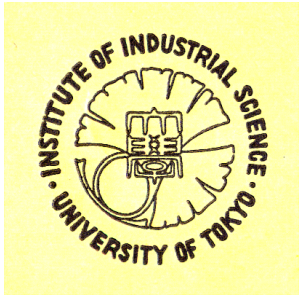
Presentation at the 4th Workshop Basing Blockchain
10:20-10:55 on October 8, 2021

ブロックチェーンの消費電力を抑える
Proof-of-Verification



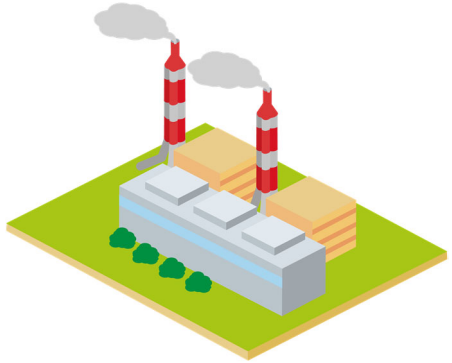
松浦 幹太
(東京大学　生産技術研究所)

Introduction

本日のパネルは「ブロックチェーンがもたらすトラストとその持続可能性」

ブロックチェーンの社会受容性を脅かす問題

- 悪意と関連深い問題
  - マネーロンダリング
  - ランサムウェア事件での身代金支払い
- 結果的に迷惑をかけるかもしれない問題
  - 投機性、中毒性
  - 消費電力（従来から採掘は問題視されてきた： ``extremely energy-hungry by design, as the currency requires a huge amount of hash calculations[1],'' ``The mining of a single bitcoin block—a block of transaction data on the bitcoin network—consumes enough energy to power more than 28 U.S. homes for a day[2]''。最近では、検証等の冗長性も問題視されつつある： ``the redundancy underlying all types of blockchain technology can make blockchain-based IT solutions considerably more energy-intensive than a nonblockchain, centralized alternative[3]''）

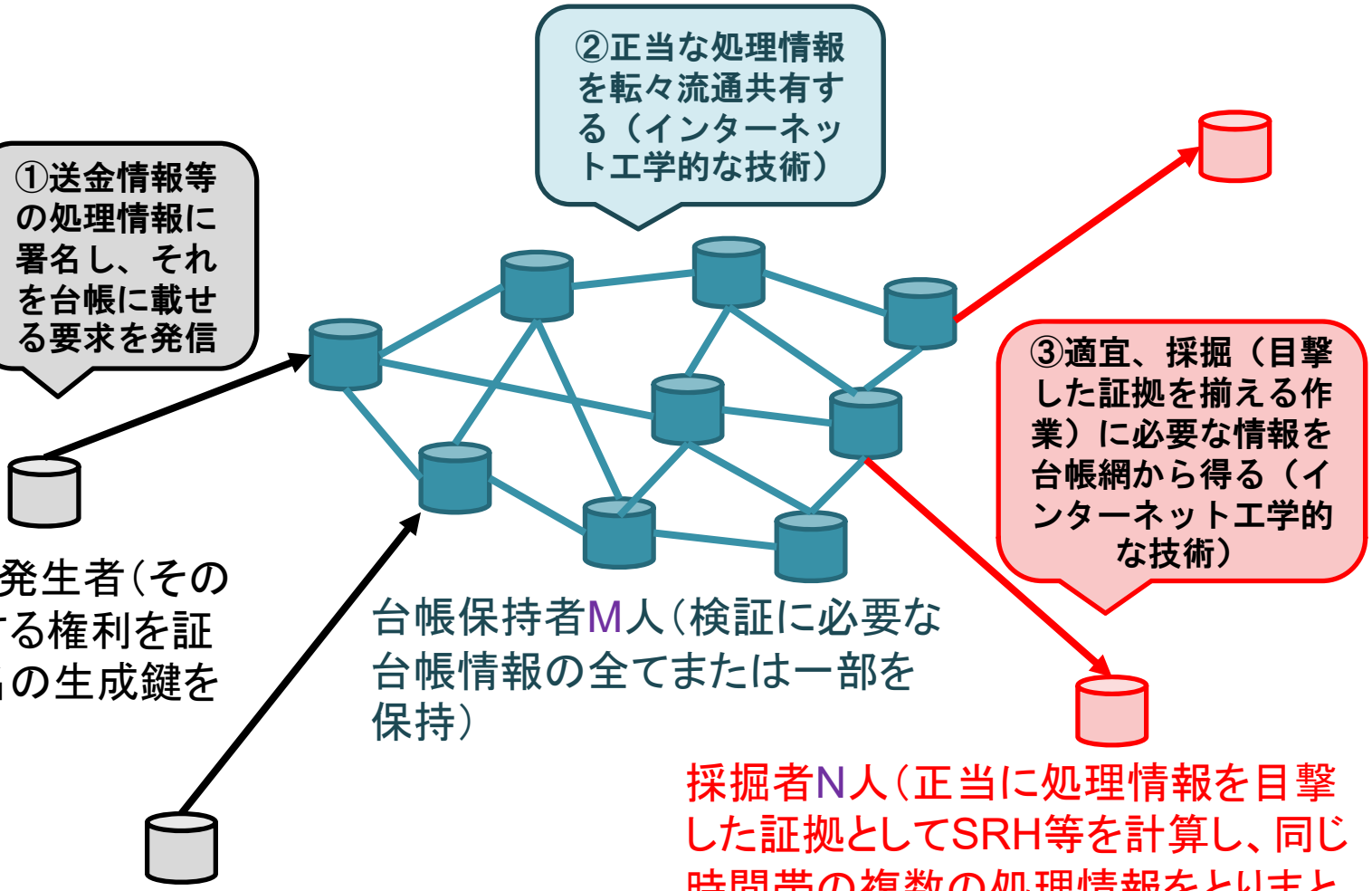


[1] A. de Vries: ``Bitcoin's Growing Energy Problem,'' Joule, vol.2, Issue5, pp.801-805, 2018.
[2] L. Kugler: ``Why Cryptocurrencies Use So Much Energy — and What to Do About It,'' Communications of the ACM, vol.61, no.7, pp.15-17, 2018.
[3] J. Sedlmeir, et al.: ``The Energy Consumption of Blockchain Technology: Beyond Myth,'' Business & Information Systems Engineering, vol.62, pp.599-608, 2020.

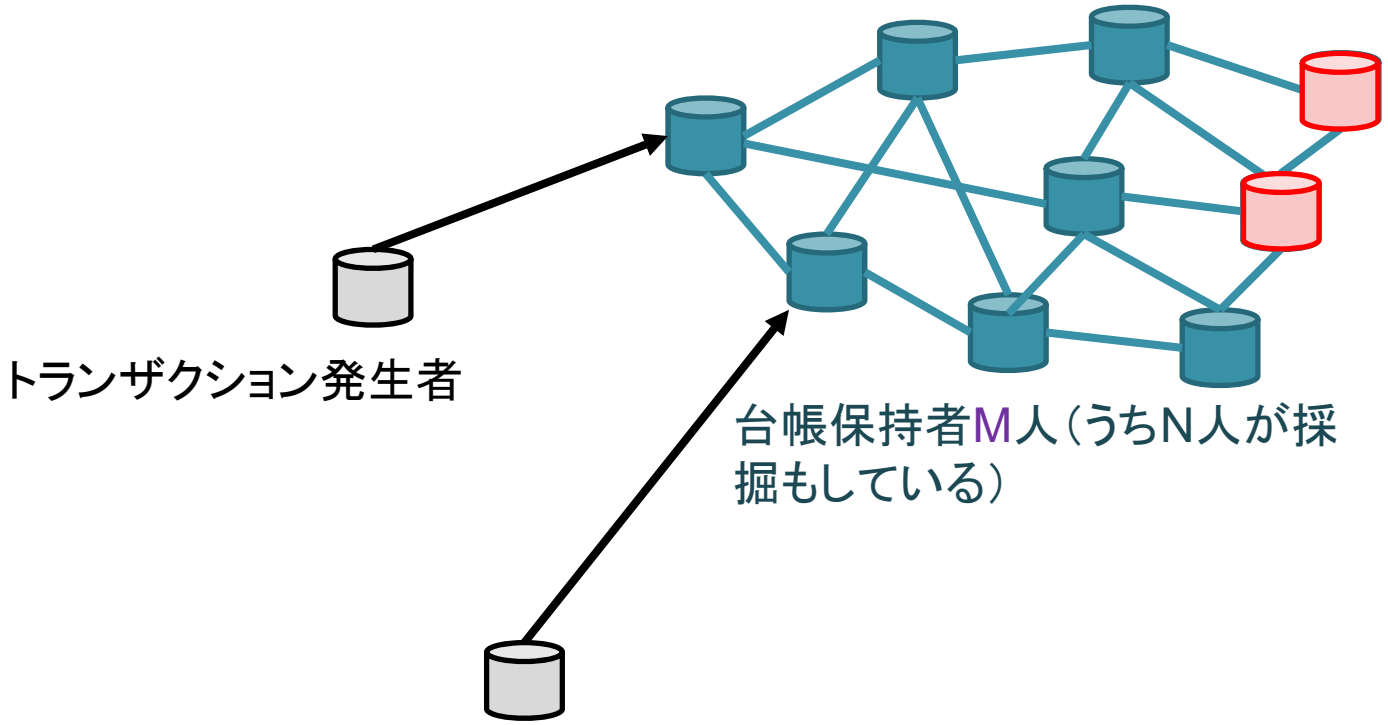
（パブリックなチェーンで）

電子署名の検証は何回？

一つの署名が最大で
M+N回検証される



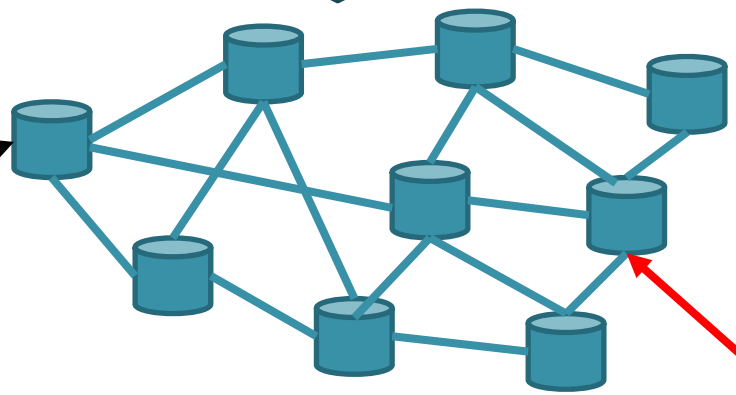
この図のように描きたい気もしますが、説明の便宜上、前のスライドのように採掘者を分けて描きます。PoVの本質には影響ありません。



（基本的なパブリックチェーンで）

電子署名の検証は何回？ → 合計で最大2M+N回

冗長！



⑤新しいブロックを転々流通共有して台帳に載せる（インターネット工学的な技術）

コンセンサスアルゴリズムで勝利者が決まる（ブロックチェーンに特徴的な技術）

⑥新しいブロックに自分の処理情報が載っていなければ、再要求

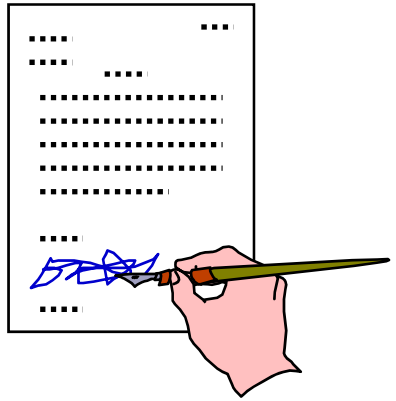
④採掘できたら「目撃したので報酬を下さい」という要求として新しいブロックを台帳網に発信（早い者勝ち）

トランザクション発生者（その処理情報を発する権利を証明する電子署名の生成鍵を持つ）

台帳保持者M人（検証に必要な台帳情報の全てまたは一部を保持）

採掘者N人（正当に処理情報を目撃した証拠としてSRH等を計算し、同じ時間帯の複数の処理情報をとりまとめた新しいブロックを作成する）

検証証明（PoV: Proof-of-Verification）



- 元々は、採掘競争に勝つために電子署名検証をサボる採掘者を許さないために考案された[4]。
  - 安全性への要請から、電子署名の生成には普通はランダムネスがある（同じ文書に同じ鍵で署名しても、生成される電子署名の認証子の値そのものはその都度異なる）。
  - そのため、たいていの電子署名検証アルゴリズムには、そのランダムネスを反映した数値を復元するプロセスが含まれる。
  - その数値は、正直に検証しなければ知り得ないものなので、PoVとして利用できる（通信オーバーヘッドが気になるならばそのハッシュ値をPoVとする）。
  - 電子署名のアルゴリズムに本来備わっているものなので、その意味ではPoVを導入することに伴うオーバーヘッドは無い。

[4] K. Matsuura: ``Proof-of-Verification for Proof-of-Work: Miners Must Verify the Signatures on Bitcoin Transactions'', Scaling Bitcoin Workshop 2019.
https://telaviv2019.scalingbitcoin.org/presentations
http://kmlab.iis.u-tokyo.ac.jp/papers/scaling19-matsuura-final.pdf

Reducing Redundancy (of Signature Verification)

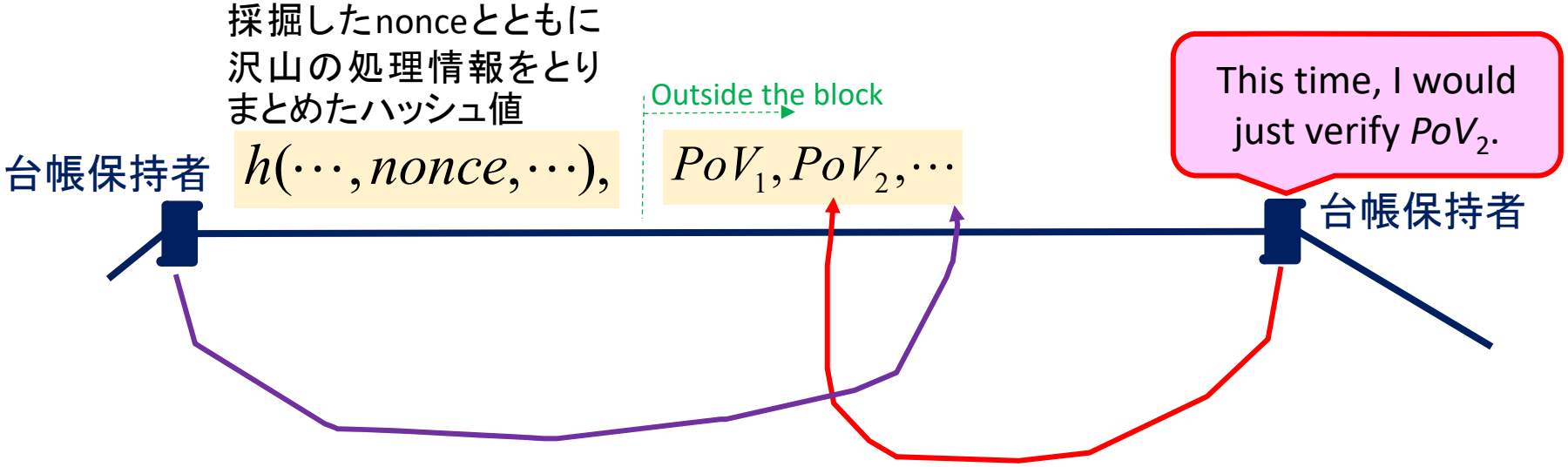
正直な

台帳保持者による検証回数の削減

合計で最大2M+N回だったものがγM+N回に！

- 処理情報の転送時（②）には検証しない。
- 新ブロックの転送時（⑤）にはランダムに選択したPoVだけを検証する（選択する割合をγとする）。

→　全体として、環境負荷を低減する。



Scaling Bitcoin Workshop 2019では口頭で示唆。その後、[5]で明示的に提案。

[5] 松浦幹太: ``検証証明（PoV: Proof-of-Verification）とその活用について'', 慶應義塾大学SFC Open Research Forum 2019, パネル討論「ブロックチェーン技術と金融資産の今後の展開」(2019)

基礎実験

（実験実施者： 細井琢朗）

- ローカルなマシンでbitcoindを利用して基本的な計算時間の変化を確認
  - 処理情報の検証時間

署名検証省略	>2.4%短縮
PoV導入	変化せず

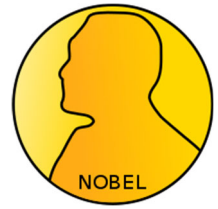
  - ブロック生成時間

署名検証省略	>3.8%短縮
PoV導入	原理的には変化しない

- 考慮すべきだが体系的に評価するには詳しい検討が必要
  - マイニングプールのように合同で採掘する者達の影響
  - レイヤー2などのサブシステムの影響
  - 計算時間＝消費電力ではない
    - 様々なタイプのステークホルダーが用いるデバイスやその動作環境等の違い（燃費の悪い嗜好を持つ者の計算負荷が少ない方がよい？でも、それでインセンティブ設計は大丈夫？）

Some Notes for Discussion

もちろん
環境負荷対策の関連研究 は色々あります



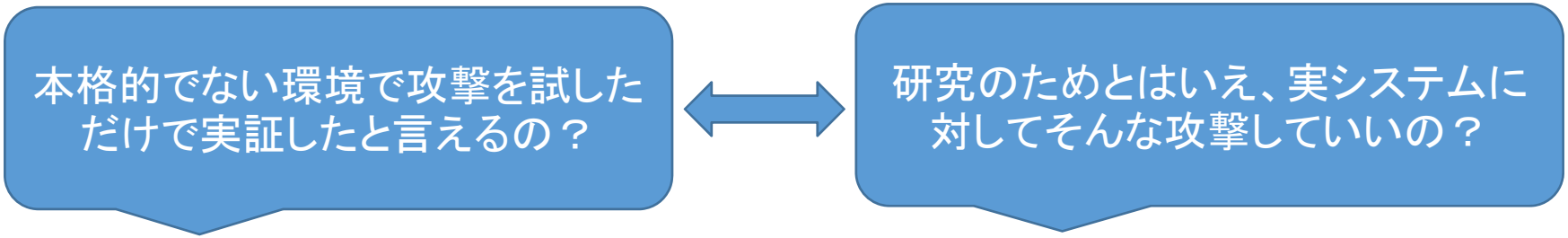
- 採掘者のタスクに起因する消費電力を削減する工夫（P2P型の運用を断念するものもある）[2], [6]
- 二重使用でないことを確認する作業の冗長性に着目[7]
- 複数の台帳保持者を連携させ検証を並列化[8]
- 気候変動抑制など社会貢献に資する応用を進め「それだけの消費電力に値する」と位置づけられるよう導く施策的アプローチ[9]

[6] P. Fairley: ``Ethereum Plans to Cut Its Absurd Energy Consumption by 99 Percent,'' IEEE Spectrum, January 02, 2019.
[7] S. Cao, et al.: ``CoVer: Collaborative Light-Node-Only Verification and Data Availability for Blockchains,'' Proc. 2020 IEEE International Conference on Blockchain, pp.45-52, 2020.
[8] M. Leshkowitz, et al.: ``Scalable Block Execution via Parallel Block Validation,'' Annals of Telecommunications, 2021.
[9] J. Truby: ``Decarbonizing Bitcoin: Law and policy choices for reducing the energy consumption of Blockchain technologies and digital currencies,'' Energy Research & Social Science, vol.44, pp.399-410, 2018.

関連研究は必ずしもライバルではない

- 多くの場合、どれが優れているか優劣を比較すべき関係ではない。
- むしろ、連携・併用してより一層の省電力化を達成できるかを検討すべき関係（共存共栄を目指す関係）である。
- 高いレベルで併用するためには、本当に連携する方がよい。
- いずれにせよ、本格的に改善が見込まれれば、技術を変えましょうと提案したくなる。

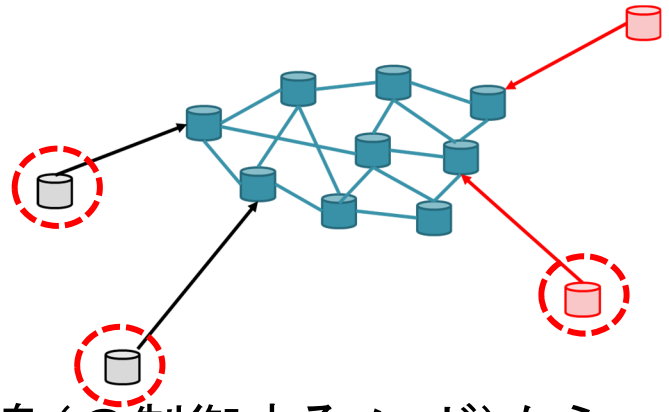
- 地球、人類、仲間、・・・



社会受容性を脅かし得る研究倫理の問題

- プロトコル一式(protocol suite)となると、一部の暗号要素技術／暗号プロトコルのように「美しく理論的な安全性証明をする」というアプローチは原則として通用しない。
  - 部品が安全でも、システムが安全とは限らない。
  - システムが安全でも、サービスが安全とは限らない。
- 安全性評価、解析研究として本格的な攻撃を実施する場合に必要な倫理的手続きとは？
  - 技術的な攻撃も、技術的でない攻撃もある。
  - サービスの盲点を突く（必ずしも不正ではないけれども）卑怯な行為もあり得る。
  - 何か問題（例えば、今日これまで見てきた消費電力問題）を解決すべく技術を変えたら、解析が振り出しに戻ることがある。

有名な攻撃論文の事例



- 利己的な採掘[10], [11]
  - 競争で有利になるよう、採掘者が自身(の制御するノード)から処理情報を台帳網へ発信するタイミング(①)を見計らう。
  - [11]のResponsible disclosureと題すセクションにおける記述:
    ``In order to promote a swift solution and to avoid a scenario where some set of people had the benefit of selective access, we published a preliminary report[9] and explained both the problem and our suggested solution in public forums.[8]''

[10] I. Eyal and E. G. Sirer: ``Majority Is Not Enough: Bitcoin Mining Is Vulnerable,'' Lecture Notes in Computer Science 8437, pp.436–454, 2014.
[11] I. Eyal and E. G. Sirer: ``Majority Is Not Enough: Bitcoin Mining Is Vulnerable,'' Communications of the ACM, vol.61, no.7, pp.95-102, 2018.
8. Eyal, I., Sirer, E.G. Bitcoin is broken. hackingdistributed.com/2013/11/04/bitcoin-is-broken/ (2013).
9. Eyal, I., Sirer, E.G. Majority is not enough: Bitcoin mining is vulnerable. arXiv preprint arXiv:1311.0243 (2013).

“The Blockchain”

- The Internetのように共通の実インフラができるか？
- 共通の実インフラはできないけれども、（暗号を深く理解して全てを自分で設計し実装するのは難しいので）多くの実システムが技術としては酷似したものを用いるか？
  - 「何故ブロックチェーンを使うの？」という問いへの本音の答えがここにある場合も少なくない（？）
  - トラストモデルの軽微な違いを運用の違い等で吸収
- 上記いずれかの意味で“The Blockchain”になるならば、基本設計段階で環境負荷に留意することや、適切な安全性評価の文化は、持続可能性のために一層重要となる。
- そうでなくても大切だと、個人的には思います。

ご静聴有り難うございました。