暗号通貨に関する IACR サマースクール及び ECRYPT ワークショップ参加報告

松本 晋一[†1]　穴田 啓晃[†2]　フォン ヤオカイ[†3]　櫻井 幸一[†3,4]

概要：2016 年 5 月 30 日から 6 月 2 日の 4 日間，ギリシャのコルフ島(ケルキラ)にて IACR 主催の暗号通貨に関するサマースクール"Blockchain Technologies: From Cryptographic E-Cash to Modern Cryptocurrencies"が開催された．またその翌日の 6 月 3 日，同国のアテネにて ECRYPT-CSA 主催の同テーマに関するワークショップ"Workshop on Cryptocurrencies"が開催された．本稿では両会合の概要について報告する．

キーワード：暗号通貨，ブロックチェーン，ビットコイン，学会参加報告

Report on IACR Summer School and ECRYPT workshop on Cryptocurrencies

Shinichi Matsumoto[†1]　Hiroaki Anada[†2]　Yaokai Feng[†3]　Kouichi Sakurai[†3,1]

Abstract: From May 30th to June 2nd, IACR held a summer school on cryptocurrencies named "Blockchain Technologies: From Cryptographic E-Cash to Modern Cryptocurrencies" in Corfu island (Kerkyra), Greece. Succeedingly ECRYPT-CSA held a one-day workshop named "Workshop on Cryptocurrencies" in Athens, Greece on June 3rd. In this report, we report the summary of these events.

Keywords: Cryptocurrency, blockchain, Bitcoin, Report on Conference

1. はじめに

2016 年の 5 月第 5 週(6 月第 1 週)，ギリシャにおいて暗号通貨/ブロックチェーンに関する二つの学術会合が連続で開催された．

5 月 30 日から 6 月 2 日の 4 日間は，ギリシャのコルフ島にてサマースクール"Blockchain Technologies: From Cryptographic E-Cash to Modern Cryptocurrencies"[1](以下，IACR サマースクール)が IACR 主催にて開催された．参加者数は目測で 130 名程であった．また参加者層としては，ドクター，ポスドクのような若い方々が多いように見受けられ，企業関係ではベンチャ系（IOHK など）が多かったようである．日本からの参加者は，本報告者（第一著者）を含め 4 名であった．

IACR サマースクールの翌日の 6 月 3 日，同国のアテネにて"Workshop on Cryptocurrencies"[2](以下，ECRYPT ワークショップ)が，ECRYPT-CSA (European network of Excellence for Cryptology – Coordination & Support Action)の主催で開催された．参加者数は目測で 25 から 30 名程であった．挙手によればその 9 割程が IACR サマースクール参加者であった．

以降の章で両会合の概要について報告する．

†1 公益財団法人九州先端科学技術研究所
Institute of Systems, Information Technologies and Nanotechnologies
†2 長崎県立大学情報セキュリティ学科
Department of Information Security, University of Nagasaki
†3 九州大学大学院システム情報科学研究院
Graduate School and Faculty of Information Science and Electrical Engineering, Kyushu University

2. IACR サマースクール

2.1 開催要項

IACR サマースクールは，コルフ島(ケルキラ島)にて催された．コルフ島は地中海東部のイオニア海に位置し，ギリシャを構成する島の中では最も北部に位置する．

会場は Corfu Imperial Hotel (図 1)であり，同ホテルはコルフ島東岸の岬の先端に位置することから，海の向こうにバルカン半島，アルバニアを望むことができる．

図 1　IACR サマースクール会場となった Corfu Imperial Hotel

運営委員及びスポンサーは下記のとおりであった.

(1) **運営委員**

- Foteini Baldimtsi, George Mason University, US
- Aggelos Kiayias, University of Edinburgh, UK
- Sarah Meiklejohn, University College London, UK)

(2) **スポンサー**

- OpenBazaar
- FrostWire
- IACR (International Association for Cryptographic Research)
- PJ Tech Catalyst
- GRNET
- Intel
- IOHK
- merlinux
- Rafik B.Hariri Institute for Computing and Computational Science & Engineering, Boston University

2.2 プログラム

(1) **Day 1(May 30th)**

- Bitcoin Overview (Joseph Bonneau, Stanford University)
- Aggelos Kiayias, University of Edinburgh, UK
- Scaling Bitcoin Securely (Aggelos Kiayias, University of Edinburgh, UK)
- Consensus (Roger Wattenhofer, ETH Zurlch, Switzerland)
- Mining (Joseph Bonneau, Stanford University, US)
- Reception

図 2　IACR サマースクール会場の模様(開場直後)

(2) **Day 2(May 31th)**

- Cryptographic e-cash (Jan Camenisch, IBM Research Zurich, Switzerland)
- Anonymity in Cryptocurrencies (Foteini Baldimtsi, George Mason University, US)
- Cryptography on the Blockchain (Vassilis Zokas, Rensselaer Polytechnic Institute, US)
- Short Talks

(3) **Day 3(June 1st)**

- Decentralization as a Privacy-Enhancing Technology (George Danezis, University College London，UK)
- Bitcoin de-anonymization in Practice (Adam Joyce, Elliptic, UK)
- Breakout Sessions
  - IOHK Session
  - Corfucoin Session

(4) **Day 4(June 2nd)**

- Anonymous Online Marketplace (Nicolas Christin, Carnegie Mellon University, US)
- The Bitcoin Economic Ecosystem (Rainer Böhme, Universität Innsbruck, AT)
- Regulation in Bitcoin (Jerry Brito, Coin Center, US)
- Alternatives to Blockchains (Sarah Meiklejohn, University College London, UK)

2.3 講演内容

以下に，講演を聴講した際の内容のメモ及び若干の見解を示す.

2.3.1 Bitcoin Overview

Joseph Bonneau (Stanford Univ.)

Bitcoin で使われている暗号プリミティブとしてハッシュ関数(SHA-256)，ハッシュポインタ，デジタル署名，(ECDSA)が解説された．次いで “Simple cryotocurrencies”と題し，二重使用(double spend)，グローバル台帳(global ledger)等が解説された．最後に，Bitcoin の取引きに関する技術上の話題として“Transaction semantics”, “Centralized ledge”, “Decentralized ledge”が取り上げられた.

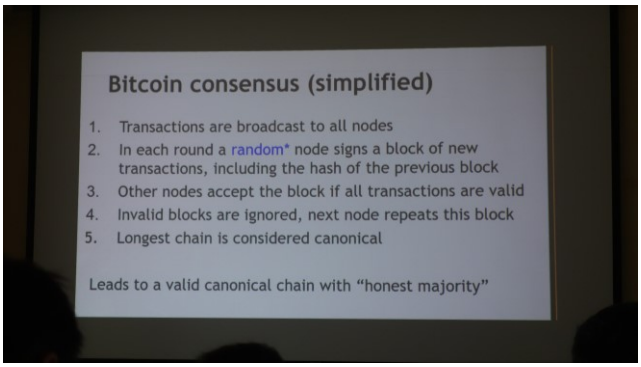

図 3　IACR サマースクール講演時の投影：“Bitcoin Overview”より.

2.3.2 Scaling Bitcoin Securely

Aggelos Kiayias (University of Edinburgh)

Blockchain プロトコルの処理時間を短縮することと，安全性を担保することの，トレードオフを理論的に議論する試みの紹介であった．

2.3.3 Consensus

Roger Wattenhofer (ETH Zurich)

ブロックチェーン技術の主要な機能の一つである合意形成をトピックに，“Fault-Tolerance & Paxos”, “Consensus”, “Authenticated Agreement”といった話題が採り上げられた．Paxos とは合意プロトコルの一種である．

2.3.4 Mining

Joseph Bonneau (Stanford Univ.)

暗号通貨の採掘について次のトピックを解説していた．“The task of Bitcoin miners”, “Mining hardware (Bitcoin)”（GPU や FPGA，ASIC を使ったマイニング），“Energy consumption & ecology”, “Mining pools”, “Mining incentives and strategies”．特にマイニングプールとこれに着眼した攻撃についての解説があった．まとめにおいて “No complete game-theoretic model exists”と言及した上で， “Things might be about to get interesting”と活性化してきている研究開発の状況で結んでいた．

2.3.5 Cryptographic e-cash

Jan Camenisch (IBM Research)

1995 年頃から 2005 年頃にかけて精力的に centralized model で online e-cash / offline e-cash を研究発表してきた研究者による講演であった．コミットメントスキーム，デジタル署名スキームやゼロ知識証明プロトコルといった暗号プリミティブを部品に，いかに匿名性や二重使用不可を備えた暗号通貨を構成するか（centralized model の下で）を丁寧に解説していた．（ただし Bitcoin を含む decentralized model との関係性は薄いと思われる．）

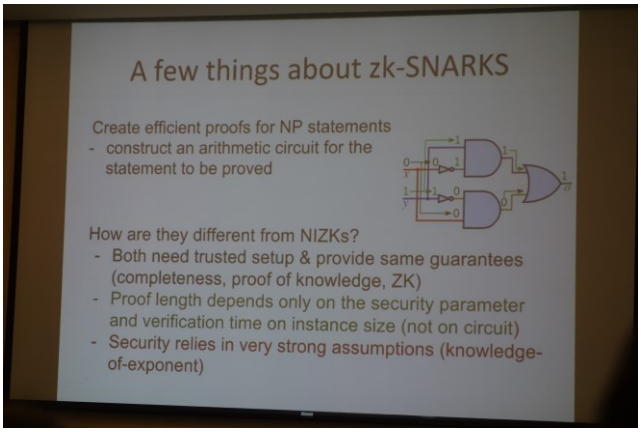

図 4　IACR サマースクール講演時の投影：“Anonymity in Cryptocurrencies” より．

2.3.6 Anonymity in Cryptocurrencies

Foteini Baldimtsi (George Mason Univ.)

匿名性を達成するための二つの主要な技術（の流れ）を解説していた．一つ目は Mixing/Tumbler Services，二つ目は Anonymous Cryptocurrencies としていた．二つ目のほうでは Zero-coin を紹介していた．使用されている暗号技術として zk-SNARK と呼ばれる，強い数論的仮定（the knowledge-of-exponent assumption）に基づき安全な非対話ゼロ知識証明について触れていた．

図 5　IACR サマースクール：コーヒーブレイクの様子

2.3.7 Cryptography on the Blockchain

Vassilis Zikas (RPI)

EUROCRYPT 2016 で採択になった論文 “Fair and Robust Multi-Party Computation using a Global Transaction Ledger”の解説であった．Bitcoin のスキームやプロトコルが解決した暗号学上の問題は何か，あるいは，どんな暗号学上の要素技術を得たか，を主題とし講演していた．Secure function evaluation や GUC (global universal composability)といった言葉が登場した．

ブロックチェーン技術を従来の暗号プリミティブの一部に組み込む研究（公開鍵証明書，NIZK の CRS，あるいは上記の MPC，等）が情報セキュリティトップカンファレンスで発表されるようになっている傾向は注目に値する（この点，日本国内は出遅れているかもしれない）．

2.3.8 Decentralization as a Privacy-Enhancing Technology
George Danezis (University College London)

分散型管理とプライバシーの関連に着目した講演であった．初めに，分散型管理と中央管理を「インフラ 対 権限機関」の構図で捉えなおす観点を説明したところが興味深かった．また最後のほうでは，decentralized network のノード数が大きくなるに連れて 1 ノード当たりの計算量（負荷）が増える漸近的解析の話があり，これも興味深かった．

2.3.9 Bitcoin de-anonymization in Practice
Adam Joyce (ELLIPTIC)

講演タイトルは “Blockchain Intelligence and Anonymity” に変更となった． “Bitcoin + Financial compliance”をキーワードに ELLIPTIC 社の事業を紹介していた．

2.3.10 Anonymous Online Marketplace
Nicolas Christin (Carnegie Mellon University)

匿名マーケットプレイスの発展と今後あるべき姿についての講演であった．途中 TOR (The Onion Router) の匿名化技術について触れた上で，違法薬物の売買を行うサイト “Silkroad” で Bitcoin が支払い通貨に使われていた点に関し見解を論じた．

2.3.11 The Bitcoin Economic Ecosystem
Rainer Bohme (Univ. of Innsbruck)

経済学の観点（ゲーム理論やグラフ理論の視点も含む）から Bitcoin の分散型管理（ブロックチェーン技術も含む）を概観した講演であった. “Principles of Network Economics” がキーワードとなっていた．

2.3.12 Regulation in Bitcoin
Jerry Brito (Coin Center)

USA 内を前提に，法規制が暗号通貨に関わる仕方を論じた講演であった．視点を表すキーワードとしては，Consumer protection, Financial Surveillance, Sanctions, Enforcement, Securities Regulation, Tax, などが挙がっていた．

2.3.13 Alternatives to Blockchains
Sarah Meiklejohn (University College London)

ブロックチェーン技術に基づき派生したとされる様々な暗号通貨及び分散型管理システムについて紹介した講演であった．

2.4 その他

2.4.1 Reception

レセプションの様子を図 6 に示す．

図 6　IACR サマースクール：
プールサイドでのレセプションの模様

2.4.2 Short Talks

- GHOST Against Byzantine Adversaries (Giorgos Panagiota)
- Towards Bitcoin Payment Networks (Patrick McCorry, Newcastle University)
- Semantic Blockchain (Matthew English)
- Decentralized Anonymous Micropayments (Peihan Miao, University of California, Berkeley)
- Broadcasting Intermediate Blocks as a Defense Mechanism Aginst Selfish Mining in Bitcoin (Ren Zhang, KU Leuven)
- Securing Bitcoin-Like Protocols Against 51% (Hong-Sheng Zhou, Virginia Commonwealth University)
- A Quick Look at Bitcoin Ransomware (Chris Carr, Norwegian University of Science and Technology)
- Bitcoin Covenant (Malte Moser, University of Münster)

2.4.3 Breakout Sessions (IOHK session)

ScoreX は github にて公開されている[16]．ScoreX は blockchain system の prototyping platform である．また，NDSS2016 にて初出の RSCoin [19]もこの場で改めて発表された．

図 7　IACR サマースクール：
ノベルティグッズ（バッグ）

3. ECRYPT ワークショップ

3.1 開催要項

ECRYPT ワークショップは ECRYPT-CSA のオーガナイズで催された．ECRYPT-CSA は EU の Horizon 2020 基金がサポートしており，2015 年から 2018 年までの 3 か年プロジェクトである[17].

ワークショップ会場はギリシャの首都アテネの Hotel Royal Olympic Athens のパノラマホール(図 8)である．同会場からはゼウス神殿やアクロポリスなど，アテネの著名な観光地が一望できた(図 9).

図 8　ECRYPT ワークショップ会場(開場直後)

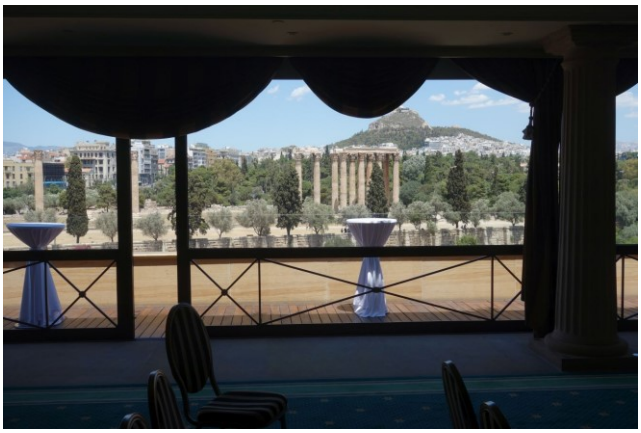

図 9　ECRYPT ワークショップ：
会場から望むゼウス神殿

3.2 プログラム

- Cryptocurrencies overview (George Danezis, University College London, UK)
- Incentives in cryptocurrencies (Joseph Bonneau, Stanford University, US)
- Alternatives to Bitcoin (Sarah Meiklejohn, University College London, UK)
- Foundations of blockchain protocols (Aggelos Kiayias, National and Kapodistrian University of Athens, GR)
- IBM initiatives on blockchain technologies (Elli Androulaki, IBM Research Zurich, CH)
- Bitcoin and Blockchain applied cryptography problems (Adam Back, Blockstream)
- Technology Industry Views on Blockchain (Claire Vishik, Intel, US)

  Sawtooth Lake[18]

3.3 講演内容

以下に，講演を聴講した際の内容のメモ及び若干の見解を示す.

3.3.1 Cryptocurrencies overview

George Danezis (University College London)

通貨や支払い方法の変遷，また貨幣制度や金融システムの基本要件など，暗号通貨の議論に立ち入る前の前提を確認し共有する説明があった．Bitcoin のような zero-governance currency，分散型管理（仮想）通貨，の可能性について論じるための布石となる基調講演であった.

3.3.2 Incentives in cryptocurrencies

Joseph Bonneau (Stanford Univ.)

Bitcoin における miner の役割と動機 (incentives) について触れた後，mining のためのハードウェアへの投資と回収の現状，また，miner の戦略や攻撃者の視点などについて説明した講演であった.

3.3.3 Alternatives to Bitcoin →Beyond Blockchain **にタイトル変更**

George Danezis and Sarah Meiklejohn (University College London, UK)

主に RSCoin [19] について説明した講演であった．基本は分散型管理だが，中央銀行の金融ポリシが介入する構想の暗号通貨であった．ブロックチェーンが分岐するリスクが生じた場合などに介入するなど，現実の運用をハイブリッド型で管理するようである.

3.3.4 Foundations of blockchain protocols

Aggelos Kiayias (National&Kapodistrian Univ. of Athens)

堅牢な取引台帳を公開かつ分散型で管理することが目的である点について認識の共有を促した後，ブロックチェーンに対する攻撃モデルや安全性の議論が妥当と言えるかどうかを論じた講演であった.

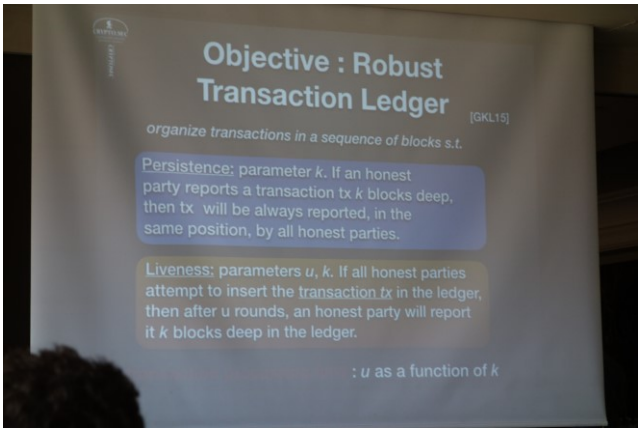

図 10　ECRYPT ワークショップ講演時の投影：“Foundations of blockchain protocol”より.

3.3.5 IBM initiatives on blockchain technologies
Elli Androulaki (IBM Research Zurich)

現存の送金システム（特に国際送金）が手続きやコストの点で課題を抱えているのに対し，Bitcoin などの分散型管理(仮想)通貨が解決を与えうるかを論じた講演であった．“Enterprise Blockchain” をキーワードに，企業が使う視点から，ユーザのアイデンティティ管理（なりすまし防止），取り引きするユーザのプライバシー，処理効率と安全性のトレードオフやスケーラビリティ，また監査可能性などについて説明していた.

3.3.6 Bitcoin and Blockchain applied cryptography problems
Adam Back (Blockstream)

はじめに blockchain イコール contract arbitration mechanism（契約調停機構：本稿著者訳）の理解を共有した後，ブロックチェーンに対して暗号技術が寄与できることを論じた講演であった．Merkle ツリー，デジタル署名，ゼロ知識証明などの各種暗号技術の機能及び処理効率への影響を説明していた.

図 11　ECRYPT ワークショップ講演時の投影：“Bitcoin and Blockchain applied cryptography problems”より.

3.3.7 Technology Industry Views on Blockchain
Claire Vishik (Intel)

産業界がブロックチェーン技術に注目し，開発に注力している現状を説明していた．Intel が開発中の “hyperledger” である“Sawtooth Lake” [18]についても触れていた.

4. まとめ

2016 年の 5 月第から 6 月にかけてギリシャで催された暗号通貨/ブロックチェーンに関する二つの学術会合について，その概要を報告した.

謝辞

第一著者に関し，本研究は JSPS 科研費 JP26330169 の助成を受けたものです.

第二，第三，第四著者に関し，本研究は JSPS 科研費 JP15H02711 の助成を受けたものです.

参考文献

[1] “Bitcoin Summer School 2016”, https://bitcoinschool.gr, (参照 2016-07-21)
[2] “Workshop on Cryptocurrencies – Athens, Greece”, https://www.cosic.esat.kuleuven.be/ecrypt/csa/cryptocurrencies/index.shtml (参照 2016-07-21).
[3] “Bitcoin overview”, https://bitcoinschool.gr/slides/session1.pdf (参照 2016-07-21).
[4] “Scaling Bitcoin Securely”, https://bitcoinschool.gr/slides/session2.pdf (参照 2016-07-21).
[5] “Consensus”, https://bitcoinschool.gr/slides/session3.pdf (参照 2016-07-21).
[6] “All about mining”, https://bitcoinschool.gr/slides/session4.pdf (参照 2016-07-21).
[7] “Cryptographic e-Cash”, https://bitcoinschool.gr/slides/session5.pdf (参照 2016-07-21).
[8] “Anonymity in Cryptocurrencies”, https://bitcoinschool.gr/slides/session6.pdf (参照 2016-07-21).
[9] “Cryptography on the Blockchain”, https://bitcoinschool.gr/slides/session7.pdf (参照 2016-07-21).
[10] “Decentralization as a Privacy-Enhancing Technology”, https://bitcoinschool.gr/slides/session8.pdf (参照 2016-07-21).
[11] “Blockchain Intelligence and Anonymity”, https://bitcoinschool.gr/slides/session9.pdf (参照 2016-07-21).
[12] “Beyond Silk Road: Developments in anonymous online marketplaces”, https://bitcoinschool.gr/slides/session10.pdf (参照 2016-07-21).
[13] “The Bitcoin Economic Ecosystem”, https://bitcoinschool.gr/slides/session11.pdf (参照 2016-07-21).
[14] “Regulation of Bitcoin”, https://bitcoinschool.gr/slides/session12.pdf (参照 2016-07-21).
[15] “Alternatives to Blockchains”, https://bitcoinschool.gr/slides/session13.pdf (参照 2016-07-21).
[16] “GitHub - input-output-hk/ Scorex: Modular blockchain framework. Public domain”, https://github.com/input-output-hk/Scorex (参照 2016-07-21).
[17] “ECRYPT”, www.ecrypt.eu.org/csa/ (参照 2016-07-21).
[18] “Introduction – Sawtooth Lake latest documentation”, https://intelledger.github.io/introduction.html (参照 2016-07-21).
[19] “RSCoin”, http://www.internetsociety.org/events/ndss-symposium-2016/ndss-2016-programme (参照 2016-08-10).