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 (46)

しゅどう　かずゆき

- 得意な領域

基盤的なソフトウェア

非集中分散システム

今日の内容

Java JIT コンパイラ
shuJIT (1998)

書籍 Binary Hacks
(2006)

P2P ライブ配信ソフト
UG Live (2007)

Overlay Weaver

P2P 基盤ソフト
Overlay Weaver (2006)

SimBlock

ブロックチェーン
シミュレータ SimBlock (2019)

- 居場所　国の研究所　ベンチャー企業　大学

早大 → 2001年 産総研 → 2006年 ウタゴエ(株) → 2008年 12月 東工大

暗号通貨 / cryptocurrency

- 2,000 種類以上
- 各国政府は暗号資産 / crypto asset と呼ぶ

暗号通貨の祖

- Bitcoin / ビットコインの価格推移

Blockchain.com より

- 乱高下、盗難事件、…
  それでも時価総額 16 兆円が載っている

講演の概要

- 暗号通貨・ブロックチェーンの **技術** p.4 ～
  - 非集中、turstless に二重使用を防止する仕組み
  - 首藤研の取り組み「ネットワーク」
- 暗号通貨・ブロックチェーンと **社会** p.21 ～
  - 盗難事件
  - 通貨
  - Libra by Facebook 社
  - 世界はソフトウェアでできている
  - Decentralized Finance (DeFi) と Decentralized Autonomous Organization (DAO)
  - Web3

暗号通貨・ブロックチェーンの**技術**

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.

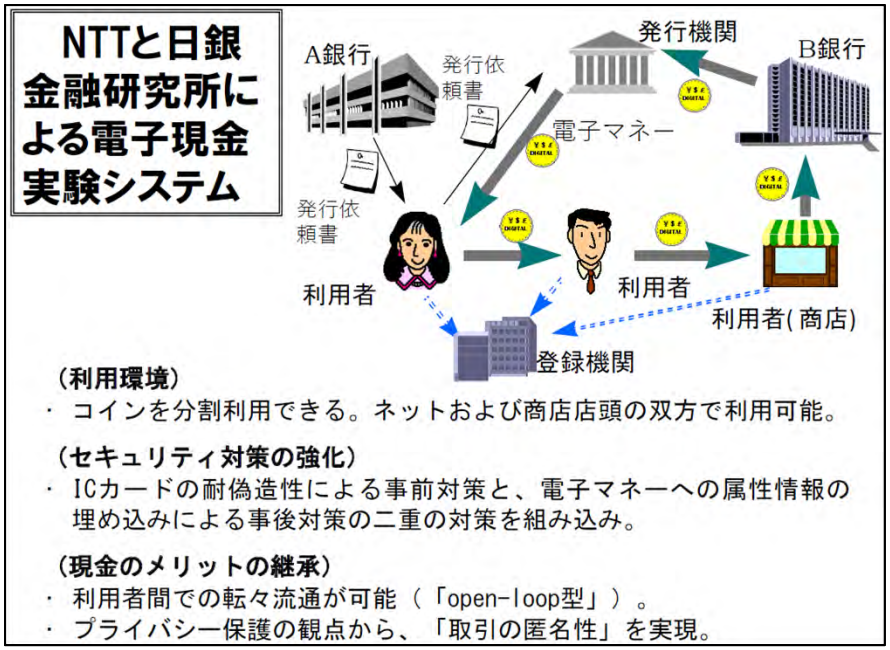
See bitcoin.org for screenshots.

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

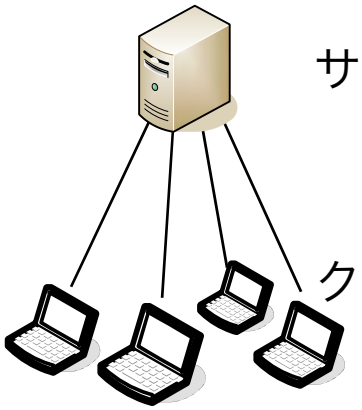


岩下直行氏 (日銀 → 京大) のスライド

- SUICA / スイカなんかすごい。
  - 7,500万枚 (2019/1), 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

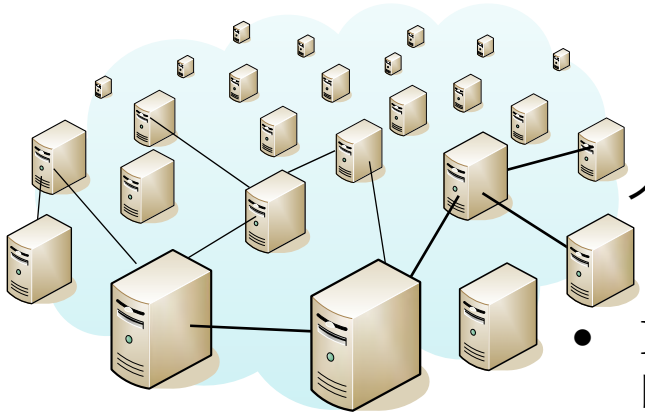
Bitcoin の技術は何が違ったか？

- 非集中的 / decentralized 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



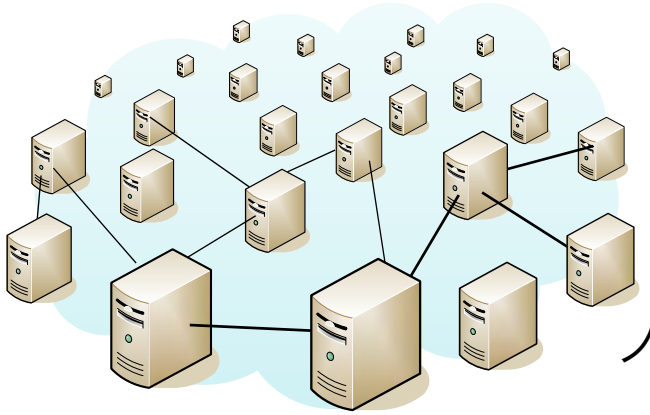
非集中
分散システム

- 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

Bitcoin の技術は何が違ったか？

- 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 は悪意ないノード (運用者) である必要がある。



ピア / peer
ノード / node

非集中 分散システム (peer-to-peer)

Bitcoin の非集中 分散システム

- 約 1万ノード
  - 他のノードと直接通信しない裏のノードを含めると、数万？

GLOBAL BITCOIN NODES DISTRIBUTION

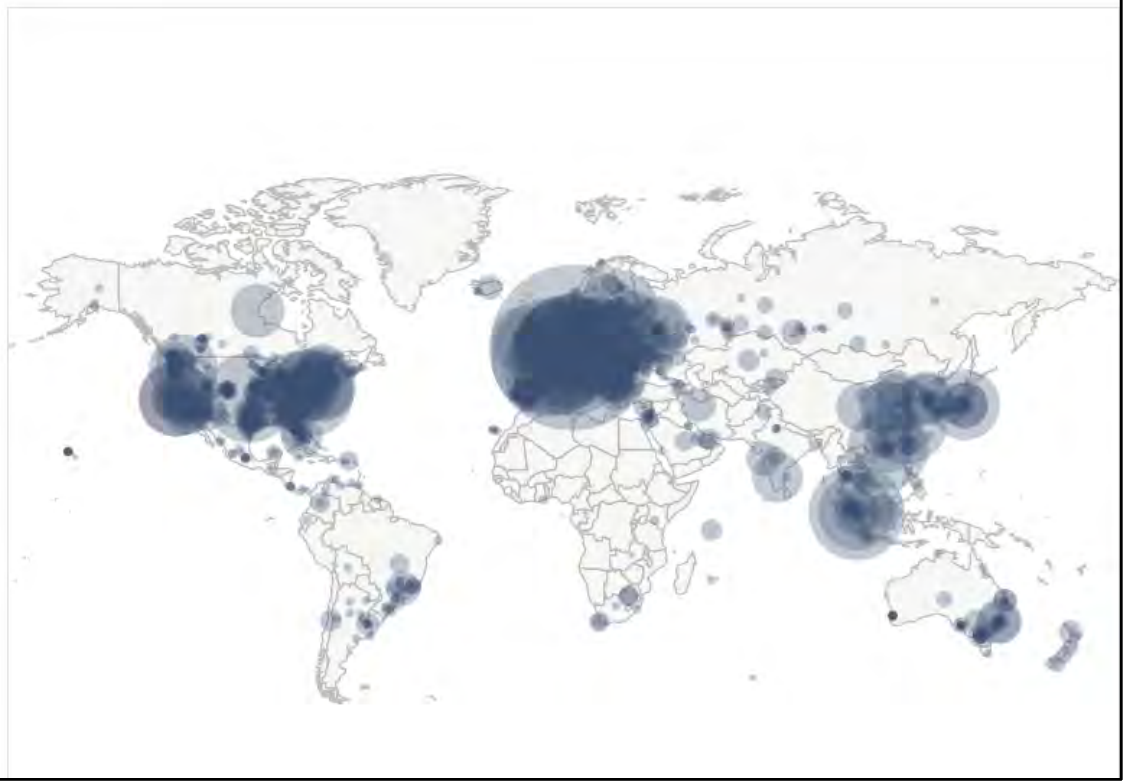
Reachable nodes as of Fri Jan 24 2020 12:04:27 GMT+0900 (日本標準時).

10753 NODES

24-hour charts »

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

RANK	COUNTRY	NODES
1	United States	2354 (21.89%)
2	Germany	1833 (17.05%)
3	n/a	1737 (16.15%)
4	France	597 (5.55%)
5	Netherlands	474 (4.41%)
6	Canada	326 (3.03%)
7	United Kingdom	325 (3.02%)
8	Singapore	322 (2.99%)
9	China	260 (2.42%)
10	Russian Federation	237 (2.20%)



http://bitnodes.earn.com/ より

暗号通貨、ひいては
ブロックチェーンを支える技術

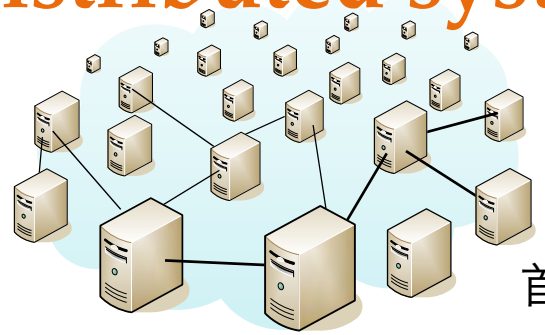
- お金のやりとり以外にも使えるのでは？
- ブロックチェーン として一般化：
  - **誰かを信用することなしに (trustless)**
    データを不整合なく確定させていく仕組み
    例：二重使用

次項以降で解説

- 支える技術：

暗号理論 / cryptography

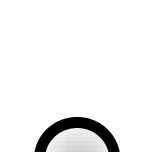
分散システム / distributed systems



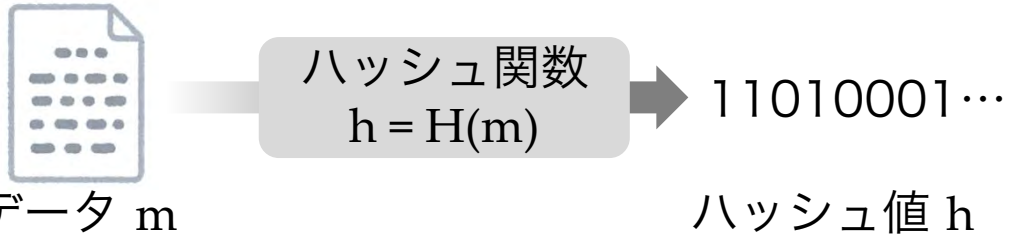
首藤の専門

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)

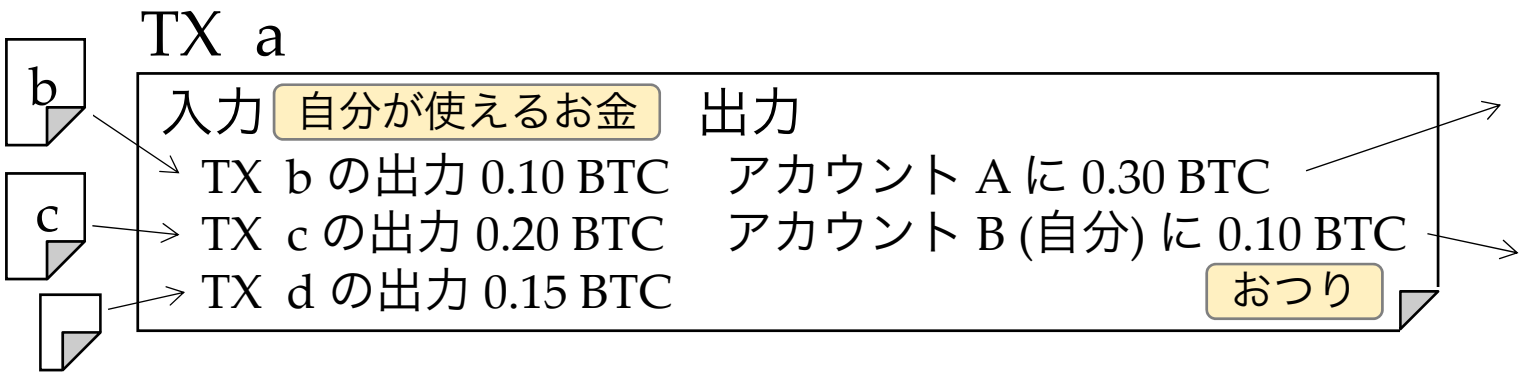


- (暗号学的) ハッシュ関数
  - データごとの固有の数値 ＝ ハッシュ値 (128 ～ 512ビット) を算出できる。
    データの指紋を採れるようなもの。
  - ハッシュ値を与えられても、データの側は作り出せない。一方向。
  - 署名 (上記) の際、データ自体ではなく、ハッシュ値に対して署名する。



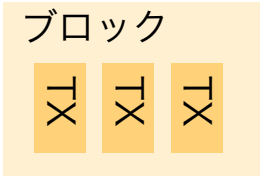
ブロックチェーンのデータ構造

- トランザクション (TX と略記)　　お金の動き



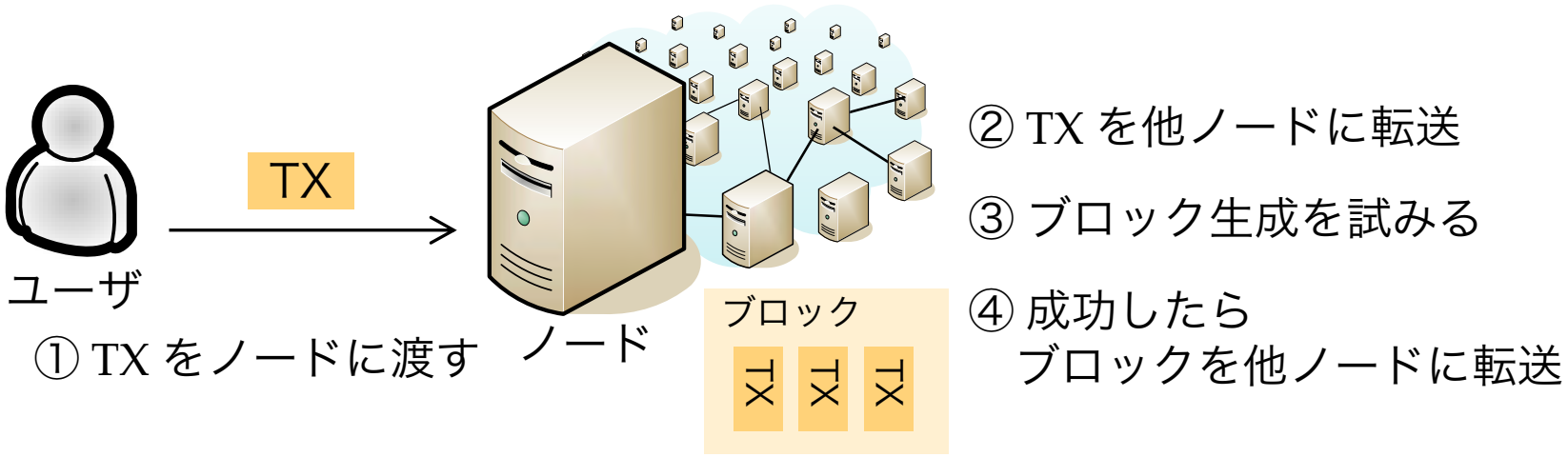
  - 自分に使用の権限があることや、確かに自分が発行した TX であることは、署名 (前項) で示す。
  - TX を矛盾 (二重使用) なく連鎖させていく。

- 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

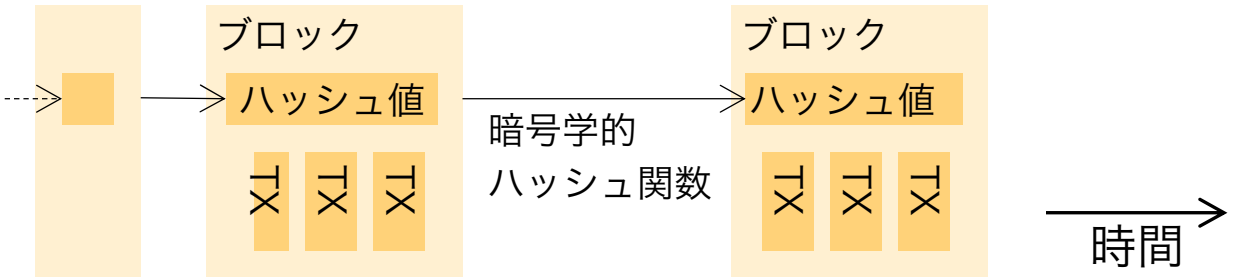


- ① ユーザが TX をノードに渡す。
- ノード群は
  - ② 受け取った TX を他ノードに転送する。
  - ③ TX 群をブロックにまとめて、ブロック生成を試みる。
    計算競争 = Proof of Work (PoW) に勝つと生成できる。
    ④ ブロック生成に成功したら、他ノードに転送する。

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



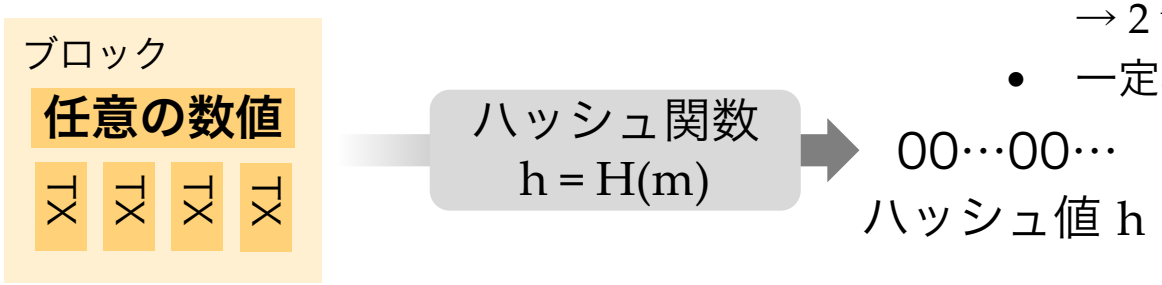
  - 各ノードは最新ブロックの次を生成しようとする。
    生成は容易ではない (次項：計算競争)。
  - TX を改ざんするには、
    後続ブロックすべてを作り直さねばならない。
    しかし、作り直しはほとんど不可能 (次項：計算競争)。
    → 改ざん困難

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

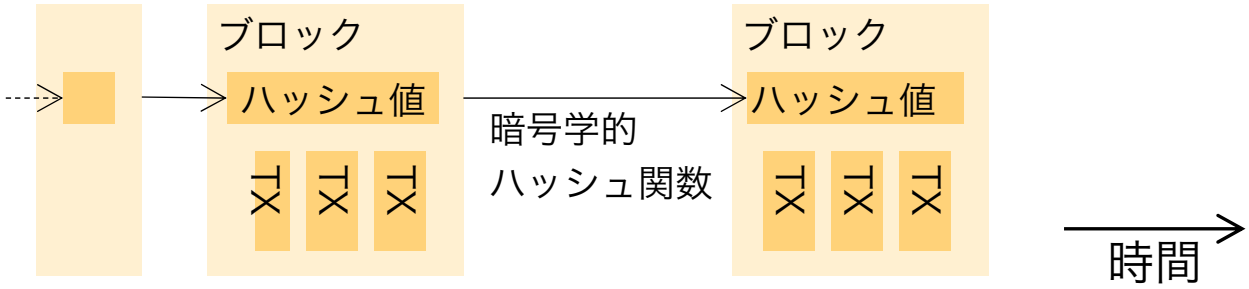
- ブロック中の、任意に決めてよい部分を変更して試しまくる
- ハッシュ値は乱数のようなもの
  → 2^n 回に 1回、成功する
- 一定期間ごとに難易度 n を調整する



  - 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

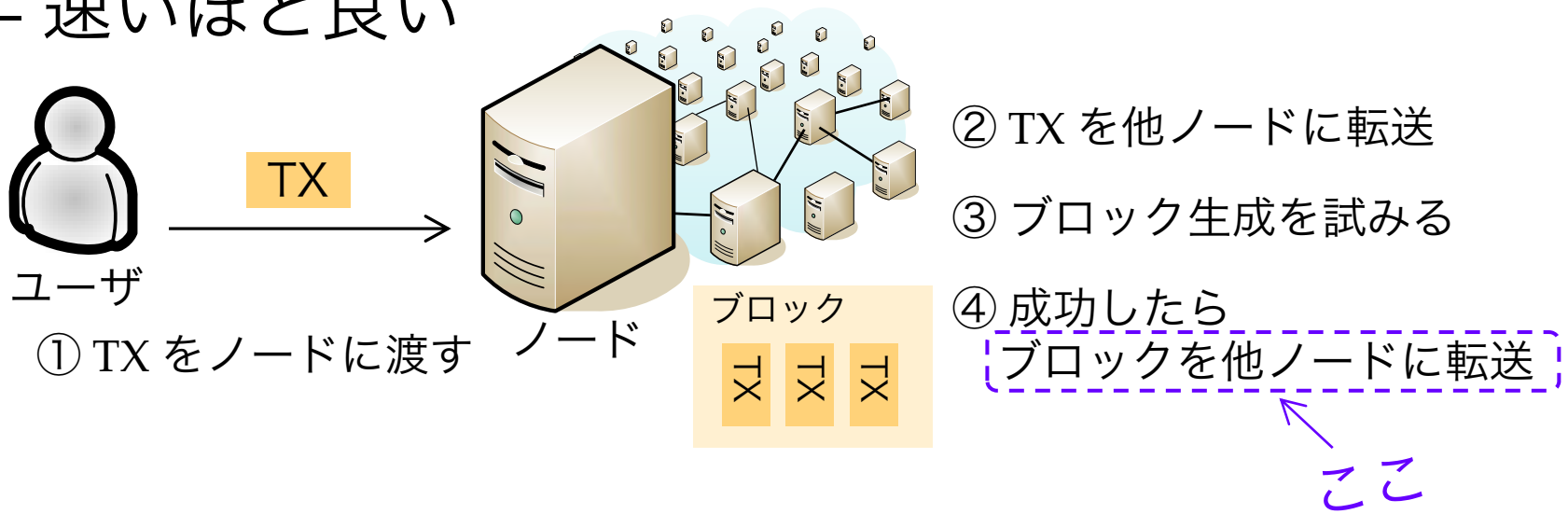
専用チップを
山のように並べる

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「ネットワーク」

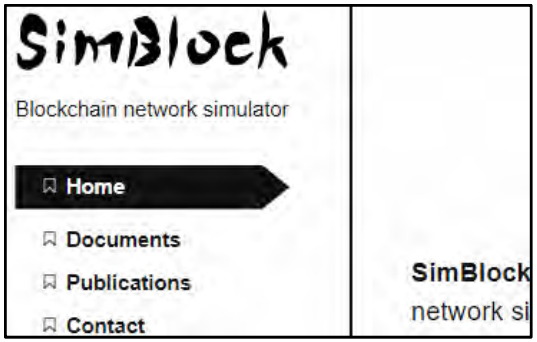
- ブロック転送・伝搬の速さが**性能** (TX / 秒) と**安全性**に影響する
  - 速いほど良い



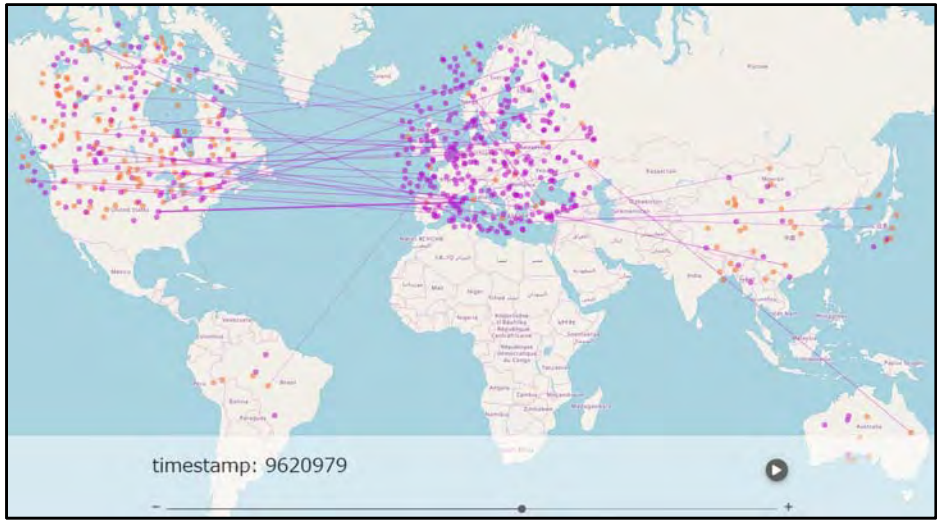
- 実地での研究はほとんど不可能
  - ソフトの変更版を 1万ノードに使わせることは不可能
- そこで…

シミュレータ SimBlock

- ブロックチェーン「ネットワーク」のシミュレータ
  - By 首藤研, 2019/6/27 公開



ウェブサイト



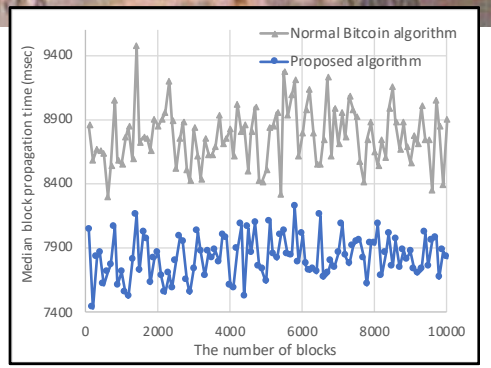
Visualizer
https://dsg-titech.github.io/simblock-visualizer/

  - インターネットとブロックチェーンを模擬
    - ブロックチェーン (Bitcoin, Litecoin, Dogecoin)：ブロックのサイズ, ブロック生成間隔, …
    - インターネット：帯域幅, 通信遅延

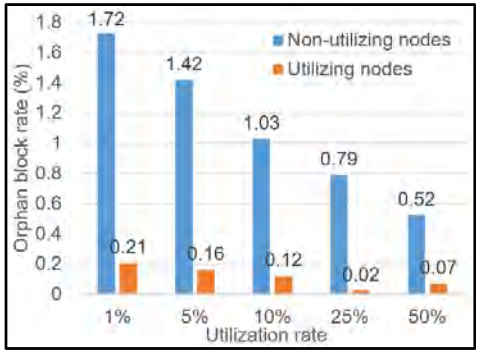
ブロックチェーン「ネットワーク」の研究

説明し切れませんが
雰囲気だけでも

- 隣接ノード選択 (2018)
  - 速いノードを選んでつながっておくと、ブロックが速く伝搬する。



- 伝搬時間 推定 (2017 ～ 2019)
  - ノード間のブロック伝搬時間を、測らず、推定する。隣接ノード選択等に活かす。
- リレーネットワークの効果測定 (2018 ～)
  - ブロック伝搬専用ネットワークである リレーネットワークをシミュレート。効能を測定。



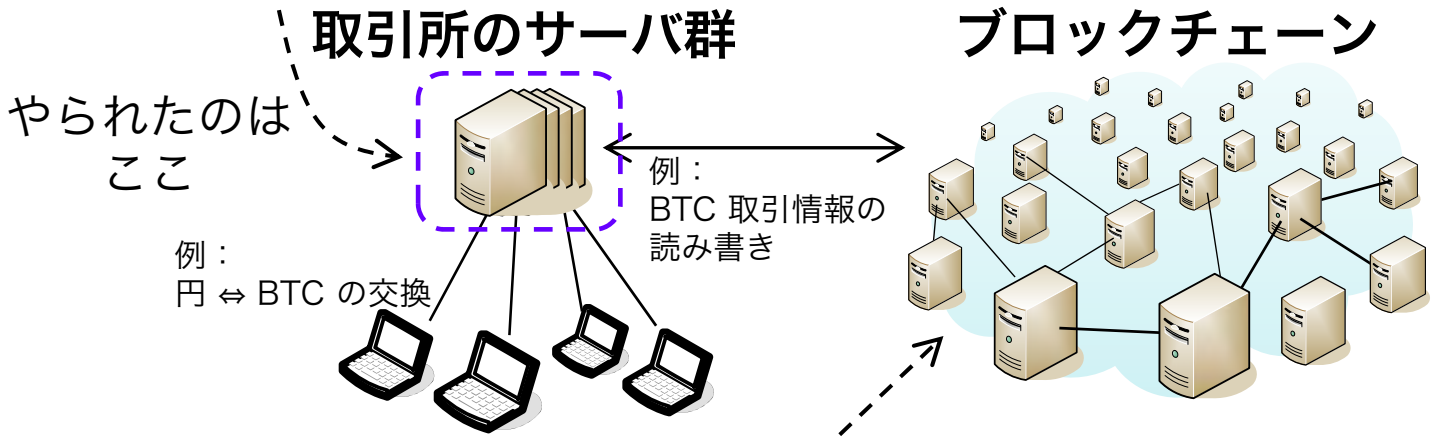
- 攻撃への対抗策とその効果測定 (2019 ~)
  - 例：攻撃手法 selfish mining と対抗策 GHOST をシミュレート。

より**高性能**、より**安全**なブロックチェーンへ

暗号通貨・ブロックチェーンと
社会

盗難事件

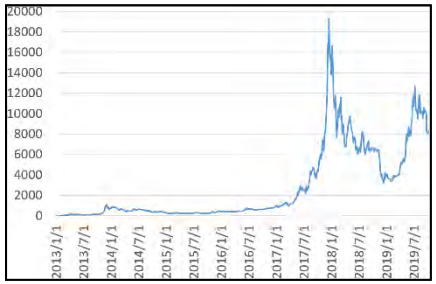
- 盗まれまくってる…
  - 2018年 1月 コインチェック社　　580億円
  - 2018年 9月 テックビューロ社 (Zaif)　70億円



- 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
- 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

Libra / リブラ by Facebook 社

2019年 6月 18日(火) 発表, 2020年 開始予定

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、ブロックを作れるのは協会メンバのサーバ群のみ。
    5年以内に、誰でも。
- 2020年開始予定だが、**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？
  - 予定されていた創設メンバ 5社、離脱。
    - Visa, Mastercard, Stripe, eBay, PayPal → 大手 決済企業が不在に。

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

Web3 ≒ 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)

- Web3 ≒ 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