

京都工業会 ブロックチェーンセミナー
2025年 3月 11日(火)

暗号通貨と それを支える ブロックチェーン

首藤 一幸

京都大学

bit.ly/shudo20250311



Kyoto U.

首藤 一幸 (51)

しゅどう かずゆき



魔法のようなソフト

大規模
分散システム

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 

2023/ 4 未踏アドバンスト PM

2018/11 (株)アーリーワークス 顧問

2019/ 1 Miraise (シード特化ファンド) メンター

2022/ 7 GMOインターネットグループ(株) 技術顧問

2022/10 GMO AI & Web3(株) 顧問

2024/ 6 メルカリR4D 研究開発アドバイザリーボード

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, ネット100個中 10個執筆

P2P のアルゴリズム, 2009 ~

構造化オーバーレイ / 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, 分権性, 公平性

2025年 3月

講演の概要

- ブロックチェーンの 起源・価値 p.3 ~
 - 暗号通貨, Bitcoin
 - トラストレスに二重使用を防止
- ブロックチェーンの 基礎 p.14 ~
- ブロックチェーンに基づく
イノベーション p.24 ~
 - スマートコントラクト, DeFi, DAO
- ブロックチェーンと 社会 p.29 ~
 - 盗難事件, 通貨, Libra
- まとめ p.35



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

cryptocurrency

または仮想通貨, 暗号資産

crypto asset

- デジタルなお金は、いろいろある。

- Suica, PASMO, PayPay, ○○ポイント, ...



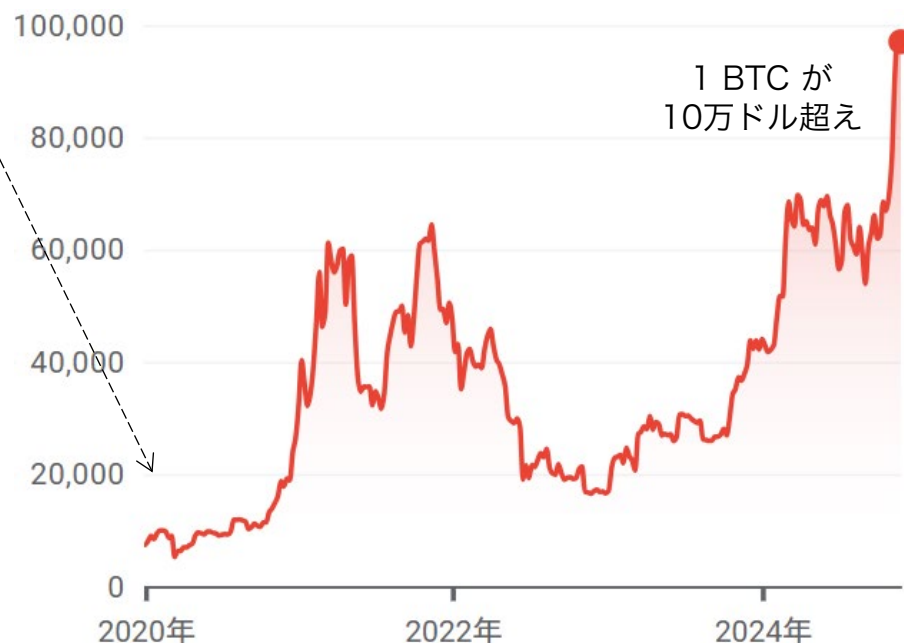
2万種類以上あるとか

- 暗号通貨** : Bitcoin (BTC), Ethereum (ETH), Ripple (XRP), ...

- Bitcoin に端を発する、**非集中的** (後述) なもの

- Bitcoin 時価総額 250兆円 「通貨」になりたいが現状「資産」

Bitcoin (1 BTC) 価格



暗号通貨の起源

- 2008年の論文

ネットで見つかる。
和訳も見つかる。
眺めるのもいいのでは？

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

Satoshi Nakamoto
が誰なのかは、
今日に至るまで不明

Bitcoin v0.1 released

Satoshi Nakamoto [satoshi at vistomail.com](mailto:satoshi@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.

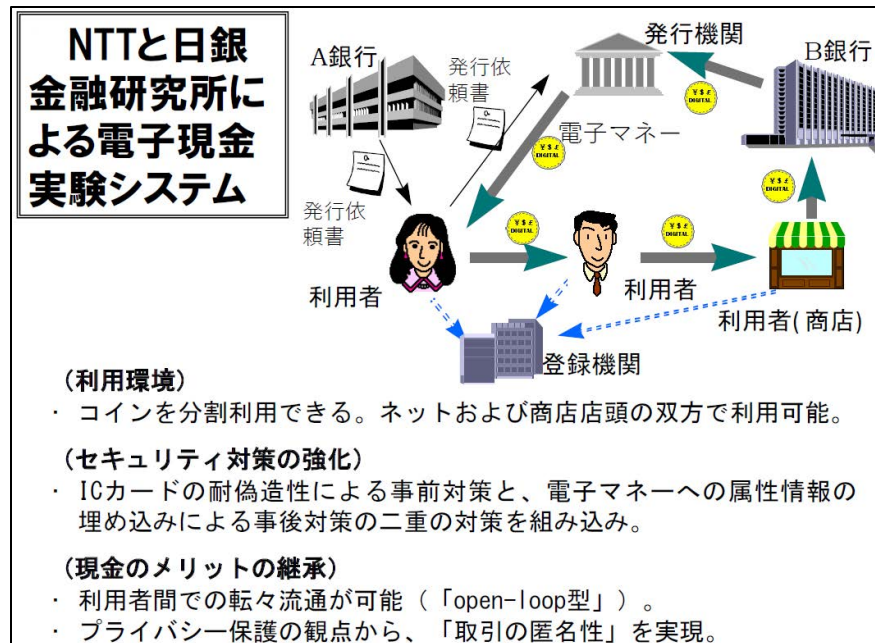
See bitcoin.org for screenshots.

Download link:

<http://downloads.sourceforge.net/bitcoin/bitcoin-0.1.0.rar>

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

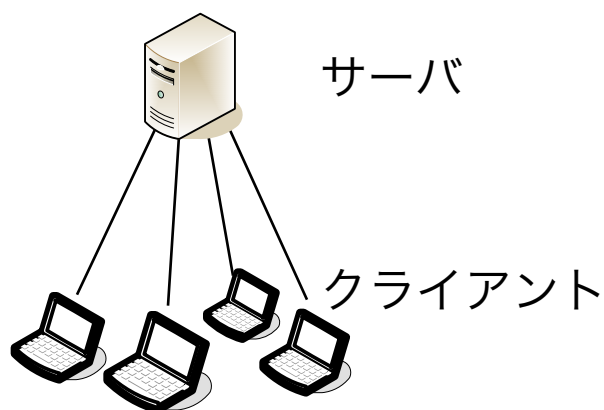
- SUICA / スイカなんかすごい。
 - 8,000万枚 (2020/12), 200ミリ秒 (要求仕様), 平均 105件/秒 (2019/8/2)
 - 集中的な仕組みでこの性能を出すために、様々な工夫

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

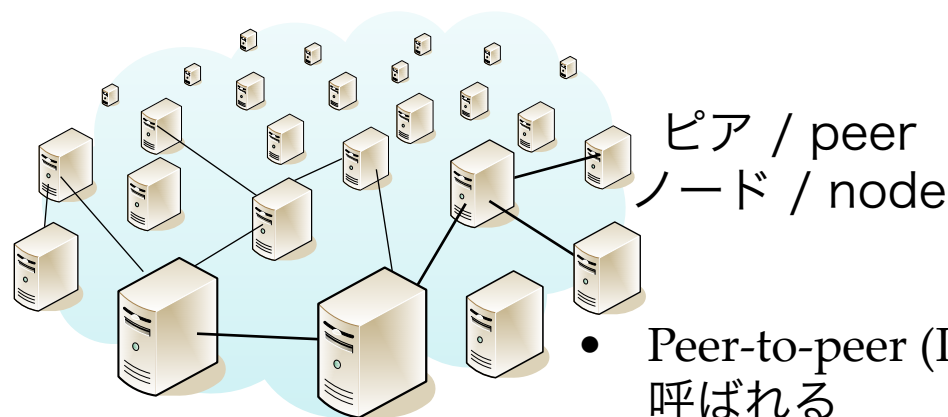
– 非集中 ⇔ 集中 / centralized

- 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

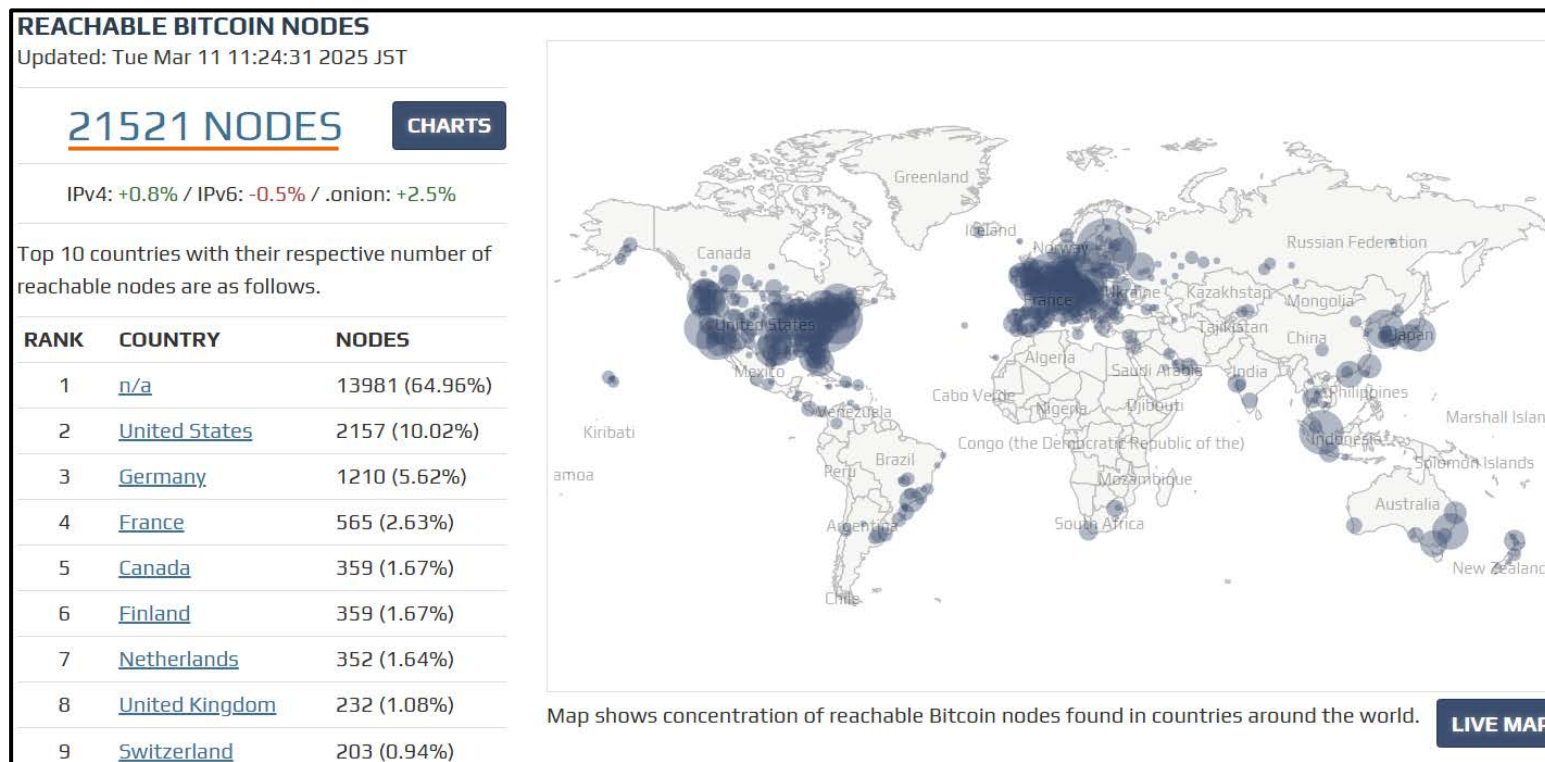


非集中
分散システム

- 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

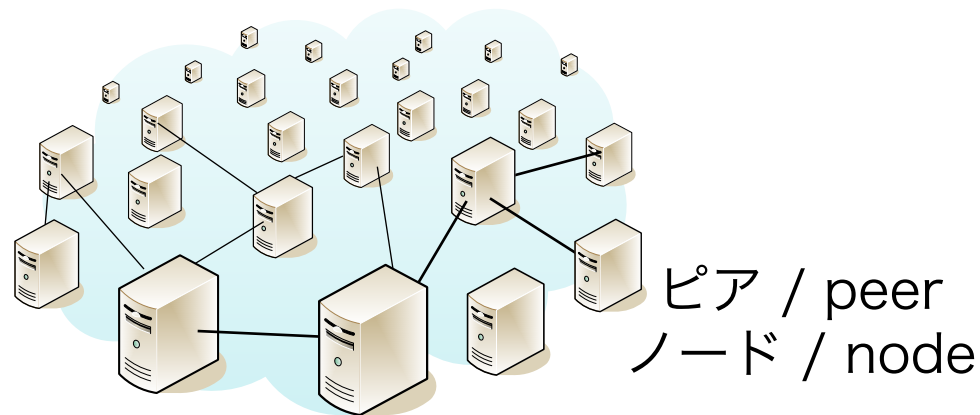


<https://bitnodes.io/> より

- **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



非集中 分散システム (peer-to-peer)



- 誰かを信用する必要がない → 「^{トラストレス}trustless」
 - 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

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

耐故障性

fault tolerant

- 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

● 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

permissioned
blockchain

● 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

パブリック

ブロックチェーン向け

プライベート, コンソーシアム

ブロックチェーン向け

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

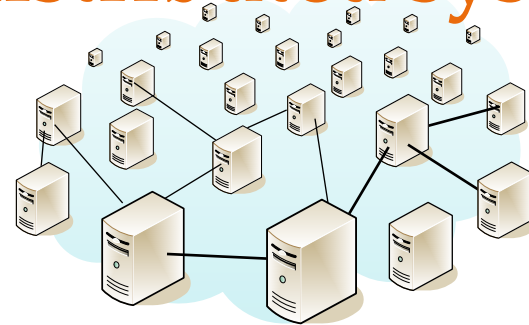
- 支える技術：

暗号理論 /
cryptography



公開鍵暗号方式, 署名,
(暗号的) ハッシュ関数,
乱数生成方式, ...

分散システム /
distributed systems



首藤の専門

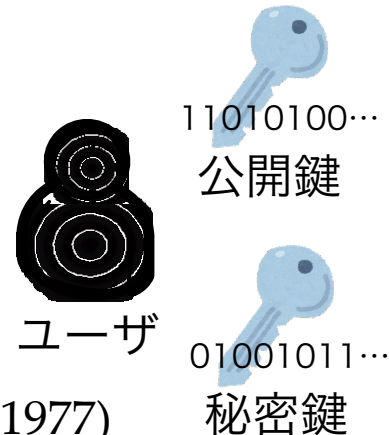
peer-to-peer ネットワーク,
flooding, 複製, 整合性,
分散合意アルゴリズム, ...

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

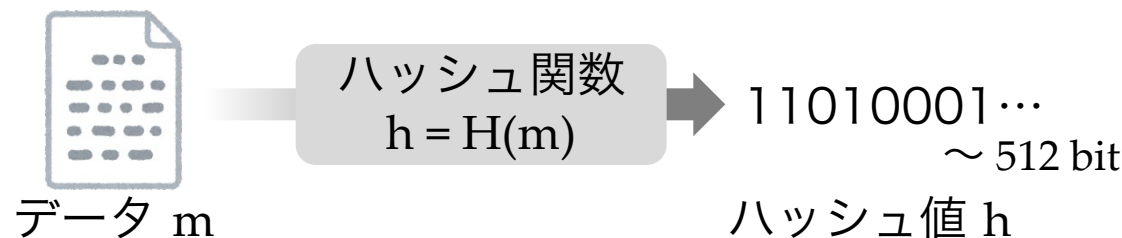
- 1人が2つの鍵を持つ：秘密鍵と公開鍵。
一方で暗号化、もう一方で復号。
- 秘密鍵で署名。公開鍵で検証。なりすましを防げる。
- 一方向性関数に基づいて構成する。

例：大きな整数の乗算は容易、因数分解は大変 → RSA 暗号 (1977)



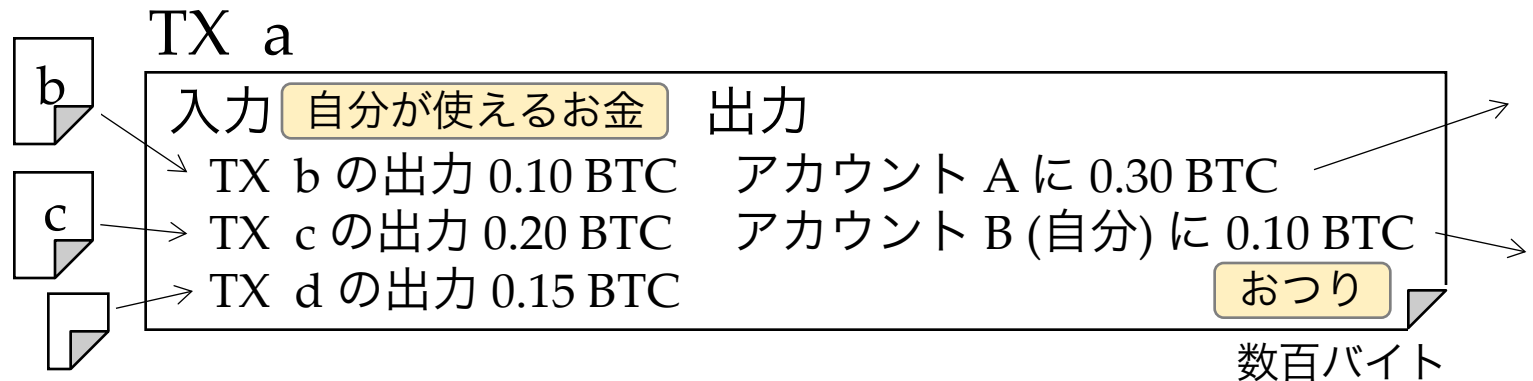
● (暗号学的) ハッシュ関数

- 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。

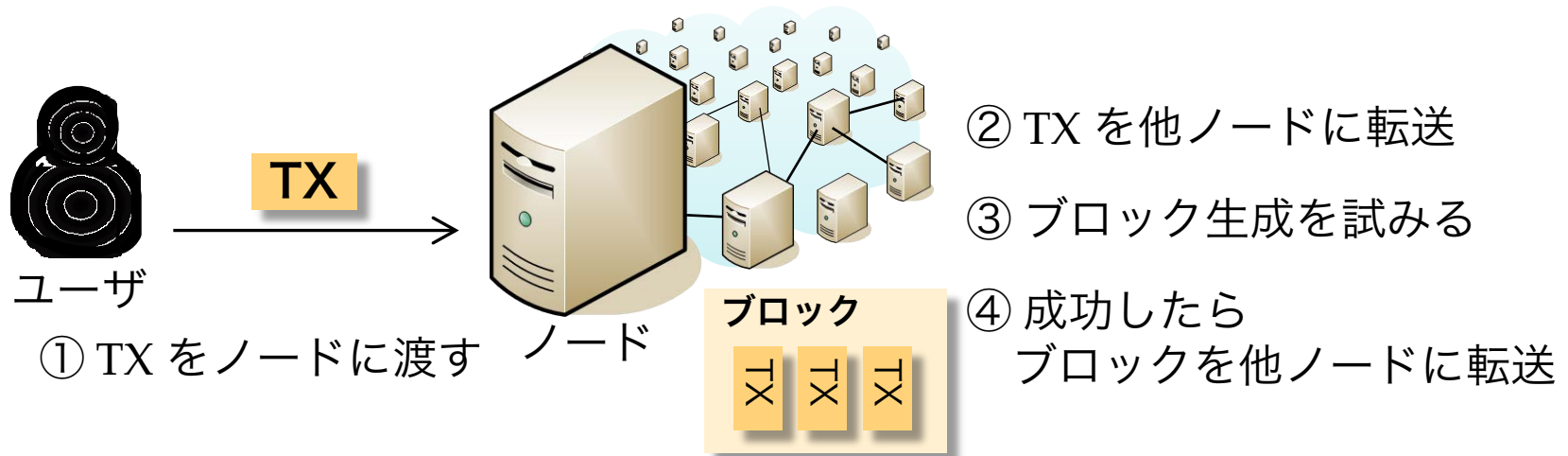
• ブロック

ブロック



- TX をたくさんまとめたもの。1 MB (メガバイト) くらい (Bitcoin)
- 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。
- 次ページ 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。
- 2ページ後

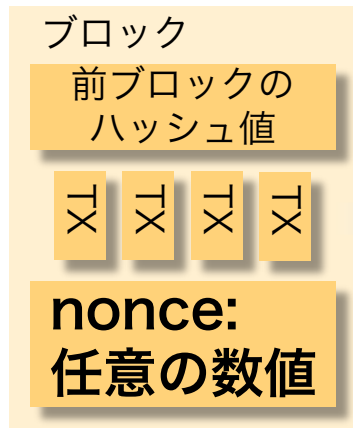
ブロック生成の計算競争

● 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：

数値として n より小さなハッシュ値を出せ



暗号的
ハッシュ関数
 $h = H(\text{ブロック})$

00...00...
ハッシュ値 h

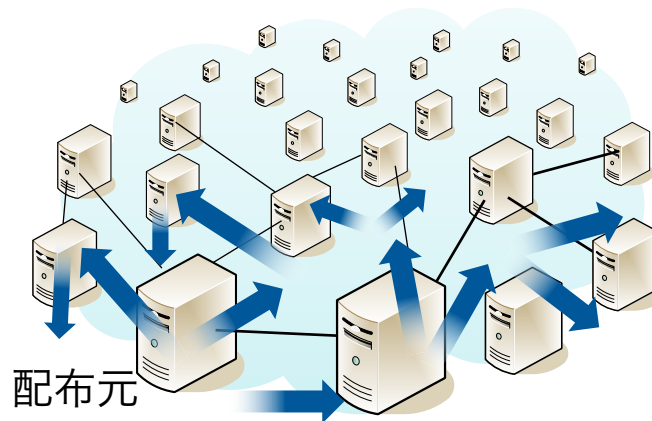
- ブロック中の、任意に決めてよい部分を変更して試みまくる
- ハッシュ値は乱数のようなもの
→ ごく稀に、成功する
- 一定期間ごとに難易度 n を調整する

① TX をノードに渡す

- 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。

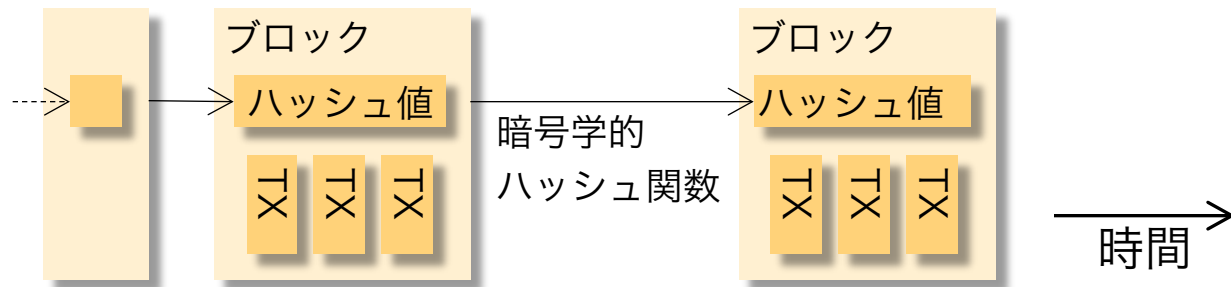


配布元
ノード (サーバ) のネットワーク

- 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**

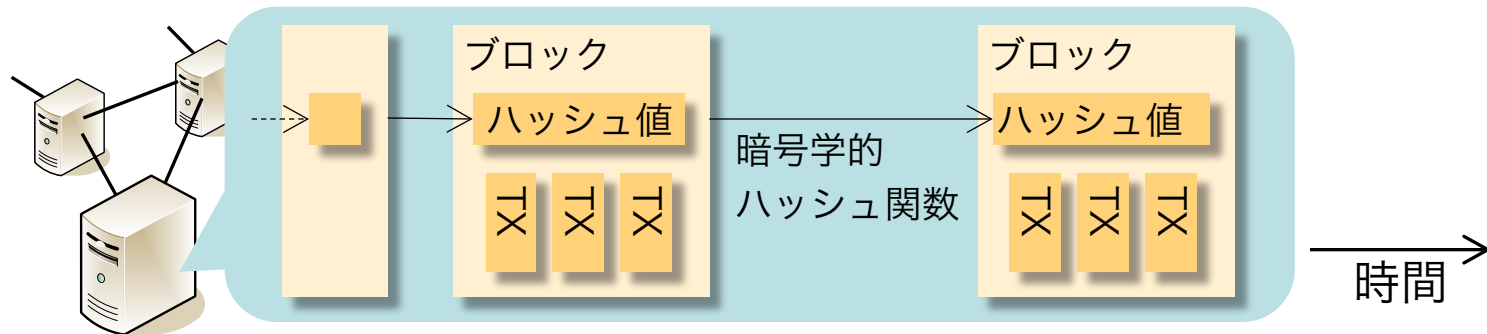


- 各ノードは最新ブロックの次を生成しようとする。
生成は容易ではない (次項：計算競争)。
- TX を改ざんするには、
後続ブロックすべてを作り直さねばならない。
しかし、作り直しはほとんど不可能 (次項：計算競争)。
→ **改ざん困難**

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

- 原発 ○ 個分の消費電力

マイニング専用データセンタ

<https://imgur.com/a/CcIhX> より

→ 電力を食わない Proof of Stake (PoS) がそろそろ実用
e.g. Ethereum は 2022年 9月、PoW から PoS に移行した



ブロックチェーンに基づく イノベーション

- 様々なイノベーション
- スマートコントラクト, DeFi, DAO, ...

様々なイノベーション

- 暗号通貨 Bitcoin (2008)
- スマートコントラクト Ethereum (2014)
- 数多のトークン / コイン ERC-20 仕様 (2015)
- NFT ERC-721 仕様 (2018)
- DeFi Uniswap (2018), ...
- DAO 定義 (2014) → The DAO (2016) → ...
- Web3 用語 (2014) → 反 Big Tech → 投資の標語

スマートコントラクト

- ブロックチェーン上で動作するプログラム

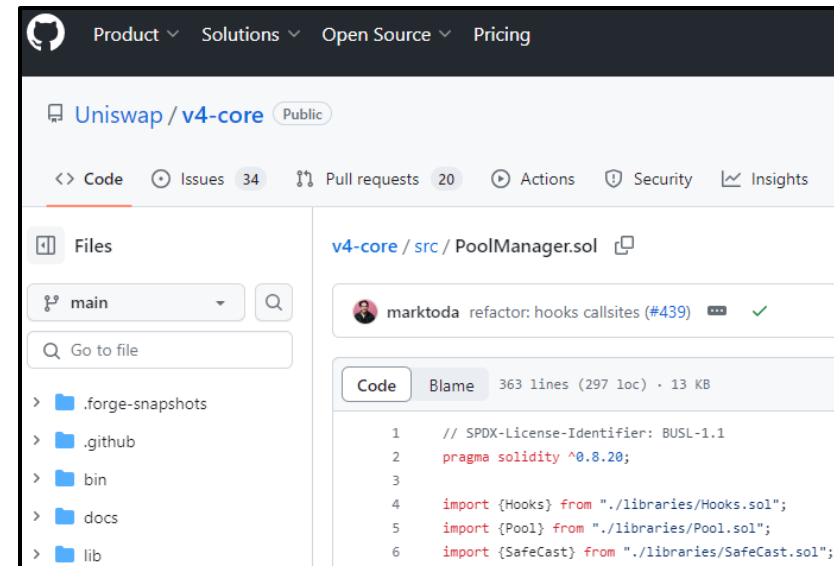
- 全ノードが同一の処理をする。
無駄っぽいけど、これによって不正を防いでいる。
- ブロックチェーン上のデータ、つまり資産を扱える。



- **Ethereum** (2014 ~) が導入

- Solidity 言語などで記述,
EVM (Ethereum仮想マシン) で実行
- おそらく、Bitcoin Script
から着想

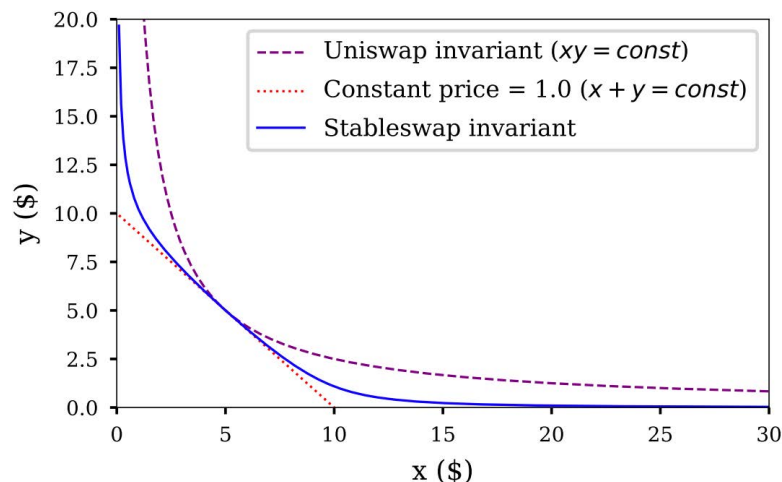
- DeFi, DAO など様々な
イノベーションの基盤



DEX (分散型取引所) である Uniswap のソースコード in Solidity 言語

DeFi (Decentralized Finance) / 分散型金融

- スマートコントラクトを用いて
様々な金融サービスを実現する試み
 - 取引所 (両替), 証券, 保険, デリバティブ, 貸借 (銀行), ...
- 代表例: DEX / 分散型取引所 Uniswap 等
 - スマートコントラクトが自動で両替



金融庁 (当時) 三輪さんの講演
2019/10/10(木) Devcon 5 にて

AMM (Automated Market Maker) の数式

DAO (Decentralized Autonomous Organization)

- Ethereum 創設者の 1人 Vitalik Buterin が提唱
 - 2014年 5月のブログ "DAOs, DACs, DAs and More: An Incomplete Terminology Guide"
 - コンピュータによる自動運営組織 (が人間を使う)
- 提唱
 - コンピュータ**プログラムが運営**する組織
 - LLM に「目的」を与えたら、けっこうできちゃいそう。さらに「センサ」と「アクチュエータ」を与えて、うまいこと実世界（めいた場所）で学習させたら、汎用人工知能 (AGI) に？
- 今日
 - 株式会社ならぬ、**トークン会社**。
 - 株式の代わりに、**特別なトークン（コイン）の持ち分に応じて、意思決定していく組織**



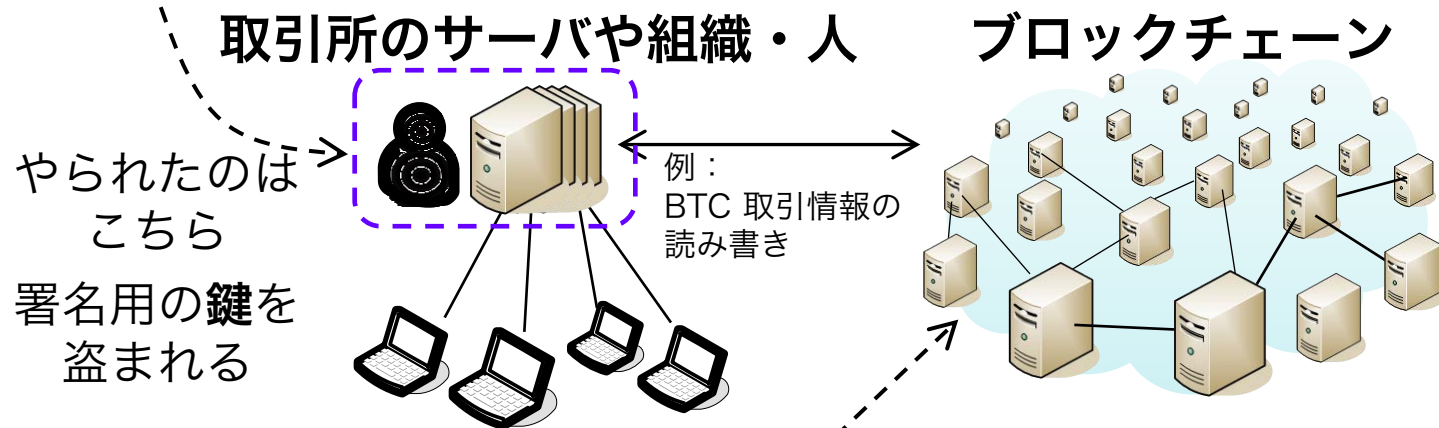
ブロックチェーンと 社会

- 盗難事件, 通貨, Libra, ...

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
- 2024年 5月 DMM Bitcoin社 480億円
- 2025年 2月 Bybit社 2,100億円



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/>

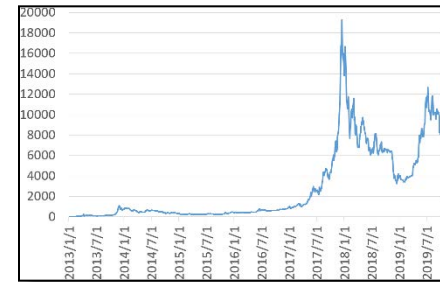
インセンティブ不整合問題: <https://bit.ly/32nvDbI> (首藤 論文)

【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。-->



- 解決案：ステーブルコイン / stablecoin BTC 価格の推移
 - 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

- 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
 - ステータブルコイン
 - 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

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이블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 → 2022年 1月 31日 サービス提供断念

- 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이블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

トラストレスが導く イノベーション

35 / 35

- ブロックチェーン周辺の 様々なイノベーション
 - 暗号通貨 Bitcoin (2008)
 - スマートコントラクト Ethereum (2014)
 - 数多のトークン / コイン ERC-20 仕様 (2015)
 - NFT ERC-721 仕様 (2018)
 - DeFi Uniswap (2018)
 - DAO 定義 (2014) → The DAO (2016) → ...
 - Web3 用語 (2014) → 反 Big Tech → 投資の標語
- Bitcoin が、もし、トラストレスでなかったら？ ※
 - Satoshi Nakamoto が管理・発行するただの電子マネーだったら、誰も買わなかっただろう。
 - 無名の個人、悪いことするかもしれないし、ミスするかもしれない。
 - トラストレスという性質が、国や大組織にしかできなかったことを **個人にまで開放**した。

参照：記事「トラストレスのメカニズム」, 情報処理, 2023年 1月号

<http://www.shudo.net/article/202301-IPSJ-trustless/>