議論します。

#### Part 2: Using Blockchains as support for State-Machine Replication

From an abstract viewpoint, blockchains provide support for a tamper-resistant distributed ledger which, in some instances, can operate without trusted third-parties and without explicit membership. The talk will relate the notion of blockchain and distributed ledger to several classical problems. A resilient log is necessary to ensure atomicity and durability of transactions. A tamper-proof ledger is required to ensure accountability and non-repudiation of transactions. A structure enforcing total order on operations is necessary to implement replicated services for high-availability and preserving service integrity. The talk will discuss how a blockchain can be used to implement the above mechanisms and what guarantees it can provide. Then, we will also discuss its limitations and provide some examples when a blockchain is simply not enough.

### 講師プロフィール

#### ■田中 圭介 教授



田中 圭介: 1992年 山梨大学 工学部 計算機科学科 卒業, 1994年 3月 北陸先端科学技術大学院大学 情報科学研究科 博士前期課程、1997年 3月 同 博士後期課程 修了, 博士(情報科学). 1997年 4月 NTT 情報通信研究所 分散環境アーキテクチャ研究部 社員, 1999年 2月 NTT 情報流通プラットフォーム研究所 情報セキュリティプロジェクト 研究主任, 2001年 4月 東京工業大学 大学院情報理工学研究科 数理・計算科学専攻 講師, 2004年 5月 同 助教授 (2007年 4月 同 准教授), 2016年 4月 東京工業大学 情報理工学院 准教授, 2016年 10月 同 教授, 2017年 4月 同 サイバーセキュリティ研究センター長 現在に至る. 東工大において現在に至るまでに、「NRI・東工大 サイバーセキュリティ教育研究共創プログラム」、「サイバーセキュリティ特別専門学修プログラム」、「Input Output 暗号通貨共同研究講座」のサイバーセキュリティ、暗号通貨・ブ

ロックチェーン技術分野の研究と教育に関するプロジェクトの立ち上げを行う。専門は暗号理論、暗号通貨とブロックチェーン技術、サイバーセキュリティ。

#### ■デファゴ クサヴィエ 教授



Xavier Defago is a professor at Tokyo Institute of Technology (Tokyo Tech) since 2016. His research interests include distributed algorithms, dependable computing, intrusion-tolerance, embedded systems, and cooperative autonomous mobile robots. Xavier obtained his master's degree in Computer Engineering in 1995 and Ph.D. in Computer Science in 2000 from the Swiss Federal Institute of Technology in Lausanne (EPFL, Switzerland). From 1995 to 1996, he worked at the NEC C&C Research Labs in Kawasaki (Japan). From 2000 to 2016, he was at the Japan Advanced Institute of Science and Technology (JAIST) as a research associate and then an associate professor. In 2013, he was also invited as a CNRS researcher in France, to work both at LIP6, UPMC, Paris, and at I3S, UNS, Inria Sophia Antipolis.