2018年10月20日
東京大学電気系同窓会講演会

ブロックチェーンの技術的な家系図と研究開発の現状

松浦幹太
（東京大学 生産技術研究所）

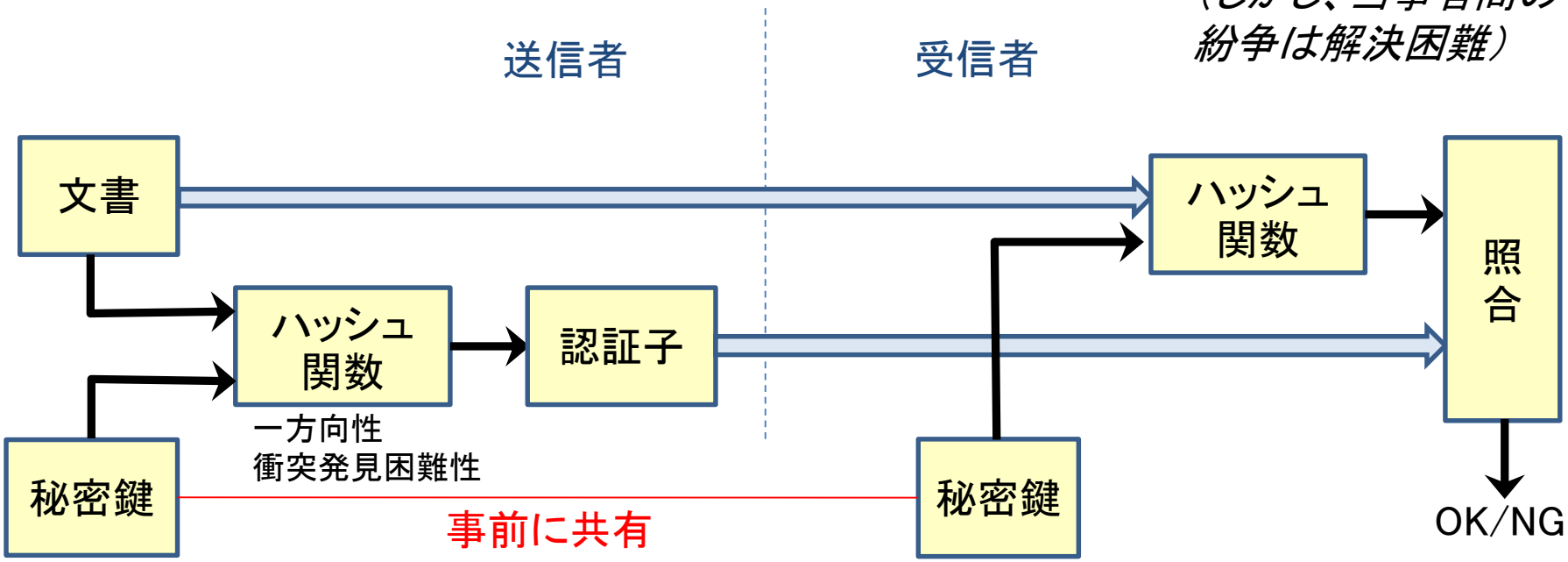
Copyright © 2018 by Kanta Matsuura, All rights reserved.

ブロックチェーンへ至る基礎に見る技術的な家系図

講義でどう教えているか

- 暗号は、秘匿性を確保する。
- メッセージ認証子は、完全性を確保する。

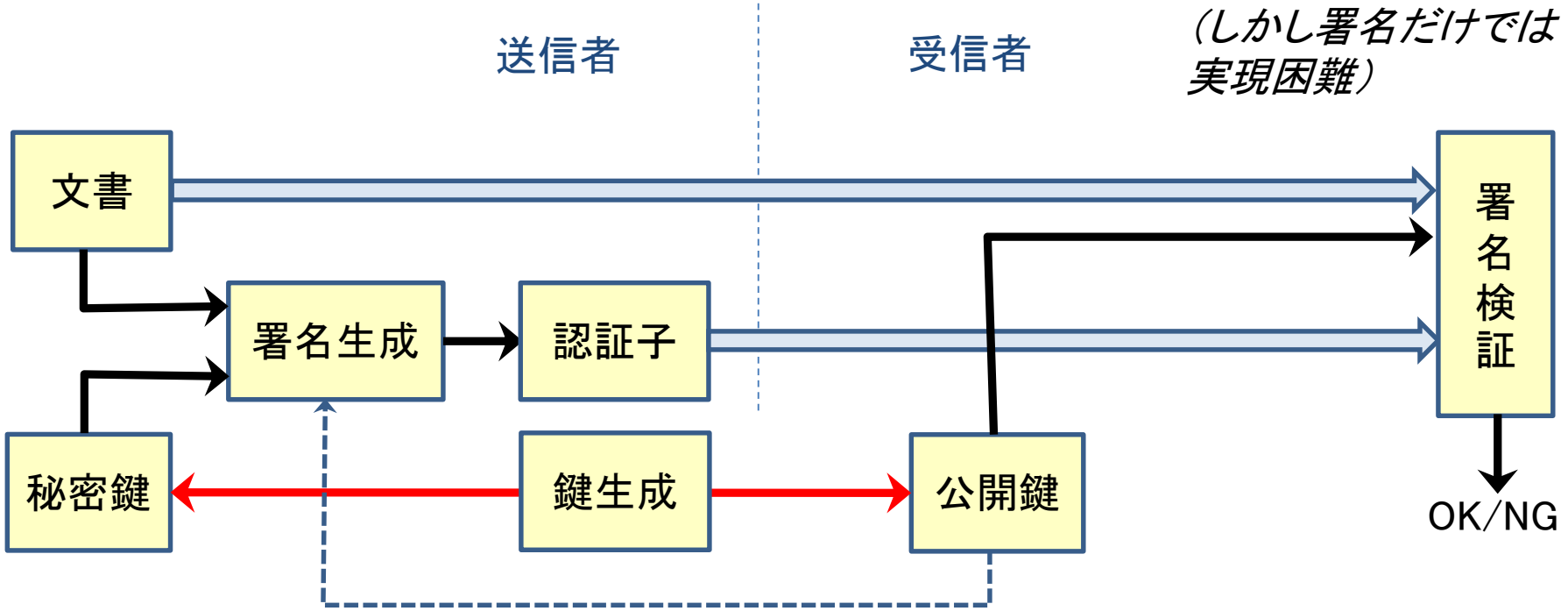
（しかし、当事者間の紛争は解決困難）



講義でどう教えているか

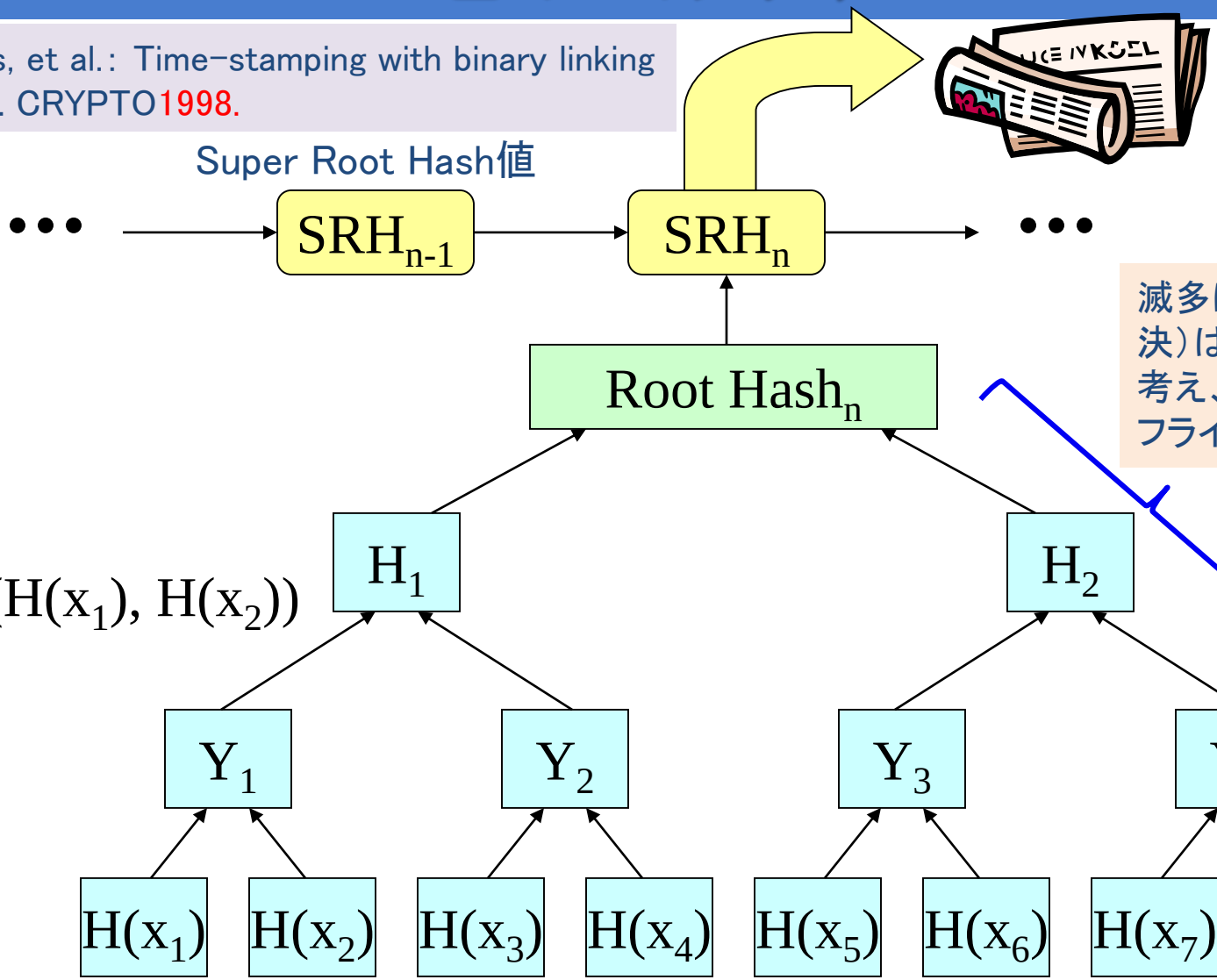
- 暗号は、秘匿性を確保する。
- メッセージ認証子は、完全性を確保する。
- 電子署名は、完全性確保＋否認不可を目指している。

（しかし署名だけでは実現困難）



電子時刻印

A. Buldas, et al.: Time-stamping with binary linking schemes. CRYPTO1998.



$Y_1=H(H(x_1), H(x_2))$

滅多に検証(紛争解決)はしなくてよいと考え、オンライン・オフラインDBで保管

宇根正志, 松浦幹太, 田倉昭: ``デジタルタイムスタンプ技術の現状と課題'', 日本銀行金融研究所 IMES Discussion Paper Series, 99-J-36 (1999)

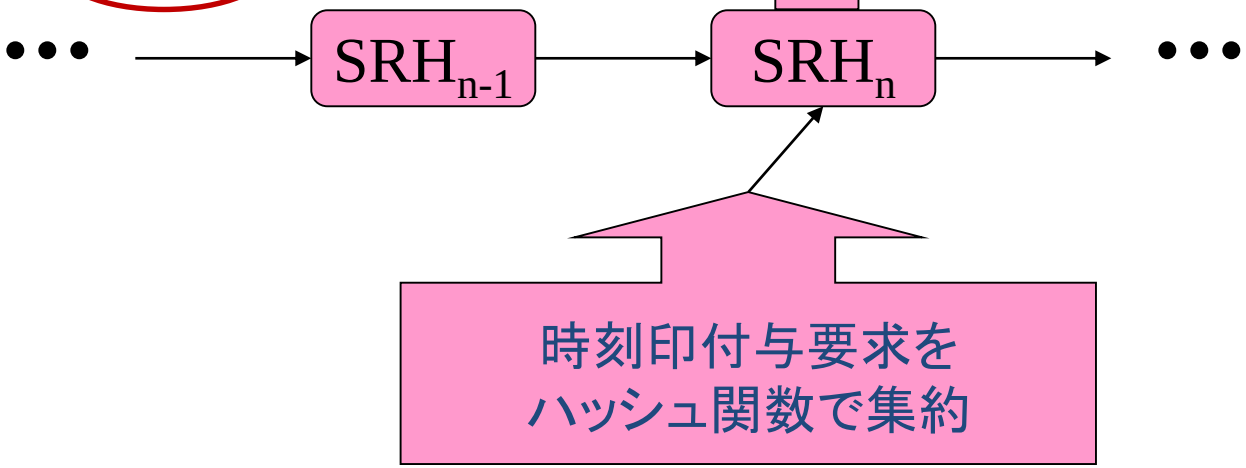
精細さに関するイノベーション

「誰が誰にいくら渡す」という処理情報に時刻印を押せば仮想通貨を実現できる。

FinTechに使える。

秒単位の電子時刻印サービス

“電子公表”



Tsutomu Morigaki, Kanta Matsuura, Osamu Sudo: ``An Analysis of Detailed Electronic Time-Stamping Using Digital TV'', Proceedings of the 2004 IEEE International Conference on e-Technology, e-Commerce, and e-Service (EEE04), pp.277-284 (2004)

基本的な仮想通貨

■ 時刻印付与対象の情報を「処理情報」とする。

- いくら支払うか（渡すか）を示す情報
- 誰に支払うかを示す情報（支払先の公開鍵のハッシュ値）
- 何を元手として支払うかを示す情報（過去にそれを受け取った時の「処理情報」のハッシュ値と自身の公開鍵）
- その元手を使う権利があることを証明する情報（正しい公開鍵に対応する秘密鍵による、今回の処理情報に対する電子署名）
- 処理情報の正当性を確認するためのコード（スクリプト）

スマート契約

- 仮想通貨以外の機能も埋め込める（その機能を主な機能と考えれば、「手数料の仕組みを埋め込める」とも言える）。
- 支払先（と支払金額の組）や元手情報は、複数記述できる。自分への支払いを含めることによって釣り銭を実現できる。

TTP排除のイノベーション

■ 公表作業をネット上の有志による「目撃」に頼る。

- 目撃者にインセンティブを与えるメカニズムが必要
- 報酬を与えるのが便利（とくに、仮想通貨の場合）
- 報酬と関連するからには、不正や混乱の防止が必要（PoW）

作業証明

■「随時公開検証」を可能にする。

- 誰でもいつでも検証できるようにP2Pシステムを組む(full replica at all the ledger nodes)。
- 10分かかる仮想通貨は「遅い」と言われるが、これでも新聞公表と比べれば桁違いに速い。
- ただし全ブロックの保持は限界をもたらす。

S. Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. http://bitcoin.org/bitcoin.pdf, 2008.

主な登場人物

■ 処理情報(取引情報)生成者

- 例えば、仮想通貨を使って支払いをする人（及び、受け取る人）
- 電子署名を生成する秘密鍵を持っている（ワレット）。

■ 台帳保持者(自律分散的に存在する ledger nodes)

- 基本的には、過去の全ての台帳情報をappend-only DBに保管

■ 台帳登録者(採掘者)

- 複数の処理情報（＋自分自身への報酬が生じるという処理情報）をまとめて台帳へ追記するブロックを作成し作業報酬を得る。

■ 台帳参照者

- 普通は、処理情報生成者、台帳保持者、台帳登録者も台帳参照者としての機能（台帳参照プログラム）を持つ。

Proof-of-Work

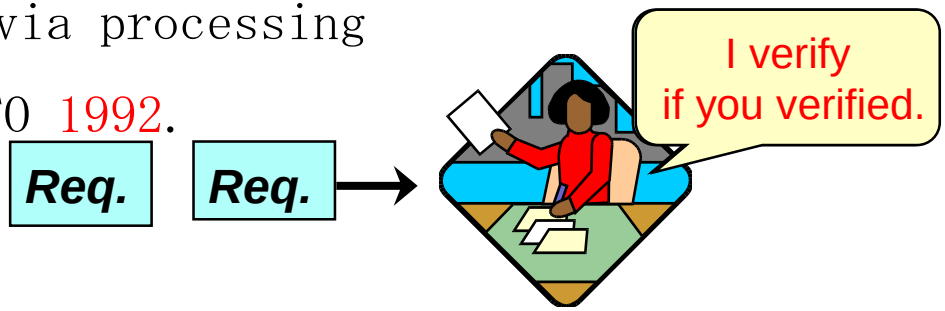
■ そこそこ重い暗号技術の計算を(攻撃者かもしれない相手に)課する。

- 「本当に頑張ったか」の検証は、第三者が効率的にできる。

■ 迷惑メール対策

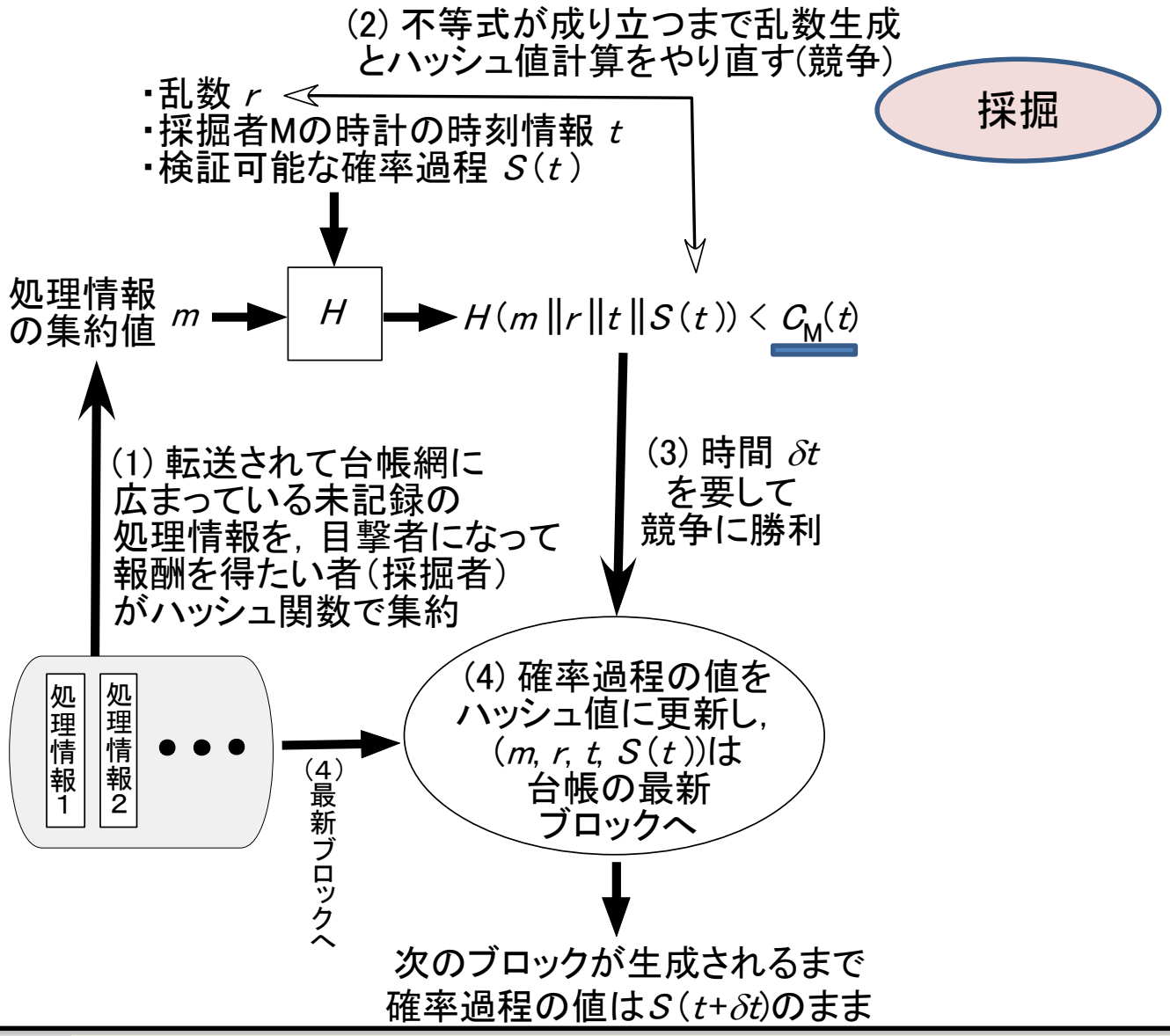
- C. Dwork, M. Naor: Pricing via processing or combatting junk mail. CRYPTO 1992.

■ サービス妨害攻撃対策



- K. Matsuura, H. Imai: Modified aggressive modes of Internet Key Exchange resistant against Denial-of-Service attacks. IEICE Trans. Info. Sys., Vol.E83-D (5), pp.972-979 (2000) (「相手が署名を検証したかどうか」を低コストで検証する技術)

ブロックチェーンの一般化



技術的な家系図の補足とまとめ

■ 要素技術や基本的な考え方の多くは、新しくない。

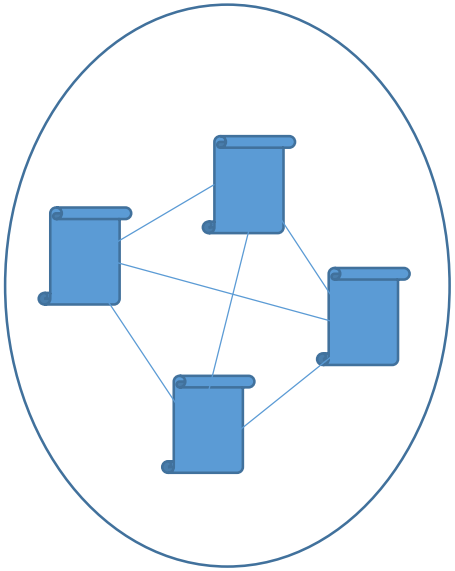
- 電子時刻印と電子公表、PoW（Proof-of-Work)(1992～2004)
- 公開鍵を（対応する秘密鍵所有者の）IDとする
  - D. Chaum: Untraceable electronic mail, return addresses, and digital pseudonyms. Commun. ACM, vol.24, no.2, pp.84-90 (1981)
- 追記型記録や証拠の保管と分散したハッシュ鎖の連携
  - B. Schneier, J. Kelsey: Cryptographic support for secure logs on untrusted machines. 7th USENIX Security Symposium (1998)
- スマート契約
  - N. Szabo: Formalizing and securing relationships on public networks. First Monday, vol.2, no.9 (1997)
- P2P、自律分散（インターネット）

要するに、歴史は長い

インターネット技術の必要性と課題

Permissionless/public chain　　Permissioned/private chain

- 各登場人物（不特定多数、または、何らかの制約のもとでの特定多数）の間での通信には、「次々と転送されて行き渡る」という通信が多い。
- 複数の採掘者が「ブロックを生成しました」と報告した場合に、誰を採用するか決めなければならない。
- 「プロトコル一式」を開発しなければ、大規模な実装はできない。
- ただし、最初からセキュリティを考えなければならない。



研究開発の現状

悲観的な側面

- 暗号技術： トップレベルの学会では、研究テーマの大きな柱となっているわけではない。
  - 学術的な新規性が少なく、論文になりにくい。
- プロトコル技術： オープンソースコミュニティ主導で進んでおり、アカデミアとの接点が十分ではない。
  - IETFにおける暗号プロトコルの標準化と、そのプロセスにおける評価不足と同じ問題が起きている。
- システム開発： スタートアップ企業に急激に資金が流入し、技術的な確からしさが確認される前に、ビジネスが始まってしまっている。
  - フィンテックでは、大手企業や公的機関等にも似た傾向（中途半端な実証実験に熱狂する傾向）がある。

既知の攻撃（例）

- 51% attack
  - 採掘のためのハッシュ計算の能力について、全世界の51%以上の能力をある1つの主体が有する場合、ブロックチェーンの更新を自由にコントロールできる。
- Transaction malleability
  - 鍵管理を含む暗号技術の弱点や自律分散技術の弱点を突いて、取引履歴を「痛いタイミングで」すり替える攻撃。
- Network de-anonymization
  - ネットワークトラフィックを観測することで、取引のプライバシを暴く攻撃。

これらに関する研究は多数ある。防御の決定的な進展はまだない。

スケーラビリティの問題

- Bitcoinでは、新たなブロックが10分に1回作られる。
- ブロックのサイズには決まった上限がある。
- そのため、10分間に処理できるトランザクション数に上限があり、その数は決済インフラで利用したいトランザクション数から考えると、はるかに少ない。
- 広い決済インフラとなるためには、スケーラビリティを劇的に向上させる必要がある。
- 安易な考え方は、プライベートチェーンへの逃避。しかし、そうするとブロックチェーンの意義が薄れる。
  - 中間的な考え方や、補助的な仕組みの活用などの研究が多い。

よく言われるフィロソフィ問題

■ ブロックサイズを大きくすると、1つのP2Pノードが保存しなければならないデータサイズ、ノードに接続されるネットワークの帯域の最低条件が上がる。

- ある程度の投資ができる人でなければ、ノードになれない。つまり、ノードになれる人が限られる。
- Bitcoinの目指す「特定の人のコントロールを受けない非中央集権的な通貨」というコンセプトに反することになる。そのため、Bitcoinのコア開発者の多くは、ブロックサイズ引き上げに反対。
- ビジネス応用を考えるスタートアップ企業などは、すぐにでもブロックサイズを引き上げて欲しい。
- ビジネスサイドとコア開発者の間で対立。採掘を事業にしたい者が議論に加わると、さらに話は複雑になる。

非中央集権的という語が様々な意味で使われ、やや混乱している。

解決・改善を目指す動き

- Bitcoinの開発コミュニティの間で様々な提案がある。
  - ブロックサイズを、単純に上げる。
  - ブロックサイズを、特定の人の支配を受けにくい形で順次上げる。
  - 補助的な仕組みを色々工夫して付け加え、ブロックチェーンの利用技術（アプリケーション）の方で、スケーラビリティを確保する。
  - 今のところ大したものはないが、粘り強く続けている。 レイヤー2
- アカデミア（経済学者も）を含めて、適切なスケーラビリティを確保するための開発者会議を開催
  - Scaling Bitcoin Workshop（2015年9月～） （2018年10月＠東京）

ポジティブな意味でのトリプルS

■ 社会(Society)を含むシステム

- 組織、制度、人も（モデル内で）扱う。
- 技術的なアプローチだけでは研究できない。
- **情報セキュリティ経済学**（信頼関係を左右する人や組織の行動原理を科学的に研究する有力なツール）が育ってきた。

■ プロトコル一式(Protocol Suite)を含むシステム

- 仕様全てを網羅的かつ詳細に、科学的な厳密さを保って記した資料はまだ無い（今後もおそらく現れない）。
- 伝統的なセキュリティ評価手法だけでは限界がある。

■ シナジー(Synergy)を考えて効果を評価

- **応用が極めて幅広い**。コスト削減だけが利点とは限らない。

仮想通貨以外の応用

仮想通貨 (Bitcoin等，2009～)

- TTP（国など）の信用の担保が困難な場合に有用（例：ギリシャ危機）。
- 先進国では規制が強まる傾向にある。
- 現状では投機性が強く、決済手段としての実証実験になっておらず改善へのサイクルも回り難い。

新たな応用への展開

他の金融分野

狭義のお金ではなく、資金移動のバックエンドの処理等に適用

- 株式、証券等
- 安価な海外送金
- 電子小切手

トラスト基盤としての他の応用

データ管理の正当性をTTPではなくBlockchainを用いて証明

- 登録状況、契約状況、権利関係など
- 事象の順序に関する厳格さと、オンラインで公開検証可能であることを利用した新サービスや監査

金融分野以外の応用例： 小口電力売買管理、食料サプライチェーン管理、医療情報システム管理、など。

参考: IEEE Blockchain for Agriculture Forum 2018（Nov. 28-29@Honolulu）

仮想通貨以外の応用

仮想通貨 (Bitcoin等, 2009～)

- TTP（国など）の信用の担保が困難な場合に有用（例：ギリシャ危機）。
- 先進国では規制が強まる傾向にある。
- 現状では投機性が強く、決済手段としての実証実験になっておらず改善へのサイクルも回り難い。

の他の応用

狭義

ではなく

系など

オンラ

を利用

共通の利点：　多様で細かな手数料（/報酬/特典）処理を、低コストで（？）埋め込める。

金融分野以外の

ェーン管理、医療情報システム管理、など。

参考: IEEE Blockchain for Agriculture Forum 2018（Nov. 28-29@Honolulu）

情報セキュリティ経済学

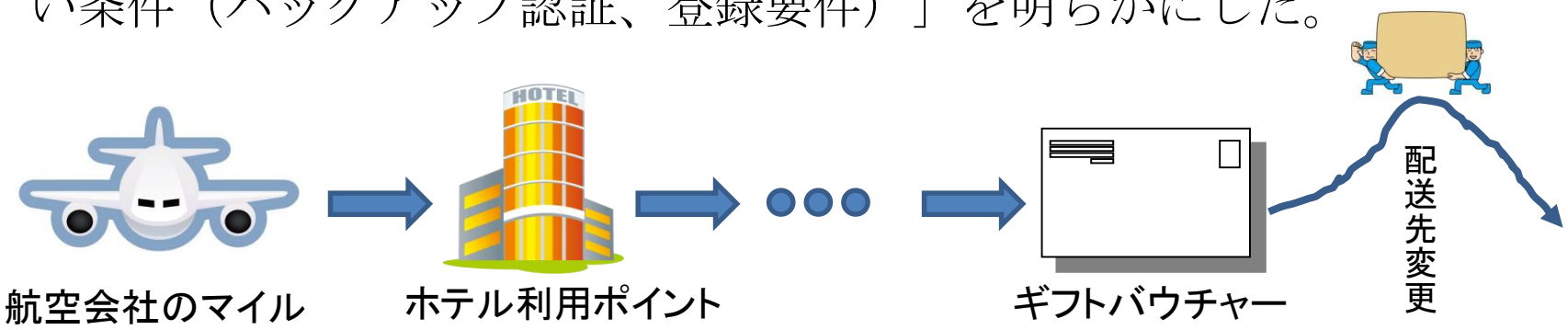
- 会議(WEIS: Workshop on the Economics of Information Security)を中心とする国際的な研究コミュニティに15年少々の歴史があり、定着してきた。

- 理論研究と実証研究が揃ってこそ威力を発揮する。
  - 情報セキュリティに関するある問題の発生要因が「経済学的最適戦略が直感に反し、人々がそれに従わないこと」にある。この事実を科学的に説明し、直感を正させる。
  - 情報セキュリティに関するある問題の発生要因が「人々が経済学的最適戦略に従うままにしておくと問題が発生するにもかかわらず、それを抑制/回避する社会制度設計などの対策が十分にとられていないこと」にある。この事実を科学的に説明し、十分な対策を促す。

ブロックチェーンの応用と好相性

■ Loyalty Program（ポイント制度やFFP）のセキュリティ

- B. Jenjarrussakul, K. Matsuura: Analysis of Japanese loyalty programs considering liquidity, security efforts, and actual security levels. WEIS2014. （後にJSSM論文賞）
- 計量経済学的な手法で「狙われやすい条件（流動性）」と「破られやすい条件（バックアップ認証、登録要件）」を明らかにした。



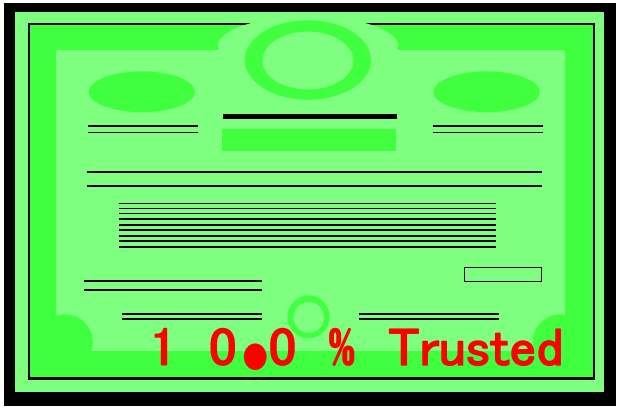
■ Bitcoinに関する地道な実証分析も色々ある。

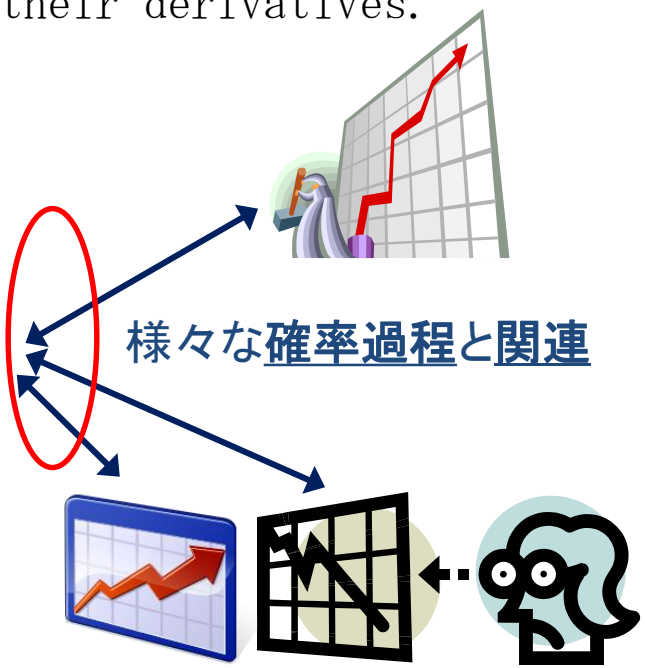
- N. Gandal et. al.: Price manipulation in the Bitcoin ecosystem. WEIS2017.
- 不可解なアカウントの取引がレート高騰を招いた証拠を提示

仮想通貨も従来から研究対象

■ 抽象化されたトークンとその金融派生商品の評価

- K. Matsuura: Security tokens and their derivatives. Technical Report 29, Centre for Communications Systems Research, University of Cambridge, 2001.
- K. Matsuura: Digital security tokens and their derivatives. Netnomics, Vol.5, No.2, pp.161-179, 2003.





（個々の時刻での値はその時刻が来れば確定するが、事前に正確に予測することはできない。）

ブロックチェーンの科学的な評価

■ 安全性評価はまだ始まったばかり。

- 本格的な実験的評価は無い。
- 暗号通貨の実システムが「生きた実験」かと思いきや、ブロックチェーンとは関係ない初歩的な問題で破られる事件に大騒ぎしている（インセンティブの観点で、情報セキュリティ経済学の研究テーマにはなり得る）（「本格的には破られていない」とも言える）。
- 一部の理論的評価(@Eurocrypt2015)にも問題があった。
- そもそもSecurity Notion（＝機能達成度＋攻撃モデル）が定まっていない。

■ パフォーマンス評価も甘い。

- 客観性と再現性はあるか？
- インターネット黎明期のNSFネットのような場が無い。

古典的な当然の課題も多い

- 鍵管理、当事者以外との情報共有、無効化、可用性
- 暗号技術の危殆化について考慮されていない
  - 中長期的な基盤としてのサステイナビリティ
- 開発されたソフトウエアの脆弱性
  - 単なるミス
  - スクリプトに関与するマルウェア

⇩

- ブロックチェーンが濫立している状態で、それぞれのブロックチェーン（と応用）で独立して自力解決できるか？
- 自力解決できた（と主張した）として、信じてもらえるか？

応用を広げる際の悩み

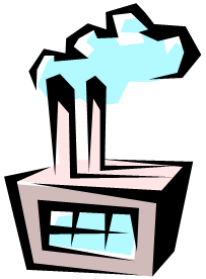
■ 適合業務、費用対効果、必要性(と十分性)

- 必要性を熱弁すると、「今のブロックチェーンで大丈夫なのか」と尋ねられて（or 心配になって）困ってしまうことがある。

■ データサイズの問題

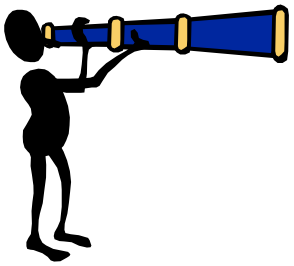
- 台帳保持者のインセンティブ

■ 環境負荷



採掘で一国に相当する電力消費

あちらこちらの動画



適切なレイヤ化を伴う「The Blockchain」への期待
（できるわけがないと思い期待していない人も、実際にできれば豹変することがある）

少なくとも、まともなコミュニティ形成には意味がある

テストネットワークの整備

- Bsafe.network: A neutral, stable and sustainable test network for blockchain technology by universities.
  - Each university *becomes a blockchain node*.
  - Research on blockchain and its applications.
    - Not limited to security.
  - Similar in intent to NSFNET for the Internet before its commercialization. *Evaluation* is needed.
    - Start-up members include Internet giants.

Internet-of-Trust ?

http://bsafe.network

産業界との窓口：BASEアライアンス

（Scaling Bitcoin Workshop 2018のアカデミックホスト）

■ Blockchain Academic Synergized Environment: ブロックチェーンの学術研究環境における産学連携のシナジーを意図。オープンな議論を旨とする。

- 慶應義塾大学 SFC研究所 および 東京大学 生産技術研究所 ソシオグローバル情報工学研究センター が設立
- 2017年度は運営方法などを検討し、2018年度から本格的に活動
  - WG:個別研究プロジェクト
  - 研究会
  - 公開イベント
  - 報告書
  - 国際標準化への貢献
  - BSafe.networkへの貢献

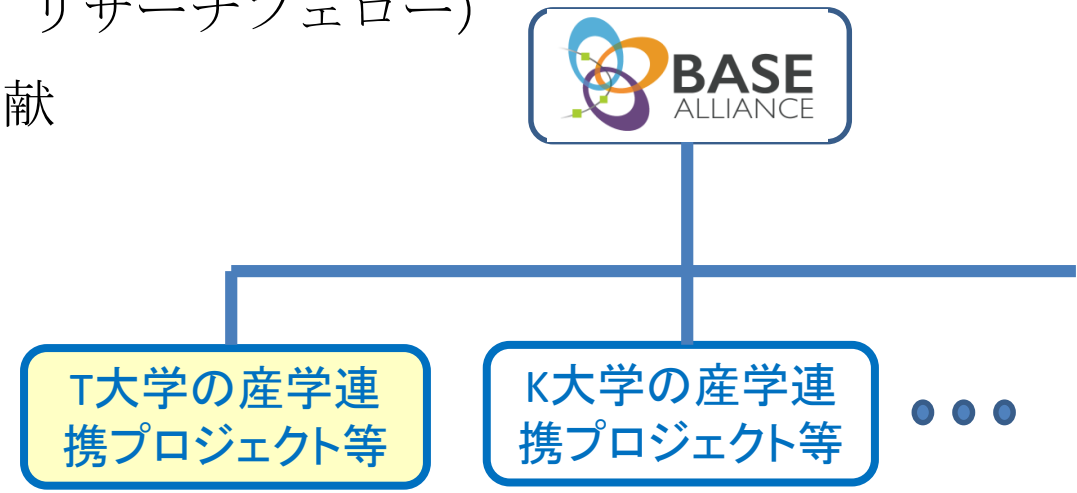
信頼関係が基礎

http://base-alliance.org/ja/about/

分散台帳とその応用技術特別研究会

■ 東京大学生産技術研究所を拠点とした活動(H28～)

- 共同研究契約ではなく、年会費制で参加できる枠組み（財団法人生産技術研究奨励会における枠組み）
- セキュリティ、経済学、評価に力点を置く
- 代表幹事：　松浦幹太（東京大学生産技術研究所　教授）
- 幹事：　松尾真一郎（同　リサーチフェロー）
- BASEを通してBSafeにも貢献
- 若手エッセイ賞の創設



http://www.iis.u-tokyo.ac.jp/shourei/ResearchCommitte/RC_gazou/rc2018/30RC-94.pdf

Public and Common Blockchain

■ シナジー(Synergy)を考えて効果を評価

- The Internetではない、IPを使った独自のネットワークを考える。
- 逆に、独自の（せいぜい業界共通の）ブロックチェーンではなく、**The Blockchain**を考える。
- **The Blockchain**では、新たなサービスの導入コストも低い。
- サービスを考えてこそ、多様なシナジーを考えることができる。
- 複数のサービスが共通のレイヤー２技術を必要としても、「The」のメリットを失わない（むしろメリットの増す）対応ができるか？
- レイヤー minus１（様々なBlockchainが乗ることを前提にして、IPや業界のネットワーク最下層に求める変革）の可能性
  - レイヤー0という語はある（意味が異なる）

むすび

ブロックチェーンの未来

- 目指すべき方向:
  - 正当な利用者の生産性を高め、社会の活力を増し、幸福をもたらす。
- 未来を担う人の関心を多く惹きつける。
  - トリプルS(Society, Protocol Suite, Synergy effects)に科学的に取り組むことは、エキサイティング。
- IT分野からのノーベル賞？
  - 経済学賞、医学・生理学賞、平和賞

ご静聴有り難うございました。