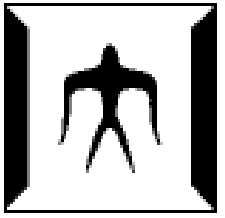
暗号通貨とブロックチェーン

首藤 一幸 / Kazuyuki Shudo
東京工業大学 情報理工学院



Tokyo Tech

首藤 一幸 (47)

しゅどう　かずゆき

1996　早稲田大学 修士課程

1998　早稲田大学 博士課程

2001　産総研 **国研**

2006　ウタゴエ(株) **スタートアップ**

2008/12 東工大 **大学**

2009/ 5 未踏 PM

Java スレッド移送システム MOBA

Java Just-in-Time コンパイラ shuJIT

17,000ダウンロード, 商用実績

P2P の基盤ソフト Overlay Weaver

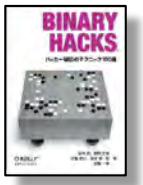
26,000ダウンロード, 15ヶ国

41ヶ国 673台以上で動作 (データベース)

P2P ライブ配信ソフト UG Live

未踏スパクリ × 2人, 商用化, 1万数千人に同時配信

書籍 Binary Hacks



著者5人, 1万数千部

P2P のアルゴリズム, 2009 ～

構造化オーバレイ / DHT の統一フレームワーク

分散データベース, 2009 ～

読み書き性能両立, Causal consistency, NVRAM / SCM

分散システムのシミュレーション, 2011 ～

1億ノード / 10台, 既存手法の20倍の性能, Apache Spark 上

ソーシャルネットワーク解析, 2013 ～

非集中 分散 機械学習, 2016 ～

ブロックチェーン, 2016 ～

2021年 1月

魔法のようなソフト

大規模分散システム

講演の概要

ブロックチェーンの…

- 起源・価値 p.3 ～ 11, 9ページ
  - 暗号通貨 Bitcoin
  - 非集中に二重使用を防止 → trustless
- 応用 p.12 ～ 17, 6ページ
  - 通貨やトークン追跡、自己主権型アイデンティティ、…
  - 留意点
- 技術 p.18 ～ 28, 11ページ
  - トランザクション承認方式
  - ブロック生成
- 研究 首藤研での取り組み p.29 ～ 58, 30ページ
- 社会 p.59 ～ 68, 10ページ
  - 盗難事件, 通貨, Libra, DeFi と DAO, Web 3, …

ブロックチェーンの
起源・価値

- 暗号通貨 Bitcoin
- 非集中に二重使用を防止 → trustless

暗号通貨　または仮想通貨, 暗号資産

cryptocurrency　　crypto asset

- デジタルなお金は、いろいろある。
  - Suica, PASMO, PayPay, ○○ポイント, …

3,000 種類以上ある

- 暗号通貨：Bitcoin (BTC), Ethereum (ETC), Ripple (XRP), …
  - Bitcoin に端を発する、非集中的 (後述) なもの
  - Bitcoin 時価総額 数十兆円　「通貨」になりたいが現状「資産」

暗号通貨の起源

- 2008年の論文

  ネットで見つかる。
  和訳もある：
  https://coincheck.blog/292
  読むのもいいのでは？

Bitcoin: A Peer-to-Peer Electronic Cash System

ビットコイン: peer-to-peer 電子現金 システム

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending.

- 2009年 1月のメール

Bitcoin v0.1 released

Satoshi Nakamoto satoshi at vistomail.com

Thu Jan 8 14:27:40 EST 2009

Announcing the first release of Bitcoin, a new electronic cash system that uses a peer-to-peer network to prevent double-spending. It's completely decentralized with no server or central authority.

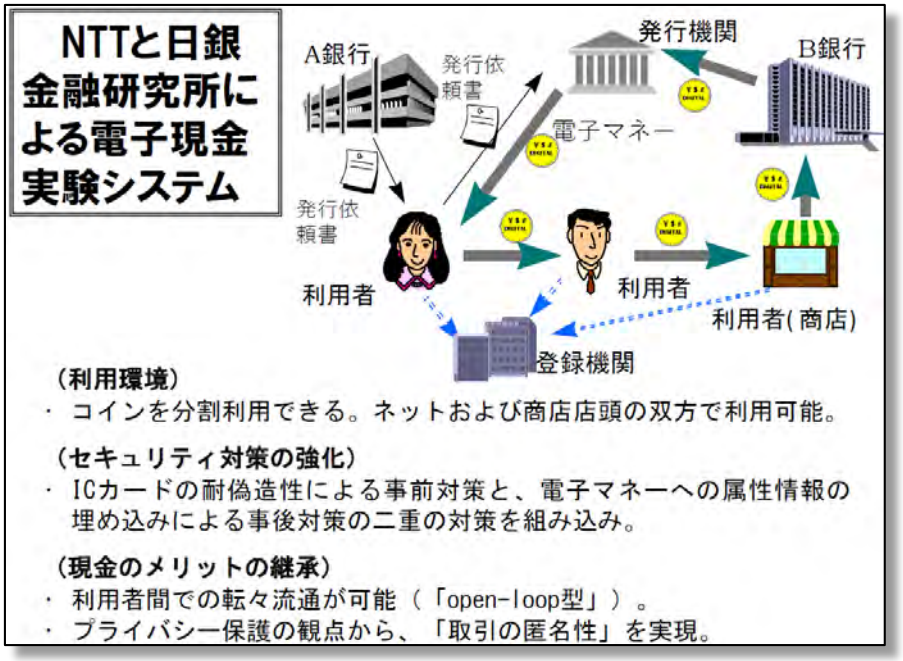
See bitcoin.org for screenshots.

Download link:
http://downloads.sourceforge.net/bitcoin/bitcoin-0.1.0.rar

Satoshi Nakamoto
が誰なのかは、
今日に至るまで不明

電子なお金は以前もあったし他にもある

- 例：NTT & 日銀 金融研究所, 1996年



岩下直行氏 (日銀 → 京大) のスライド

- Suica / スイカなんかすごい。
  - 8,200万枚 (2020/3), 200ミリ秒 (要求仕様), 平均 280件/秒 (2012年頃)
  - 集中的な仕組みでこの性能を出すために、様々に工夫

Bitcoin の非集中 分散システム

- インターネット上に約 1万ノード (サーバ)
  - インターネット側からは通信できないノードを含めると、数万

GLOBAL BITCOIN NODES DISTRIBUTION

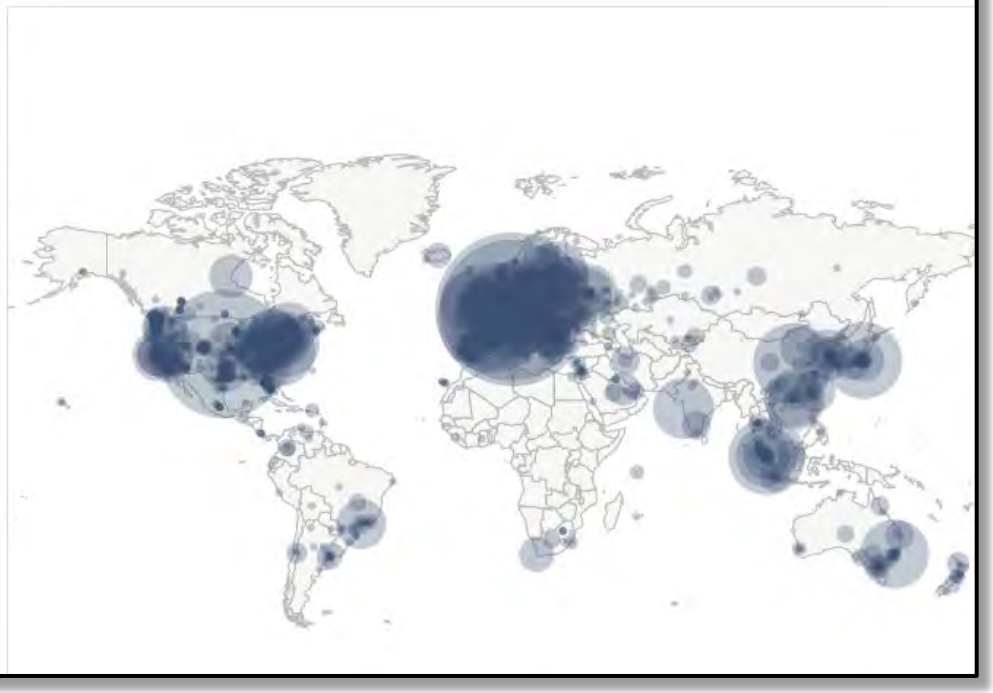
Reachable nodes as of Tue Dec 15 2020 20:04:29 GMT+0900 (日本標準時).

11329 NODES

24-hour charts »

Top 10 countries with their respective number of reachable nodes are as follow.

RANK	COUNTRY	NODES
1	n/a	2859 (25.24%)
2	United States	1924 (16.98%)
3	Germany	1755 (15.49%)
4	France	567 (5.00%)
5	Netherlands	460 (4.06%)
6	Canada	349 (3.08%)
7	United Kingdom	327 (2.89%)
8	Singapore	256 (2.26%)
9	Japan	221 (1.95%)
10	Russian Federation	219 (1.93%)



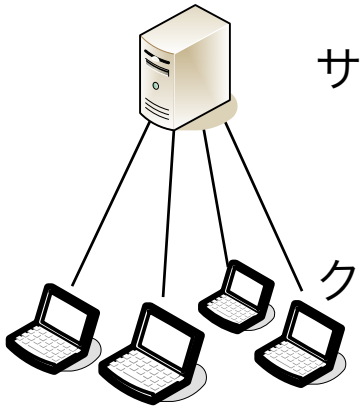
http://bitnodes.earn.com/ より

- 非集中

トラストレス / trustless

- 非集中 / decentralized

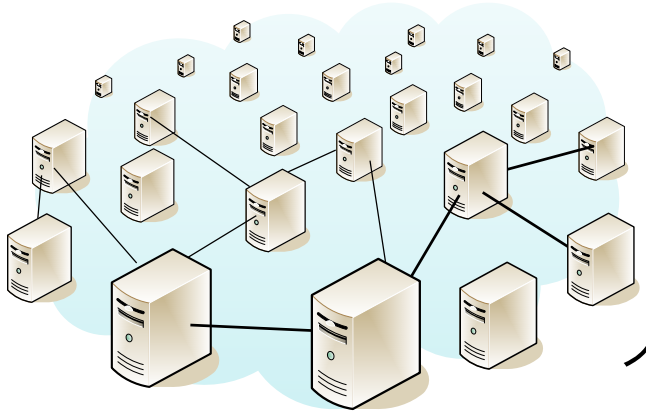
- 誰かを信用する必要がない → 「**trustless**」
  トラストレス
  - 政府, 銀行, 企業, … 等を信用する必要がない。
  - 実際は、ノードのうち例えば 2/3 は悪意のないノード (運用者) である必要がある。



サーバ

クライアント

集中的な 分散システム



ピア / peer
ノード / node

非集中 分散システム (peer-to-peer)

ブロックチェーン

- 暗号通貨 Bitcoin が提供した価値
  - 非集中 (→ トラストレス) に
  - 二重使用を防止
    - 整合性 を保つ
    - 改ざん困難性
- … これは、通貨に限らず他に応用できるのでは？

ブロックチェーン または
Distributed Ledger Technology (**DLT**) / 分散台帳技術

「ブロックチェーン」は特定のデータ構造を指す語なので、
それを嫌って、DLT と呼ぶ人も多い。

ブロックチェーンの価値

- 非集中
  decentralized
  派生 → **トラストレス**
  trustless
  派生 → **耐故障性**
  fault tolerant
  非集中に加えて
  ・複製
  ・悪意あるノードに耐えるトランザクション承認方式

二重使用の防止

- **整合性** を保つ
  consistent
  派生 → **トレーサビリティ**
  traceability
  整合性確認のために
  (全) 履歴を残すので
- **改ざん困難性**
  unalterable, tamper proof, …

ブロックチェーンの分類

permissionless Blockchain ⇔ permissioned blockchain

- パブリック ブロックチェーン　～ 数万台
  - Bitcoin, Ethereum 等
  - **誰でも**ノード (サーバ) を立てられる
    - 異なる定義もある：誰でも台帳の読み（書き）ができる

- プライベート ブロックチェーン　数台 ～ 数十台
  - **組織内で**運用
  - 専用のソフト (例: HyperLedger ○○) や Ethereum をプライベート用の設定で用いる
  - トラストレスではないから意味ないよね、と揶揄される

- コンソーシアム ブロックチェーン
  - **組織をまたいで**運用　　例: 銀行間決済
  - 運用者達が結託しそうになければ、ある程度トラストレスか？

ブロックチェーンの
応用

- 通貨やトークン、追跡、自己主権型アイデンティティ、…
- 留意点

応用：通貨やトークン

- 国際送金
  - Bitcoin の初期の使われ方
    - 例：中国の富豪が米国留学中の子息に…
- 法定通貨の代替
  - 例：アルゼンチンの Dai
    - ステーブルコイン：ETH を経由して米ドルと同価値を保つ
    - 背景：年率 50% のハイパーインフレ, かつ米ドルへの両替規制

法定通貨等と価値が連動するコイン
Ethereum 上の通貨とその単位

- トークン (つまり コイン) エコノミー
  - 例：ALIS トークン
    - 記事、執筆者、紹介者の信頼スコアがトークン獲得につながる
    - トークン獲得という動機づけ。Bitcoin 等の暗号通貨と同じ。
    - Ethereum ネットワーク上で運用 → パブリック

応用：
いろいろ

- ブロックチェーンの価値 (p.10) を活用
- 事例は、探せば山ほど見つかります。

ブロックチェーンのメリット	情報を共有しても改ざんされない	価値流通の仕組みを簡単に作れる	価値のトレーサビリティを担保できる
情報システム基盤としての利用	①学歴情報の管理（MIT） ・貿易保険（東京海上日動）	・貿易金融（オリックス、NTTデータ等多数） ②ペイメント間の送金（アリババ） ・証券取引（東京証券取引所）	・食品トレーサビリテ（ウォルマート） ・サプライチェーン管理（IBM） ③ダイヤモンド来歴管理（Everledger）
新しい社会システムの提案	・不動産取引・登記（スウェーデン） ④公的情報管理（エストニア政府）	⑤フェイクニュース対策（ALIS） ⑥広告（博報堂） ⑦IoTへの課金の組み込み（Earn.com） ⑧電力取引（デジタルグリッド）	⑨生活保護支給（英国政府） ⑩アート作品の来歴管理と利益分配（スタートバーン）

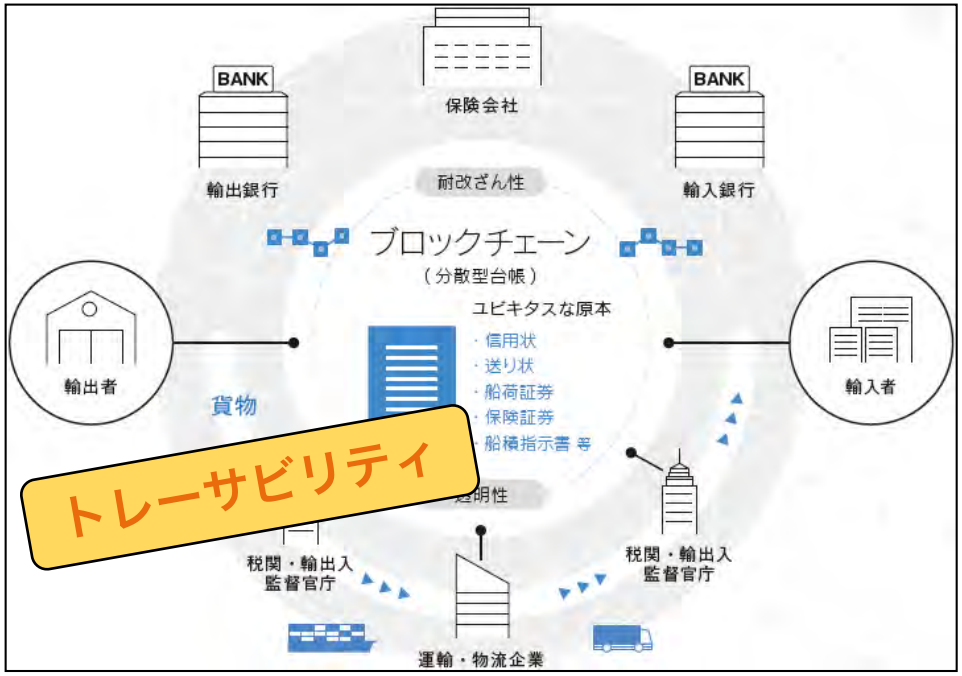
高木聡一郎氏 (東大 / GLOCOM) の資料

応用：
追跡 / trace

- IBM Food Trust
  - **食品**の来歴を追跡可能に

吉濱佐知子氏 (IBM Research - Tokyo) の資料

- TradeWaltz (NTT データ他)
  - **貨物**を追跡可能に

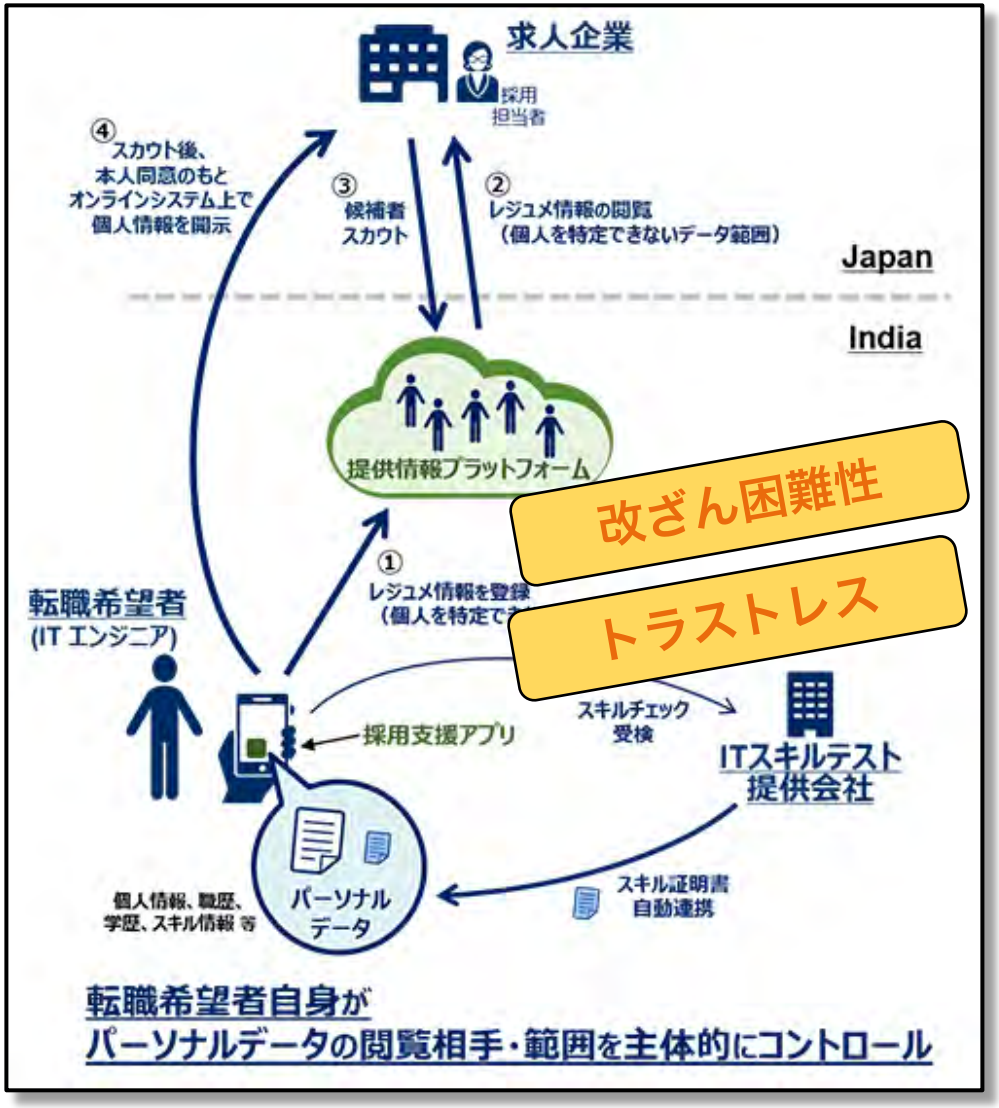


トレードワルツ社 資料

- デジタル化の恩恵 +
  ブロックチェーンの恩恵：改ざん困難・トラストレス …

self-sovereign identity / 自己主権型アイデンティティ

- 人材採用での実験
  - 転職希望者の情報が、企業に提供される



報道発表：

パーソルキャリアとNEC、ブロックチェーン技術を用い、外国人ITエンジニア向け人材採用サービスの実証実験を開始 (2020/8/13)

応用の際の留意点

- ブロックチェーンの価値 (p.10) が必要か？
  - 通常の DBMS, NoSQL の方が優れている：性能, 容量, …
- プライベート ブロックチェーン では、多くの価値が失われる：トラストレス, 改ざん困難性, …
  - 実験ではプライベートでも、運用時はコンソーシアム以上を見据える。
- データそれ自体をブロックチェーンに載せる必要はない
  - 他の DBMS との組み合わせも検討する。
    - データのハッシュ値だけブロックチェーンに載せる、等。

ブロックチェーンの
技術

- トランザクション承認方式
- ブロック生成

トランザクション承認方式

トランザクション (取引情報) をどうやって確定させていくか？

- Bitcoin：Proof of Work (PoW)
- HyperLedger Fabric：特定のサーバが順序付け

↑ トラストレスの度合いが低い？

トランザクション承認方式

不特定 & 多数のノード群で承認

Proof of Work, Stake, …

DAG 向けの方式：
Tangle (暗号通貨 IOTA)
Byteball

特定のノード (群) で承認

単一ノードが交代で承認
‖
Proof of Authority

Clique (in Ethereum)
Aura (in Parity)
Grid Ledger System
by アーリーワークス社

複数ノード群で承認
‖
Consensus algorithm /
分散合意アルゴリズム

Byzantine fault tolerance /
ビザンチン障害耐性 (BFT)
あり PBFT Ripple (悪意ノード 20%まで)
Istanbul BFT (IBFT)
LibraBFT (based on HotStuff)

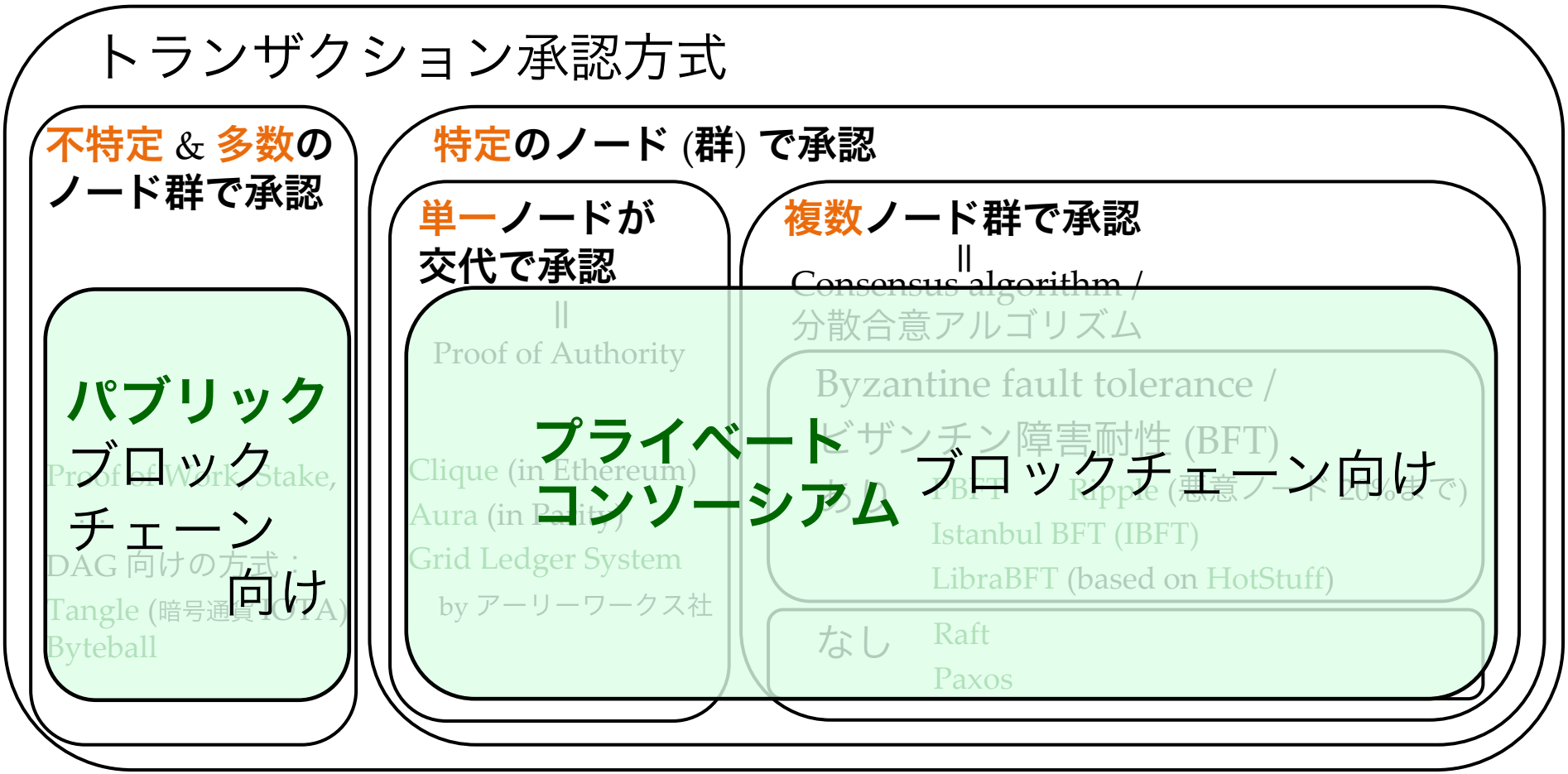
なし Raft
Paxos

トランザクション承認方式

トランザクション (取引情報) をどうやって確定させていくか？

- Bitcoin：Proof of Work (PoW)
- HyperLedger Fabric：特定のサーバが順序付け

↑ トラストレスの度合いが低い？



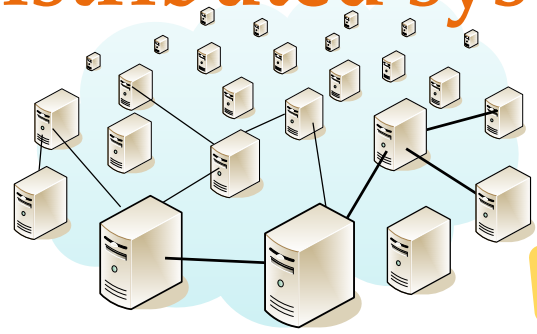
ブロックチェーンを支える技術

- ブロックチェーン
  - 誰かを信用することなしに (トラストレス)
    データを不整合なく確定させていく仕組み
    例：二重使用
- 支える技術：

暗号理論 / cryptography

公開鍵暗号方式, 署名,
(暗号学的) ハッシュ関数,
乱数生成方式, …

分散システム / distributed systems

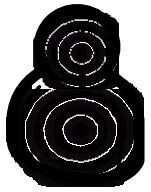


peer-to-peer ネットワーク,
flooding, 複製, 整合性,
分散合意アルゴリズム, …

首藤の専門

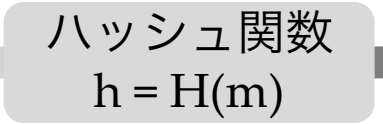
ブロックチェーンを支える技術
暗号理論

- 公開鍵暗号方式、署名
  - 1人が 2つの鍵を持つ：秘密鍵と公開鍵。
    一方で暗号化、もう一方で復号。
  - 秘密鍵で署名。公開鍵で検証。なりすましを防げる。
  - 一方向性関数に基づいて構成する。
    例：大きな整数の乗算は容易、因数分解は大変 → RSA 暗号 (1977)


ユーザ

- (暗号学的) ハッシュ関数
  - データごとの固有の数値 ＝ ハッシュ値 (128 ～ 512ビット) を算出できる。
    データの指紋を採れるようなもの。
  - ハッシュ値を与えられても、データの側は作り出せない。一方向。
  - 署名 (上記) の際、データ自体ではなく、ハッシュ値に対して署名する。

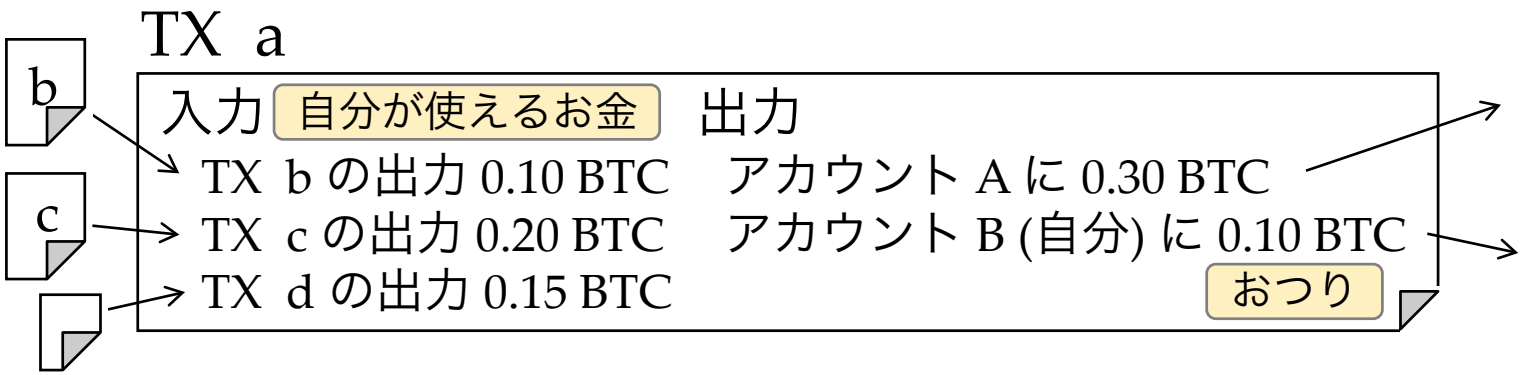

データ m



11010001…
ハッシュ値 h

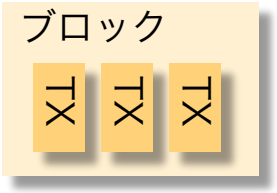
ブロックチェーンのデータ構造

- トランザクション (TX と略記)　　お金の動き



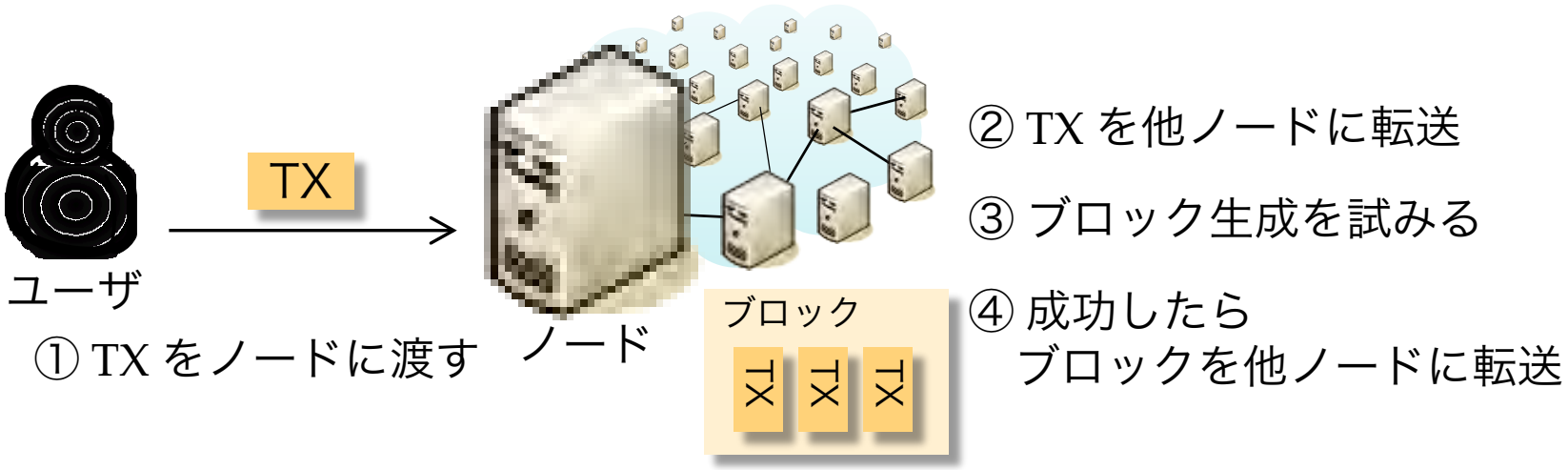
  - 自分に使用の権限があることや、確かに自分が発行した TX であることは、署名 (前項) で示す。
  - TX を矛盾 (二重使用) なく連鎖させていく。

- ブロック



  - TX をたくさんまとめたもの。
  - ブロックを生成 (= 確定) することで、TX を確定させる。

ブロックチェーンの動作

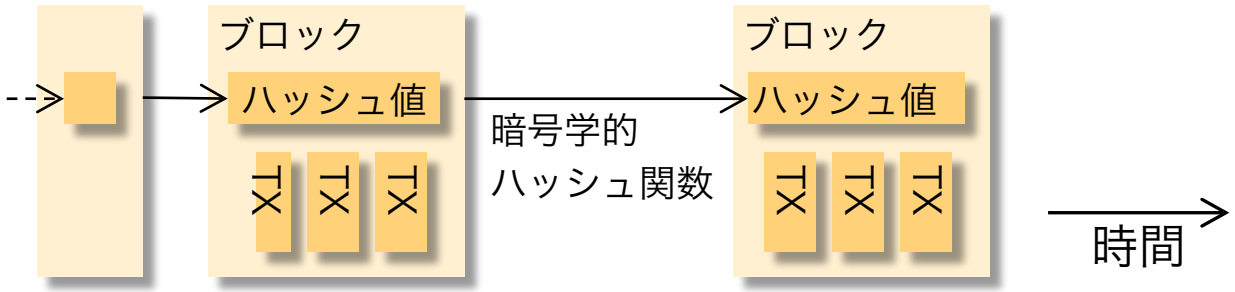


- ① ユーザが TX をノードに渡す。
- ノード群は
  - ② 受け取った TX を他ノードに転送する。
  - ③ TX 群をブロックにまとめて、ブロック生成を試みる。
    計算競争 = Proof of Work (PoW) に勝つと生成できる。
    ④ ブロック生成に成功したら、他ノードに転送する。

後述

ブロックの連鎖

- ブロックをハッシュ値で連鎖させていく
  → ブロックのハッシュチェーン
  → ブロックチェーン



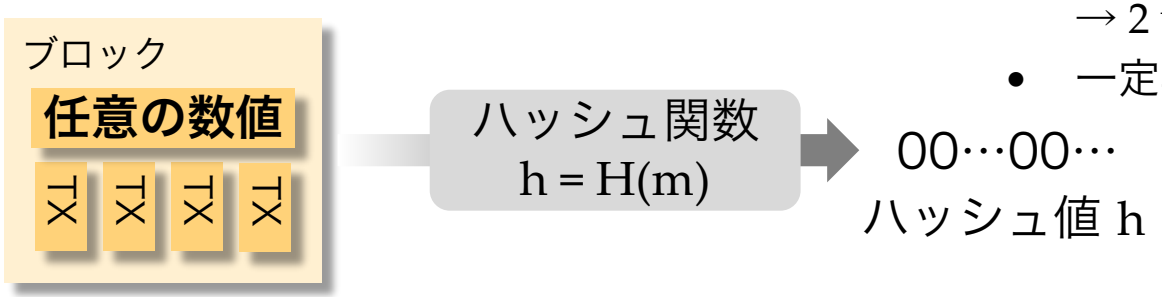
  - 各ノードは最新ブロックの次を生成しようとする。
    生成は容易ではない (次項：計算競争)。
  - TX を改ざんするには、
    後続ブロックすべてを作り直さねばならない。
    しかし、作り直しはほとんど不可能 (次項：計算競争)。
    → 改ざん困難

ブロック生成の計算競争

- Proof of Work (PoW)
  - 全ノードが頑張って計算して、
    10分に 1回 (← Bitcoin の場合) 成功するような計算問題

計算問題：
先頭に 0 が n 個連なる　ハッシュ値を出せ

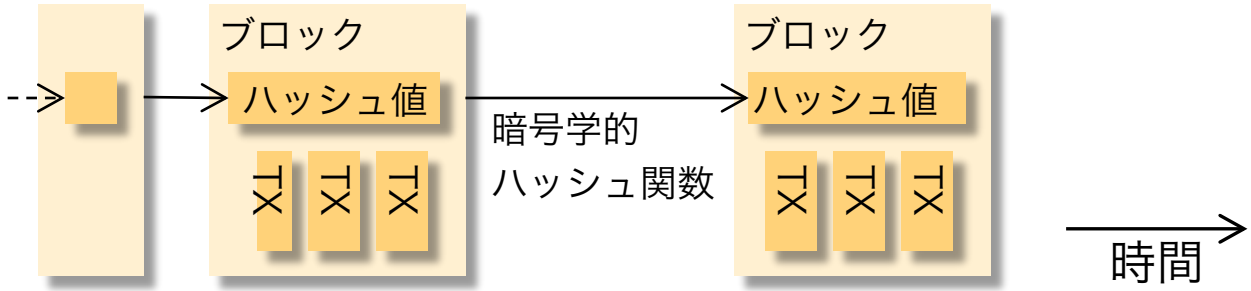
- ブロック中の、任意に決めてよい部分を変更して試しまくる
- ハッシュ値は乱数のようなもの
  → 2^n 回に 1回、成功する
- 一定期間ごとに難易度 n を調整する



  - 勝つと報酬 (BTC) を得られる。
    貴金属の採掘になぞらえてマイニングと呼ばれる。

改ざん困難性 と 二重使用防止

- 改ざん困難性
  - ブロックの連鎖 (2ページ前) と
    ブロック生成の計算競争 (1ページ前) に基づく



  - TX を改ざんするには、後続ブロックすべてを作り直さねばならない。
  - 後続ブロックを 1つ作り直すためには、全ノードで 10分かかる計算をやり直す必要がある。
- 二重使用防止
  - 各ノードは、ブロック内の全 TX を検証する。
    矛盾ある TX を含むブロックを、ノード群は受け入れない。

ブロック生成競争の問題

- Proof of Work (PoW) = ブロック生成の計算競争
  - 通称、マイニング

専用チップを
山のように並べる

マイニング専用データセンタ
https://imgur.com/a/CcIhX より

- 原発 ○ 個分の消費電力
  - 電力を食わない仕組みが研究途上：Proof of Stake (PoS) 等

ブロックチェーンの
研究

- 性能
- ツール
- セキュリティ
- 公平性
- 分権化

首藤研での 研究

- 「**ツール**」「**性能**」の研究を踏まえ、「**セキュリティ**」の研究を開始
- パブリックブロックチェーンに強く期待されている「**分権化**」 (⇔ 集中)、および、社会を支える基盤として必要な「**公平性**」の研究に着手

セキュリティ
- selfish mining 攻撃への耐性評価 [Nagayama 2019]
- Erebus 攻撃対策の性能への影響 [高山 2020b]

相互に影響

性能 含 実時間性・スケールアウト性
- 伝搬時間 推定 [神田 2019a] [Kanda 2019b]
- 隣接ノード選択 [青木 2019c] [Aoki 2019d]
- プロトコルの効果推定 [永山 2020a] [Nagayama 2020b]
- リレーネットワークの影響推定 [大月 2020a] [Otsuki 2020b]

研究手段を提供

ツール
- シミュレータ SimBlock [青木 2019a] [Aoki 2019b] [Banno 2019] [Shudo 2019]

研究手段を提供

分権化 / decentralization [高山 2020a]
- 中央集権の度合い評価
- 新アーキテクチャ [Nagayama 2020a]

公平性 / fairness
- 指標と向上手法 [神田 2020a] [Kanda 2020b]

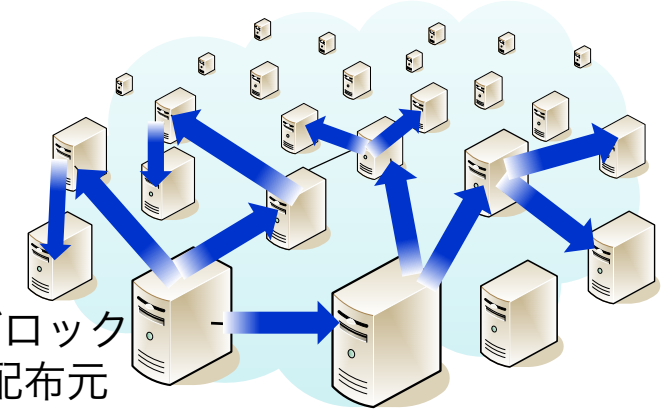
Ethereum 開発者会議 (Devcon 5) での発表 [Nagayama 2019]

ブロックチェーンの
研究

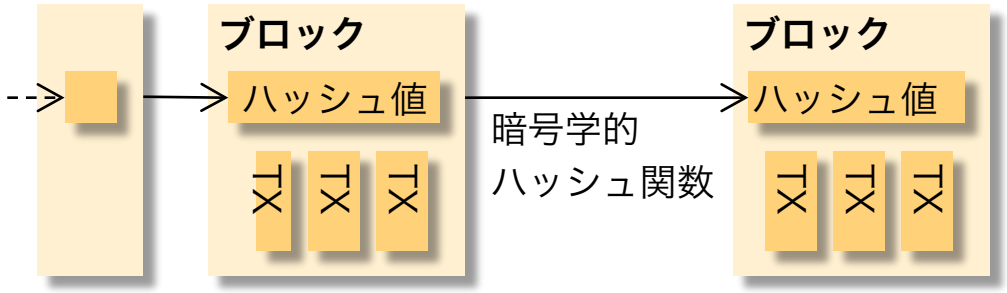
- 性能
- ツール
- セキュリティ
- 公平性
- 分権化

パブリック
ブロックチェーンの性能

- 性能：トランザクション (取引, TX) / 秒 = TPS
  - TX の例：Aさんから Bさんに 1 BTC 送金
  - 既存　　VISA (クレジットカード) 1,700 TPS, PayPal 平均 320 TPS
  - 暗号通貨　Bitcoin 7 → 27 TPS, Ethereum 15 TPS 前後　**圧倒的に不足**
- 性能向上には、ノード (サーバ) 間での
  データ伝搬の高速化が欠かせない。　理屈は次ページ



ノード (サーバ) のネットワーク

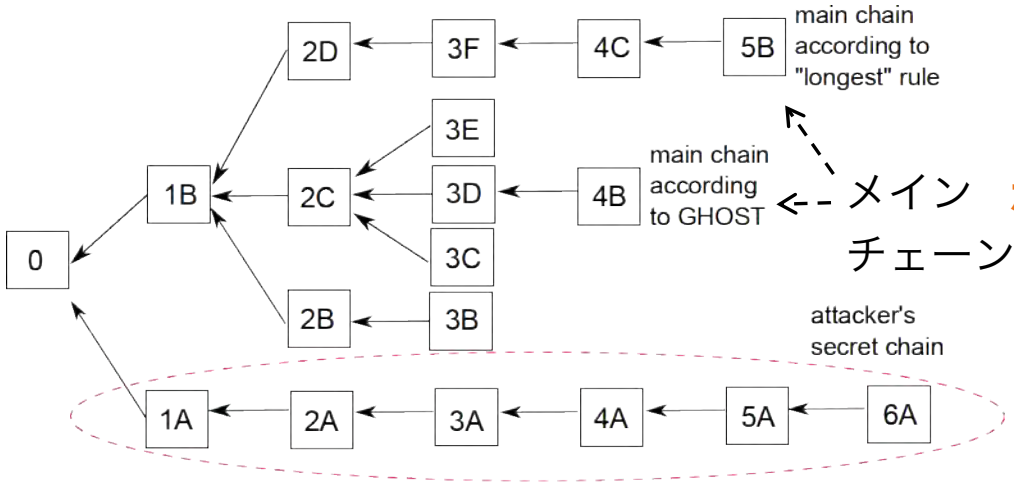


ブロックチェーンが用いるデータ構造

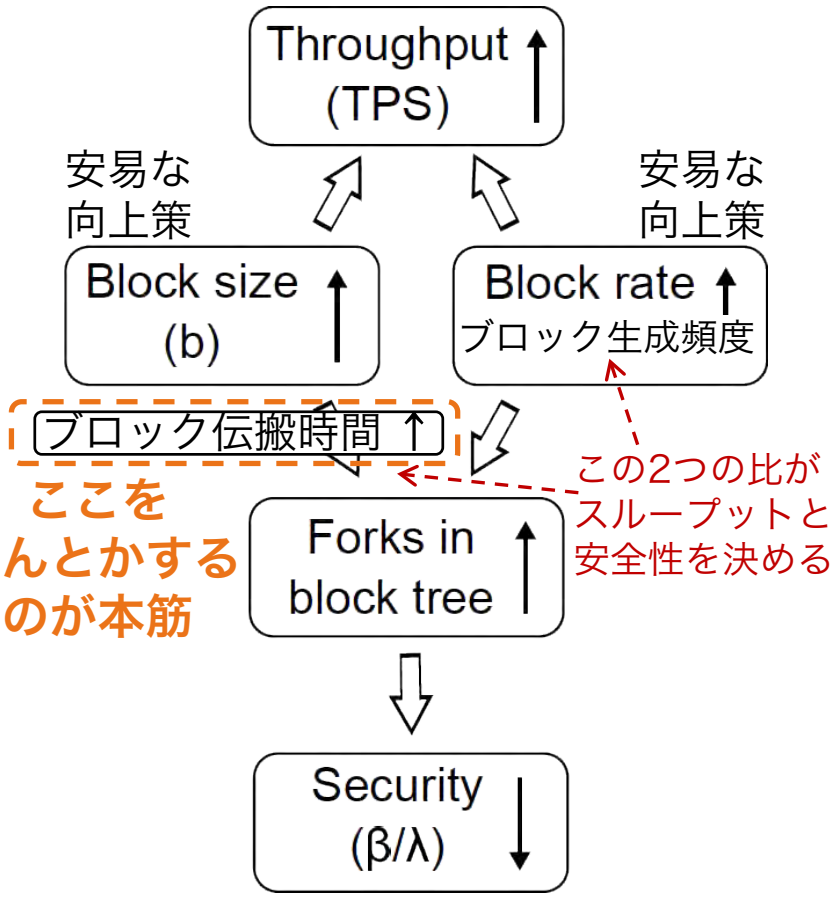
ノード間で、ブロックを伝搬させ、行き渡らせる

性能向上 vs. 安全性

- スループット(TPS)向上策が安全性の低下を招く
  - メインチェーン以外でのブロック生成が増えると、攻撃が容易に。
    例：51% 攻撃による TX 無効化
  - ブロックの生成頻度と伝搬時間の比
    ➡ フォーク発生率 ➡ 安全性 (右図)



フォークしたブロックチェーン

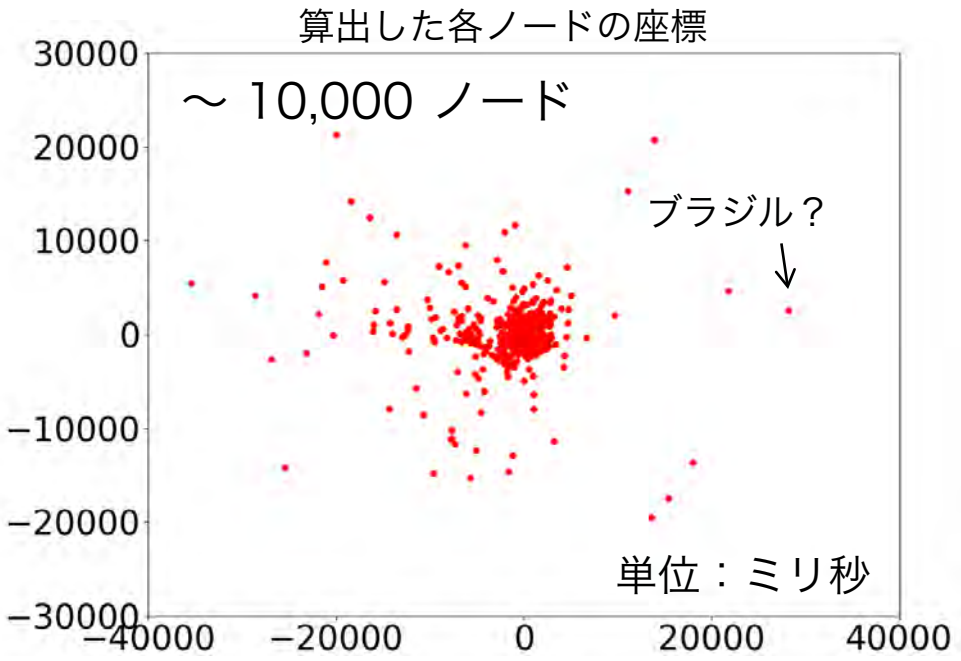


"Secure High-Rate Transaction Processing in Bitcoin", FC'15, 2015 の図

伝搬時間 推定 with ネットワーク座標系

[神田 2019a]
[Kanda 2019b]

- ネットワーク座標系 [Dabek 2004] [Chen 2007]
  - を適用して、ノード間伝搬時間を推定
  - n次元座標系＋バネモデルでの位置決め



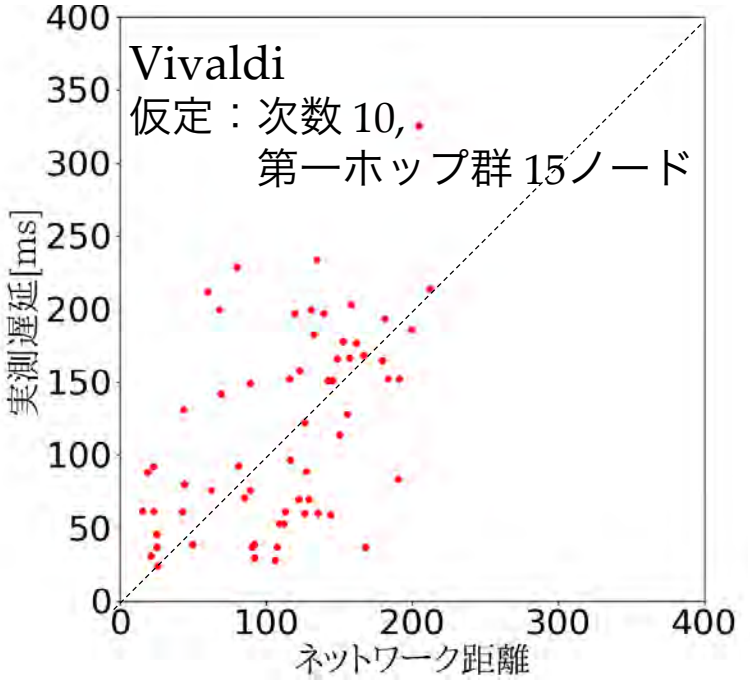
- 狙い
  - 伝搬高速化手法の指針
  - 隣接ノード選択の指針
- 現状と今後
  - 精度の向上
  - そのための
    トポロジ取得と推定

- ただ…

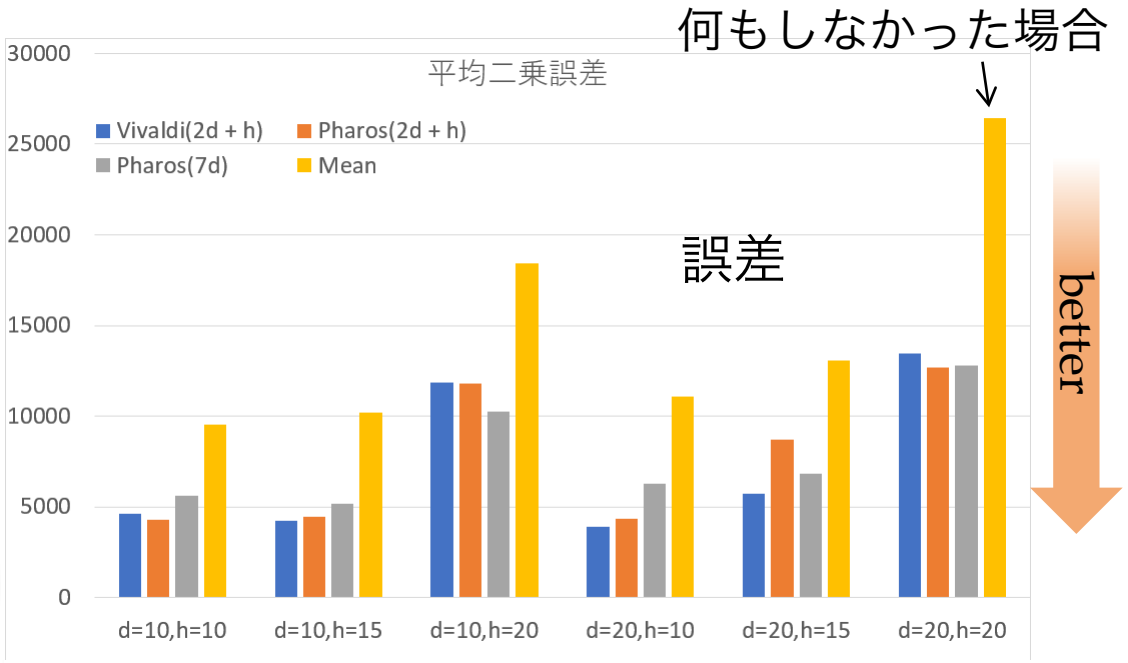
伝搬時間 推定 with ネットワーク座標系

[神田 2019a]
[Kanda 2019b]

- 精度は ほどほど



推定値と実測値が
あまり一致していない？



効果がまったくないわけでもない

- トポロジが不明なのが、ボトルネック
  - cf. “TxProbe: Discovering Bitcoin’s Network Topology …”, FC’19, 2019

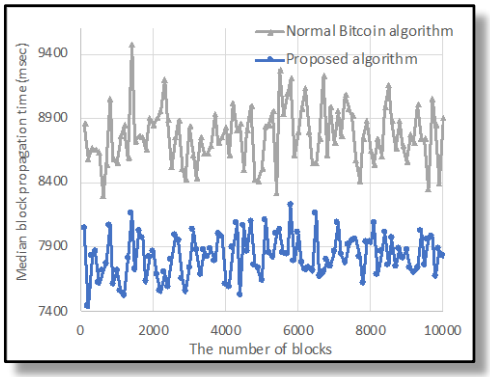
ブロックチェーンの
研究

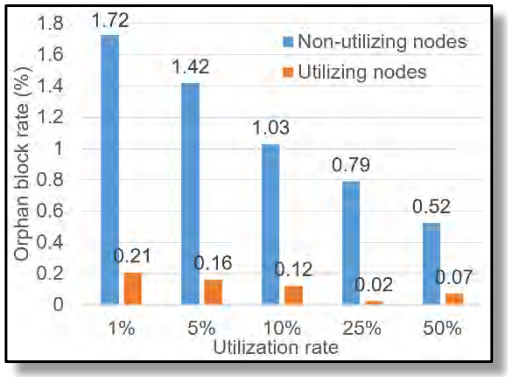
- 性能
- ツール
- セキュリティ
- 公平性
- 分権化

シミュレータ SimBlock

[青木 2019a] [Aoki 2019b] [Banno 2019] [Shudo 2019]

- ブロックチェーン「ネットワーク」のシミュレータ
  - 2019年 6月 27日(木) 公開・プレスリリース
  - ノード間でのブロック伝搬をシミュレート
    - インターネットの帯域幅・通信遅延：2015年, 2019年
      - 世界 6地域の、地域内 / 地域間 帯域幅と通信遅延
    - ブロックチェーンのノードの挙動：
      Proof of Work のマイニング所要時間, ブロックの転送, Compact Block Relay
      - Bitcoin, Litecoin, Dogecoin のパラメータ
  - 可視化ツール
  - 研究の例：

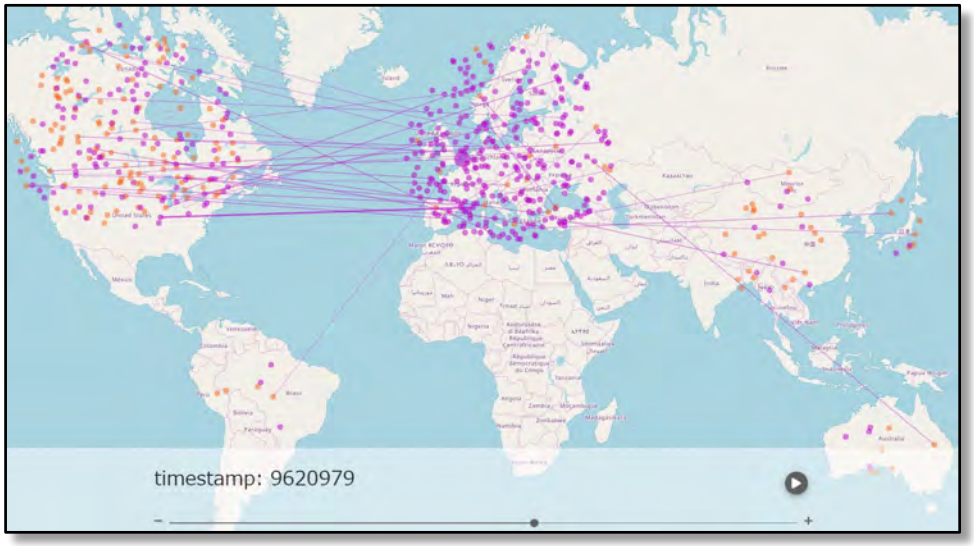




隣接ノード選択　リレーネットワーク 効果推定

シミュレータ SimBlock

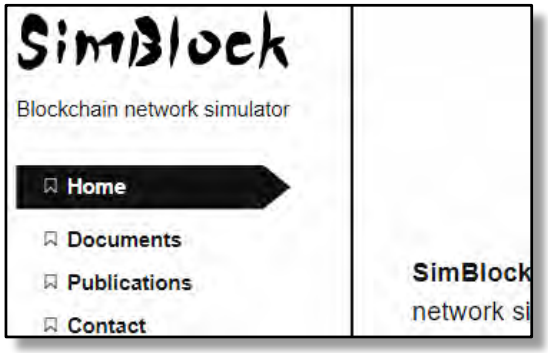
[青木 2019a] [Aoki 2019b] [Banno 2019] [Shudo 2019]

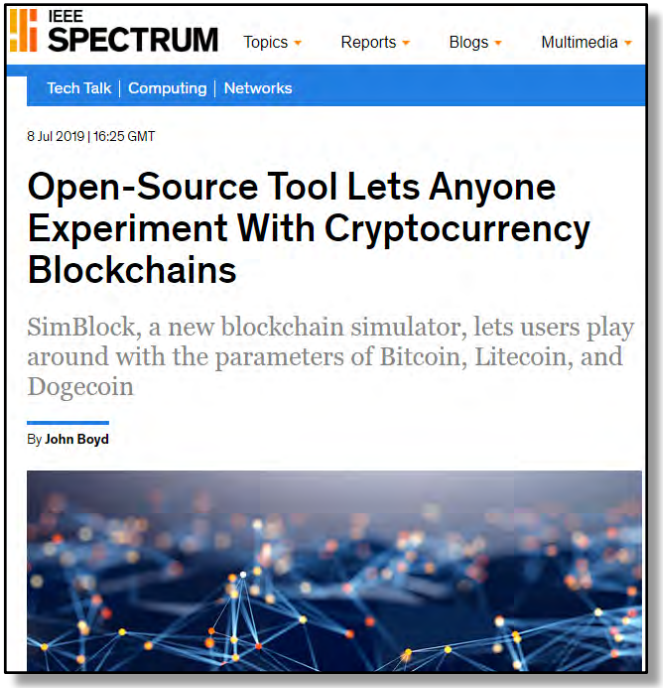


Visualizer

縮小 Bitcoin ネットワーク,
600 ノード

ウェブ
サイト





IEEE Spectrum
記事

IEEE ICBC 2019 デモ,
ソウル, 2019年 5月

ブロックチェーンの
研究

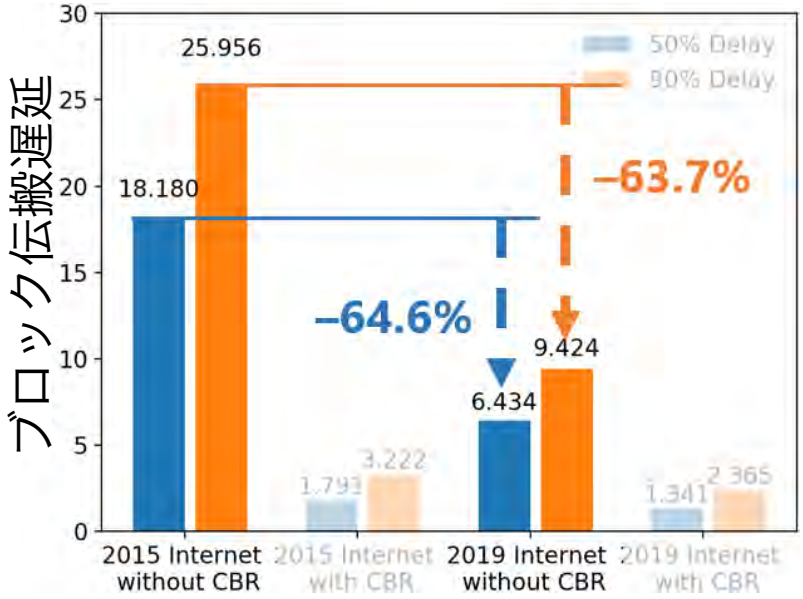
再び

- 性能
- ツール
- セキュリティ
- 公平性
- 分権化

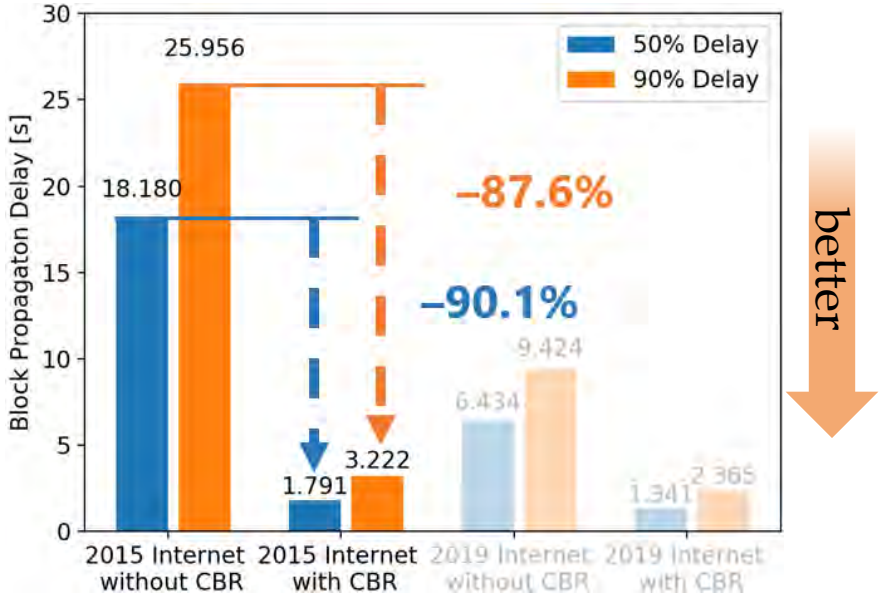
インターネット高速化と Compact Block Relay の影響

[永山 2020a]
[Nagayama 2020b]

- SimBlock を発展させたので、影響を調査
  - 2019年のインターネットの帯域幅・遅延
  - Bitcoin の Compact Block Relay プロトコル 2016年 8月の 0.13.0 が実装
    - ブロック伝搬の高効率化、ひいては高速化



<



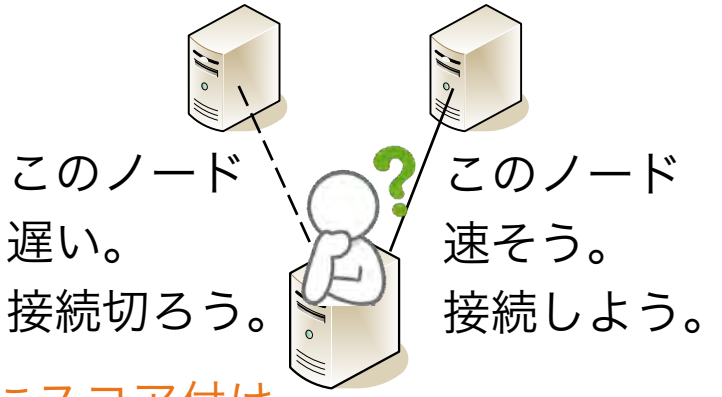
インターネット高速化 (2015→2019) の影響

Compact Block Relay の影響

隣接ノード選択

[青木 2019c] [Aoki 2019d]

- 速く通信できる相手と優先的につながる
  - peer-to-peer 分野でメジャーな手法
    - 僕らもやった：DHT での proximity neighbor selection [Miyao 2013]
- この研究のために、シミュレータ SimBlock を開発した

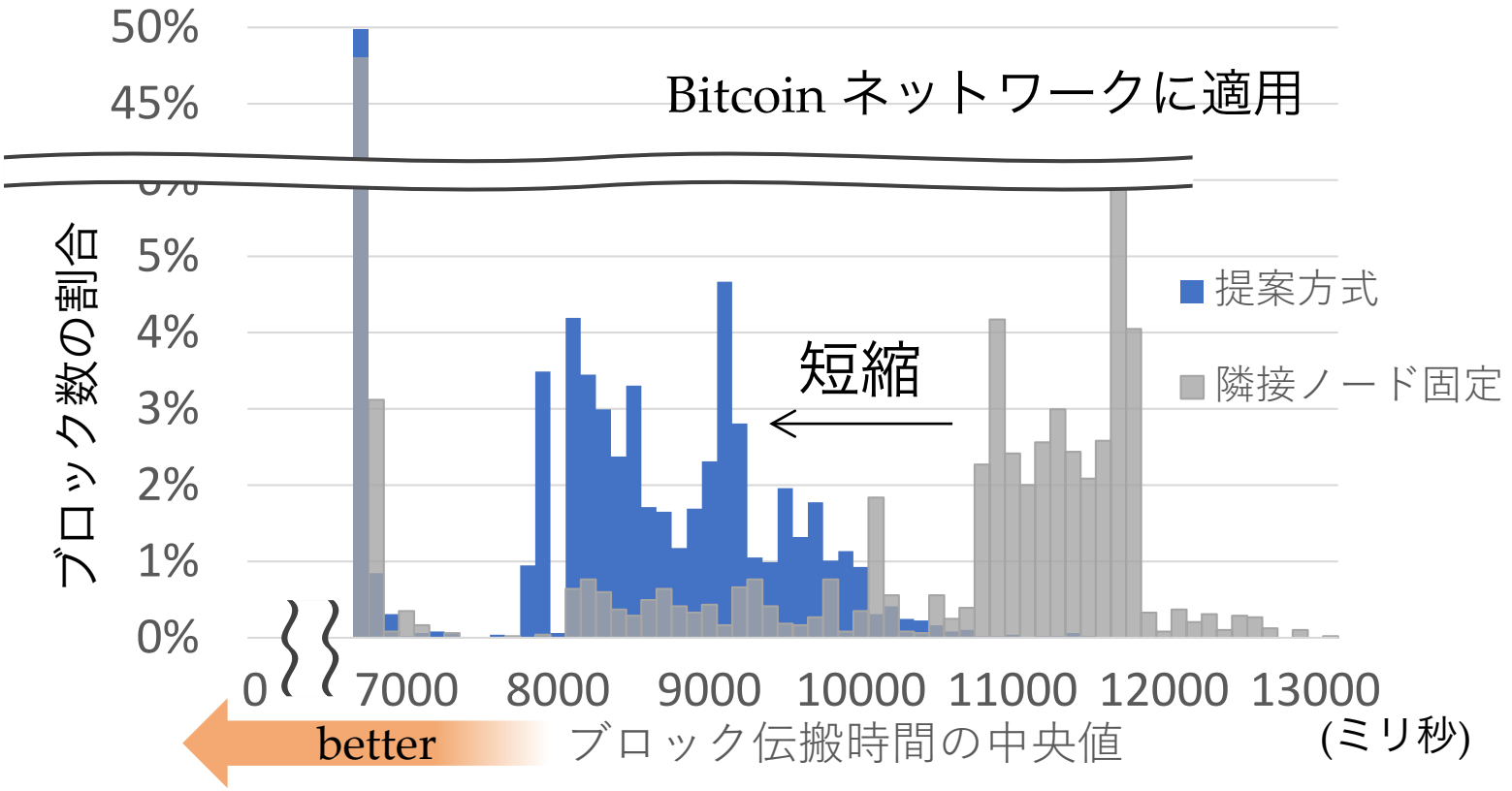


- 手法
  - ブロックを配信してくれた相手ノードすべてにスコア付け
    - スコア = (ブロック配信時刻 – 生成時刻) の指数重み付き平均値
  - 10 ブロック受信するごとに隣接ノードを選択し直す
    - ただし、新しいノードとつながるために、K ノードは知っているノード群からランダムに選ぶ
    - 予備実験の結果：K = 1, P (伝搬時間 最新値の重み) = 0.3

隣接ノード選択

[青木 2019c] [Aoki 2019d]

- そこそこ縮まった
  - 伝搬に時間がかかったブロック群で、11.5 秒 → 8.5 秒 くらい

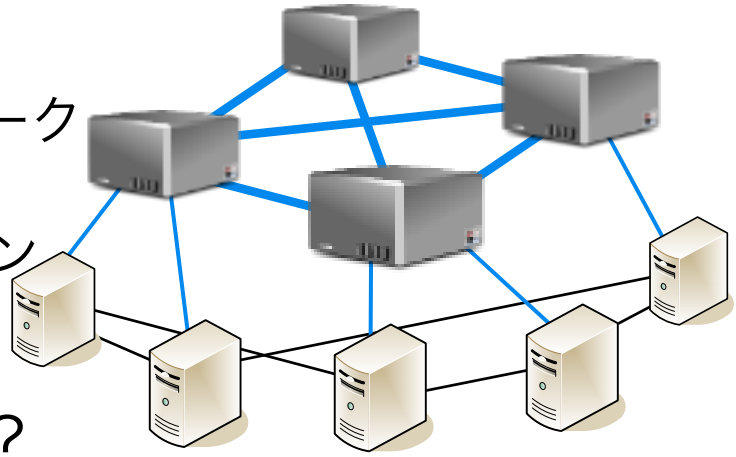


- 注：2015年のインターネットを対象として実験

リレーネットワーク 効果推定

[大月 2020a] [Otsuki 2020b]

- リレーネットワーク
  - ブロック高速配信ネットワーク
  - bloXroute (2018), FIBRE (2016), Falcon (2016), BFRN (2014), …
  - bloXroute: Falcon をやっていた Cornell U. の人達がビジネスとして開始



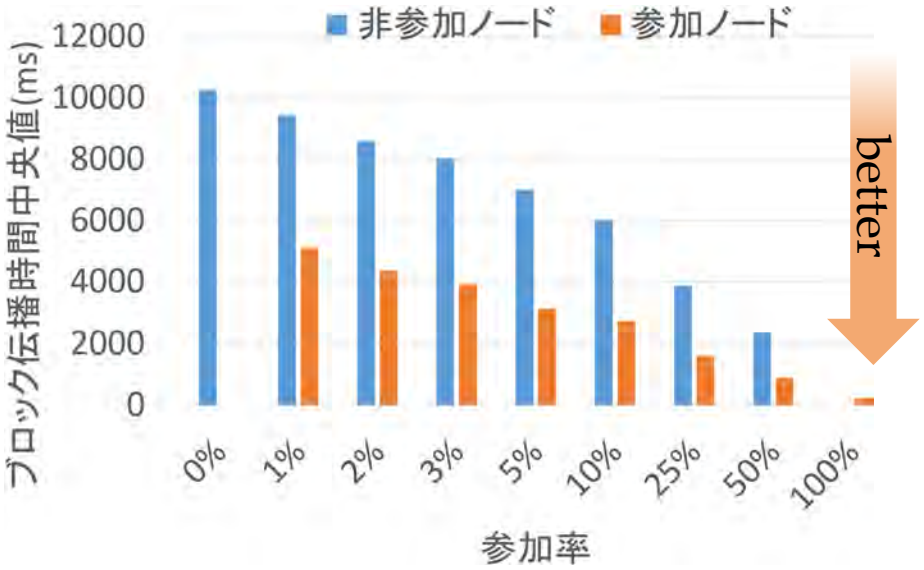
リレーネットワークの例: FALCON

- 効果は？
  - 孤立ブロックはどのくらい減る？
  - ブロックを早く受け取れるのだから、マイニング成功率が上がる？

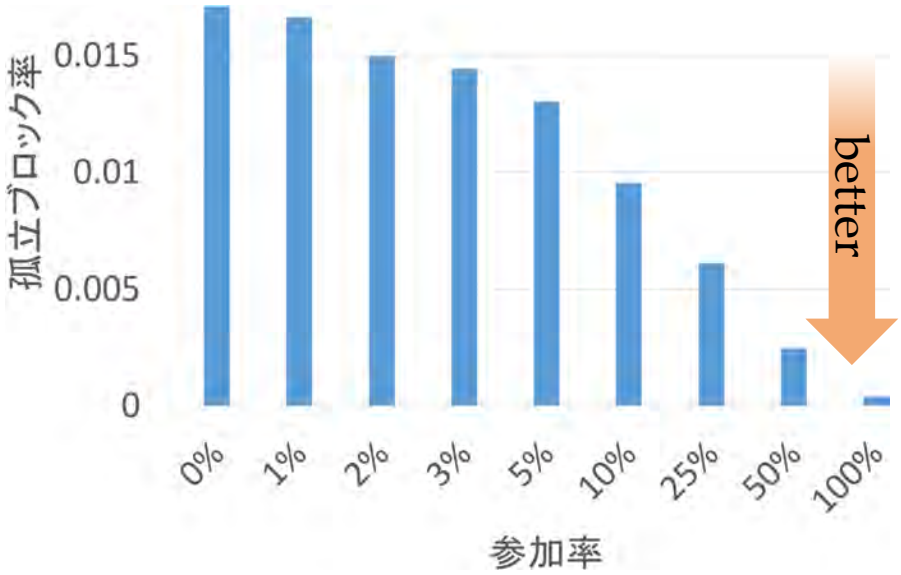
リレーネットワーク 効果推定

[大月 2020a] [Otsuki 2020b]

- SimBlock 上の Bitcoin ネットワークで実験
  シミュレータ
- ネットワーク レベル：



伝搬が速くなった！



孤立ブロックが減った！

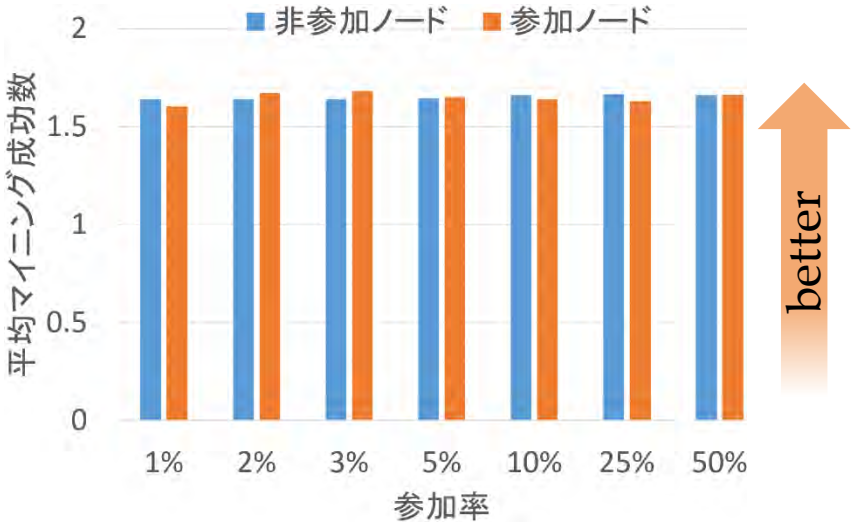
↑
フォークによって発生した、
メインチェーンから外れたブロック

- では、ノード レベルでは？

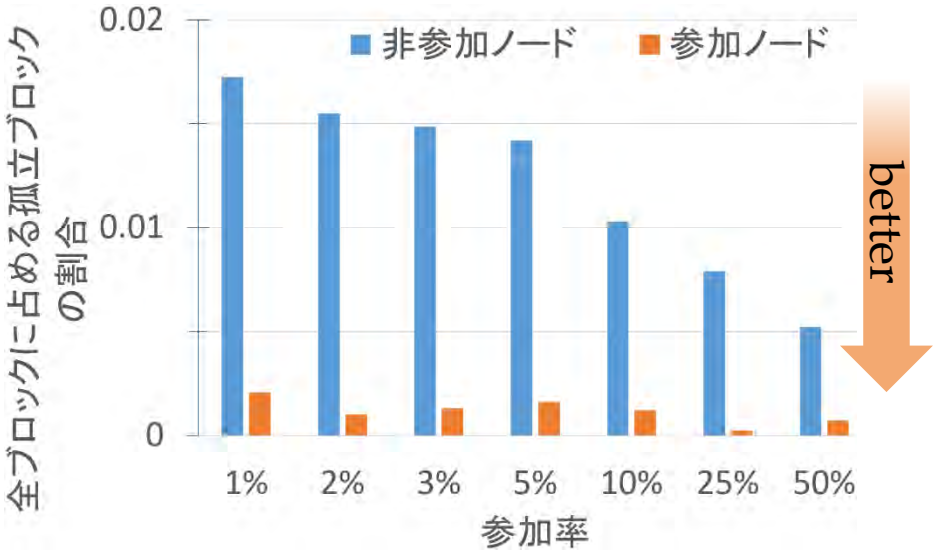
リレーネットワーク 効果推定

[大月 2020a] [Otsuki 2020b]

- ノード レベル：



マイニング成功率は
変わらないが…



生成したブロックが
孤立ブロックになって
しまう率が低下！

➡ マイニング報酬 増加

これがリレーネットワークの効能

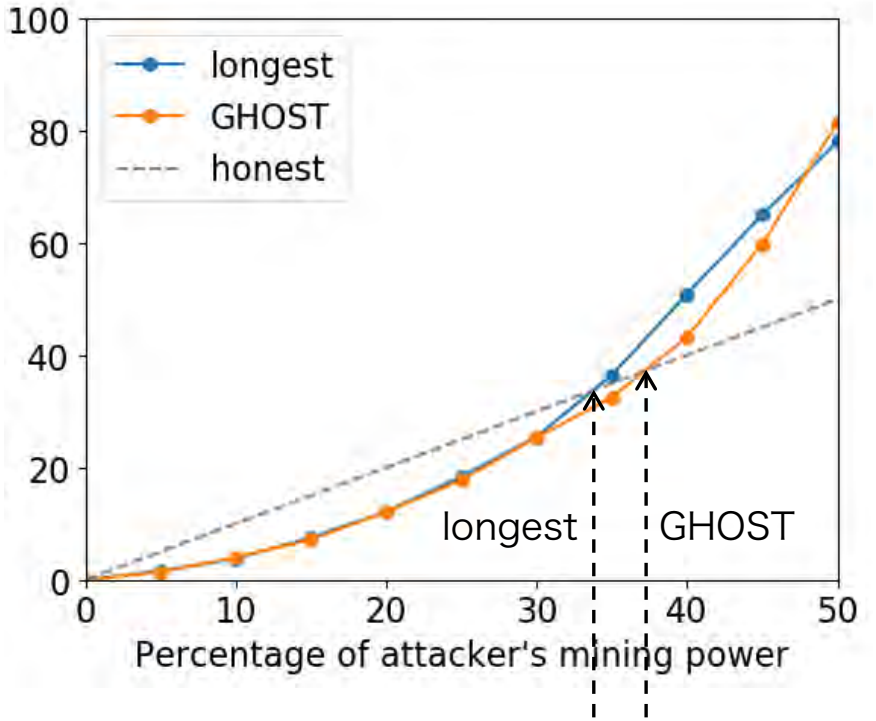
ブロックチェーンの
研究

- 性能
- ツール
- セキュリティ
- 公平性
- 分権化

selfish mining 攻撃を模擬

[Nagayama 2019]

- メインチェーンを決める規則 longest, GHOST の、攻撃への耐性を比較



攻撃で利得を得るために必要な
Proof of Work 計算能力 占有率

selfish mining 論文 (FC'13)
の値によく合致

シミュレート成功

Ethereum のシミュレート
という目論見への第一歩

→ 開発者会議 Devcon 5 で発表

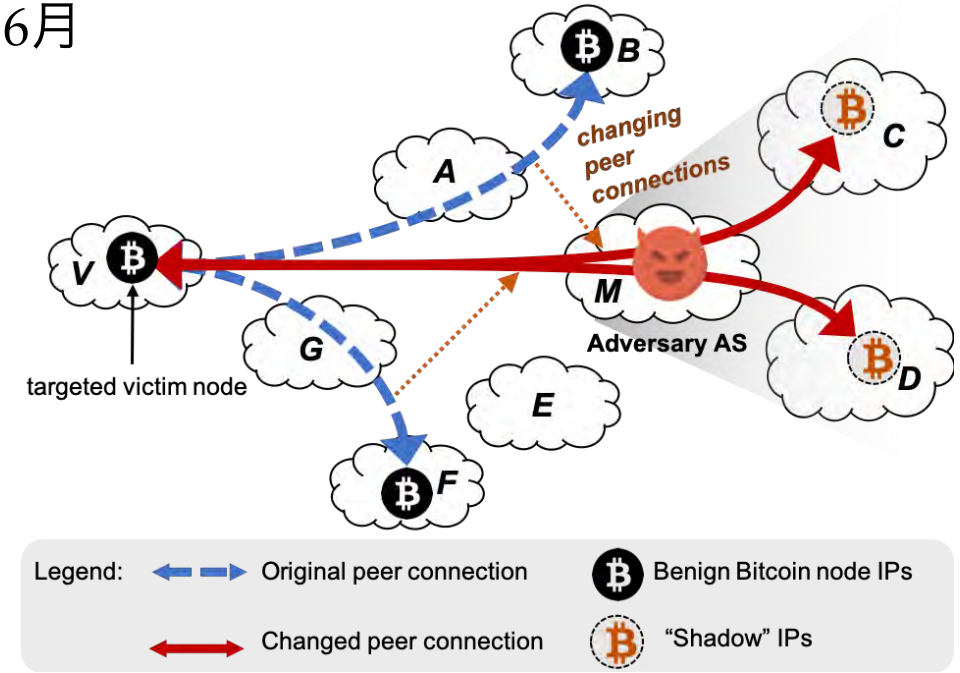
Devcon 5, 大阪,
2019年 10月

Erebus 攻撃対策の影響推定

[高山 2020b]

- Erebus 攻撃 (IEEE S&P 2020)
  - ネットワーク分割攻撃 → 様々な使いみち
  - AS を制御する攻撃者がノードを攻撃。
    対象ノードを攻撃者のノードに多く接続させる。
- 対策 in Bitcoin 0.20.0, 2020年 6月
  - ノードが学習する
    接続相手候補の数を
    AS ごとに制限。

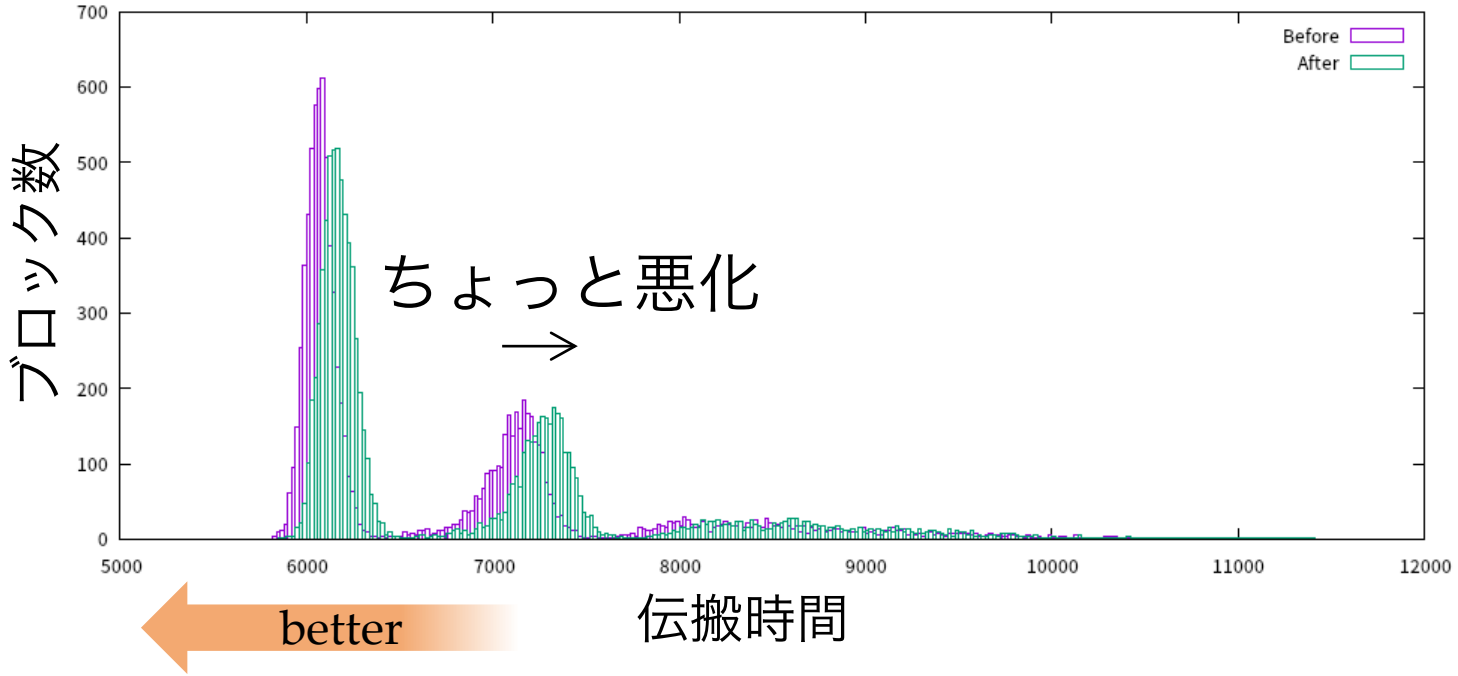
通信相手に、これまで
なかった制約が課せられ、
通信性能低下？



Erebus 攻撃対策の影響推定

[高山 2020b]

- ブロック伝搬時間、ちょっと悪化
  - 50%ile：3556 → 3562 ms (+ 6 ms)
  - 90%ile：6729 → 6846 ms (+ 117 ms)



- routing 攻撃をシミュレートできた

ブロックチェーンの
研究

- 性能
- ツール
- セキュリティ
- 公平性
- 分権化

ノード間の公平性指標とブロック生成間隔調整

[神田 2020a]
[Kanda 2020b]

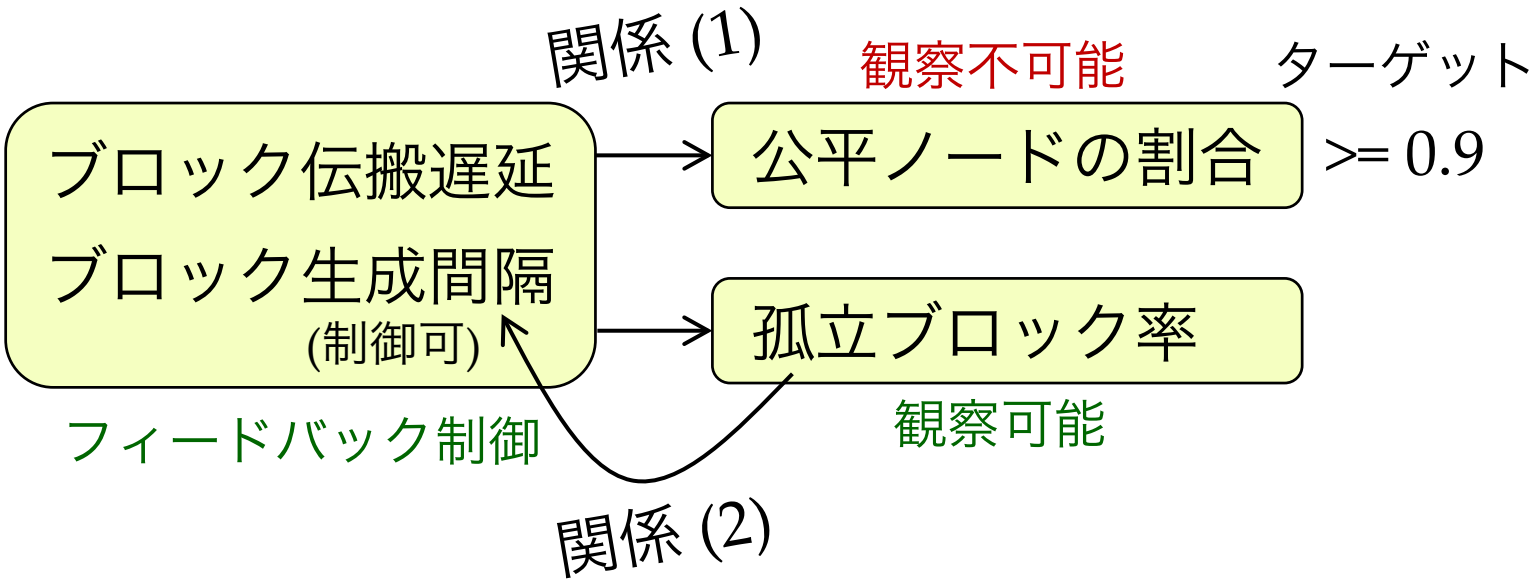
- 公平とは
  - マイニング成功率がハッシュレート (計算能力) に比例
  - …しかし、伝搬遅延によりブロックの受信が遅れると、その分、マイニングに費やせる時間が減る → 不公平
    - Ethereum なら、
      ブロック間隔 13秒前後 – 伝搬遅延が実質マイニング時間

- 既存の公平性 [Cromon 2016] ← 雑すぎる
  - 90% のノードが一瞬でもマイニングできれば公平
- 提案：**(X, ε) 公平性**
  - 充分長いブロックチェーンに対して、
    割合 X のノードが不公平を被る確率 ε 以下。
  - 今回、X = 0.9, ε = 0.01 。

ノード間の公平性指標とブロック生成間隔調整

[神田 2020a]
[Kanda 2020b]

- (0.9, 0.01) 公平性を保つブロック生成間隔調整法
  - 公平ノードの割合は事後にしか算出できない。
  - 代わりに、ブロック生成間隔を通じて**孤立ブロック率を制御**する。



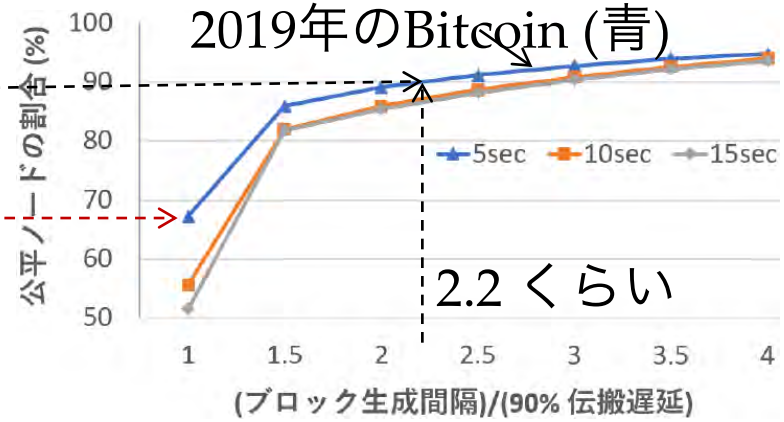
ノード間の公平性指標とブロック生成間隔調整

[神田 2020a]
[Kanda 2020b]

- 関係 (1)
  - ブロック伝搬遅延の分布はガンマ分布であると仮定し、Bitcoin での実測値を元に、公平ノードの割合を算出

狙い：
X = 0.9

既存の公平性



ブロック生成間隔 / 90%ile 伝搬遅延 が
2〜3 以上ならよさそう

- 関係 (2)
  - 孤立ブロック率は、ブロックの伝搬遅延と生成間隔の関数 [Decker 2013]

	$\frac{\text{ブロック生成間隔}}{\text{90\%伝搬遅延}} = 2$	$\frac{\text{ブロック生成間隔}}{\text{90\%伝搬遅延}} = 3$
5sec	14.6%	9.8%
10sec	14.2%	9.6%
15sec	14.1%	7.2%

孤立ブロック率
14.6% 〜 9.8% 以下を狙う

シミュレータ SimBlock 上で
制御の実験 → 成功

例：ネットワーク帯域幅が変化しても公平ノードの割合が高く保たれた

ブロックチェーンの
研究

- 性能
- ツール
- セキュリティ
- 公平性
- 分権化

Proof of Stake 各プロトコルの中央集権の度合い

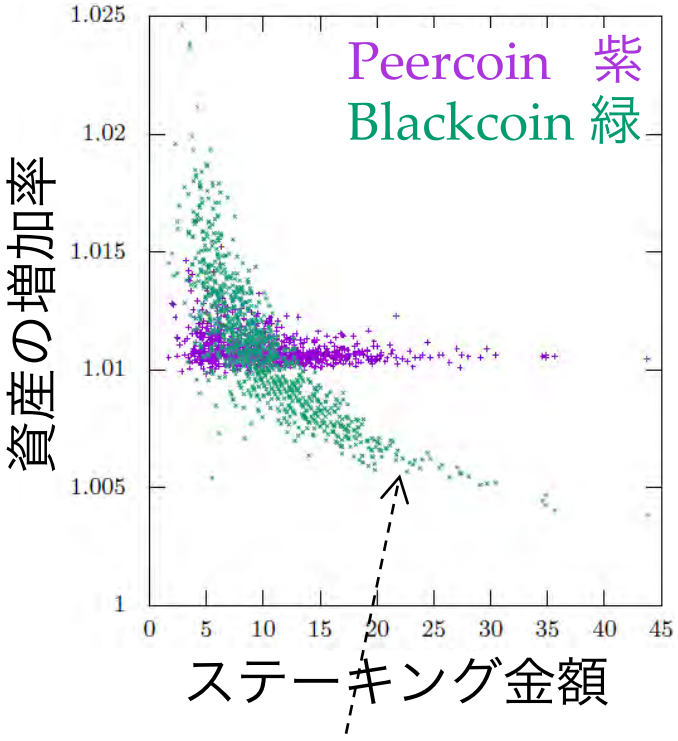
[高山 2020a]

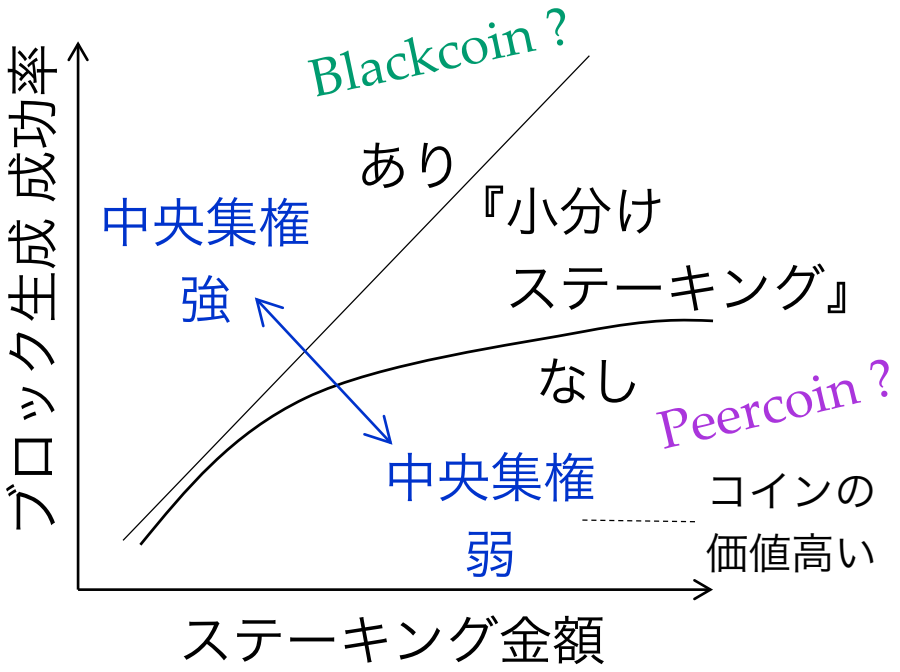
- Proof of Stake (PoS)
  - 各ノードは、持ち金 or deposit 金額に応じて、ブロック生成権を得られる
- プロトコルによって、
  中央集権の度合いがどう変わってくるか？
  - Peercoin [King 2012] – PoS を提案
    - 当選確率：コイン年齢 / coin age (= 金額 × **未使用期間**) に比例
      - 51% 攻撃を防ぐ、という主張：
        攻撃用にコインを買っても、コイン年齢が若くて役立たない。
    - 報酬：コイン年齢に比例
  - Blackcoin (2014年 〜) 1.2
    - 当選確率：単に金額に比例, ただし最低未使用期間はあり
      - コイン年齢の危険性を指摘：
        皆、オフラインのままコイン年齢を稼ぐ → 51% 攻撃の危険。
    - 報酬：固定額

Proof of Stake 各プロトコルの中央集権の度合い

[高山 2020a]

- 結論：Blackcoin 1.2 > Peercoin
  - 『小分けス(略)』Peercoin はなし、Blackcoin 1.2 はあり、に落ち着くだろう。

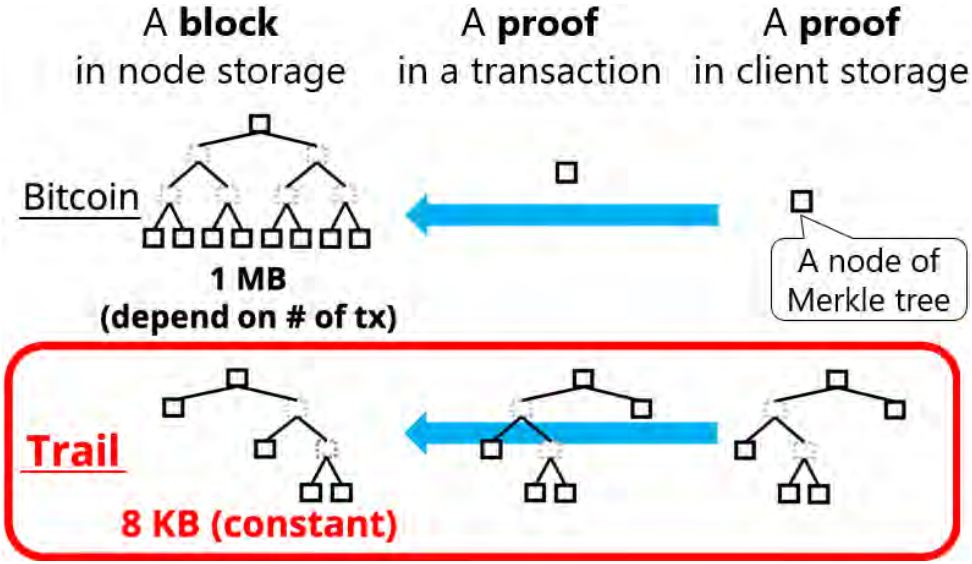




ステーキング金額が大きいと損。おかしい。
→『小分けステーキング』で改善できる

ノードの保持データ量が少ないブロックチェーン用データ構造

- 大きな台帳データがノード運営の負担で、分権化 / decentralization を妨げている。 [Nagayama 2020a]
  - Bitcoin 322 GB, Ethereum 195 GB (2021年 1月)
- 提案：
  - ノードの保持データ量が少ないデータ構造 Trail
  - 代わりに、クライアントが自己責任で TX を保存・バックアップ



ブロックチェーンの研究：まとめ

- 性能、ツール、セキュリティ、公平性、分権化、…の研究を紹介

- ネットワーク面からの性能の研究は、そろそろ…

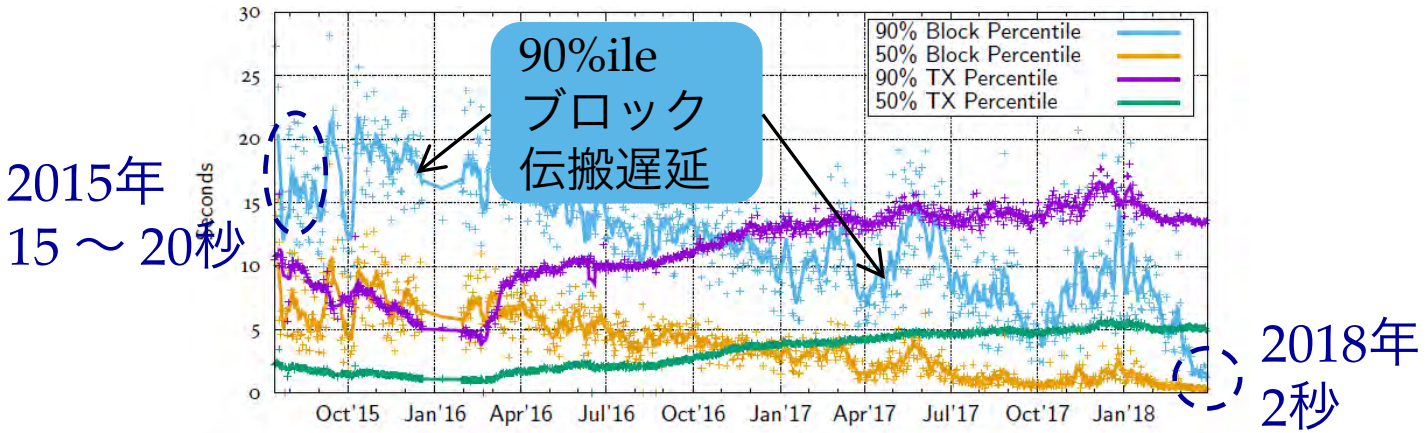


Figure 4.12: Bitcoin propagation delay for block and transaction propagation (50 % and 90 % percentiles). T. Neudecker: “Security and …”, Ph.D. thesis, 2018年

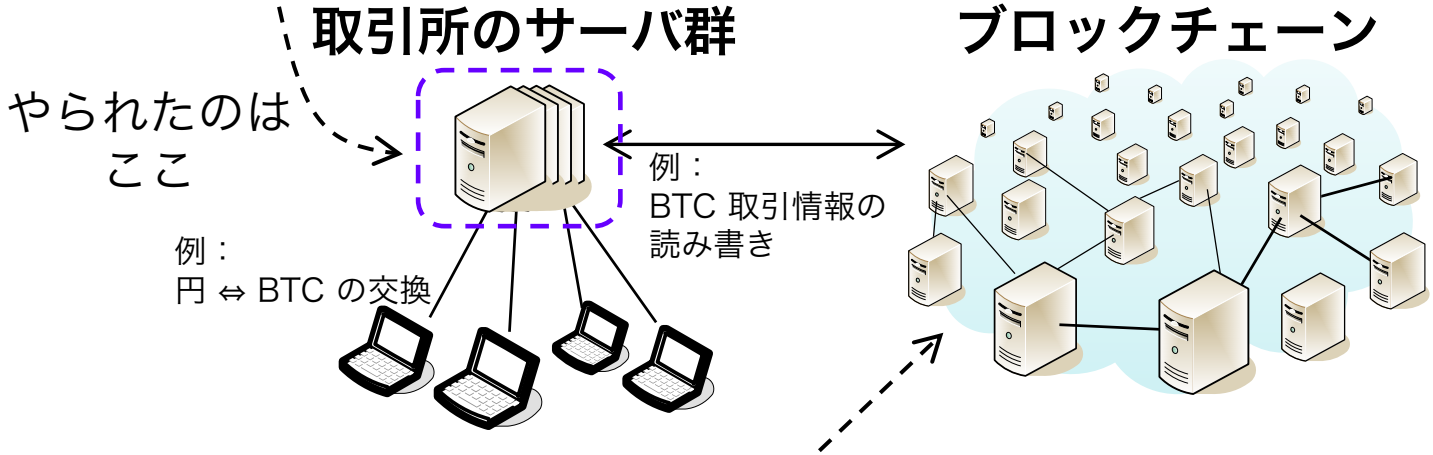
- 現在～今後：
  セキュリティ (攻撃手法と対策の考案と評価), Ethereum 2.0, 応用, …

ブロックチェーンと
社会

– 盗難事件, 通貨, Libra, DeFi と DAO, Web 3, …

暗号通貨の盗難事件

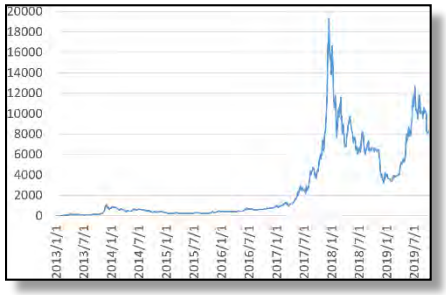
- 盗まれまくってる…
  - 2018年 1月 コインチェック社　　580億円
  - 2018年 9月 テックビューロ社 (Zaif)　70億円



- しかし、こちらをやられたケースもある
  - 2018年 5月 Bitcoin Gold　　20億円
  - 2018年 5月 MONA (モナコイン)　1,000万円
  - 2020年 8月 Ethereum Classic　　6億円
- 51% 攻撃は、金しだい： https://www.crypto51.app/
- インセンティブ不整合問題： https://bit.ly/32nvDbI

【通貨】 流通手段・支払い手段として機能している貨幣

- 暗号通貨で支払った / 受け取ったこと (→ 決済)、ありますか？ ビックカメラとか
  - コインチェック社の方だって、決済手段としての普及を目指してた。
- …
- 乱高下するので、決済に使いにくい。-->



BTC 価格の推移

- 解決案：ステーブルコイン / stablecoin
  - 米ドルや円といった法定通貨との交換レートを一定に保つ → 法定通貨 並みに安定
  - そう甘い話でもない。

    cf. https://blog.liquid.com/ja/insight/what-is-stablecoin-190510

    無担保型は、期待が下がって、調整のための資産を使い果たして破綻、があり得る

Libra / リブラ by Facebook 社

2019年 6月 18日(火) 発表

Libra 協会の
創設メンバ

- 世界統一通貨
- 大義は financial inclusion / 金融包摂
- こなれた設計
  - よくできた財布アプリ (ウォレット)：Calibra
  - ステーブルコイン
    - 通貨バスケット：US$ 50%, € 18%, 円 14%, ポンド 11%, SGD 7%
  - 当初、取引承認は協会メンバのサーバ群が行う。5年以内に、誰でも。
- **前途多難**
  - 各国の金融当局が強く警戒。
    - 金融政策が効かなくなる。
      cf. 「決済のイノベーションと中央銀行の役割」by 日銀 黒田総裁 (2019/12)
  - 予定されていた創設メンバが次々と離脱。
    - Visa, Mastercard, Stripe, eBay, PayPal, … → 大手 決済企業が不在に

Libra / リブラ by Facebook 社

2020年 4月 16日(木) White Paper v2.0

- 世界統一通貨 → まず単一通貨から
- 大義は financial inclusion / 金融包摂
- こなれた設計
  - よくできた財布アプリ (ウォレット)：Calibra
  - ステーブルコイン
    - 通貨バスケット：US$ 50%, € 18%, 円 14%, ポンド 11%, SGD 7%
  - 当初、取引承認は協会メンバのサーバ群が行う。5年以内に、誰でも。
- **前途多難**
  - 各国の金融当局が強く警戒。
    - 金融政策が効かなくなる。
      cf. 「決済のイノベーションと中央銀行の役割」by 日銀 黒田総裁 (2019/12)
  - 予定されていた創設メンバが次々と離脱。
    - Visa, Mastercard, Stripe, eBay, PayPal, … → 大手 決済企業が不在に

Libra 協会の
創設メンバ

見合わせ

Libra / リブラ → Diem に改名

2020年 12月 1日(火) 発表

- 世界統一通貨 → まず単一通貨から
- 大義は financial inclusion / 金融包摂
- こなれた設計
  - よくできた財布アプリ (ウォレット)：Calibra
  - ステーブルコイン
    - 通貨バスケット：US$ 50%, € 18%, 円 14%, ポンド 11%, SGD 7%
  - 当初、取引承認は協会メンバのサーバ群が行う。5年以内に、誰でも。
- **前途多難**
  - 各国の金融当局が強く警戒。
    - 金融政策が効かなくなる。
      cf. 「決済のイノベーションと中央銀行の役割」by 日銀 黒田総裁 (2019/12)
  - 予定されていた創設メンバが次々と離脱。
    - Visa, Mastercard, Stripe, eBay, PayPal, … → 大手 決済企業が不在に

Libra 協会の
創設メンバ

見合わせ

世界はソフトウェアでできている

≒ コンピュータプログラム　とも言える

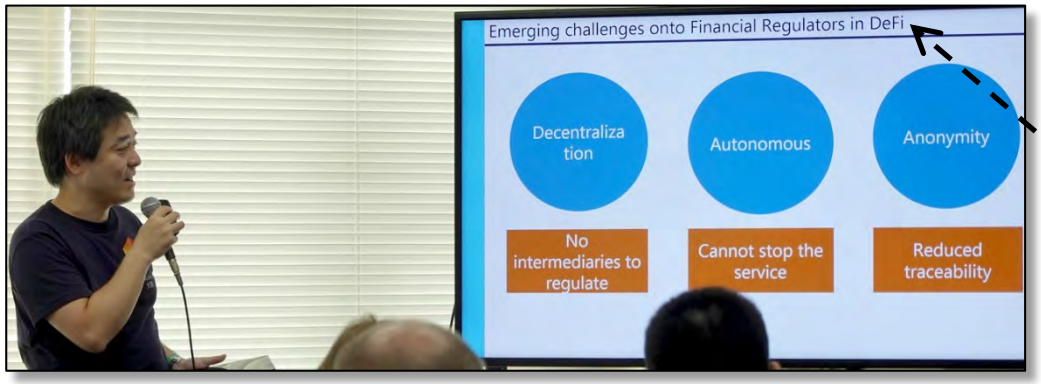
- 例
  - 銀行：皆さんの預金はコンピュータ上の数字・データに過ぎない
  - 株式市場：プログラムが高速に取引し、人間は太刀打ちできない
  - 自動車：各種制御 (エンジン内のガソリン噴出量とか), 自動運転
  - 交通 IC カード (SUICA 等)
  - 天気予報

- 社会はかなりコンピュータが支配している。
  → 皆、コンピュータをある程度知る必要 がある。
  - 東工大 1年生向け講義「コンピュータサイエンス」
  - リクルート社等、新入社員全員にプログラミング教育
    - コンピュータにできることを知らないと、まともなサービス設計ができない。

図の出典：　https://tech.nikkeibp.co.jp/dm/article/WORD/20060418/116236/

Decentralized Autonomous Organization (DAO) と Decentralized Finance (DeFi)

- DAO (いわば、自動運営組織)
  - "An organization represented by rules encoded as a computer program that is transparent, controlled by shareholders and not influenced by a central government" (Wikipedia より)
    コンピュータプログラムが運営する組織
    - 例：Bitcoin では、プログラムが通貨を発行している。
  - 現状、DAO は皆 DeFi ↓ かもしれない。
- DeFi (分散型金融)
  - 非集中であるブロックチェーンで 様々な金融を実現しようという試み
    - 取引所, 証券, 保険, デリバティブ, 貸借 (銀行), …



金融庁の方の講演
2019/10/10(木)

Emerging challenges onto Financial Regulators in DeFi

Decentralized Autonomous Organization (DAO) と Decentralized Finance (DeFi)

- DAO (いわば、自動運営組織)
- DeFi (分散型金融)

- 強力な手段：スマートコントラクト / smart contract
  - ブロックチェーン上でのプログラム実行
    - cf. Ethereum の Solidity 言語
  - いわば world wide computer を実現

社会の中で、ソフトウェアで動く範囲は広がる一方

Web 3 ≒ decentralized web

- Web 2.0 (2005年頃 〜)
  - 双方向 = 誰もが発信 (ブログや SNS)
  - リッチなユーザ体験 = 動的なウェブページ等
  - ウェブ検索 (それ以前は Yahoo! 等ポータルサイトからアクセス)

- Web 3 ≒ decentralized web
  - Web 2.0 は GAFAM らテックジャイアントが支配した！
    → 実はかなり中央集権
  - 次は非集中に！
  - データ (Web 1.0) や対話 (Web 2.0) だけでなく
    (ブロックチェーンに) 価値も載せて！
    - これまでネットに載りにくかった社会活動をより広範にサポート

対外発表 (1)

- ツール
  - [青木 2019a] 青木優介, 大月魁, 金子孟司, 坂野遼平, 首藤一幸: “**SimBlock: ブロックチェーンネットワークシミュレータ**”, 信学技報, Vol.118, No.481, IA2018-70, p.219-224, 2019年 3月
  - [Aoki 2019b] Yusuke Aoki, Kai Otsuki, Takeshi Kaneko, Ryohei Banno, Kazuyuki Shudo: "**SimBlock: A Blockchain Network Simulator**", Proc. CryBlock 2019 (in conj. with INFOCOM 2019), 2019年 4月
  - [Banno 2019] Ryohei Banno, Kazuyuki Shudo: “**Simulating a Blockchain Network with SimBlock**”, Demonstration, Proc. IEEE ICBC 2019, pp.3-4, 2019年 5月
  - [Shudo 2019] Kazuyuki Shudo: "**SimBlock**", lightning talks, P2P Summit, Devcon 5, Ethereum Foundation, 2019年 10月

対外発表 (2)

- 性能
  - [神田 2019a] 神田伶樹, 首藤一幸: “**ビットコインネットワーク上でのデータ伝搬遅延推定**”, 信学技報, Vol.118, No.481, IA2018-77, pp.317-322, 2019年 3月
  - [Kanda 2019b] Reiki Kanda, Kazuyuki Shudo: “**Estimation of Data Propagation Time on the Bitcoin Network**”, Proc. AINTEC 2019, pp.47-52, 2019年 8月
  - [青木 2019c] 青木優介, 首藤一幸: “**ブロックチェーンネットワークにおける隣接ノード選択**”, 信学技報, Vol.118, No.481, IA2018-71, pp.225-232, 2019年 3月
  - [Aoki 2019d] Yusuke Aoki, Kazuyuki Shudo: “**Proximity Neighbor Selection in Blockchain Networks**”, Proc. IEEE Blockchain 2019, pp.52-58, 2019年 7月
  - [大月 2020a] 大月魁, 首藤一幸, 坂野遼平: “**ビットコインに対するリレーネットワークの影響**”, 信学技報, Vol.119, No.460, NS2019-192, pp.89-94, 2020年 3月
  - [Otsuki 2020b] Kai Otsuki, Ryohei Banno, Kazuyuki Shudo: “**Quantitatively Analyzing Relay Networks in Bitcoin**”, Proc. IEEE Blockchain 2020, pp.214-220, 2020年 11月
  - [永山 2020a] 永山流之介, 首藤一幸, 坂野遼平: “**コンパクトブロックリレーとインターネット高速化を考慮したビットコインネットワークシミュレーション**”, 信学技報, Vol.119, No.460, NS2019-208, pp.179-183, 2020年 3月
  - [Nagayama 2020b] Ryunosuke Nagayama, Ryohei Banno, Kazuyuki Shudo: "**Identifying Impacts of Protocol and Internet Development on the Bitcoin Network**", Proc IEEE ISCC 2020, pp.506-510, 2020年 7月

対外発表 (3)

- セキュリティ
  - [Nagayama 2019] Ryunosuke Nagayama, Kazuyuki Shudo: "**Simulating Ethereum Network with SimBlock**", lightning talks, Devcon 5, Ethereum Foundation, 2019年 10月
  - [高山 2020b] 高山柊: "**Erebus攻撃への対策がBitcoinネットワーク性能に与える影響**", 首藤研 演習成果発表会, 2020年 7月
- 公平性
  - [神田 2020a] 神田伶樹, 首藤一幸: "**公平なProof-of-Workブロックチェーンに向けたブロック生成間隔調整**", 信学技報, Vol.119, No.460, NS2019-206, pp.169-174, 2020年 3月
  - [Kanda 2020b] Reiki Kanda, Kazuyuki Shudo: "**Block Interval Adjustment Toward Fair Proof-of-Work Blockchains**", Proc. ICDE 2020 Workshops (BlockDM 2020), pp.1-6, 2020年 4月
- 分権化
  - [Nagayama 2020a] Ryunosuke Nagayama, Ryohei Banno, Kazuyuki Shudo: "**Trail: A Blockchain Architecture for Light Nodes**", Proc. IEEE ISCC 2020, pp.511-517, 2020年 7月
  - [高山 2020a] 高山柊, 永山流之介, 大月魁, 首藤一幸: "**Proof-of-Stakeブロックチェーンの中央集権化へのコイン年齢の影響**", 信学技報, Vol.119, No.460, NS2019-207, pp.175-178, 2020年 3月