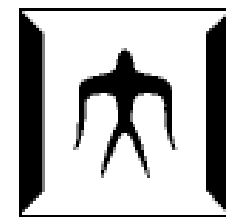


モビリティ変革コンソーシアム
第10回 テーマ勉強会
2020年 8月 31日(月)

ブロックチェーンの 技術と社会

首藤 一幸
東京工業大学

SimBlock



Tokyo Tech

<http://www.shudo.net/publications/202008-lecture-blockchain/>

首藤 一幸 (46)

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 

2018/11 (株)アーリーワークス 顧問

2018/11 (一財) GMOインターネット財団 理事

2019/ 1 Miraise (シード特化ファンド) メンター

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 ~

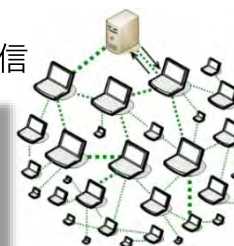
1億ノード / 10台, 既存手法の20倍の性能, Apache Spark 上

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 ~

Overlay Weaver



魔法のようなソフト

大規模
分散システム

2020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

- 応用

- 通貨やトークン追跡、自己主権型アイデンティティ、...
- 応用の検討

- 技術

- トランザクション承認方式
- 東工大 首藤研の取り組み

- 社会：現在 ～ 未来

- 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

起源：暗号通貨 Bitcoin

Cryptocurrency

- 3,000 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 23 兆円が載っている

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？

- 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: 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.

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.

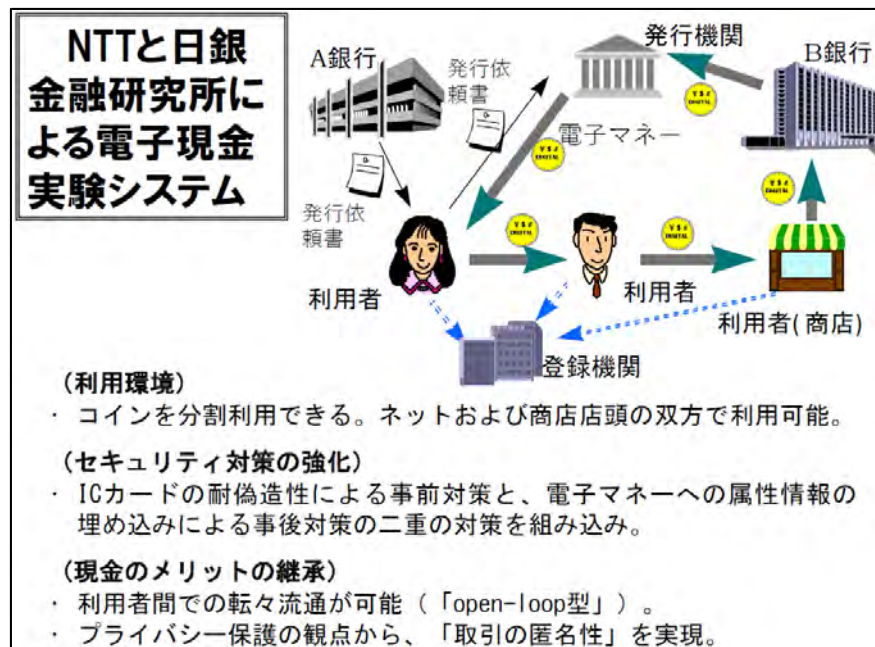
See bitcoin.org for screenshots.

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

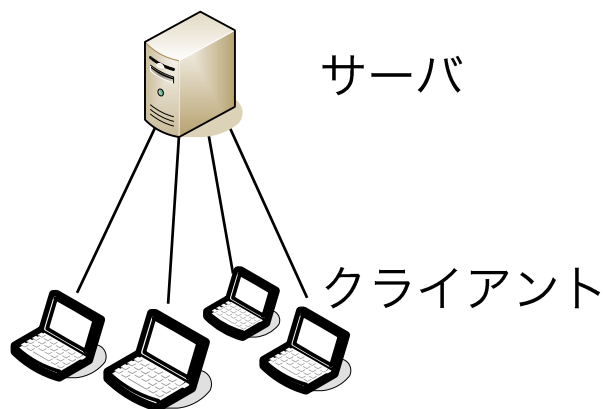
- SUICA / スイカなんかすごい。
 - 8,000万枚 (2020/12), 200ミリ秒 (要求仕様), 平均 105件/秒 (2019/8/2)
 - 集中的な仕組みでこの性能を出すために、様々な工夫

Bitcoin の技術は何が違ったか？

- 非集中的 / decentralized に
二重使用 / double-spending を防止した

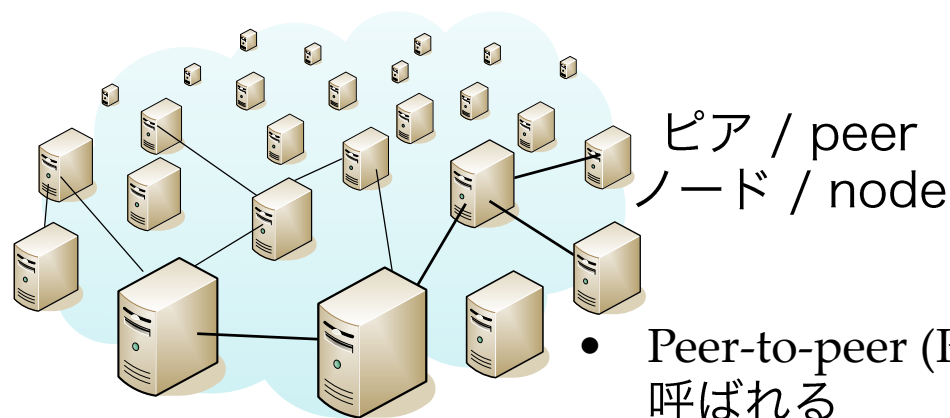
– 非集中 ⇔ 集中 / centralized

- 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

• 約 1万ノード

- 他のノードと直接通信しない裏のノードや
Tor 越しの (いわゆるダークウェブ上) ノードを含めると、数万？

GLOBAL BITCOIN NODES DISTRIBUTION

Reachable nodes as of Sun Aug 16 2020
18:40:55 GMT+0900 (日本標準時).

10485 NODES

24-hour charts »

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

RANK	COUNTRY	NODES
1	n/a	2719 (25.93%)
2	United States	1881 (17.94%)
3	Germany	1755 (16.74%)
4	France	576 (5.49%)
5	Netherlands	437 (4.17%)
6	Canada	294 (2.80%)
7	Singapore	253 (2.41%)
8	United Kingdom	245 (2.34%)
9	Russian Federation	220 (2.10%)
10	China	174 (1.66%)



12. Japan

141

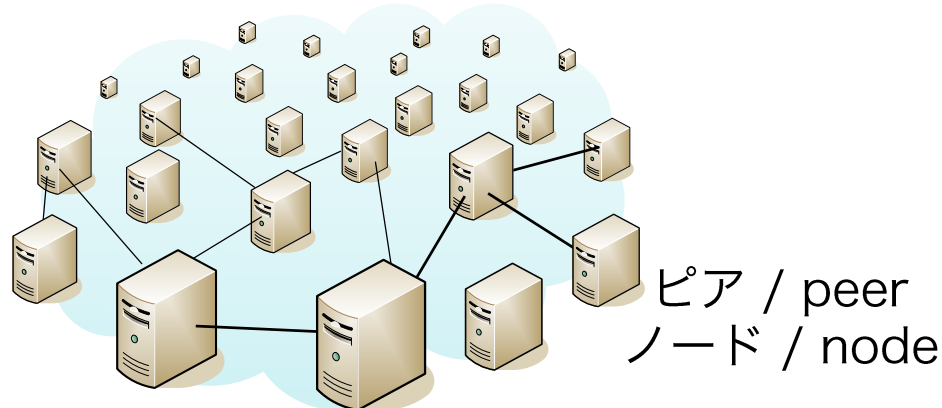
<http://bitnodes.earn.com/> より

トラストレス / trustless

- 非集中 / decentralized



- 誰かを信用する必要がない → 「**trustless**」
 - 政府, 銀行, 企業, ... 等を信用する必要がない。 トラストレス
 - 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。



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

← 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

 **bitcoin**


ethereum

● 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

 **HYPERLEDGER
FABRIC**

● 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 応用

- 通貨やトークン、追跡、自己主権型アイデンティティ、...
- 応用の検討

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이블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.11) 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 <u>されない</u>	価値流通の仕組みを簡単に 作れる	価値の <u>トレーサビリティ</u> 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ィ (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) ⑦ IoT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)

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

- 他に、IBM TradeLens (貿易追跡プラットフォーム)
 - HyperLedger Fabric で運用 → プライベート or コンソーシアム

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

17 / 35

- 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)



応用の検討

● 発想

- ブロックチェーンの価値 (p.11) から考える
- 「台帳」から考える
- (もちろん) 類似事例から考える

● 条件

- 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、NoSQL の方が優れている：性能、容量、...
組み合わせるのがよい。
 - 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
- 東工大 首藤研の取り組み

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

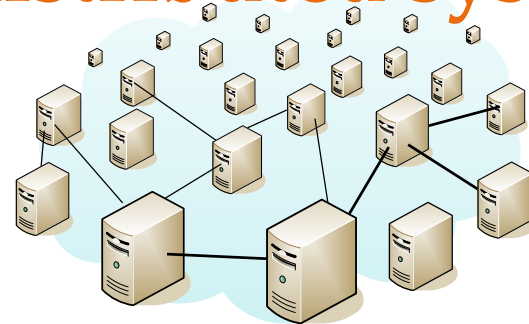
- 支える技術：

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, ...

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？

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

パブリック
ブロック
チェーン
向け

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)

PBFT (悪意ノード 1/3 未満で)

Istanbul BFT (IBFT)

LibraBFT (based on HotStuff)

なし Raft
Paxos

プライベート
コンソーシアム
ブロックチェーン向け

Proof of Work (PoW)

Bitcoin の発明

● 不特定多数によるトランザクション承認

12 / 28

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

TX a

入力 自分が使えるお金 出力

TX b の出力 0.10 BTC アカウント A に 0.30 BTC

TX c の出力 0.20 BTC アカウント B (自分) に 0.10 BTC

TX d の出力 0.15 BTC おつり

- 自分に使用する権限があることや、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。

13 / 28

ブロックチェーンの動作

① TX をノードに渡す

② TX を他ノードに転送

③ ブロック生成を試みる

④ 成功したら ブロックを他ノードに転送

- 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。

14 / 28

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

ブロック

ハッシュ値

ハッシュ関数

時間

- 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

15 / 28

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みまくる

ハッシュ値は乱数のようなもの

→ 2^{32} 回に 1回、成功する

一定期間ごとに難易度 n を調整する

ブロック

任意の数値

ハッシュ関数 $h = H(m)$

00...00... ハッシュ値 h

- 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。

説明は割愛

- 特定の誰かを信頼せずとも済む → **トラストレス**

東工大 首藤研での研究

2019年 10月以降の成果

- 「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

攻撃への対策の性能への影響 [高山 2020c]

攻撃への耐性 [Nagayama 2019]



相互に影響

性能

含 実時間性
スケールアウト性

[永山 2020a]

スケールアウト性

[永山 2020b]

プロトコルの効果推定

[Nagayama
2020b]

リレーネットワークの
影響推定

[大月 2020a]

[大月 2020b]

研究手段を
提供



研究手段を提供

ツール

シミュレータ [Shudo 2019]

SimBlock

ブロック・トランザクション エクスプローラ [Taegy 2020]

分権化 / decentralization

手法の影響評価 [高山 2020a]
[高山 2020b]

新アーキテクチャ [Nagayama
2020a]

公平性 / fairness

指標と向上手法 [神田 2020a]
[神田 2020b]
[Kanda 2020]

研究手段を
提供

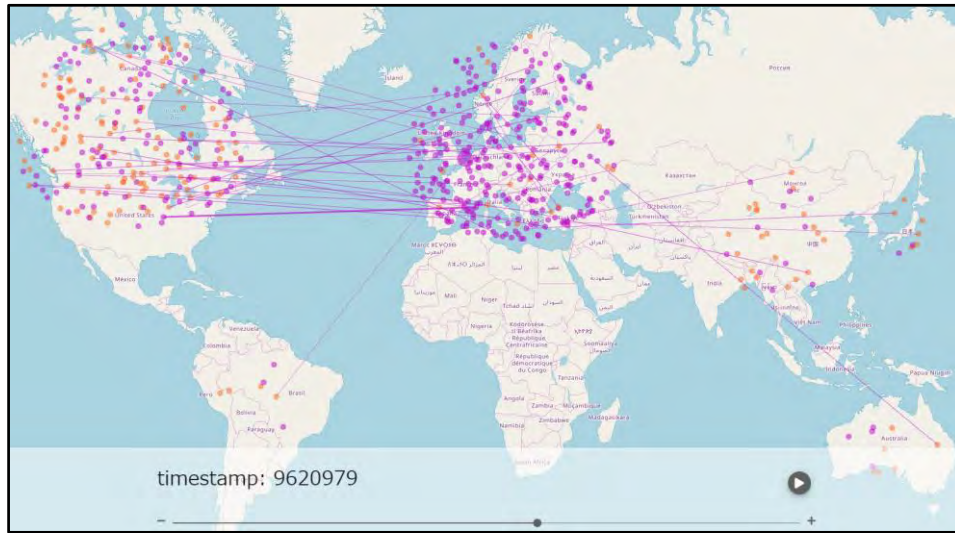


2019年 9月までに取り組んだ研究目標

開発者会議 (Devcon 5) での発表

ブロックチェーン「ネットワーク」シミュレータ SimBlock

首藤研の取り組み

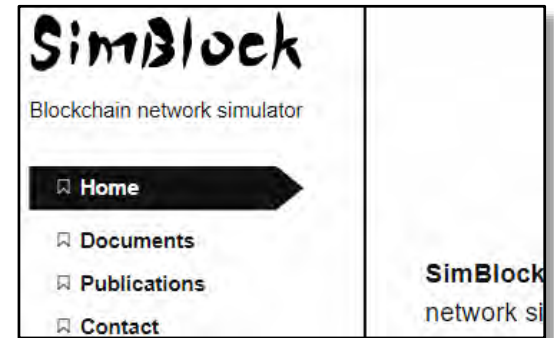


ビジュアライザ 縮小 Bitcoin ネットワーク,
600 ノード



IEEE ICBC 2019 デモ,
ソウル, 2019年 5月

ウェブ
サイト



IEEE Spectrum
記事



LayerX 社と共同研究 2020年 8月～

● Ethereum 2.0 に貢献

LayerX Labs、東京工業大学 首藤研究室とブロックチェーンのコンセンサスアルゴリズムに関する共同研究を開始 -国内外の学術機関とのオープンイノベーションを強化-

2020.8.28





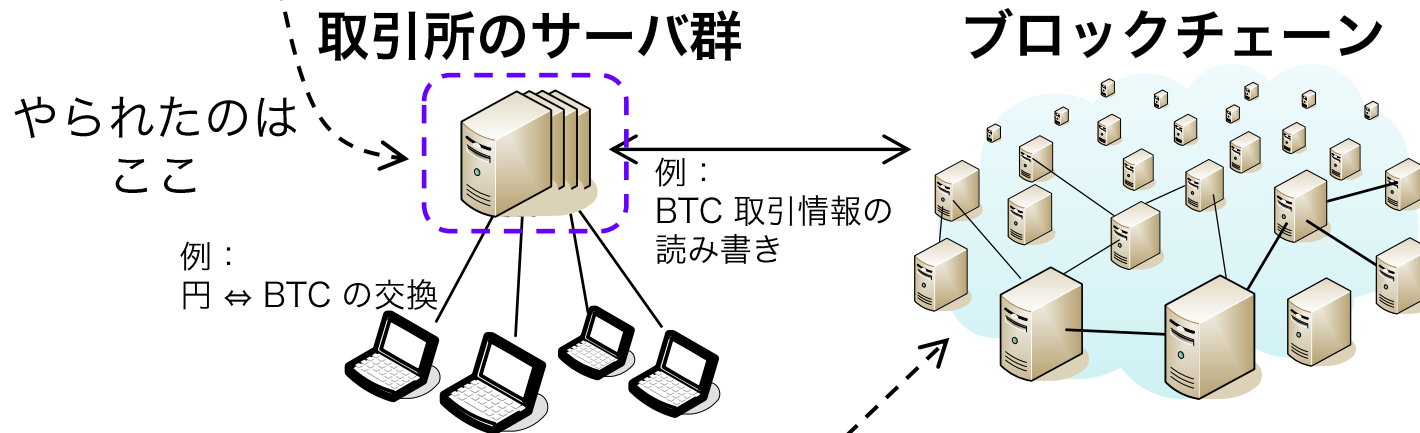
ブロックチェーンと 社会

- 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

New !

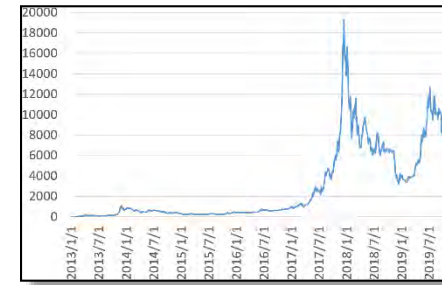
- 51% 攻撃は、金しだい： <https://www.crypto51.app/>
- インセンティブ不整合問題： <https://bit.ly/32nvDbI>

【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。-->



- 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

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。



Libra 協会の
創設メンバ

↓
見合わせ

● 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

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。

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**