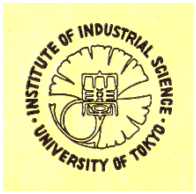
2019年2月15日
Third Basing Blockchain WS

ブロックチェーンの一般化とレイヤー・マイナス・ワン

松浦幹太
（東京大学 生産技術研究所）

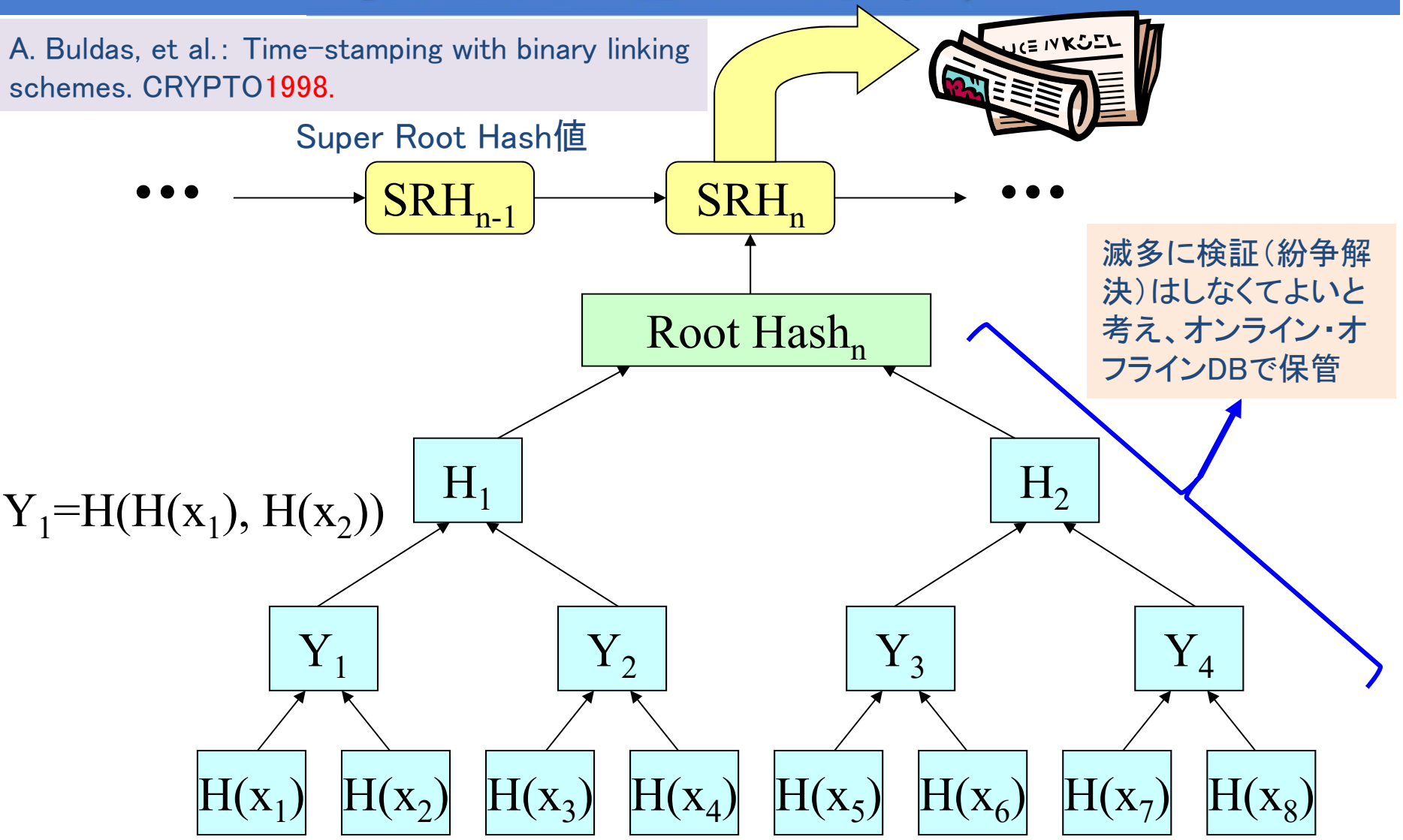


東京大学 THE UNIVERSITY OF TOKYO

基礎

安全な電子時刻印

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

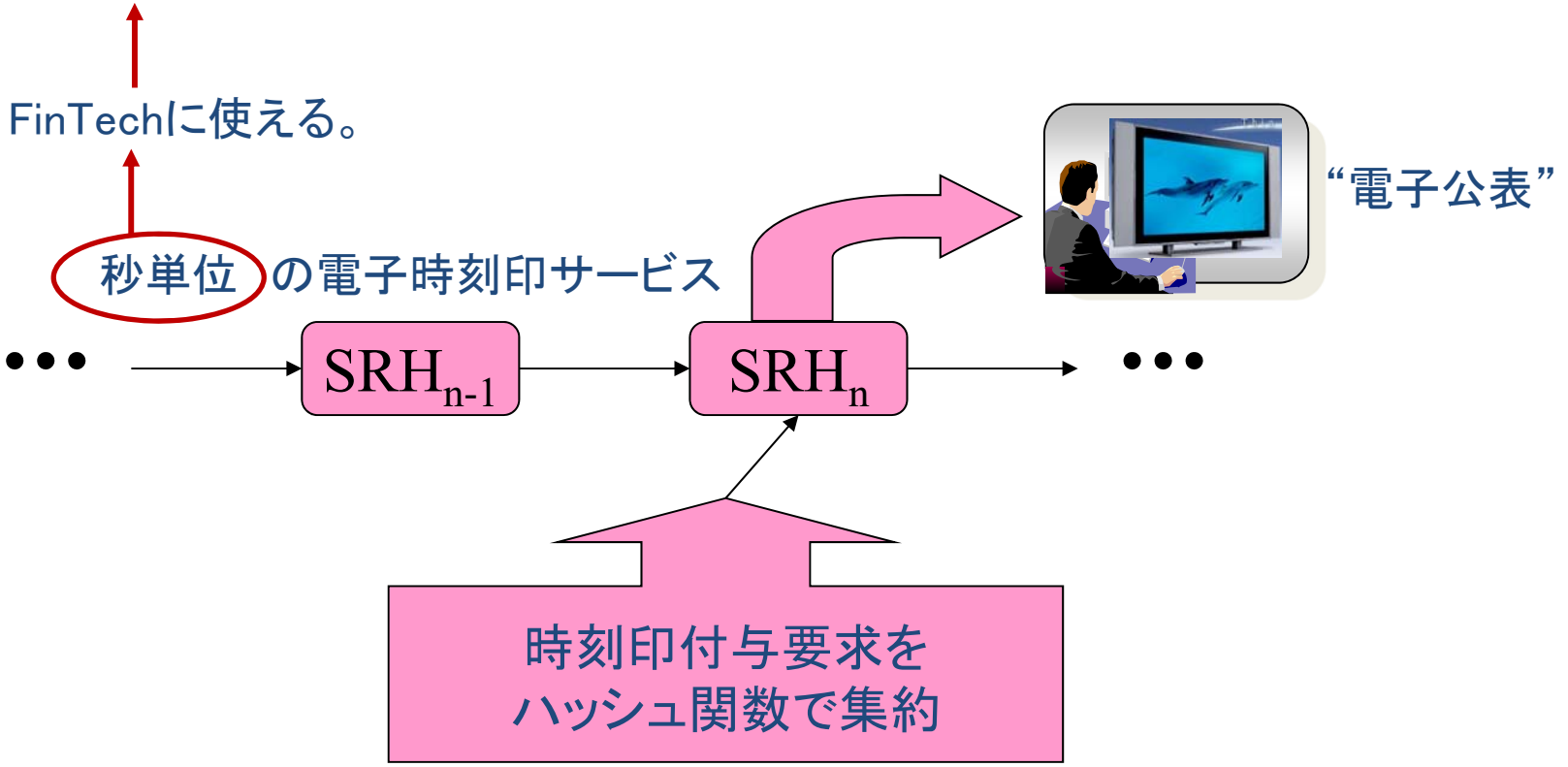


滅多に検証(紛争解決)はしなくてよいと考え、オンライン・オフラインDBで保管

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。



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。

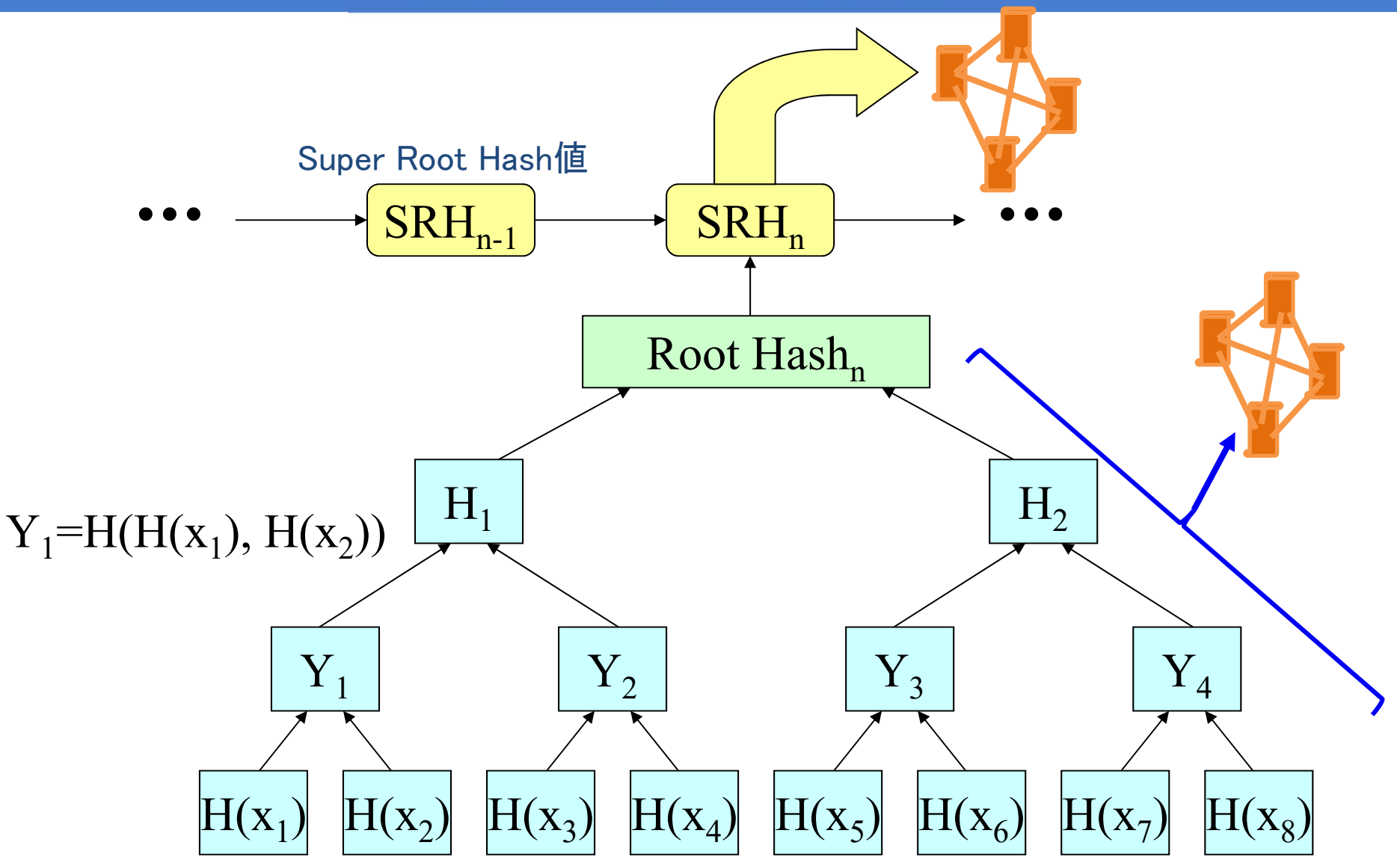
- 目撃者にインセンティブを与えるメカニズムが必要
- 報酬を与えるのが便利（とくに、仮想通貨の場合）
- 報酬と関連するからには、不正や混乱の防止が必要（PoW）
  作業証明

■「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)。
- 約10分かかる仮想通貨は「遅い」と言われるが、そ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・全データ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.

全データの保存


Super Root Hash値
SRH$_{n-1}$
SRH$_n$
Root Hash$_n$
Y_1=H(H(x_1), H(x_2))
H_1
H_2
Y_1
Y_2
Y_3
Y_4
H(x_1)
H(x_2)
H(x_3)
H(x_4)
H(x_5)
H(x_6)
H(x_7)
H(x_8)

一般化

- Kanta Matsuura: “Token Model and Interpretation Function for Blockchain-Based FinTech Applications.” IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Vol.E102-A, No.1, pp.3-10 (January 2019)(オープンアクセス)
- 松浦幹太:「情報セキュリティ基礎講義」コロナ社 (2019年2月18日出版予定)

素朴な（かつ大きな）疑問

- 単純な電子時刻印が保証しているのは「あるデータがある時既に存在しており、それ以降、改ざんされていない」こと。
  - 要するに、十分古いということ。
- 十分新しいこと（「あるデータが、その時まで存在せず、その時になって初めて誕生したこと」）を保証することは可能か？
- 「十分な頻度でバックアップを繰り返せば、データの自然劣化はいくらでも抑えられること（＝デジタル化の利点）」が、仇となりかねない。

ブロックチェーンを一般化した解釈は、インセンティブ設計と組み合わせて疑問に答える一つの可能性を示している。

ブロックチェーンの一般化

■ 適合確率過程(adapted stochastic process)の利用

- 時間とともに変化し、将来の値を正確に予測することはできないが、その時が来ればその時刻 t の実現値(occurrence) S(t)を誰でも知ることができる（例： 株価、気温）。
- 後で実現値を信頼できるリソースから取り出して参照できる。

- ナンス r
- 時刻(又は実現値のindex) t_n
- 確率過程の実現値 $S(t_n)$

不等式を満たすまで、ナンスの生成とハッシュ計算を繰り返す(この探索がWorkで、最終的な r がProof)。

処理情報を集約したルートハッシュ値 RHn → H → $SRHn = H(RHn \| r \| t_n \| S(t_n)) < ターゲット値$

時間 δt_n が経過して勝利者が決まれば確率過程の実現値が変化: $S(t_n+\delta t_n) = SRHn$

（ドリフトは無い）

自律分散では、ここが難しい。

ハッシュ関数

- **ブロックチェーンでは、様々な使い方（要件の異なる使い方）が混在していて紛らわしい。**
  - 一方向性が要求される（暗号学的ハッシュ関数としての）使い方：PoW（SRHを決める過程）
  - 衝突発見困難性が要求される（暗号学的ハッシュ関数としての）使い方：　ルートハッシュ値の計算過程
  - 単なるインデックスとしての（データベース工学的な）使い方：トランザクションID，ユーザID
- **具体的に実装する際になすべき工夫は、本来、それぞれの使い方で異なる。**
  - 現在のブロックチェーンにおける実装の完成度は低い（かもしれない）。

学術的に一般化したモデルを把握した上で

基盤としてのブロックチェーン

を考えたい

広がる応用

仮想通貨 (Bitcoin等，2009～)

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

ポイント還元制度

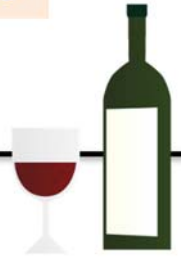
トラスト基盤としての他の応用

データや経過の正当性を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、研究倫理、など。

参考: IEEE Blockchain for Agriculture Forum 2018



サプライチェーン管理

（ポイントはIT化であり、ブロックチェーンは構成要素の一つ。AI も重要な役割を果たす。）

- 利点
  - 不正や誤りを削減、防止
  - 在庫管理を改善
  - 配送コストを最小化
  - 文書化のための遅延を削減
  - 無駄な廃棄の削減
  - 問題の迅速な発見

（などが期待されている。）

■課題

- サプライチェーンの全過程での記録のディジタル化
- 情報の透明性と適切なアクセシビリティ
- 自律分散系における認証
- 既存のネットワークとの統合
- 並列経路（例えば複数のパートナーにまたがる仕入れ）の扱い
- データ所有権をどう考えるか

（などが確実に存在する。）

一般的な利点と課題

- **多様で細かな手数料(/報酬/特典/差別化)処理を、比較的容易に埋め込むことができる。**
  - ただし、そのブロックチェーンに仮想通貨が乗っていなければ、必ずしも特別便利ではない。
  - 金融分野の視点で見た仮想通貨のリスクが問題となり得る。
- **適切なレイヤー化によって、異なるアプリケーションの要件にそれぞれ対応できる可能性がある。**
  - ただし、これまでの取り組みはレイヤー２に偏っている。
  - レイヤー・マイナス・ワン（様々なチェーンが乗ることを前提にして、IPや業界のネットワークの下位層に求める変革 and/or 共通の「The Blockchain」や語彙の整備）の可能性

コスト削減と深く関連

安全性モデルと深く関連

混沌とした現状

- GitHubで見つかったブロックチェーン関連のプロジェクト数： 86,034件
  - 実質的には9,375件程度との指摘あり（多くのプロジェクトがフォークしている）。
- 速いペースで誕生： 年平均8,603件（ただし2016年に26,885件）
- 生存率： たった8%しか活動が続いていない（フォークしたものに限れば5%）。
- 平均寿命： 1.22年

Deloitte analysis of GH Torrent data and GitHub API data, as of October 12, 2017.など

共通の関心事：人材育成

第1回BASEアライアンス・ユース・アワード

2018年10月のCSS2018での広報

（院生の方、申し訳ありません）

- 応募資格：　日本の大学の四年生またはそれ以下の学年の学生(中高生を含む)
- 募集内容：　自由なテーマでブロックチェーンについて論じるオリジナルのエッセイ（単著）を、A4用紙で2ページ以内にまとめてご応募下さい（テーマ例：地球環境とブロックチェーン）。
- 締切：　2018年11月16日（延長しました）
- 詳細はBASEアライアンスHPにて

締切延長

- 普通は、投稿が少ない状況などを踏まえて決断します。
- 時系列の投稿数推移の披露は、ナイトセッション等での定番です。
- しかし、このアワードに対しては、応募がなかったので延長しました。
- そして、延長した締切になっても、応募がありませんでした（涙）。

我々は何をすべきか

- 研究者は、そう簡単にはあきらめない。
- 教育者は、あきらめない。
- 押して駄目なら引いてみる。
  - 応募資格の拡大
- 謙虚になる。
  - もはや締切延長ではない。

第2回BASEアライアンス・ユース・アワード

（「第1回は応募がなかった」という記録を残す。）

- 応募資格： 応募時点で現役の学生（中学生、高校生、大学の学部生、大学院学生、社会人大学院学生も可）
- 募集期間： 2019年2月15日～3月31日
- 詳細は、ホームページをご覧下さい。
- 奮ってご応募下さい（「自称若手」歓迎）。

ご静聴有り難うございました。