ブロックチェーン技術における鍵管理
～ブロックチェーン技術における鍵漏洩課題の分析～

研究年度　平成　31 年度
研究期間　平成　31 年度
研究代表者名　松崎　なつめ

I.　はじめに

ブロックチェーンは，中央集権的な信頼機関を設けずに，各ノードが分散的に配置され，安全に金銭や契約などの「価値」をやり取りする技術である．「分散型台帳技術」とも称される．2009 年から運用開始されたビットコインなどの暗号通貨を支える技術として開発・運用されている．最近では，暗号通貨のみならず，医療情報管理やサプライチェーンなどの，ブロックチェーン技術を用いた応用システムが盛んに提案されている．

一方，ブロックチェーン技術には，数学的／論理的に未評価な課題があるといわれており，その１つが「鍵管理」である．暗号通貨においては，個々が有する秘密鍵を用いて生成する署名は，通貨そのものに直結しており，鍵の生成，管理，失効のライフサイクルにおいて，安全な管理が必要である．

本報告書では，ブロックチェーン技術における鍵管理について整理して，今後の研究の方向性を示す．

II.　研究内容

1　ブロックチェーンについて

ブロックチェーンは，中央集権的な信頼機関を設けずに，各ノードが分散的に配置され（図１），安全に金銭や契約などの「価値」をやり取りする技術である．各ノードが価値のやり取りの履歴をタイムスロットごとのブロックに順次記録し，他のノードに送付する．各ノードが同じ情報を管理するため，障害に強く分散管理台帳とも称される．

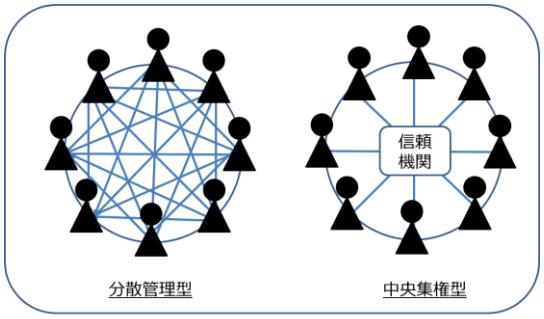

図１．分散管理型システム

ブロックチェーンにおいては，公開鍵暗号が署名目的で用いられ，「価値」を移動する元が自身の秘密鍵を用いて取引に署名を施し，ブロックチェーンに記録する．記録された署名は，分散ノードがそれぞれ対応する公開鍵を用いて確認する．暗号通貨においては，「価値」の移動は移動する元が，暗号通貨を使うことに対応する．

2　鍵管理とは

鍵管理とは，鍵の生成，保管，更新，廃棄の鍵ライフサイクルと，万が一の鍵漏洩時の対策までを設計，運用することにより暗号システムの安全性を維持することである． 図２に，[1]から抜粋した鍵のライフサイクルを示す．

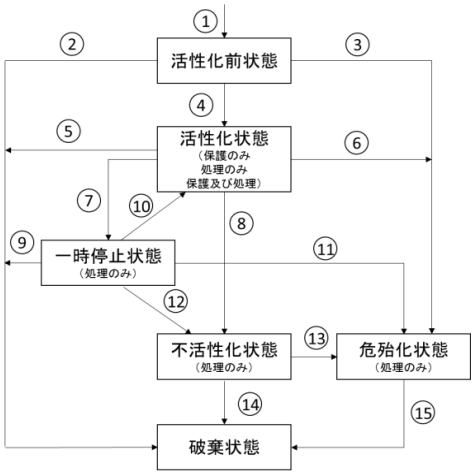

図２．鍵のライフサイクル[1]

公開鍵基盤（PKI：Public Key Infrastructure）は，現在，最も実績のある鍵管理である．例えば SSL/TLS のサーバ鍵管理で使われている．サーバは個々に鍵ペアを任意に生成し，所定の第三者認証機関に公開鍵を提示して，証明書を発行してもらう（図２の活性化状態）．証明書は，公開鍵とその持ち主本人の識別子を入力して生成した第三者認証機関の署名を含む．つまり，証明書は，鍵が間違えなくその本人のものであることを，第三者認証機関が保証するものである．証明書には一般に有効期限があり，有効期限が切れると鍵が無効化される（不活性状態）．有効期限内であっても，例えば鍵が漏洩した場合は，第三者認証機関が発行する証明書無効化リスト（CRL：Certification Revocation List）の確認により，対応する証明書を無効化（危殆化状態）することができる．

3　ブロックチェーン鍵管理の特徴と PKI 適用の課題

先に述べた通り，PKI は，鍵とその本人を関連づけるものであり，もともと人やサーバやデバイスといった対象物を信頼していることが前提で，それと鍵を紐づけることにより，鍵を信頼する．

一方，ブロックチェーンでは，鍵は「価値」そのものに直結しているといわれている[2]. 例えば暗号通貨の場合は，秘密鍵を用いることでその通貨を利用可能である．逆に秘密鍵が漏洩することは，通貨を紛失することに対応する． PKI における，信頼ができる「本人」は，基本的には明示されない．むしろ暗号通貨の場合は，鍵は，その持ち主である「本人」には関連付けないことが必要となる．

以下，ブロックチェーンの鍵管理に，PKI を適用する際の課題として私が考える点を挙げる．

(1)プライバシ保護

ブロックチェーンを暗号通貨に適用する場合は，鍵と本人が関連付かない仕組み（一般にプライバシ保護と言われる：取引から本人が特定されないこと，複数の取引が同一の本人によるものと特定されないこと）が必要である．これは，現

在のキャッシュの特性を引き継ぐ要件であり，暗号通貨においても必要と考えられている．一方，PKI は鍵と本人の間を保証するものである．最終的には第三者認証機関と，本人の両方を信用することにより，鍵を信用することができる．このため，単純に PKI を用いると，本人が特定されプライバシ保護が満たされないことになる．これに対して，複数の鍵を用意したり，鍵を使い捨てにする方法が考えられているが，いずれにしても本人を信頼する PKI と，本人と紐づかないことを要件とするブロックチェーンは，そのままでは組み合わせ困難と考えられる．

(2)信頼できる第三者認証機関

PKI は，各ノードが第三者認証機関を信頼することで成り立つ．そのため，そもそも第三者認証機関仮定しないブロックチェーンの分散管理システムにはなじまないとの意見がある．一方，分散システムであっても，第三者認証機関を設けてよいとの考えで，ブロックチェーンへの PKI 適用を推奨する提案がある（例えば[3]では，(1)に述べたプライバシ保護は，犯罪行為やマネーロンダリングのデメリットがあると記載されている）．

(3)漏洩した鍵の無効化

ブロックチェーンにおいて例えば鍵が漏洩した場合，漏洩した鍵を無効化することは必要な要件である．PKI では，鍵を無効化する場合，信頼のおける第三者認証機関が，その本人からの失効申請をもとに証明書失効リスト（CRL：Certification Revocation List）を発行して，鍵と本人間の保証を切断する．しかしながら，ビットコインのようなブロックチェーンでは，利用者を管理する主体はなく，鍵は利用者で自由に生成される．そのため，生成した本人が失効申請しているのかどうかを判断することや，鍵が漏洩した場合は，失効申請が正当なものかを判断することは困難であると考えられる．また，そもそも紛失してしまった鍵の場合は，正しい失効申請を生成することすらも難しい．

以上述べた通り，ブロックチェーンにおいては，PKI では信頼の源の１つである「本人」が管理されておらず，さらに，本人と鍵の間を関連づけないことが，必要な要件となっているところに，PKI が適用困難である根源があると考えられる．

4　鍵漏洩対策について

ブロックチェーンにおける鍵漏洩対策として，すでに考えられている方法を以下挙げる．

①　鍵に使用回数制限，使用可能期間を設ける[2]

万が一鍵が漏洩したとしても，その被害を最小化するための方法である．鍵で取引可能となる上限の価値を決める方法も考えられる．ただし，鍵の使用に関す

る制御部分を如何に安全に実装するかが課題である．

② 新しい鍵に資産を置き換える[2]

鍵の漏洩が疑われる場合に，鍵が不正に使われる前に，新しい鍵を生成して，そこに資産を乗せ換える．これは，知らないうちに不正に使われている場合には効果がない．

③ 多重署名（マルチシグ）を用いる[2]

複数の鍵を用いることで，取引が有効となる仕組みである．例えば自分で複数の鍵を別々の媒体で管理したり，自分とサービス事業者で鍵を分けて管理することで，鍵の漏洩リスクを低減することができる．ビットコインで提案されている方法である．ただし，鍵漏洩のリスクは低減できるが，複数の鍵を安全に管理・運用するための手間が増える．秘密分散や閾値署名などを用いる方法も，考え方としては同様である．なお，複数の鍵を用いて取引をすることにより，鍵漏洩リスクが低減するだけでなく，プライバシ保護が向上するとの研究もある．グループ署名の１つであるリング署名[4]を用いる方法であり，複数のノードのうちどのノードが署名を施したのか分からなくする方法である．暗号通貨の１つ Monero で採用されている．

④ 生体情報から秘密鍵を生成する[5]

生体情報の揺らぎを補正し，秘密鍵を抽出した後，公開鍵暗号方式に基づく電子署名を生成方法であり，PBI（Public Biometrics Infrastructure）と称して[5]で提案されている．鍵を利用するたびに生体情報から秘密鍵を抽出することによりストレージに保存する必要がなくなるため，鍵の紛失，漏洩のリスクを軽減する．しかしながら，秘密鍵を用いる場合（例えば，暗号通貨を使う場合）に，かならず生体情報を用いる必要があるため，応用シーンを制限し，生体情報に関係するプライバシ問題が新たに生じると考えられる．また，秘密鍵を抽出したあとに安全に消去する仕組みが必要である．

⑤ HSM を用いる[2]

鍵を，ハードウェア内のセキュアな領域や，外部からアクセス困難で安全性が認定されたモジュール HSM（Hardware Security Module）に格納することで鍵漏洩を防止する．ただし，HSM から読み込んだ鍵をコピーすることは可能であり，鍵を利用する場合に，コピーされた鍵か，HSM から読み込んだ正しい鍵かを区別できる仕組みが別途必要になると考えられる．

⑥ 追跡トークンを用いる[6]

漏洩した鍵に対応したアドレス（公開鍵）に追跡トークンという印をつけて，不正に使われることを抑止する方法である．2018 年に CoinCheck 社における暗号通貨流出事件において，有志によりモザイク（NEM における独自トークン）を対応するアドレスに付したことで，流出通貨の利益化が抑止できたという報告

がある．[6]の論文では，このトークンを付すことによって，トークン付与者が恨まれるリスクを低減するため，トークン付与者の匿名性を確保する方法が提案されている．提案方法では，リング署名の改良であるアカウンタブルリング署名を用いている．追跡トークンについては，そのトークンの信頼性をどのように確保するのかなど，様々な課題があり，興味深い研究であると考える．

以上の鍵漏洩対策はそれぞれ一定の効果があり，組み合わせによりリスクは低減すると考えられる．一方，以下の課題は依然として残ると考えられる．

・漏洩自身を防ぐものではない
・漏洩した価値が，自分に返ってくるわけではない
・そもそも，紛失して手元に鍵自身がなくなった場合は，無効化できない

III. 研究成果

Ⅱに述べた内容から， 鍵漏洩リスクと鍵漏洩対策に関して，次の研究の方向性があると考えられる．

１）利用者を管理せずに PKI を実現する研究
２）既存の漏洩対策の効果的な組み合わせを検討する研究
３）PKI における第三者認証機関を，分散システムに対応して，分散ノードの信頼度に置き換える研究
４）追跡トークンの信頼性を確保する研究
５）鍵漏洩自身を防ぐ方法，漏洩した価値が自分に返ってくる方法や紛失して手元に鍵がなくなった場合の無効化方法の研究

これらの検討課題を導出したことが，研究成果であり，今後これらに優先度を付与して検討を深める．

IV. 終わりに

本報告書では，ブロックチェーンの鍵管理の課題と，現在のディジタル署名の鍵管理として実用化されている PKI の適用を検討することで，課題解決の研究の方向性について整理した．

今後，導出された検討の方向性に優先度を付与して，検討を深める．

補足：

今回，主に CSS2019, SCIS2020, FC2020 の論文からブロックチェーン技術を調査した（参考文献一覧２に示す）．その調査の中で感じたことを以下に示す．

・日本と海外（特にアメリカ）では，注目しているところが異なる．日本のほうが，２周くらい遅れている．研究者が少ない．

・日本では，ブロックチェーン自身の研究よりも，その改ざん困難性を用いた応用やブロックチェーンに入力するデータの確からしさにフォーカスした研究が多い．
・海外では，ブロックチェーンのスケーラビリティを向上する方法として，主にオフチェーンの仕組みにフォーカスしている．実用性を拡張する研究である．
・鍵管理は，海外でも研究が少ない．さらに，進める必要性を感じる．技術だけでなく，マネージメントや仕組みとの組み合わせが必要と考えられる．

参考文献一覧１

[1] E.Barker, 鍵管理における推奨事項, NIST Special Publication 800-57 Part 1 Revision 4 （IPA 訳）2016.
[2] 松尾，楠，崎村，佐古，佐藤，林，古川，宮澤，ブロックチェーン技術の未解決問題，日経 BP，2018.
[3] Web の記事，
https://www.cybertrust.co.jp/blog/certificate-authority/pki/block-chain-and-pki-vol1.html
[4] Rivest.R, Shamir.A, Tauman.Y, How to leak a secret, ASIACRYPT 2001.
[5] 長沼，鈴木，高橋，加賀，山田，國廣，吉野，PBI を用いたブロックチェーン向け鍵管理技術，SCIS2019.
[6] 佐藤，江村，面，ブロックチェーンシステムにおける匿名トークン付与に関する一考察，CSS2019.

参考文献一覧２

＜CSS2019＞

2C1-1: 匿名暗号資産（Monero/Zcash/Grin）ブロックチェーンの匿名性に関する考察
才所 敏明（(株)IT 企画）辻井 重男（中央大学研究開発機構）櫻井 幸一（九州大学大学院システム情報科学研究院）
2C1-2: BLDAG: Generalization of the Blockchain into Bi-Layered Directed Acyclic Graph
Atsuki Momose（Nagoya University）Jason Paul Cruz（Osaka University）Yuichi Kaji（Nagoya University）
2C1-3: 分散型認証基盤に向けたスマートコントラクトを用いた相互認証方式の提案
掛井 将平（名古屋工業大学）白石 善明（神戸大学，株式会社国際電気通信基礎技術研究所）毛利 公美（岐阜大学）中村 徹（株式会社国際電気通信基礎技術研究所）橋本 真幸（株式会社国際電気通信基礎技術研究所）齋藤 彰一（名古屋工業大学）
2C1-4: ブロックチェーンシステムにおける匿名トークン付与に関する一考察

佐藤 哲平（筑波大学）江村 恵太（情報通信研究機構）面 和成（筑波大学 / 情報通信研究機構）

2C2-1: ブロックチェーン技術を用いた分散セキュリティログ管理手法の提案

田口 裕介（法政大学　理工学研究科　応用情報工学専攻）金井 敦（法政大学　理工学部　応用情報工学科）谷本 茂明（千葉工業大学　社会システム科学部　プロジェクトマネジメント学科）

2C2-2: ビットコインにおける手数料を考慮したオフチェーントランザクションの管理

長嶺 隆寛（東京大学生産技術研究所）松浦 幹太（東京大学生産技術研究所）

2C2-3: RA: スマートコントラクトの安全性解析にむけたシンボリック実行ツール

知念 祐一郎（大阪大学大学院 情報科学研究科）矢内 直人（大阪大学大学院 情報科学研究科）クルズ ジェイソン　ポール（大阪大学大学院 情報科学研究科）岡村 真吾（奈良工業高等専門学校）

2C2-4: データ暗号化機能を組み込んだチェーンコードの実装に関する研究

佐伯 美緒（大阪大学）小島 英春（大阪大学）矢内 直人（大阪大学）土屋 達弘（大阪大学）

＜SCIS2019＞

1D1-1 ブロックチェーンを用いたインセンティブ付与を考慮した効率的な IoT 機器ファームウェア配布手法

福田 竜央(筑波大学)、面 和成(筑波大学/情報通信研究機構)

1D1-2 非協力的なペイメントチャネル終了時の公平な手数料追加プロトコル

◎長嶺隆寛(東京大学生産技術研究所)、松浦幹太(東京大学生産技術研究所)

1D1-3 スマートコントラクトを用いた IoT 機器の効率的な認証手法

◎市野樹也(筑波大学)、面和成(筑波大学 / 情報通信研究機構)

1D1-4 ブロックチェーンシステムにおける匿名信頼性付与手法の実装・評価

◎佐藤哲平(筑波大学)、江村恵太(情報通信研究機構)、面和成(筑波大学/情報通信研究機構)

1D1-5Post-quantum zk-SNARKs for Arithmetic Circuit

○長沼健(日立製作所)、井上淳雄(日立ソリューションズ)、岡崎嶺明(日立ソリューションズクリエイト)、吉野雅之(日立製作所)、Basu Anirban(日立製作所)、國廣昇(筑波大学)

1D2-1Casper the Subjective Finality Gadget

◎Ryuya Nakamura(The University of Tokyo/LayerX)

1D2-2Interactive Cryptocurrency Transaction Graph Visualization through Bottom-up/Top-Down Hybrid Data Processing

◎Gusenbauer Matthias(Tokyo Institute of Technology / SBA Research)

1D2-3Smart contract with secret parameters

◎Marin Thiercelin(Osaka University/EPFL)、Chen-Mou Cheng(Osaka University)、Serge Vaudenay(Osaka University)、Atsuko Miyaji(Osaka University)

1D2-4Load Balancing for Sharded Blockchains

◎岡南 直哉(筑波大学 / LayerX)、中村 龍矢(東京大学 / LayerX)、西出 隆志(筑波大学)

1D2-5Faster Scriptless Multi-Hop Payment for Bitcoin

◎ Kanta Kurazumi(Tokyo Institute of Technology) 、 Mario Larangeira(Tokyo Institute of Technology, IOHK)、Keisuke Tanaka(Tokyo Institute of Technology)

2E1-1Design Practices for Wholesale Central Bank Digital Currencies from the World

◎Edwin Ayisi Opare(KAIST)、Kwangjo Kim(KAIST)

2E1-2 ブロックチェーンを用いた鍵更新なしフォワード安全公開鍵暗号

◎怒田 晟也(筑波大学)、Jacob C. N. Schuldt(産業技術総合研究所)、西出 隆志(筑波大学)

2E1-3 ブロックチェーンを利用した電子投票システムの安全性

Misni Harjo Suwito(Mercu Buana University)、Sabyasachi Dutta(University of Calgary)、○櫻井 幸一(九州大学)

2E1-4 外国人被疑者取調べにおける通訳システムのプロトタイプの開発と評価

◎脇田　和宏(東京電機大学)、佐々木　良一(東京電機大学)

2E1-5Implementation of Covert Communication Based on Bitcoin Regtest Self-built Network

◎王惟正(会津大学)、张乐君(揚州大学)、韩昭阳(会津大学)、邱琛(会津大学)、黄华锟(会津大学)、苏春华(会津大学)

4D1-1 暗号通貨マイニング通信の深層学習による分類

◎遠藤　さや(東京工業大学)、石井　将大(東京工業大学)、田中　圭介(東京工業大学)

4D1-2DAG 技術ベースの暗号資産の匿名性に関する考察

○才所敏明((株) IT 企画)、辻井重男(中央大学研究開発機構)、櫻井幸一(九州大学　大学院システム情報科学研究院)

4D1-3 ブロックチェーンを応用した暗号資産の匿名性に関する一考察

○宮前　剛(富士通研究所)、松浦　幹太(東京大学生産技術研究所)

4D1-4 ブロックチェーンを用いた規制克服技術の考察

○宝木 和夫(産総研)、ウォルゲムト スベン(日立製作所)、久保田 隆(早稲田大学)、三科 雄介(産総研)、梅澤 克之(湘南工科大学)、渡邊 創(産総研)

4D2-1IoT サプライチェーン: 安全性の課題とブロックチェーンの試み

Haibo ZHANG(Kyushu Univ.)、Toru Nakamura(Advanced Telecommunications Research Institute International)、Yuto Nakano(KDDI Research, Inc.)、○Kouichi Sakurai(Kyushu Univ.)

4D2-2Universal sampler を用いない Proof of Human-work の構成とその応用に関する研究

◎角田理尚(東京工業大学)、尾形 わかは(東京工業大学)、高橋 健太(株式会社日立製作所)、西垣 正勝(静岡大学)

4D2-3TEE による IoT デバイスとブロックチェーン間の信頼性の仲介

◎エンケタイワン　バトニヤマ(NEC)、井上明子(NEC)

4D2-4 ブロックチェーンによるダイナミック周波数共用システムの検討

○近藤　健(中央コリドーICT 推進協議会)、山澤　昌夫(中央大学研究開発機構)、角田　篤奏(中央大学国際情報学部)、才所　敏明(中央大学研究開発機構)、五太子　政史(中央大学研究開発機構)、佐藤　直(中央大学研究開発機構)、辻井　重男(中央大学研究開発機構)、野田　啓一(慶応義塾大学 SFC 研究所)

4D2-5 オフチェーン技術を用いた履歴データの検証が可能な広告配信履歴記録システムの提案

◎中川　紗菜美(NEC)、梶ヶ谷　圭祐(NEC)

<Financial Cryptography 2020>

Leveraging Bitcoin Testnet for Bidirectional Botnet Command and Control Systems. Federico Franzoni (Universitat Pompeu Fabra), Vanesa Daza (Universitat Pompeu Fabra), Iván Abellán (Universitat Pompeu Fabra)

Security Analysis on dBFT protocol of NEO. Qin Wang (Swinburne University of Technology), Jiangshan Yu (Monash University), Zhiniang Peng (Qihoo 360 Core Security), Vancuong Bui (Swinburne University of Technology), Shiping Chen (Csiro, Data61), Yong Ding (Cyberspace Security Research Center), Yang Xiang (Swinburne University of Technology)

Breaking the encryption scheme of the Moscow internet voting system. Pierrick Gaudry (CNRS, Inria, Université de Lorraine), Alexander Golovnev (Harvard University)

Short Paper: XOR Arbiter PUFs have Systematic Response Bias. Nils Wisiol (Technische Universität Berlin), Niklas Pirnay (Technische Universität BerlinSelfish Mining Re-Examined. Kevin Alarcón Negy (Cornell University), Peter R. Rizun (Bitcoin Unlimited), Emin Gün Sirer (Cornell University)

Fairness and Efficiency in DAG-based Cryptocurrencies. Georgios Birmpas (University of Oxford), Elias Koutsoupias (University of Oxford), Philip Lazos (Sapienza University of Rome), Francisco J. Marmolejo Cossío (University of Oxford)

Stake Shift in Major Cryptocurrencies: An Empirical Study. Rainer Stütz

(Austrian Institute of Technology), Peter Gaži (IOHK), Bernhard Haslhofer (Austrian Institute of Technology), Jacob Illium (Chainalysis)

Coded Merkle Tree: Solving Data Availability Attacks in Blockchains. Mingchao Yu (University of Southern California), Saeid Sahraei (University of Southern California), Songze Li, Salman Avestimehr (University of Southern California), Sreeram Kannan (University of Washington), Pramod Viswanath (University of Illinois at Urbana-Champaign)

Decentralized Privacy-Preserving Netting Protocol on Blockchain for Payment Systems. Shengjiao Cao (Ant Financial), Yuan Yuan (Ant Financial), Angelo De Caro (IBM Research), Karthik Nandakumar (IBM Research), Kaoutar Elkhiyaoui (IBM Research), Yanyan Hu (IBM Research)

The Arwen Trading Protocols. Ethan Heilman (Boston University/Arwen), Sebastien Lipmann (Arwen), Sharon Goldberg (Boston University/Arwen)

SoK: A Classification Framework for Stablecoin Designs. Amani Moin (Cornell University), Kevin Sekniqi (Cornell University), Emin Gün Sirer (Cornell University)

SoK: Layer-Two Blockchain Protocols. Lewis Gudgeon (Imperial College London), Pedro Moreno-Sanchez (TU Wein), Stefanie Roos (TU Delft), Patrick McCorry (PISA Research), Arthur Gervais (Imperial College London)

MicroCash: Practical Concurrent Processing of Micropayments. Ghada Almashaqbeh (Columbia), Allison Bishop (Proof of Trading and Columbia), Justin Cappos (New York University)

LockDown: Balance Availability Attack against Lightning Network Channels. Cristina Pérez-Solà (Universitat Oberta de Catalunya), Alejandro Ranchal-Pedrosa (University of Sydney), Jordi Herrera-Joancomarti (Universitat Autònoma de Barcelona), Guillermo Navarro-Arribas (Universitat Autònoma de Barcelona), Joaquin Garcia-Alfaro (Institut Polytechnique de Paris)

Ride the Lightning: The Game Theory of Payment Channels. Zeta Avarikioti (ETH Zurich), Lioba Heimbach (ETH Zurich), Yuyi Wang (ETH Zurich), Roger Wattenhofer (ETH Zurich)

How to profit from payments channels. Oguzhan Ersoy (Delft University of Technology), Stefanie Roos (Delft University of Technology), Zekeriya Erkin (Delft University of Technology)

Boomerang: Redundancy Improves Latency and Throughput in Payment Networks. Joachim Neu (Stanford University), Vivek Bagaria (Stanford

University), David Tse (Stanford University)

DLSAG: Non-Interactive Refund Transactions For Interoperable Payment Channels in Monero. Pedro Moreno-Sanchez (TU Wien), Arthur Blue, Duc Le (Purdue University), Sarang Noether (Monero Research Lab), Brandon Goodell (Monero Research Lab), Aniket Kate (Purdue University)

Cerberus Channels: Incentivizing Watchtowers for Bitcoin. Zeta Avarikioti (ETH Zurich), Orfeas Stefanos Thyfronitis Litos (University of Edinburgh), Roger Wattenhofer (ETH Zurich)

RingCT 3.0 for Blockchain Confidential Transaction: Shorter Size and Stronger Security. Tsz Hon Yuen (The University of Hong Kong), Shi-feng Sun (Monash University), Joseph K. Liu (Monash University), Man Ho Au (Hong Kong Polytechnic University), Muhammed F. Esgin (Monash University), Qingzhao Zhang (Shanghai Jiao Tong University), Dawu Gu (Shanghai Jiao Tong University)

Address clustering heuristics for Ethereum. Friedhelm Victor (Technical University of Berlin)

What are the Actual Flaws in Important Smart Contracts (and How Can We Find Them)?. Alex Groce (Northern Arizona University), Josselin Feist (Trail of Bits), Gustavo Grieco (Trail of Bits), Michael Colburn (Trail of Bits)

Characterizing Code Clones in the Ethereum Smart Contract Ecosystem. Ningyu He (Peking University), Lei Wu (Zhejiang University), Haoyu Wang (Beijing University of Posts and Telecommunications), Yao Guo (Peking University), Xuxian Jiang (PeckShield, Inc)

Short Paper: Smart Contracts for Government Processes Case Study and Prototype Implementation. Magnus Krogsbøll (IT University of Copenhagen), Liv Hartoft (IT University of Copenhagen), Tijs Slaats (University of Copenhagen), Søren Debois (IT University of Copenhagen)