Blockchain Technologies and their Road towards Common Infrastructure

松浦幹太
（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）

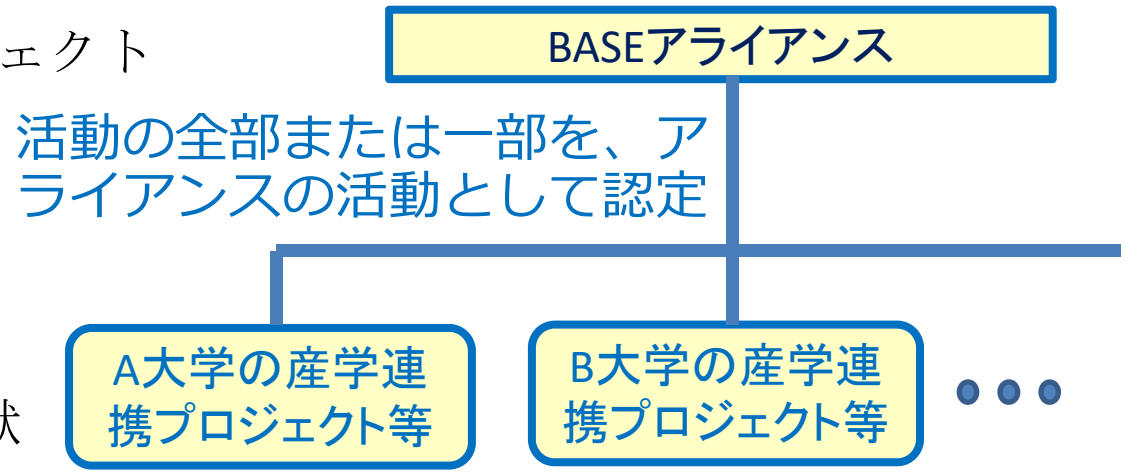
BASEアライアンス

■ 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

信頼関係が基礎

- 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



ブロックチェーンの研究

■ 要素技術や基本的な考え方の多くは、新しくない。

- 電子署名
- ハッシュ関数
- POW (Proof-of-Work)
  - C. Dwork, M. Naor: Pricing via processing or combatting junk mail. CRYPTO 1992.
  - 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.
- 追記型記録や証拠の保管と分散した鎖の連携
  - B. Schneier, J. Kelsey: Cryptographic support for secure logs on untrusted machines. 7th USENIX Security Symposium, 1998.

では、一体、何がとくに面白いのか？

エキサイティングなトリプル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。

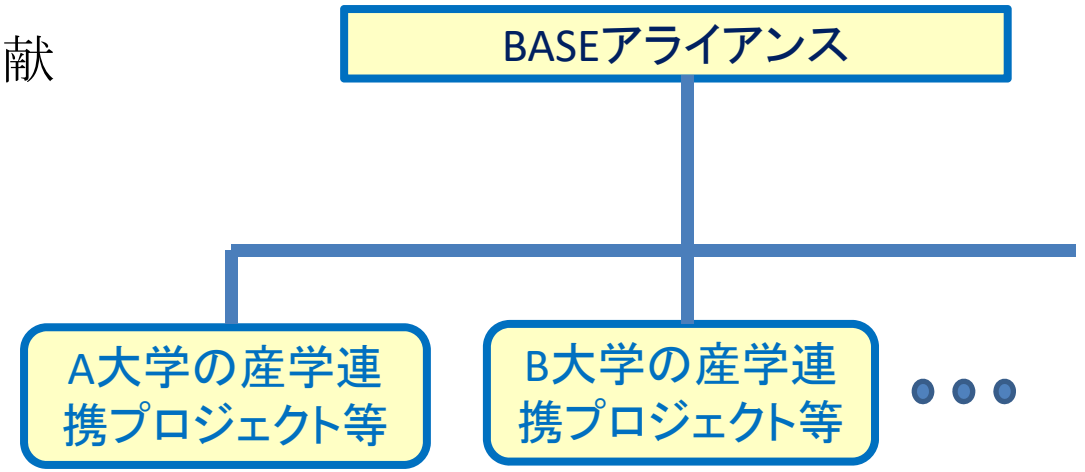
■ シナジー(Synergy)を考えて効果を評価

- コスト削減だけが利点とは限らない。

RC94：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



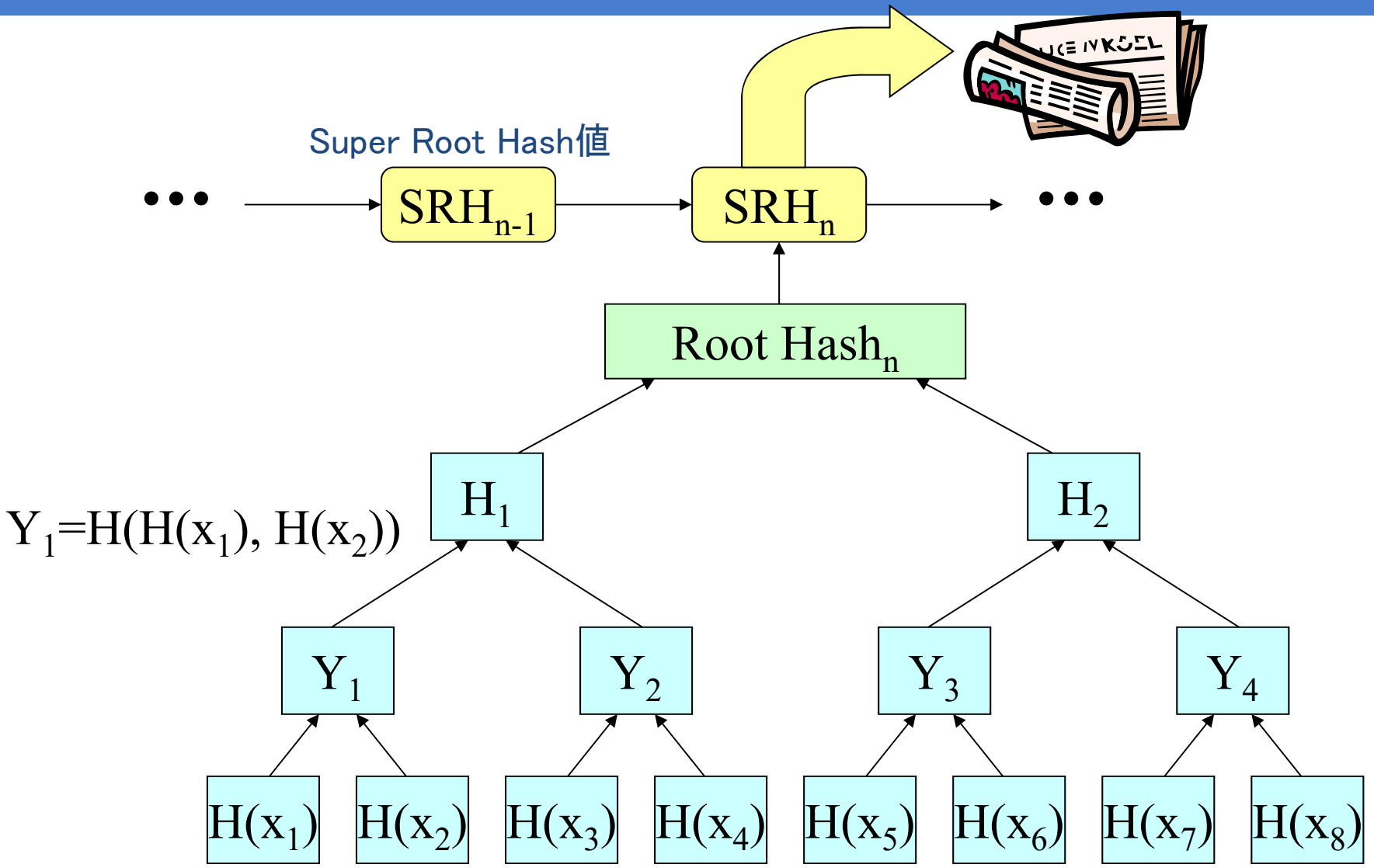
http://www.iis.u-tokyo.ac.jp/shourei/ResearchCommitte/RC_gazou/rc2018/30RC-94.pdf

Public and Common Blockchain

■ シナジー(Synergy)を考えて効果を評価

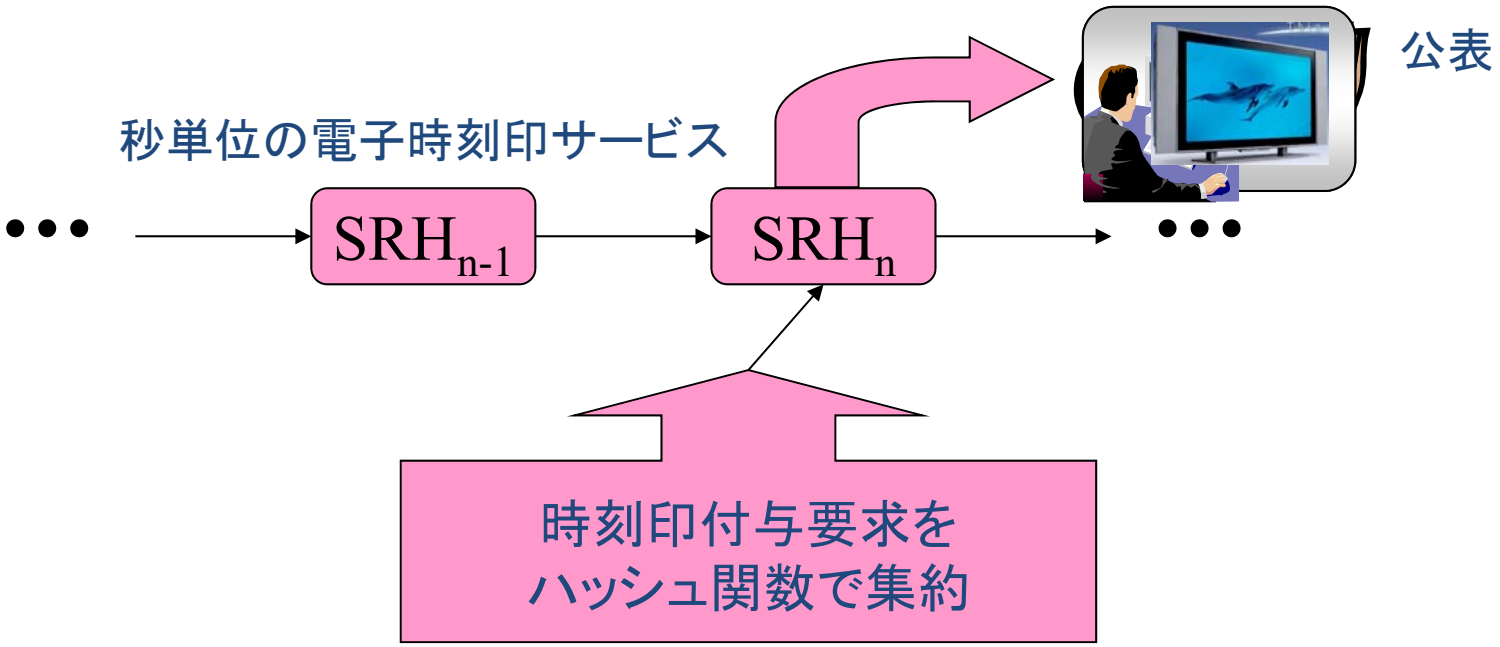
- コスト削減だけが利点とは限らない。
- しかし、コスト削減への期待は大きい。
- The Internetではない、IPを使った独自のネットワークを考えてみる。
- ブロックチェーンを使った独自の（せいぜい、業界共通の）ネットワークではなく、The Blockchainを考えてみる。
- 「The XXXX」では、新たなサービスの導入コストも低い。
- サービスを考えてこそ、多様なシナジーを考えることができる。
- いくつかの新サービスが共通のレイヤー２技術を必要とするケースにも、「The」のメリットを失わない（むしろメリットの増す）対応ができるか？

タイムスタンプ(1990年代前半)



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)

精度に関するイノベーション



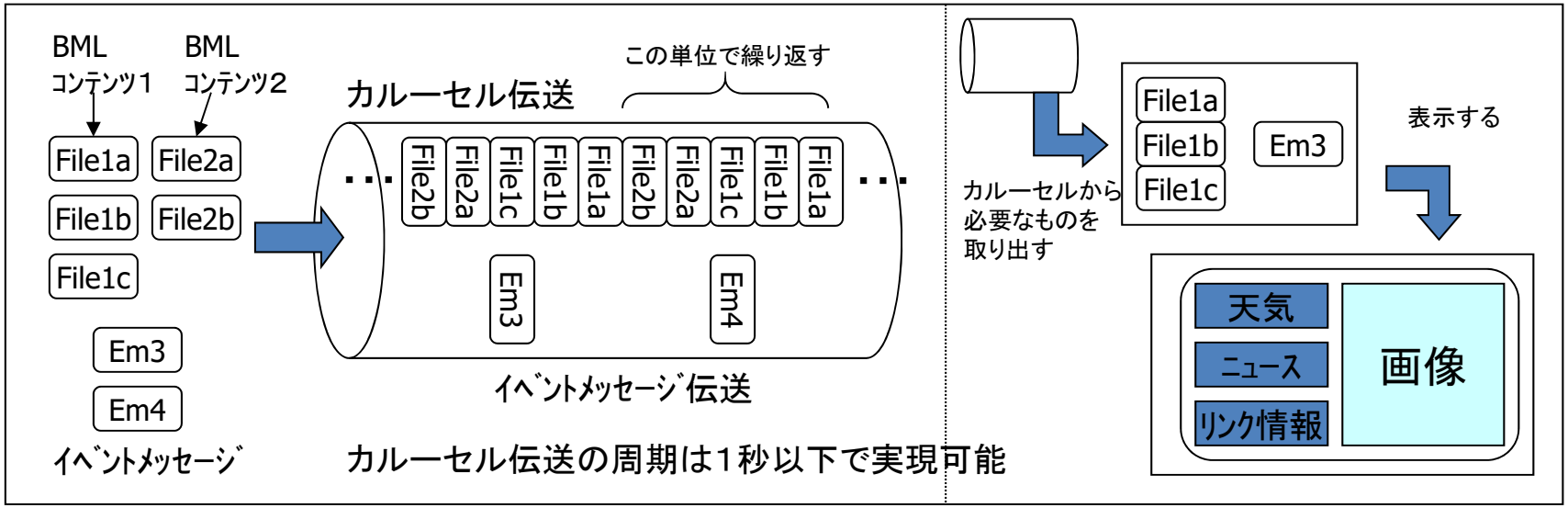
Tsutomu Morigaki, Kanta Matsuura, Osamu Sudo: ``An Analysis of Detailed Electronic Time-Stamping Using Digital TV'', Proceedings of the 2004 IEEE International Conference on e-Technology, e-Commerce, and e-Service (EEE04), pp.277-284 (2004)

周辺技術に立ち入る必要性

Digital TVは、テレビ放送、音声放送に加えて、データ放送サービスが存在

データ放送サービスでは、テレビ放送とは独立してデジタルデータを放映することができる。伝送方式は以下に示す通り、XMLを放送用に機能追加したBMLで記述したデータをデータカルーセル方式で伝送する。

DSM-CC（Digital Storage Media Command and Control）ダウンロードカルーセル方式



データ放送でリンク情報を掲載すれば、秒単位以下の精度で公表が可能

むすび

- 費用対効果を考えて、ブロックチェーンとその応用に取り組む時に、インフラ技術としての視点を強く持つ。
- 効果を高める工夫が、ブロックチェーンの外に飛び出す。
- レイヤー2コンペティションをBSafe.networkで扱う意義
- 「電子証拠物工学」としての体系的な研究