応用物理学会 超集積エレクトロニクス産学連携委員会
夏の学校
2022年 8月 26日(金)

ブロックチェーンにおける性能とセキュリティの関係

首藤 一幸
京都大学

bit.ly/VLSI-202208-shudo

Kyoto U.

首藤 一幸 (48)

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**

2022/ 4 京大

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

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

1万数千部, ネタ100個中 10個執筆

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 ～

シミュレータ SimBlock, 性能と安全性, 新アーキ

魔法のようなソフト

大規模分散システム

2022年 8月

講演の概要

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, …

1万 9千種類あるとか

- 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.

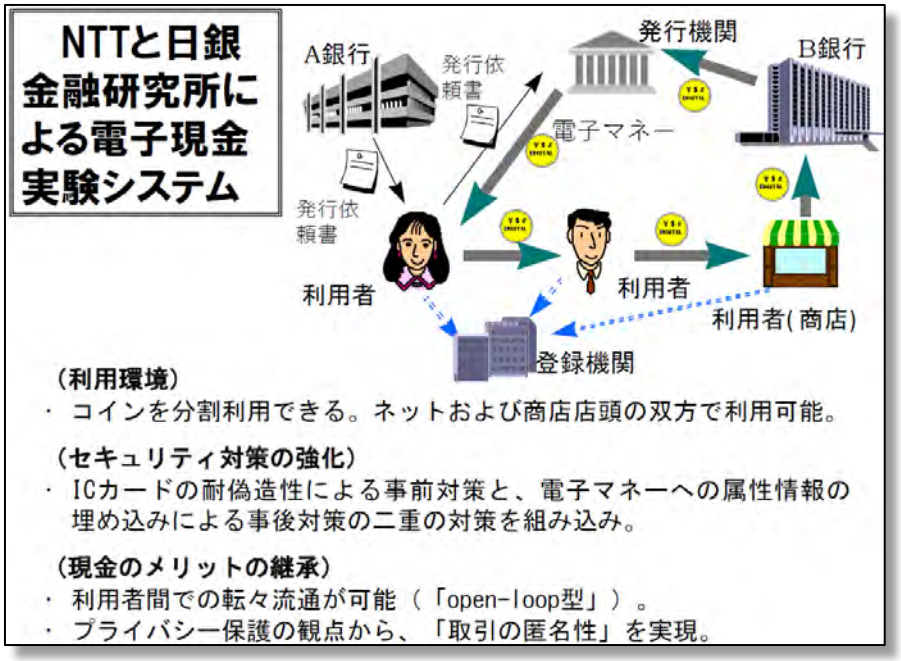
See bitcoin.org for screenshots.

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

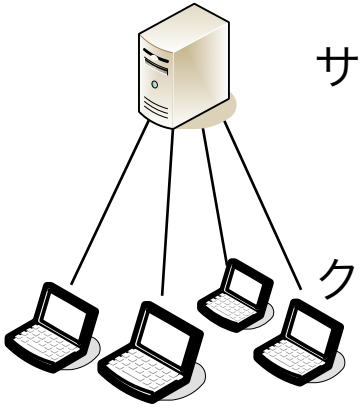


岩下直行氏 (日銀 → 京大) のスライド

- SUICA / スイカなんかすごい。
  - 8,000万枚 (2020/12), 200ミリ秒 (要求仕様), 平均 105件/秒 (2019/8/2)
  - 集中的な仕組みでこの性能を出すために、様々に工夫

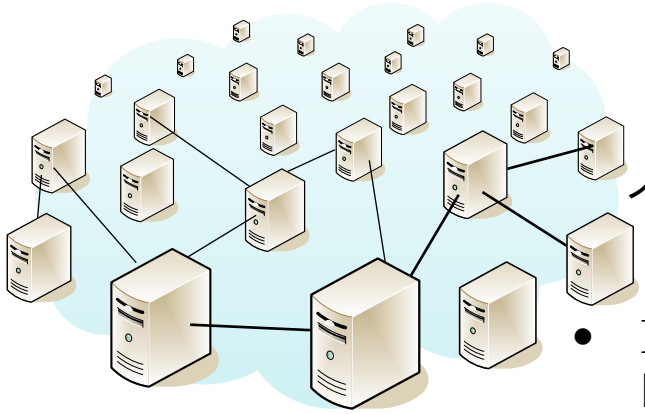
Bitcoin の技術は何が違ったか？

- 非集中 / decentralized → トラストレス に二重使用 / double-spending を防止した
  - 非集中　⇔ 集中 / centralized
    - 親分がいない



集中的
分散システム

- 普通はこちら
- 作りやすい
- 管理しやすい



非集中
分散システム

- Peer-to-peer (P2P)と呼ばれる
- 例: Skype (電話), Gnutella (ファイル共有)
- スケール (台数増) しやすい, 耐故障

Bitcoin の非集中 分散システム

- インターネット上に 1万数千ノード (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

REACHABLE BITCOIN NODES

Updated: Wed Aug 17 16:06:24 2022 JST

13294 NODES　CHARTS

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

RANK	COUNTRY	NODES
1	n/a	6260 (47.09%)
2	United States	1928 (14.50%)
3	Germany	1406 (10.58%)
4	France	453 (3.41%)
5	Netherlands	371 (2.79%)
6	Canada	302 (2.27%)
7	Finland	234 (1.76%)
8	United Kingdom	225 (1.69%)
9	Russian Federation	191 (1.44%)
10	Singapore	146 (1.10%)

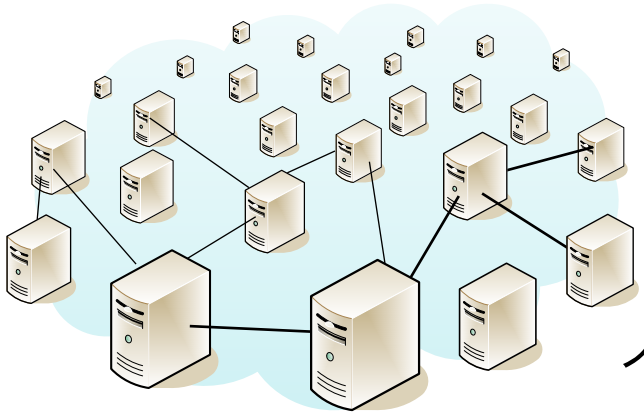
Map shows concentration of reachable Bitcoin nodes found in countries around the world.　LIVE MAP

https://bitnodes.io/ より

- 非集中 → 一部壊れても全体は動作し続ける

トラストレス / trustless

- 非集中 / decentralized



ピア / peer
ノード / node

非集中 分散システム (peer-to-peer)

- 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。

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
  分散システム
  decentralized

→ **トラストレス**
trustless

→ **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

- 暗号理論
  cryptography

→ **整合性**
fault tolerant

派生 → **トレーサビリティ**
traceable

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, …

→ 二重使用の防止

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
基礎

- 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)

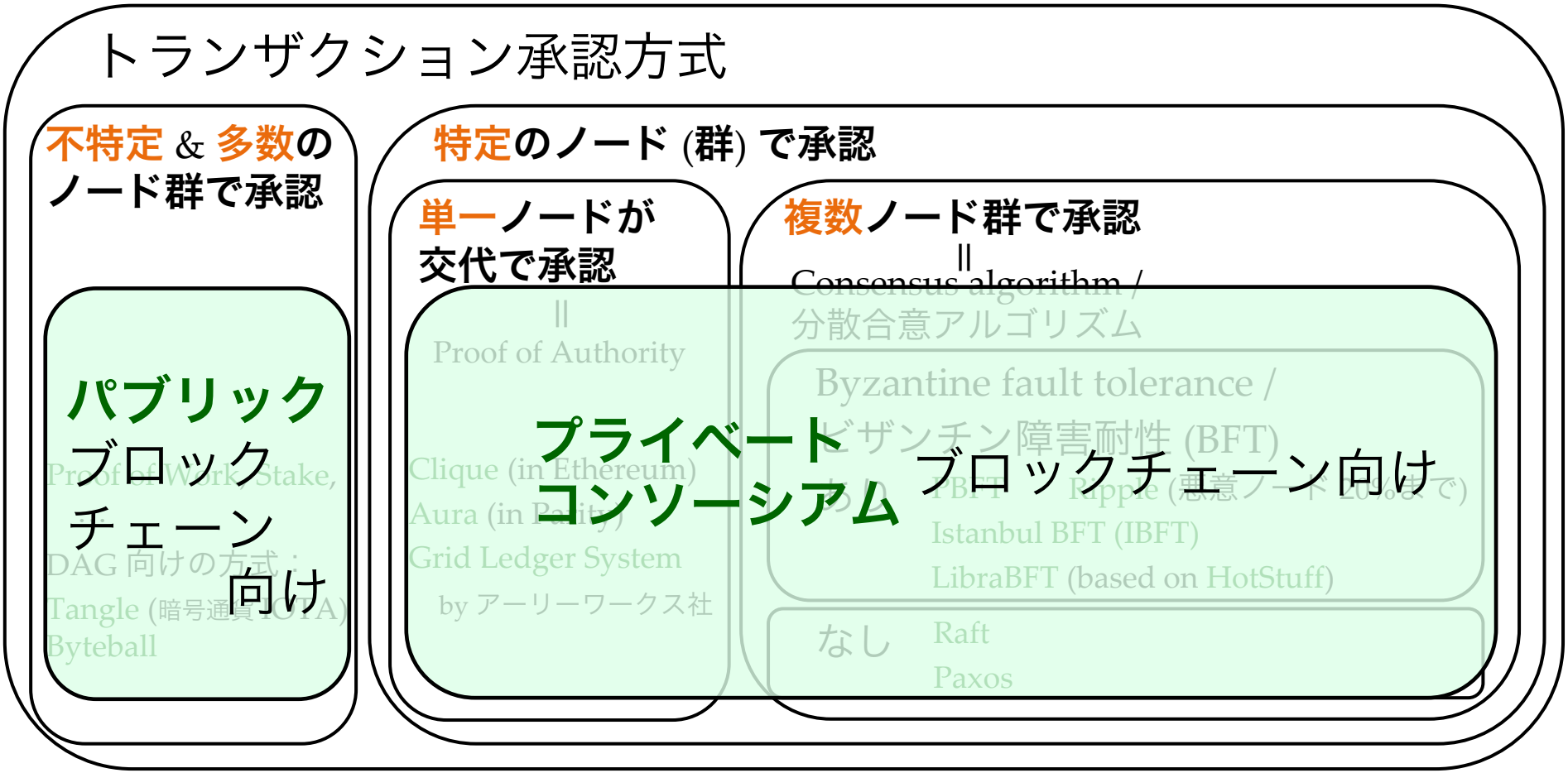
なし Raft
Paxos

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？



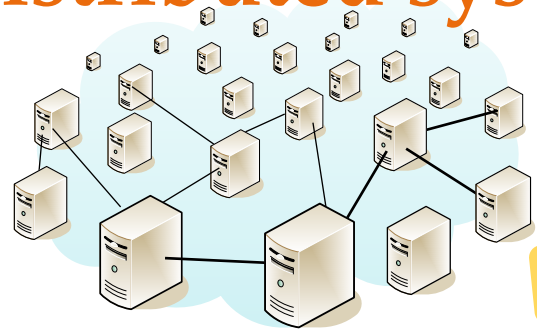
ブロックチェーンを支える技術

- 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

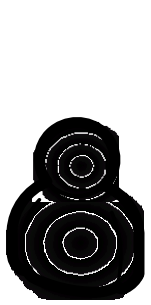


peer-to-peer ネットワーク,
flooding, 複製, 整合性,
分散合意アルゴリズム, …

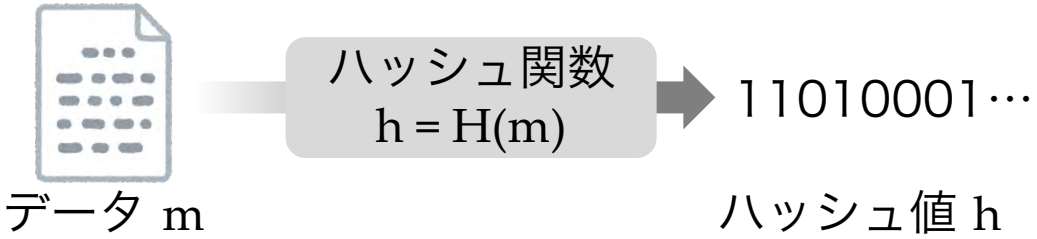
首藤の専門

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)

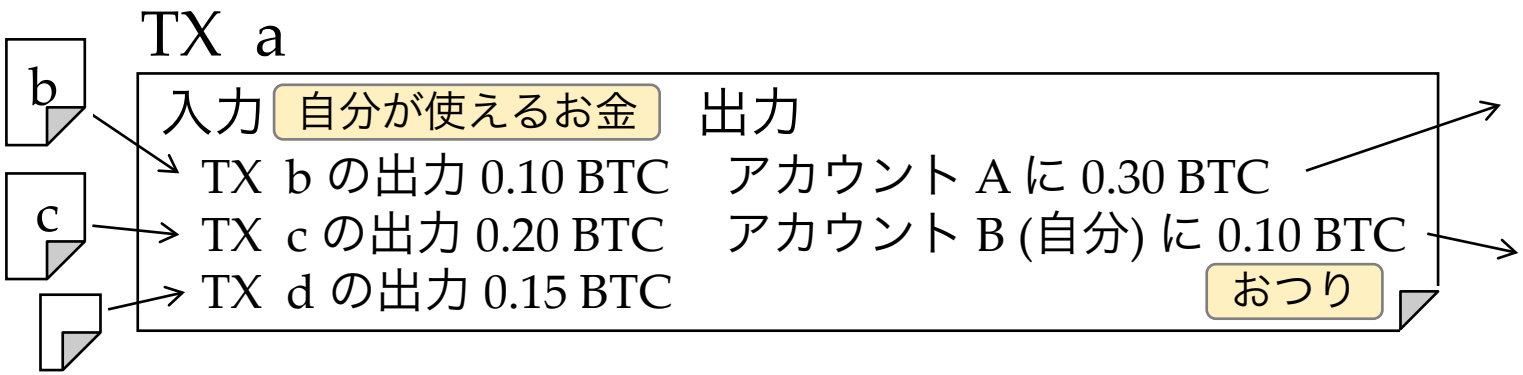


- (暗号学的) ハッシュ関数
  - データごとの固有の数値 ＝ ハッシュ値 (128 ～ 512ビット) を算出できる。
    データの指紋を採れるようなもの。
  - ハッシュ値を与えられても、データの側は作り出せない。一方向。
  - 署名 (上記) の際、データ自体ではなく、ハッシュ値に対して署名する。



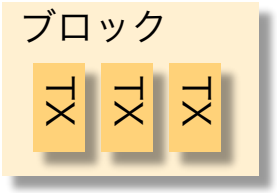
ブロックチェーンのデータ構造

- トランザクション (TX と略記)　　お金の動き



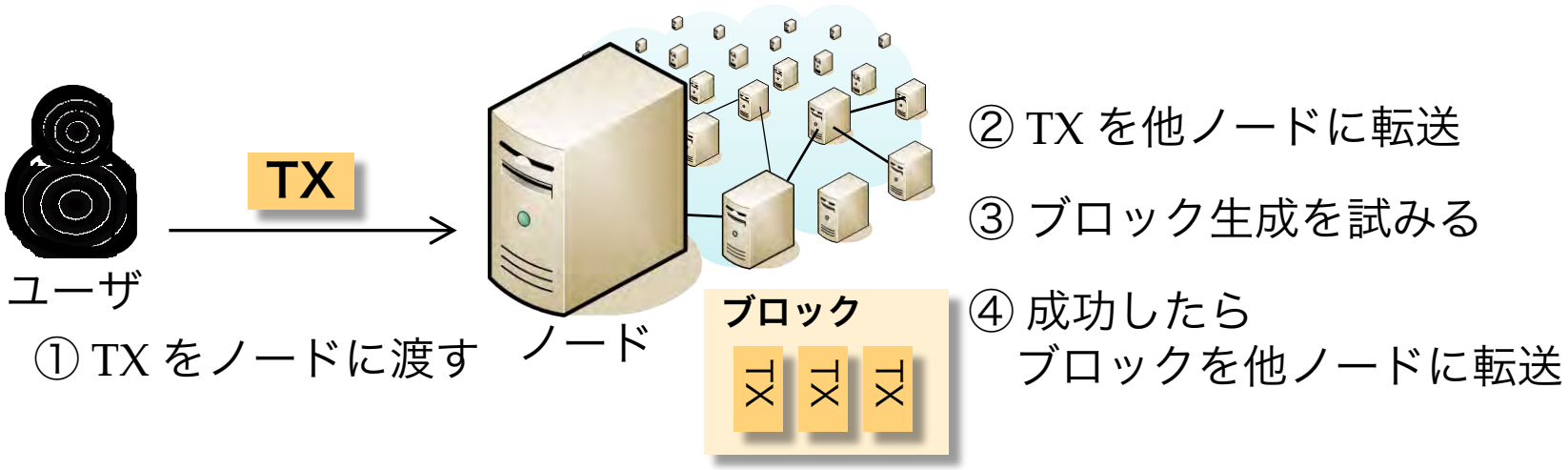
  - 自分に使用の権限があることや、確かに自分が発行した TX であることは、署名 (前項) で示す。
  - TX を矛盾 (二重使用) なく連鎖させていく。

- 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



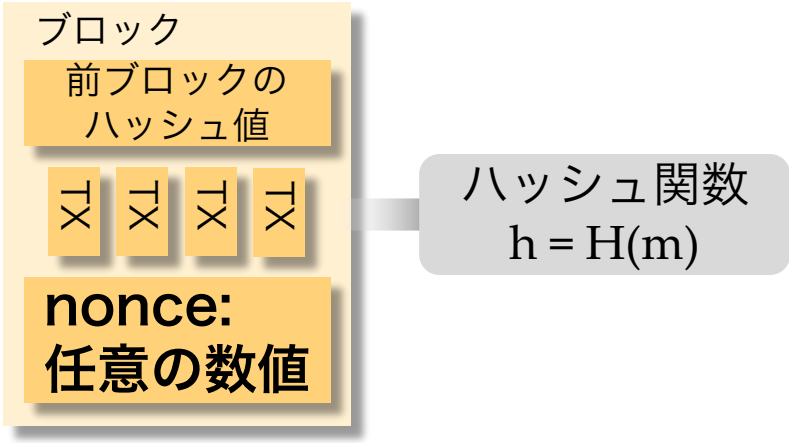
- ① ユーザが TX をノードに渡す。
- 　ノード群は
  - ② 受け取った TX を他ノードにブロードキャストする。
  - ③ TX 群をブロックにまとめて、ブロック生成を試みる。
    計算競争 = Proof of Work (PoW) に勝つと生成できる。
    ④ ブロック生成に成功したら、
    他ノードにブロードキャストする。

次ページ
2ページ後

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

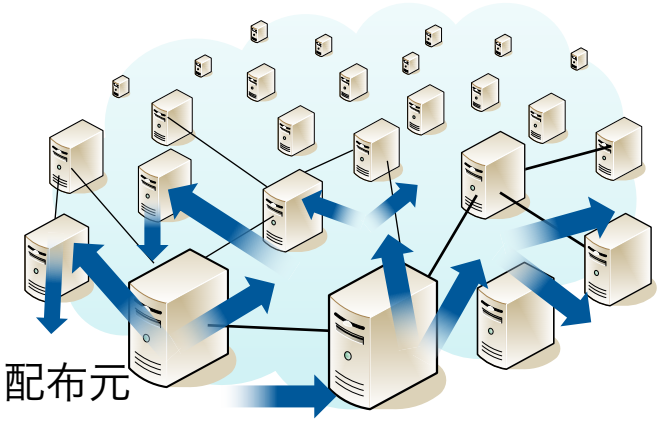


- ブロック中の、任意に決めてよい部分を変更して試しまくる
- ハッシュ値は乱数のようなもの
  → 2^n 回に 1回、成功する
- 一定期間ごとに難易度 n を調整する

  - 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。

ブロックや TX のブロードキャスト

- 手段：flooding / フラッディング
  - ノード群は、アプリケーションレベルの peer-to-peer ネットワークを構築している。
    - Bitcoin の場合：outbound 接続 8 + inbound 接続 125
  - 受け取ったら、隣接ノードすべてに転送する。

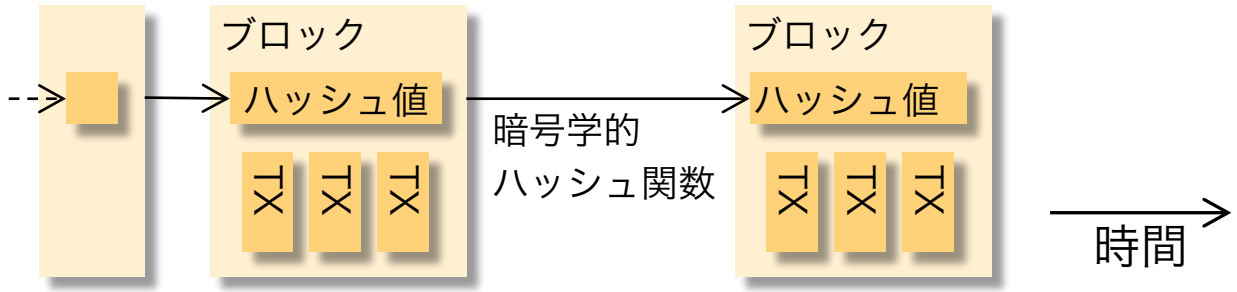


ノード (サーバ) のネットワーク

- 全ノードが同一のブロックチェーンを持つ

ブロックの連鎖

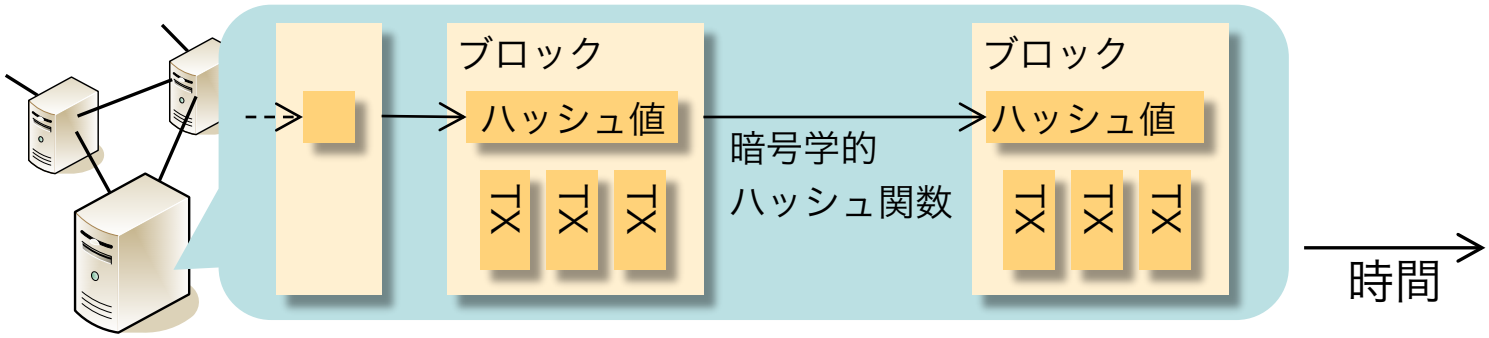
- ブロックをハッシュ値で連鎖させていく
  → ブロックのハッシュチェーン
  → ブロックチェーン



  - 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

改ざん困難性 と 二重使用防止

- 改ざん困難性
  - **計算競争** (3ページ前) で生成された**ブロックの連鎖** (1ページ前) を**全ノードが保持** (2ページ前) していることに基づく



  - 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、ブロックを受信したら、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 Proof of Stake (PoS) がそろそろ実用
e.g. Ethereum 2.0

性能とセキュリティの関係

- 性能 = トランザクション処理数 / 秒 (TPS)
- フォーク
- 性能向上 vs. セキュリティ

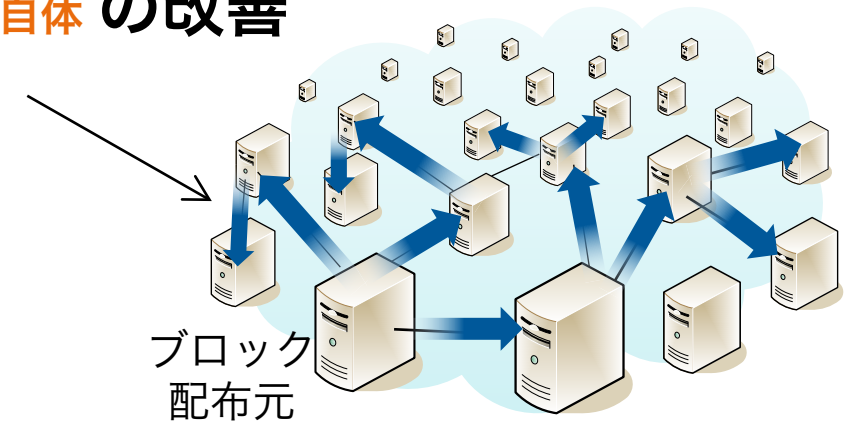
パブリック
ブロックチェーンの性能

- 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**

- 性能向上へのアプローチ
  - **base layer = ブロックチェーン自体 の改善**
    - ブロック伝播の高速化が必要
  - sharding
    - 分割
  - Layer 2 / second layer
    - base layer の上で…

次ページ以降

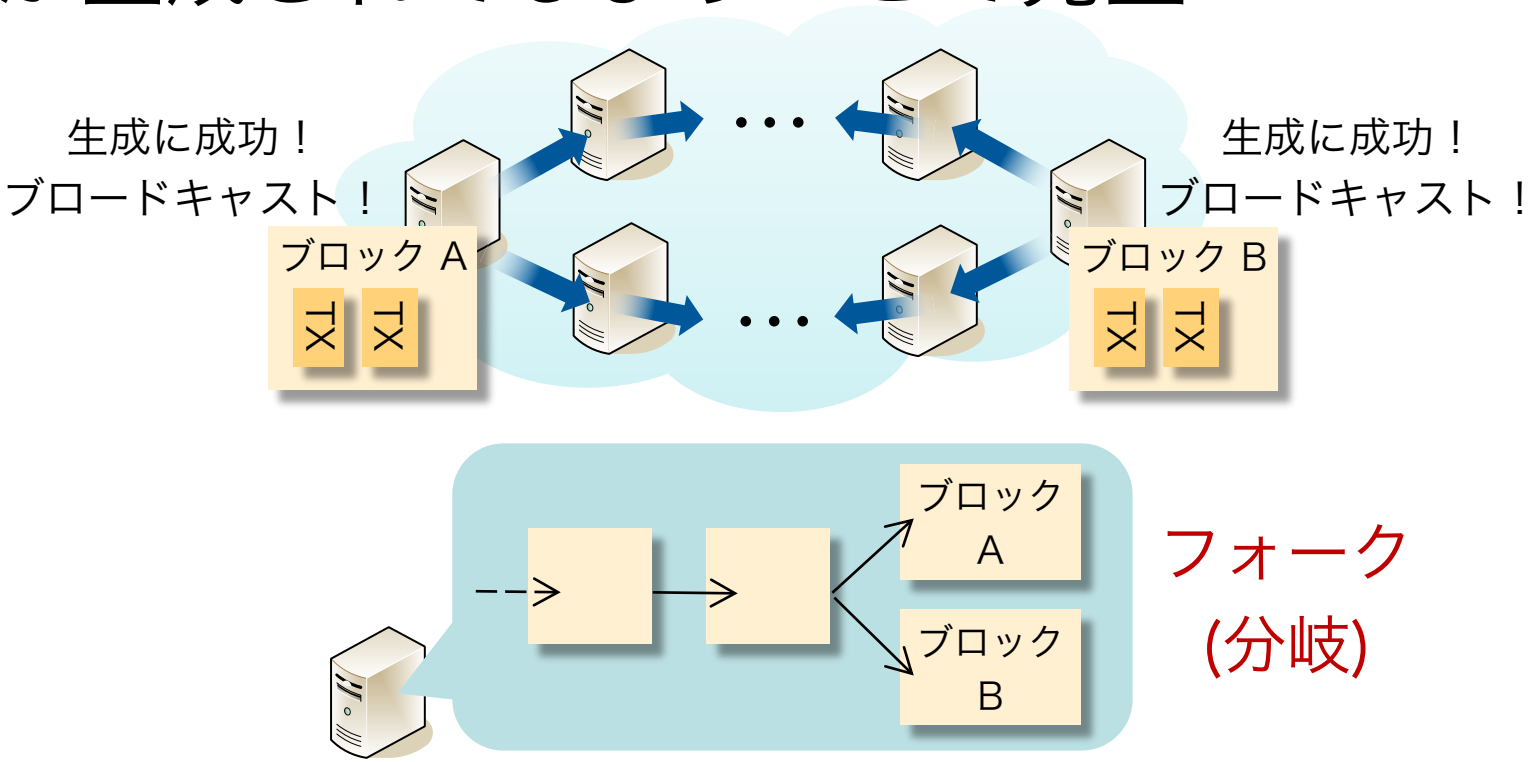
割愛



ノード (サーバ) のネットワーク

前提知識：
ブロックチェーンの フォーク (分岐)

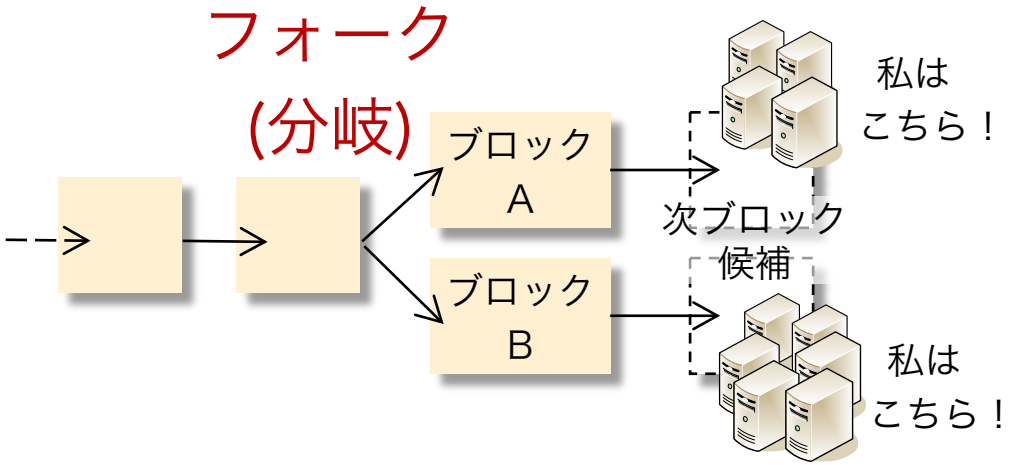
- ブロックが行き渡る前に、別のブロックが生成されてしまうことで発生



- セキュリティを低下させる

フォークとセキュリティ

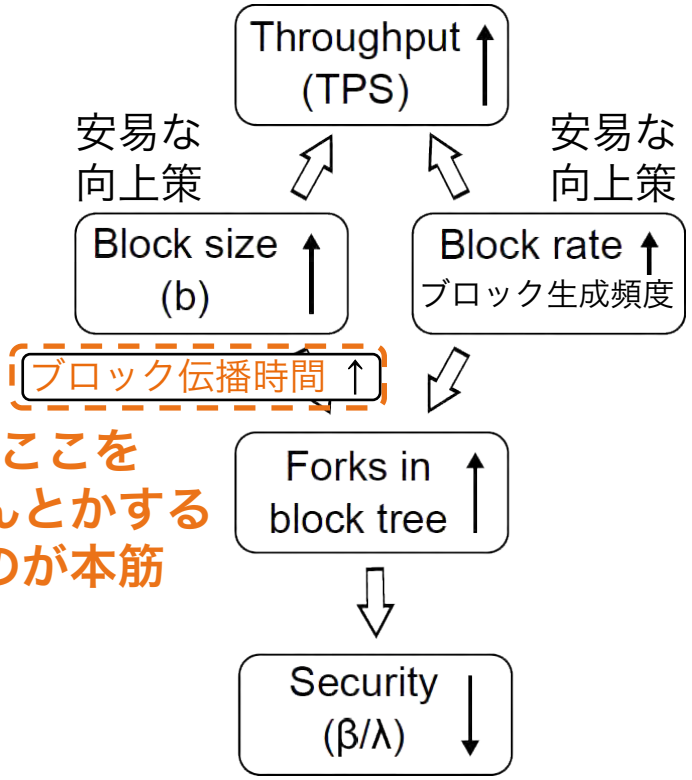
- フォークはセキュリティを低下させる
  - マイニングの計算能力 --- ハッシュパワー --- が分散してしまう → 攻撃が容易になる
    - 51% 攻撃 – 過半数のハッシュパワーで、既存ブロックを無効化
    - block withholding attack – 生成したブロックを隠しておき、一気に…
    - selfish mining - 生成したブロックを隠しておき、いいタイミングで…



- どのチェーンが正統かを決める規則 --- fork choice rule --- がノード群に仕込まれているが、全ノードが収束するまで多少時間はかかる

性能向上 vs. セキュリティ

- 安易な性能向上策は、フォークを増やし、セキュリティを低下させる
  - **ブロックサイズの増加**
    - 例: 1 MB → 8 MB → 32 MB (Bitcoin Cash)
    - ○ 性能 (TPS) が向上
    - △ 比例して、ブロック伝播時間が延びる
      → フォーク発生率 増加
  - **ブロック生成頻度の向上**
    - 例: 10 分 → 1秒
    - ○ 性能 (TPS) が向上
    - △ 行き渡る前の生成が起こりやすくなる
      → フォーク発生率 増加



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

- 補うために **ブロック伝播時間の短縮**が必要

首藤研での研究

- ツール
- 性能
- セキュリティ
- 公平性
- 分権化
- 外部依存の削減

→ トラストレスに貢献

研究成果

- 「ツール」「性能」から「セキュリティ」「トラストレス」へ

セキュリティ

[Nagayama 2019]

- selfish mining 攻撃への耐性評価
- Erebus 攻撃対策の性能への影響 [高山 2020b]
- PoS への攻撃手法と耐性調査 [大月 2021a] [Otsuki 2021c]

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] 他
- 隣接ノード選択 [青木 2019b] [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 2020c] 他
- ブロードキャスト木の適用 [Banno 2020] [Banno 2021]
- ブロック送信元 切り替え [櫻井 2022a]
- ブロック生成間隔 調整 [荒川 2022a] [Arakawa 2022b]

研究手段を提供

ツール

- シミュレータ SimBlock [青木 2019a] [Aoki 2019c] [Banno 2019] [Shudo 2019e]

研究手段を提供

インセンティブ不整合問題

[Shudo 2018b] [首藤 2018c]

- ブロックチェーン間アプリ移行

トラストレス / trustless

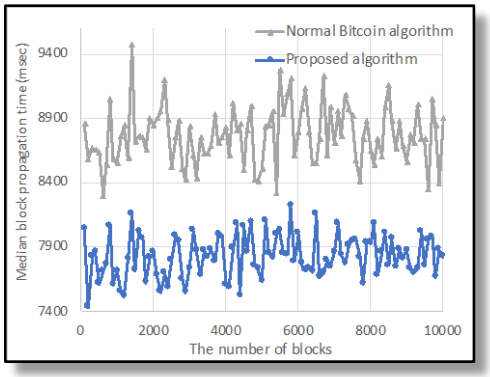
- 中央集権の度合い評価 [高山 2020a]
- 新データ構造 [Nagayama 2020a] [Nagayama 2022]
- データ集約 [Song 2022a] [Song 2022b]
- 時計合わせ [三木 2022a] [Miki 2022b]
- 公平性指標と向上手法 [神田 2020a] [Kanda 2020c]

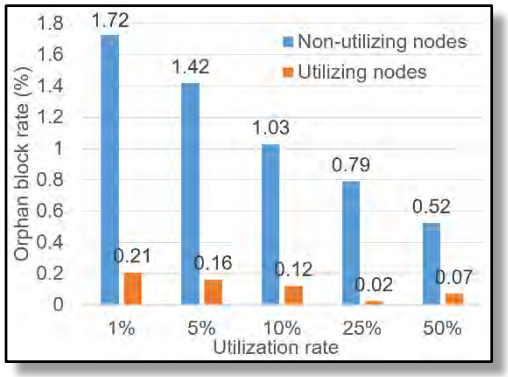
Ethereum 開発者会議 (Devcon 5) での発表 [Nagayama 2019]

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：

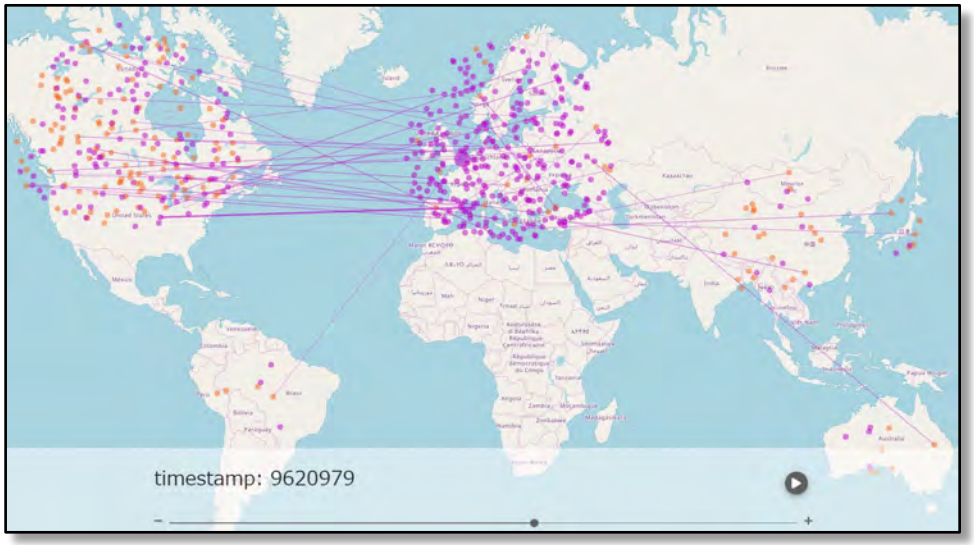




隣接ノード選択　リレーネットワーク 効果推定

シミュレータ SimBlock

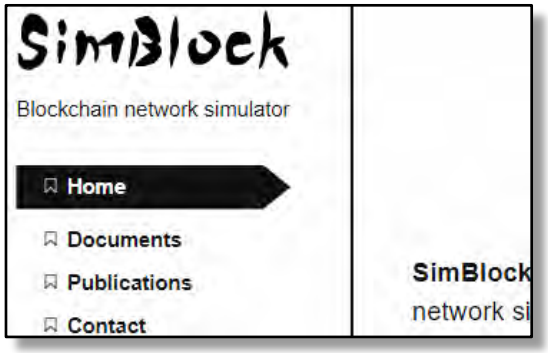
[青木 2019a] [Aoki 2019b] [Banno 2019] [Shudo 2019]



Visualizer

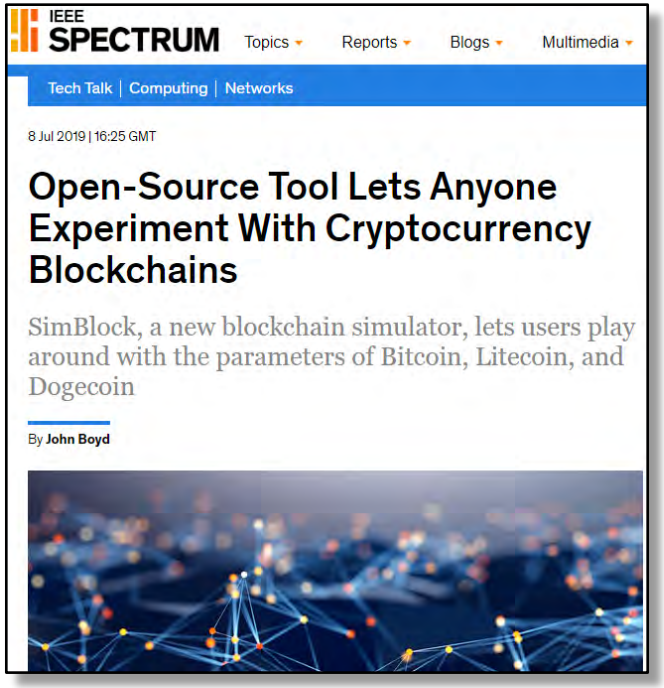
縮小 Bitcoin ネットワーク,
600 ノード

ウェブ
サイト



IEEE ICBC 2019 デモ,
ソウル, 2019年 5月

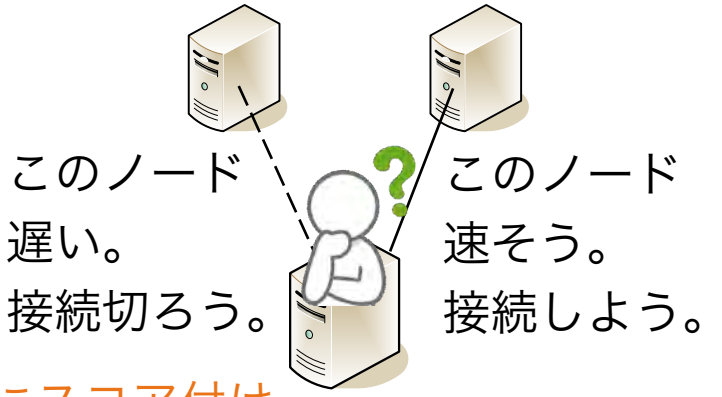
IEEE Spectrum
記事



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

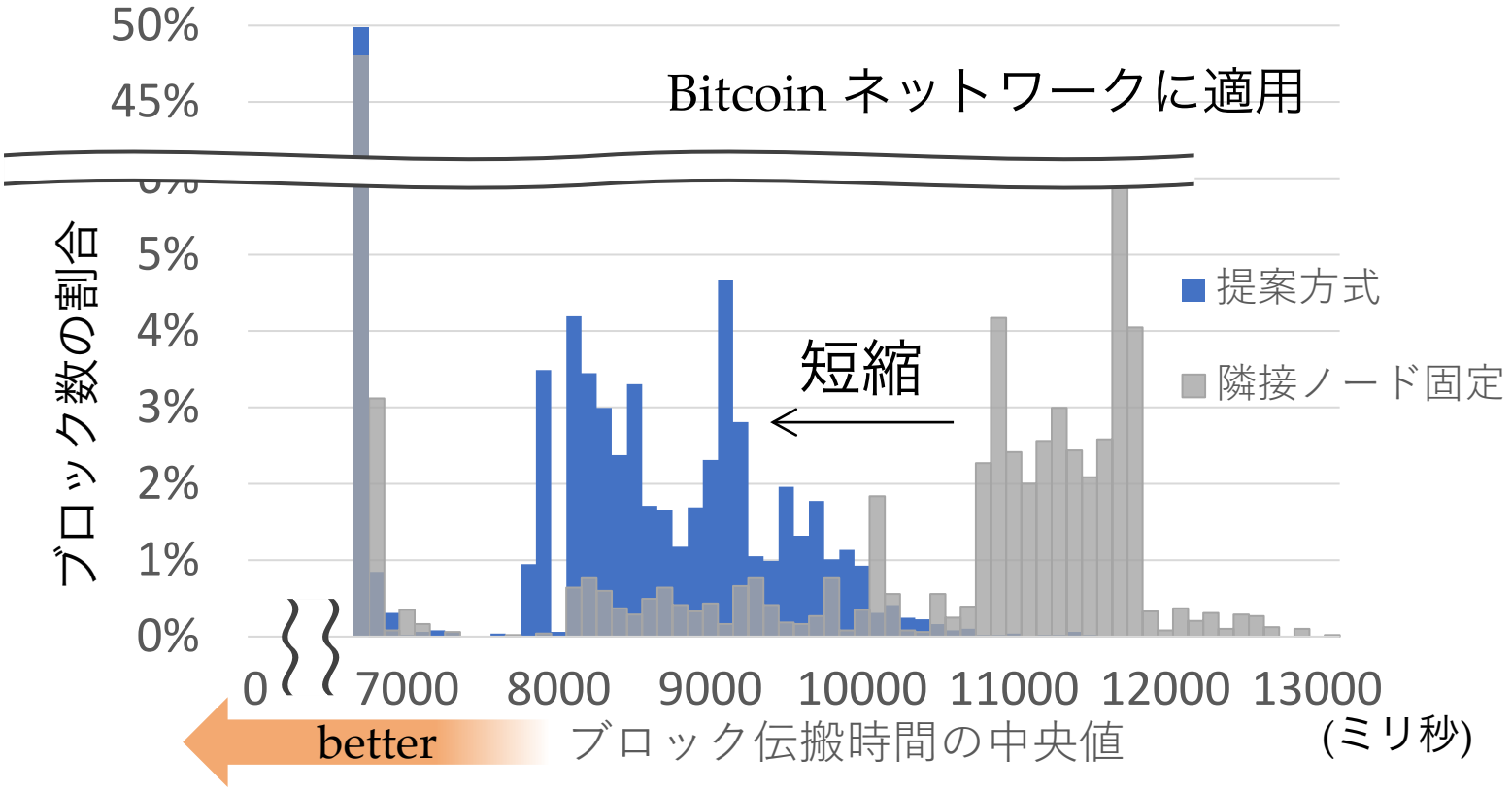


- 手法
  - ブロックを配信してくれた相手ノードすべてにスコア付け
    - スコア = (ブロック配信時刻 – 生成時刻) の指数重み付き平均値
  - 10 ブロック受信するごとに隣接ノードを選択し直す
    - ただし、新しいノードとつながるために、K ノードは知っているノード群からランダムに選ぶ
    - 予備実験の結果：K = 1, P (伝搬時間 最新値の重み) = 0.3

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

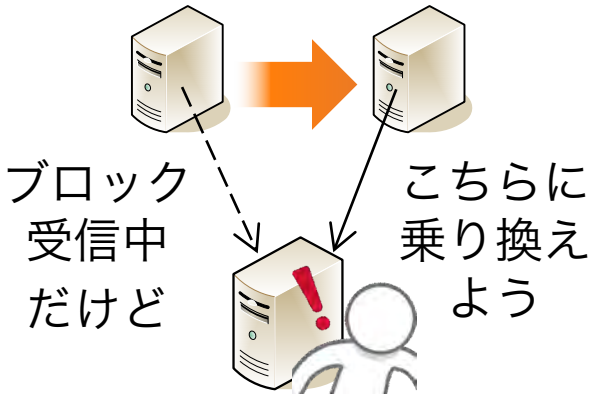


- 注：2015年のインターネットを対象として実験

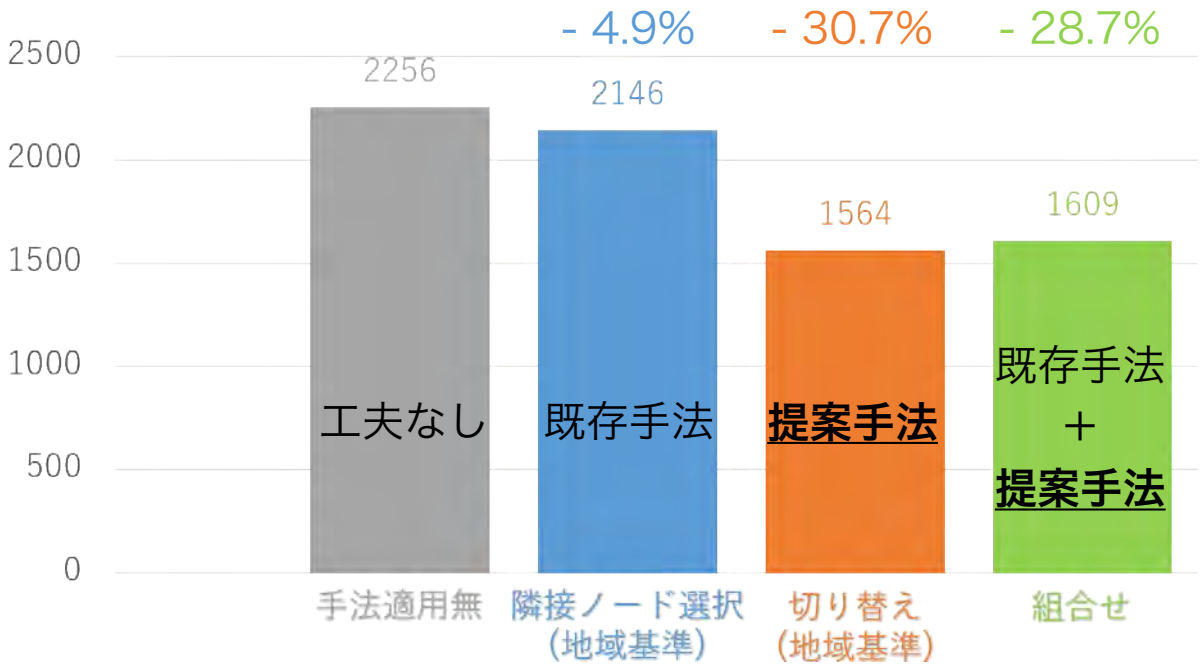
ブロック送信元ノードの 切り替え

[櫻井 2022a]

- ブロック受信中であっても、
  別ノードからの受信に切り替えてしまう。
  - 既に受信したデータは、基本的に、再度、受信する。それでも性能向上。
  - 再度の受信をしないためには、プロトコルの拡張が要る。



手法

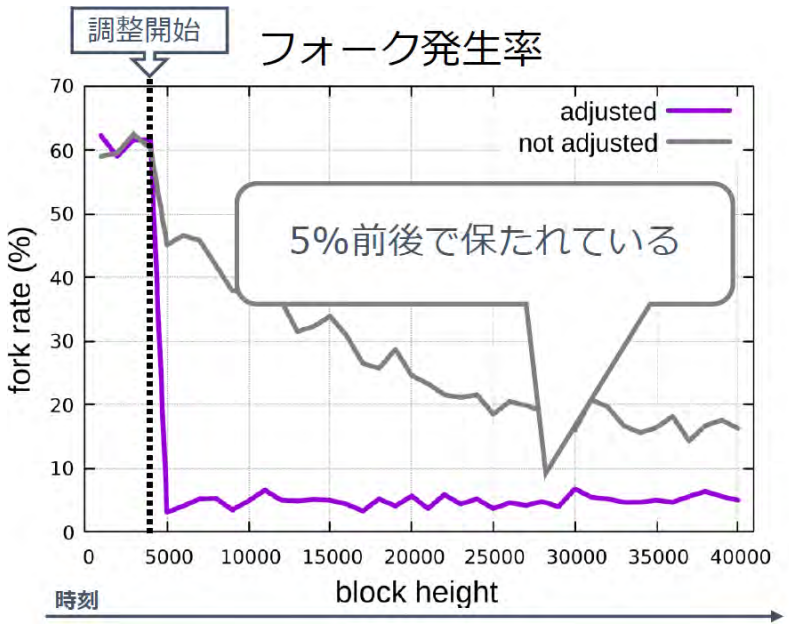


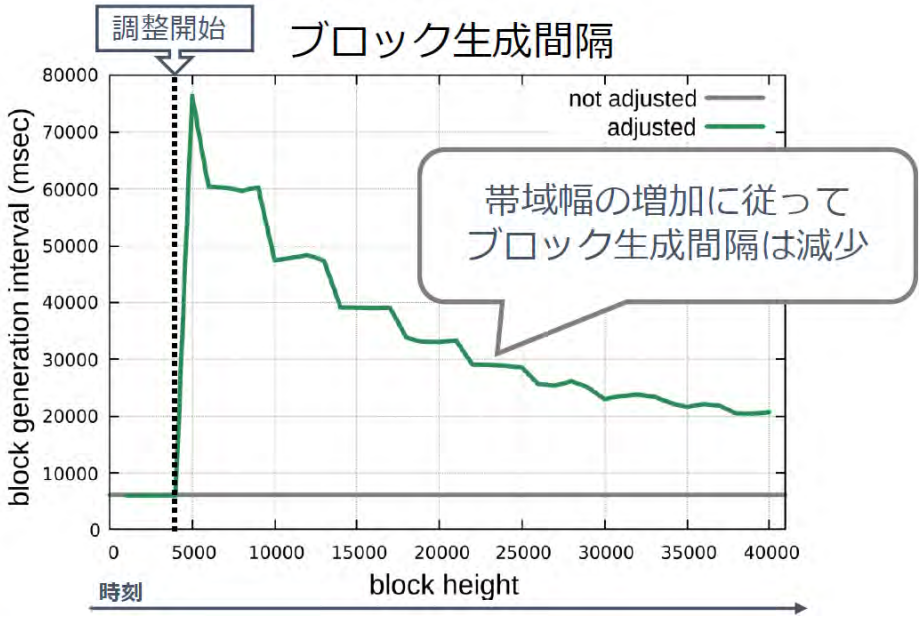
90% のノードにブロックが行き渡るまでの時間

ブロック生成間隔の動的調整

[荒川 2022a] [Arakawa 2022b]

- 前提: 性能 (TPS) = ブロックあたりの TX数 / ブロック生成間隔
  - 当初の Bitcoin: 7 TPS = 1 MiB / 250 byte / 600 秒
- 手法: ブロック生成間隔を適切に縮める。
  - セキュリティは犠牲にしない = フォーク発生率を一定に抑える
  - フォーク発生率は、一部のノード群へのブロック到着時刻から算出。





手法の良し悪し：適用可能性

- 「その手法で Bitcoin を改善できるの？」

- 適用可能性のレベル
  - (1) 一部のノードが採用すれば効果が出る 😍
    - 草の根で、適用できる
  - (2) 全ノードが採用する必要がある
    - (2-1) 移行手順を設計できる 😢
      - 例: まずは並存して…
    - (2-2) 移行手順を設計できない 😭
      - 新しいブロックチェーンネットワークを立ち上げる時にだけ適用可

隣接ノード選択

送信元ノード切り替え

生成間隔調整

まとめ

- ブロックチェーンの起源・価値、基礎、性能とセキュリティの関係、首藤研での研究を紹介
- ネットワーク面のみからの 性能の研究は、そろそろ…

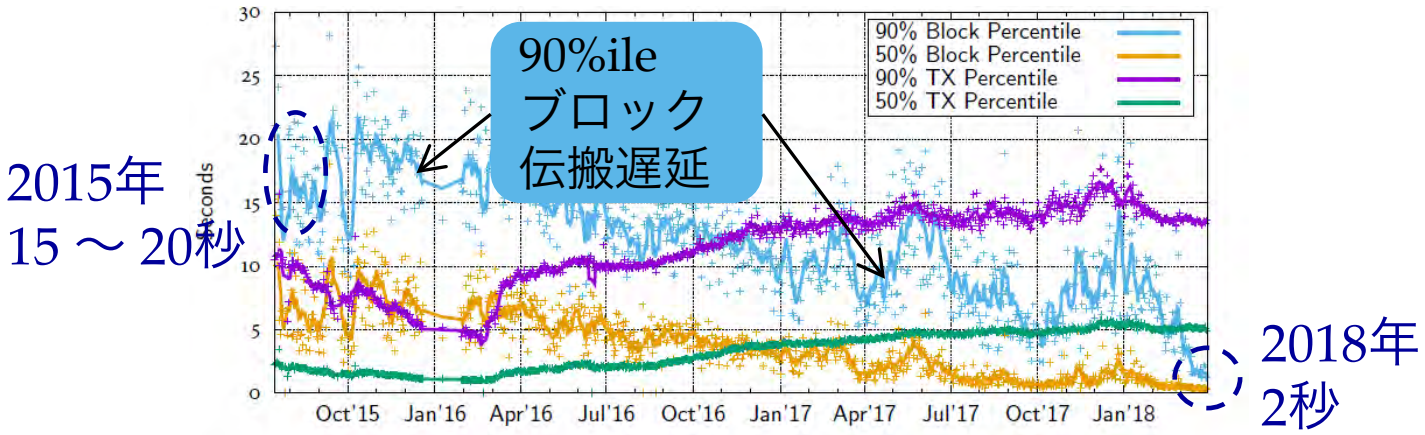


Figure 4.12: Bitcoin propagation delay for block and transaction propagation (50 % and 90 % percentiles). T. Neudecker: “Security and …”, Ph.D. thesis, 2018年

- 現在 ～ 今後：
  セキュリティや、公平性などトラストレスに近いところ