いまさら人に聞けないブロックチェーン技術

鈴木 茂哉

慶應義塾大学大学院 政策・メディア研究科 特任准教授

慶應義塾大学 SFC研究所 ブロックチェーン・ラボ

<shigeya@wide.ad.jp>

@ ISOC-JP ワークショップ 2017/10/23

ブロックチェーン技術

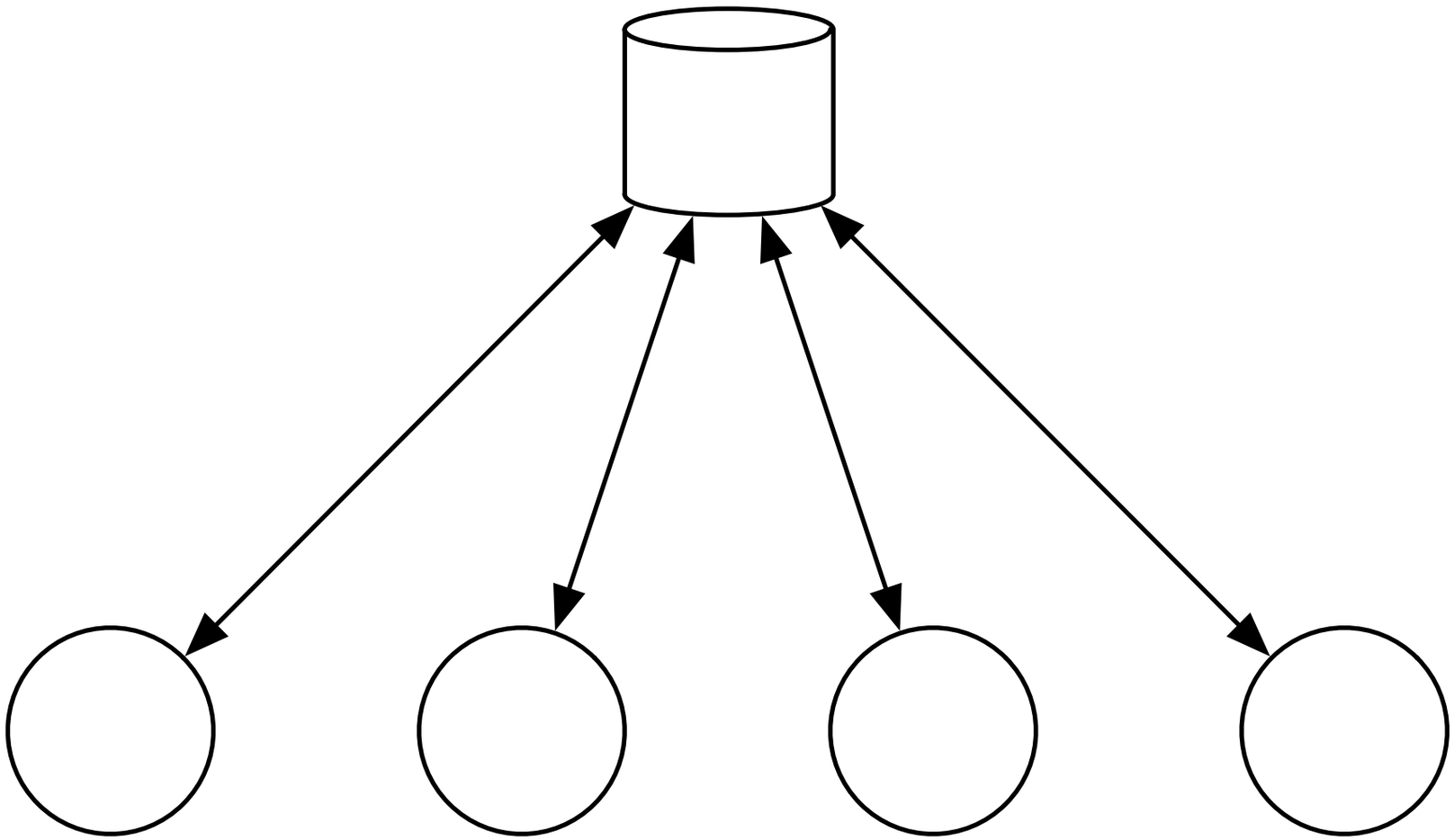
【ブロックチェーン】とは何か

- Blockchain - ブロック チェーン - ブロックの連鎖

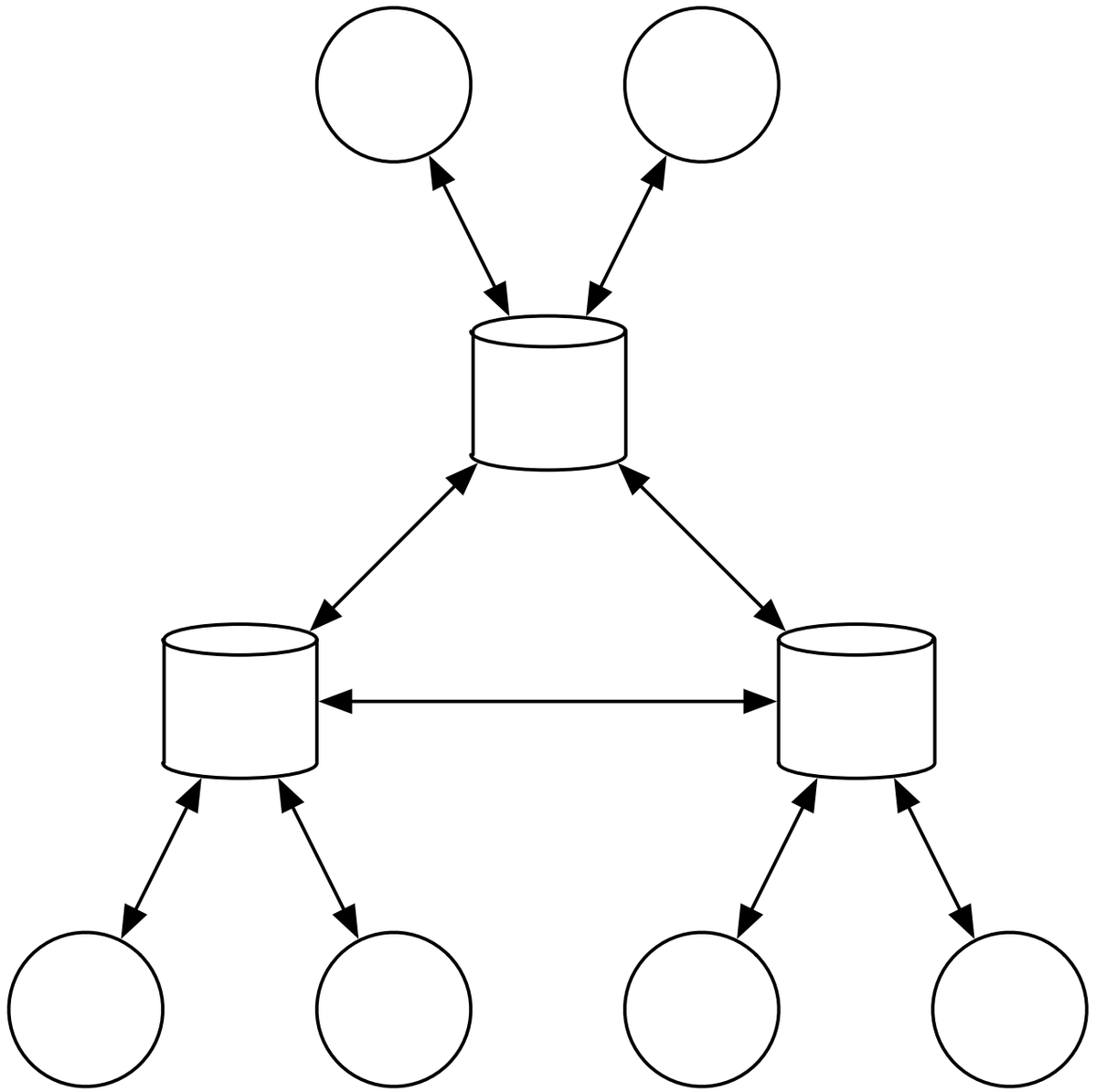
- データベースのデザインの一形態で、以下のような特性を持つ:
  - 完全分散型
  - 中心的な役割を果たす構成要素が不要
  - 信頼できる権限を持つ主体が不要

- 台帳として使う事が出来る

中央集中型のデータベース

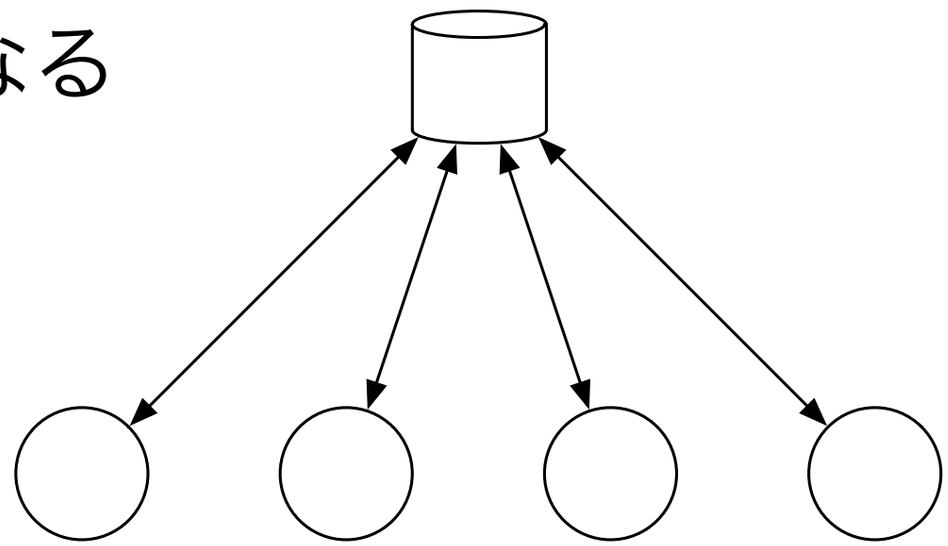


分散型データベース



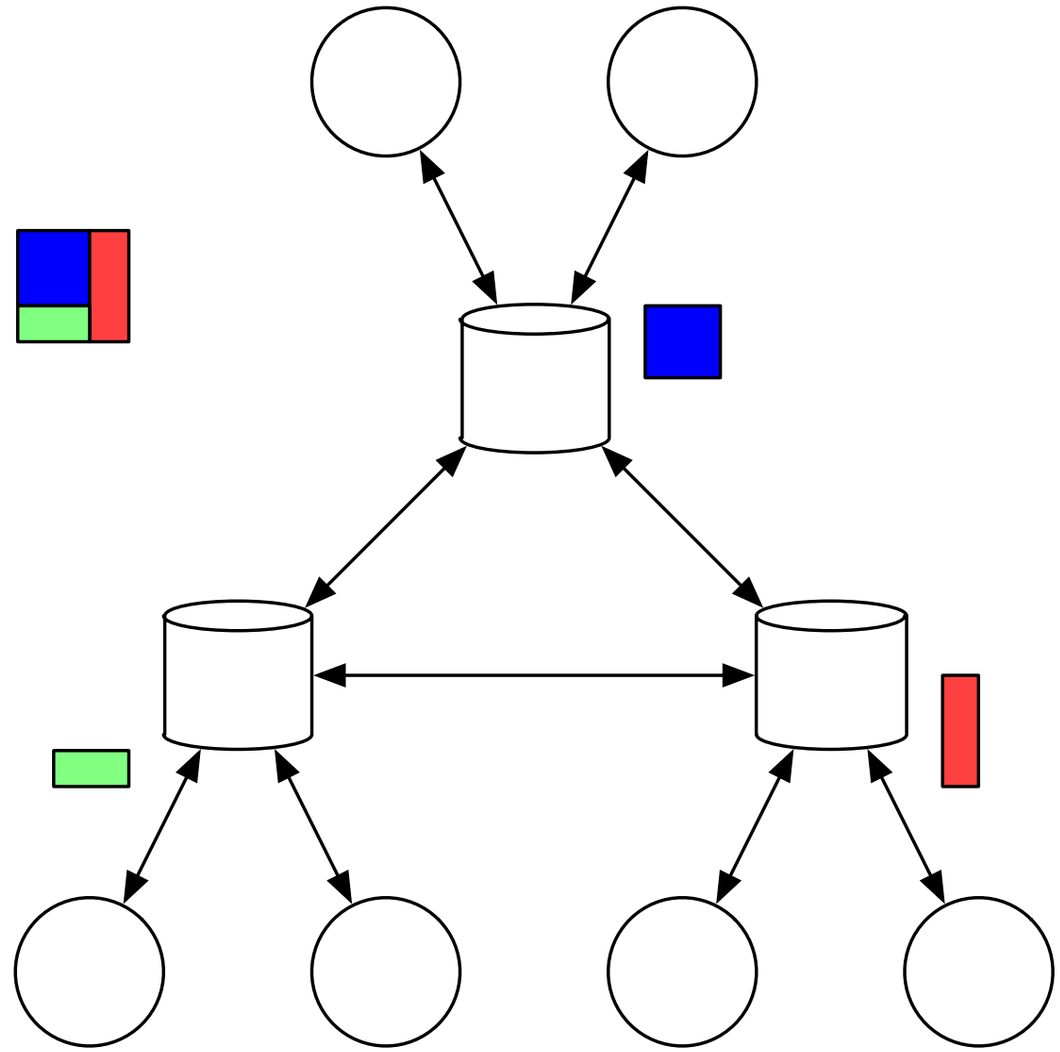
中央集中型データベースの利点と欠点

- 利点
  - 管理しやすい
  - データの所有者を管理しやすい
- 欠点
  - 単一の信頼できる主体が必要となる
  - 単一の障害点



分散型データーベースの利点と欠点

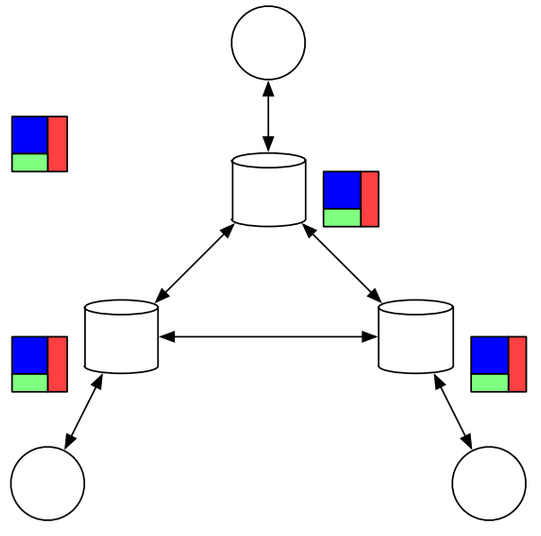
- 利点
  - 高速に処理できる可能性がある
  - 大規模かできる可能性がある
  - 障害などについて強くできる
- 欠点
  - 一貫性を保つのが難しい
  - 取引型の更新が難しい



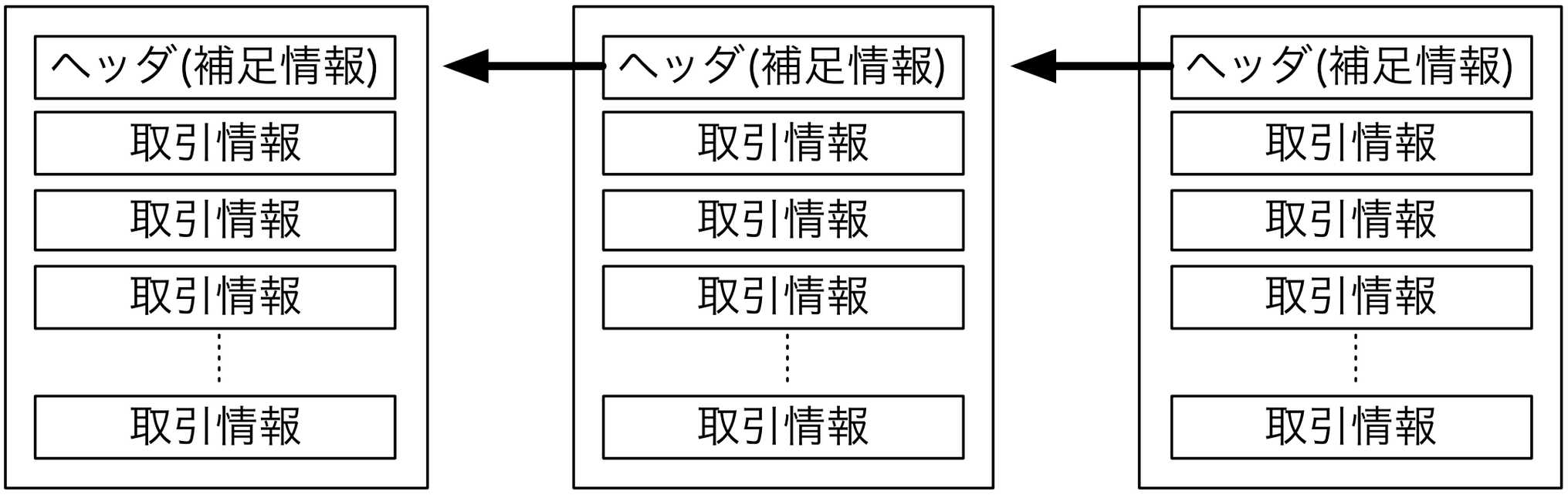
データベースとしてのブロックチェーン

- 分散型であるが、
  - 他のデータベースと異なる特徴を持っている:
    - 全ての参加ノードが、全ての記録を保持する
    - 取引記録は、どのノードで、いつ起きても良い

- 中央管理主体をもたずに、検証され、合意されたデータ記録できる



ブロックのチェーン



Bitcoin

- Bitcoin前: デジタル通貨の開発、Peer-to-Peer システムの研究と発展
  - Wei Dai による b-money (1998)

- Bitcoin についての論文の発表 = **ブロックチェーンの発明**

  "Bitcoin: A Peer-to-Peer Electronic Cash System,"
  Satoshi Nakamoto (2008)

- Bitcoin取引所 MtGox でのトラブル (Feb 2018)

- 今日 2017 年 10月24日 - 約 67万円 / 1BTC

Bitcoinの革新性

- ピアツーピアの **直接的な 価値** の受け渡しを可能とした

- 分散データベースにおいても、二重支払いが起きないことを、信用できる第三者抜きで可能とした

Bitcoinの発明

- "Proof of Work" と呼ばれるメカニズムにより、二つの問題を同時に解決した:
  - **必要充分かつ単純な合意形成メカニズム**の提供により、Bitcoin帳簿に対する更新における合意形成をネットワーク上のノード間で分散された形でできるようになった
  - 合意形成へ参加することが誰によっても可能であるため、**合意形成において誰が影響力を持つのかを決定するという政治的な問題を排除**した

- これを、**単一のメンバリストに記載される**といった参加における**型どおりの**障壁を、合意形成においての、あるノードにおける１票の強さを、そのノードの計算資源の量に直接的に比例する形とする**経済的な**障壁へと置き換えた

Ethereum White Paper から - https://github.com/ethereum/wiki/wiki/White-Paper

Proof of Work

- Proof of Work (PoW)とは、どれだけのハッシュ(SHA256)計算力を証明者が保持しているのかを、ブロックヘッダの一部の値(nonce)を書き換えながら計算を繰り返すことで証明する
  - ブロックを構成する要素に対するハッシュ計算の結果が、特定条件を満たすようになるまで、ヘッダの一部を変更しつつ繰り返す
  - 構成要素: 付随情報（ヘッダ）＋小さい整数
    - (トランザクション群はマークル木による間接参照)
  - ハッシュ計算は、SHA256の出力をもう一度SH256で計算する形で二度行う

マイニングと報酬

- マイニング(採掘)とは、ブロックヘッダをハッシュした結果、指定した数の0が先頭から並ぶようなnonceを持つブロックヘッダを強引に検索することである
- 計算可能量は時間を経る毎に増加するので、問題の難しさが定期的に見直される
  - 難しさは、ハッシュの結果の先頭から0が何個続いているのかで決定する。
  - 計算量の調整は2016ブロック毎に起きる

- 【採掘】に成功すると、二つの報酬を得られる
  - Coinbaseといわれる報酬 (採掘したことに対する直接報酬)
  - 取引手数料
    - (あとで少し詳しく)

採掘の難易度調整

- 計算量は、ブロックヘッダに対してのSHA256 (x2) の結果の最初の部分に、何個 0 が続いているかで調整する
- 2016ブロック採掘される毎に、ブロック生成が10分程度になるように、難易度調整される

bitcoind

- Bitcoinのサーバは bitcoind と呼ばれるプログラムで、Peer-to-Peer ネットワークノードである
  - デフォルトのフルノードとして起動すると、Bitcoin P2Pネットワークに参加し、他のBitcoinノードからブロックを自動的にダウンロードして、完全なBitcoinブロックチェーンを保持するようになる

- Bitcoinには複数実装あり、かつ、実装の分岐（フォーク）が起きている

オペレーションモード

- Public
  - ブロックチェーン全体を公開することが前提

- Permissioned (Private)
  - ブロックチェーンに対するアクセス、ブロックを追加出来る者に制限

Bitcoin における支払いの表現

暗号学的関数

公開鍵暗号

- 公開鍵暗号を用いると、事前の鍵の共有なしに、情報を暗号化して伝えることができる

- 「秘密鍵」と「公開鍵」の組み合わせで以下を実現できる:
  - **デジタル署名**: 秘密鍵で作られた署名を、その秘密鍵に対応する公開鍵を用いて確認することができる
  - **メッセージの暗号化**: 公開鍵を用いて暗号化されたデータは、その公開鍵に対応する秘密鍵を用いてのみ、暗号解除できる

- 公開鍵は、誰の目に触れても構わない
- 秘密鍵は、鍵の所有者が確実に管理する必要がある

公開鍵暗号についての補足

- 秘密鍵の所有者は、対応する公開鍵によって暗号化されたメッセージを暗号解除できる唯一の主体である
- 秘密鍵の所有者は、対応する公開鍵で有効性を確認可能な署名を作成できる唯一の主体である

- 鍵の持ち主が**実際に誰であるのか**は、別途確認が必要である（署名が有効であると主張している人と同一であるか、など
  - このために、公開鍵暗号基盤 (Public Key Infrastructure - PKI) が用いられる
  - マイナンバーカードには、公開鍵暗号鍵ペアと証明書が入っている

暗号学的ハッシュ関数

- 「ハッシュ関数」とは、可変長のデータから、当該データに対して固有な、固定の長さの短いデータを、生成できる関数である

- 二つのデータA と B が与えられたとき、ハッシュ関数の出力は、この A と B が全く同じ内容(一切、違いが無い)場合、同じとなる

- 情報セキュリティで用いるのに充分な特性を持つハッシュ関数を、とくに「暗号学的ハッシュ関数」と呼ぶ

- ハッシュ関数は、一方向関数(トラップドア関数) の一種で、出力結果から入力を作り出す、すなわち、逆関数を作成することが極めて困難である

ハッシュ関数とデジタル署名

- メッセージを公開鍵暗号鍵ペアの秘密鍵で署名するとき、メッセージ全体を署名（暗号化）することも可能だが、署名の大きさの点や計算量などで無駄がある。
- このため、通常は、デジタル署名においては、メッセージの要約として、暗号学的ハッシュ関数を用い、ハッシュ関数の出力を署名する

Bitcoinの内部表現

通貨の表現形式

- Bitcoin ネットワークへの参加者、あるいはBTC(Bitcoin通貨自信)の所有者は、公開鍵暗号鍵ペアを作り、支払元と受取先として用いる。これをBitcoinアドレスと言う

- Bitcoinブロックチェーンは、Bitcoinアドレス間のBTCの移動を「トランザクション」として記録する。なお、支払いは一対一で行われるとは限らない

- Bitcoinブロックチェーンは、それぞれのBitcoinアドレスに結びついたBTCの残高を記録保持していない。記録された全てのトランザクションの結果をもって、最終的な残高となる

BTCはどこから生み出されるのか

- BTCは二つの出元から生み出される:
  - Bitcoinブロックチェーンの一番最初のブロック（Genesis Block）で示されたBTC
  - Bitcoinブロックチェーンの最後のブロックが繋がれたときに、そのブロックの解を発見した者への報奨として与えられるBTC

The Genesis Block

```
1   /**
2    * Build the genesis block. Note that the output of its generation
3    * transaction cannot be spent since it did not originally exist in the
4    * database.
5    *
6    * CBlock(hash=000000000019d6, ver=1, hashPrevBlock=00000000000000, hashMerkleRoot=4a5e1e, nTime=1231006505,
     nBits=1d00ffff, nNonce=2083236893, vtx=1)
7    *   CTransaction(hash=4a5e1e, ver=1, vin.size=1, vout.size=1, nLockTime=0)
8    *     CTxIn(COutPoint(000000, -1), coinbase
     04ffff001d0104455468652054696d65732030332f4a616e2f32303039204368616e63656c6c6f72206f6e206272696e6b206f66207365636
     f6e64206261696c6f757420666f722062616e6b73)
9    *     CTxOut(nValue=50.00000000, scriptPubKey=0x5F1DF16B2B704C8A578D0B)
10   *   vMerkleTree: 4a5e1e
11   */
12  static CBlock CreateGenesisBlock(uint32_t nTime, uint32_t nNonce, uint32_t nBits, int32_t nVersion, const CAmount&
     genesisReward)
13  {
14      const char* pszTimestamp = "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks";
15      const CScript genesisOutputScript = CScript() << ParseHex
        ("04678afdb0fe5548271967f1a67130b7105cd6a828e03909a67962e0ea1f61deb649f6bc3f4cef38c4f35504e51ec112de5c384df7ba
        0b8d578a4c702b6bf11d5f") << OP_CHECKSIG;
16      return CreateGenesisBlock(pszTimestamp, genesisOutputScript, nTime, nNonce, nBits, nVersion, genesisReward);
17  }
```

`./src/chainparams.cpp`

“Wallets”

- Bitcoinネットワークを用いるノード全てがブロックチェーンを保持している(フルノード)であるわけではない

- Wallet (財布) と呼ばれるタイプのアプリケーションは、以下のような機能をもっている
  - 公開鍵暗号の鍵ペアの生成　→ Bitcoinアドレスに読み替えられる
  - 生成した鍵ペアの管理
  - 鍵ペアを用いる事で、BTCを送ったり受け取ったりできる

- 鍵は、主にプライバシー確保のため、多数生成され、組み合わせて使われる

トランザクション

- トランザクションは二者間で行われる。二者間は
  - 入力側は公開鍵自身を指定する
  - 出力側は公開鍵のハッシュを指定する

- 一つのトランザクションは、複数のインプットとアウトプットを指定できる

- トランザクションをトランザクション自身のハッシュを持って特定することが、Bitcoinのデザインの欠陥からできない
  - Mt.Gox 事件

未使用トランザクション出力
Unspent Transaction Output (UTXO)

- 未使用トランザクション出力 (UTXO) は、他のトランザクションで入力として指定されたことが無いトランザクションのことであり、これから支払いに用いることができる(トランザクションで入力として指定できる)
  - ごく一部の例外がある (OP_RETURN)

- ある時点での全てのUTXOの合計は、発行済みのBitcoin通貨の合計額である
- ある時点で、ある者が所有するBTCの合計は、その者が所有する公開鍵で支払い可能なUTXOの合計である

- ビットコインブロックチェーンは、特定の者が持つBTCの合計額を記録していない。全てのトランザクションによる取引結果をもって、状態が特定される

Transaction Data Structure

Transaction

Version	
Input Counter	Inputs…
Output Counter	Outputs…
Lock time	

Inputs

Transaction hash	
Output Index	
Unlocking Script Size	Unlocking Script
Sequence #	

Outputs

Amount	
Locking Script Size	Locking Script

スクリプト

- スタックマシン
  - (Do you know FORTH?)

- スクリプトのコードは以下のような形式:
  - 値をスタックに積む
  - 複数のパラメータをスタックから取り出して実行し、結果をスタックに積む

- 意図的にチューリング不完全なデザイン
  - (ループなし、限定的制御フロー)

ロッキングスクリプト

- トランザクションの出力にはロッキングスクリプトが置かれる

- ロッキングスクリプトは、トランザクションで指定された額を払い出すための条件を指定する

- 通常は、ロッキングスクリプトによって、支払いが許される公開鍵がスタック上にプッシュされる、scriptPubKeyと呼ばれるスクリプトが用いられる

アンロッキングスクリプト

- アンロッキングスクリプトは、トランザクションの全てのインプットに配置される
- 入力を結びつける先のUXTOに含まれているロッキングスクリプトに対応して、ロッキングスクリプトの示した条件を満たすようなスクリプトを指定する

- アンロッキングスクリプトによる通常の払い出しは、UTXOのロッキングスクリプトで指定されている公開鍵に対応する秘密鍵の所有者（すなわちUTXOの所有者) による署名と、対応する公開鍵であり、scriptSigと呼ばれるスクリプトである

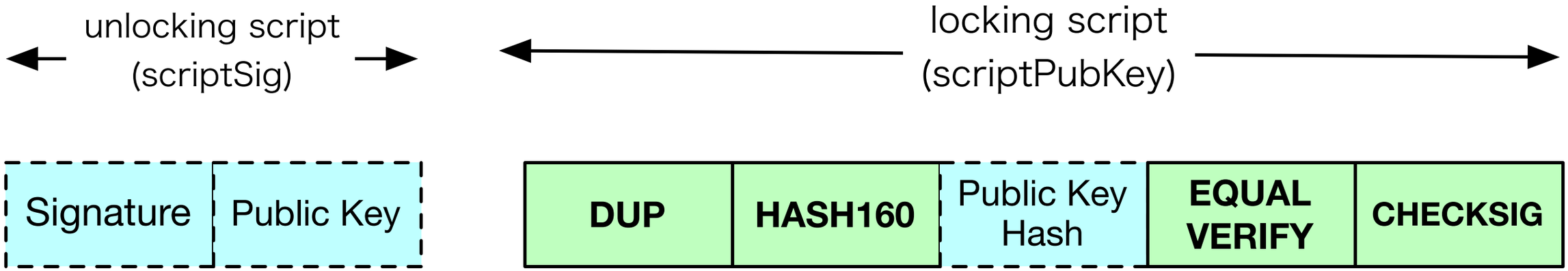
スクリプトの実行

- 以前のBitcoin実装では、UXTOをアンロックされること—つまり払い出しが可能か — を検証するために、アンロッキングスクリプトとロッキングスクリプトを結合して順次実行していた

- 現在のバージョンでは、ロッキングスクリプト、アンロッキングスクリプトの順に、分離された環境で実行される

- 双方実行した後に、スタック上に成功を示す TRUE という値のみが残っていたときに、UXTOの支払いが可能であると判定される。スタックがこれ以外の状態のときは、支払いが起きない

スクリプトの例



スクリプトの柔軟性

- Pay-to-Public-Key-Hash (前のスライドのもの)
- Multi-Signature (N個の指定された鍵のうち、M個で署名されている)
- Data Output (OP_RETURN によるデータ埋め込み)
- 蛇足: Mt.Gox

トランザクション

Transaction

Version	
Input Counter	Inputs…
Output Counter	Outputs…
Lock time	

Inputs

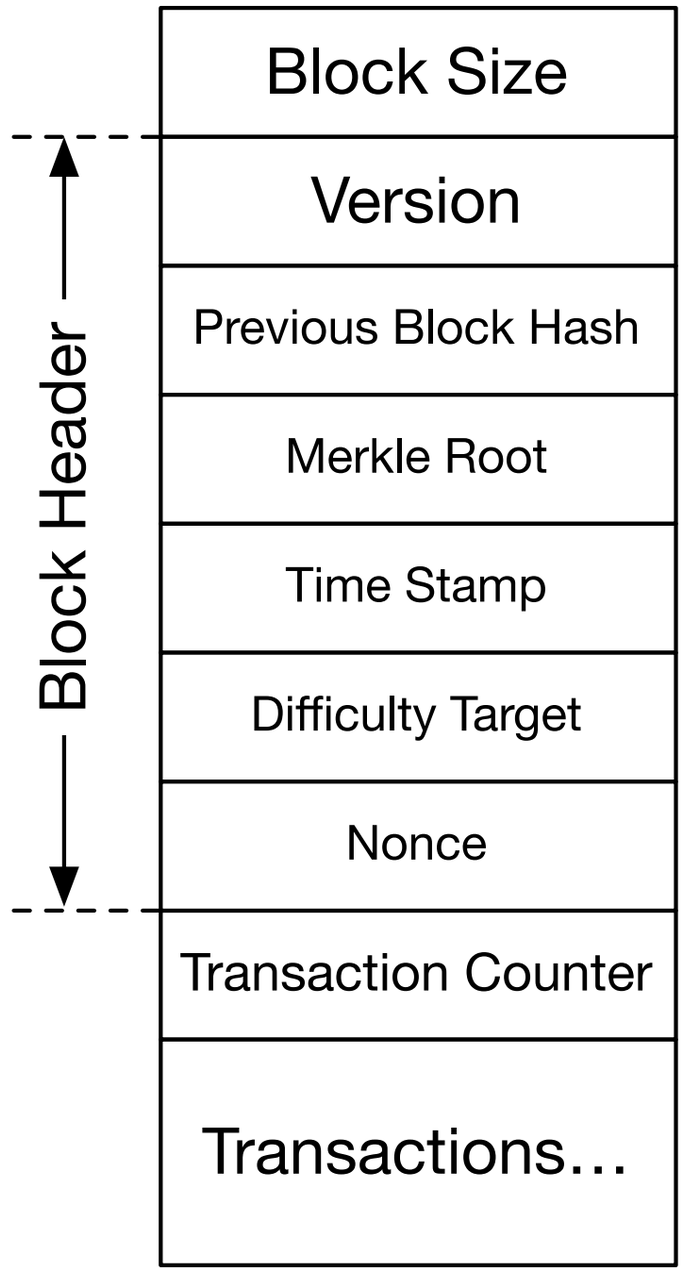
Transaction hash	
Output Index	
Unlocking Script Size	Unlocking Script
Sequence #	

Outputs

Amount	
Locking Script Size	Locking Script

ブロック

- ブロックの識別子は、ブロックヘッダの値を二度SHA256かけた結果



報酬

- Coinbase 報酬 (採掘報酬)
  - 一つのブロックをマイニングすることに 12.50 BTC
    - 2016/7/19 時点。210000ブロック採掘されるごとに、半減される
- トランザクション料
  - ブロック中の全てのトランザクションの、全アウトプットのBTC合計から全インプットのBTC合計を引いたもの
  - トランザクション料は、トランザクションを投入するものが指定する
    - 高いトランザクション料を払うトランザクションほど早く処理される可能性が高まる

ネットワーク上でのデータ配布

1. 新たに作成されたトランザクションは全てのノードに広告される
2. 受け取ったノードは、トランザクションをプールに入れておく
3. それぞれのノードは独自の判断基準にしたがってプールからトランザクションを選び、ブロックを構成する
4. それぞれのノードは、Proof of Work によって、当該ブロックにおける解を見付けようとする
5. PoW の値(nonce)を見付けたら、当該ブロックを全てのノードに広告する
6. 広告されたブロックを受信したノードは、全てのトランザクションが正しく、かつ、二重支払いが無いことを確認し、確認できたときのみ、ブロックを有効な者として受け付ける
7. ノードはブロックを受け付けたことを、続くブロックに対する作業を始める際、受け付けたブロックのハッシュをヘッダに含めることで示す

Bitcoin以外のブロックチェーン実装

ブロックチェーン実装

- Bitcoin
  - リファレンス実装多数 (C++, go lang, …)
  - フォークされた実装多数
- Ethereum
- Hyperledger Project
  - Fabric

Ethereum

Ethereum

- Blockchain Application Platform
- Turing Complete Scripting
  - With Concept of Gas

- Important Difference from Bitcoin Blockchain:
  - It records not only transaction logs, but also states
  - It can keep states (key-value pair) data for scripts

Hyperledger Project

Hyperledger Project

- Projects
  - Blockchain Implementations: Fabric, Iroha, Sawtooth Lake
  - Tools: Explorer, Cello

Hyperledger Fabric

- Feature [HYPER]
  - Modular and Pluggable
  - Realistic operation of private blockchain in its mind:
    - Can select not only Proof of Work, but also able to use Practical Byzantine fault tolerance (PBFT) [PBFT]

- Goes on to Live as SaaS on 19th of March 2017 [HLS]

Related Technologies

Lightning Network

- The computation time to mine a block is about 10min.
- It is also said to be “safe” to observe six blocks for the transaction to be secured.
- This cause full transaction require up to 60min.

- Lightning [LIGHT] is a service which act as side-chain (chains next to main blockchains) to provide faster and frequent transactions among participating parties

Proof of Stake

- Proof of Work is using huge amount of computation power to compete. In a point of view, this is a waste of energy, and also not so fair
- Replacement of Proof of Work — Proof of Stake is under discussion, and Ethereum is planning to switch to Proof of Stake[POS]

Extreme Consensus

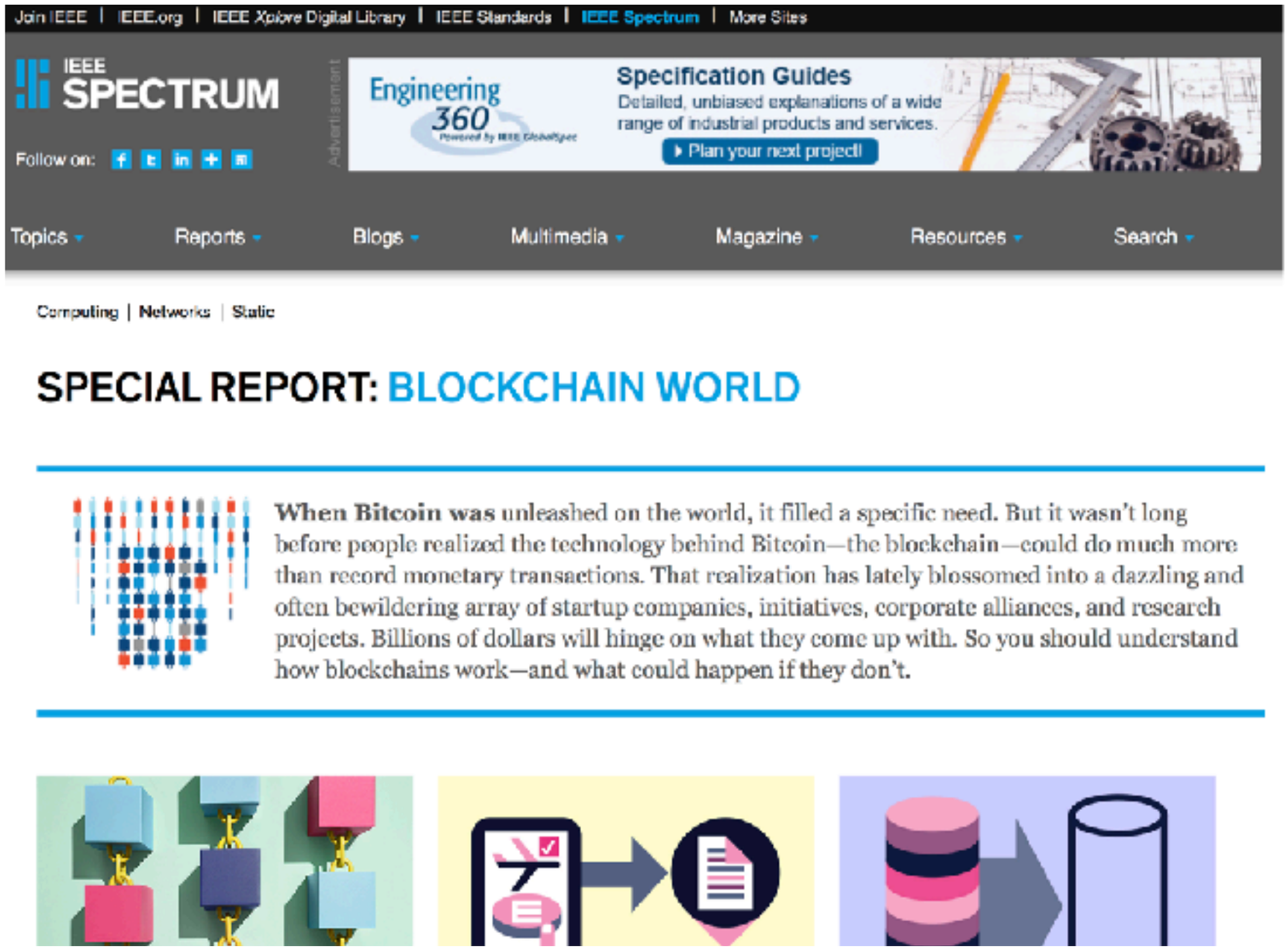
- Whether or not to make reasonable changes to Bitcoin… [TWOT]

- Who has actual power to do that?
- Is Bitcoin Core developer has power?
- Does the organization who has large computing power has huge influence?

雑多な話題

IEEE Spectrum 10月号特集

"Blockchain World"



https://spectrum.ieee.org/static/special-report-blockchain-world

Bitcoin Stats @ 2017/10/24

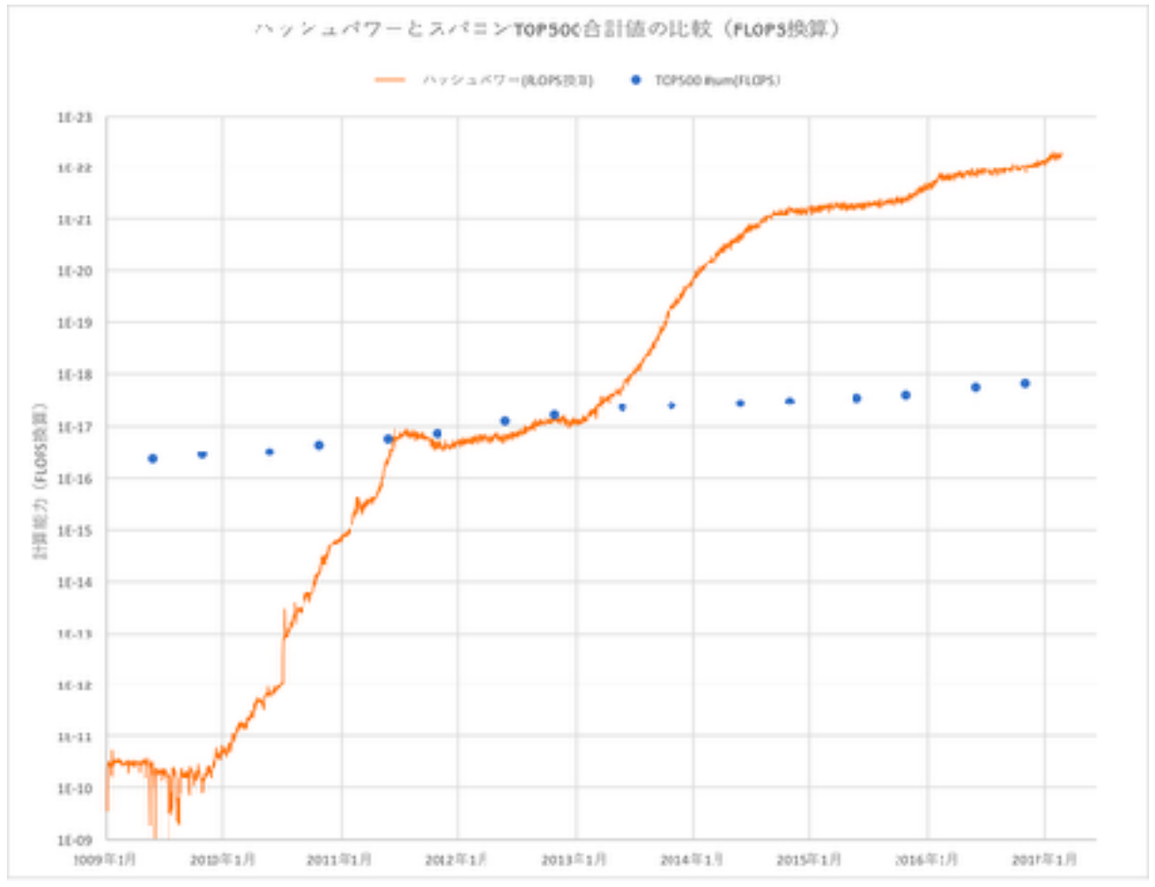
ハッシュレートの推移

10EH/s

Source: https://blockchain.info/en/charts/hash-rate?timespan=all

ハッシュパワーの総計

- 推定方法は議論の余地があるが、現在のスーパコンピュータトップ500の全ての計算力の8万倍あるという概算がある[1]



[1]「ビットコインのP2Pネットワークは世界最大のコンピュータ」なのか？

http://knowledge.sakura.ad.jp/knowledge/7858/

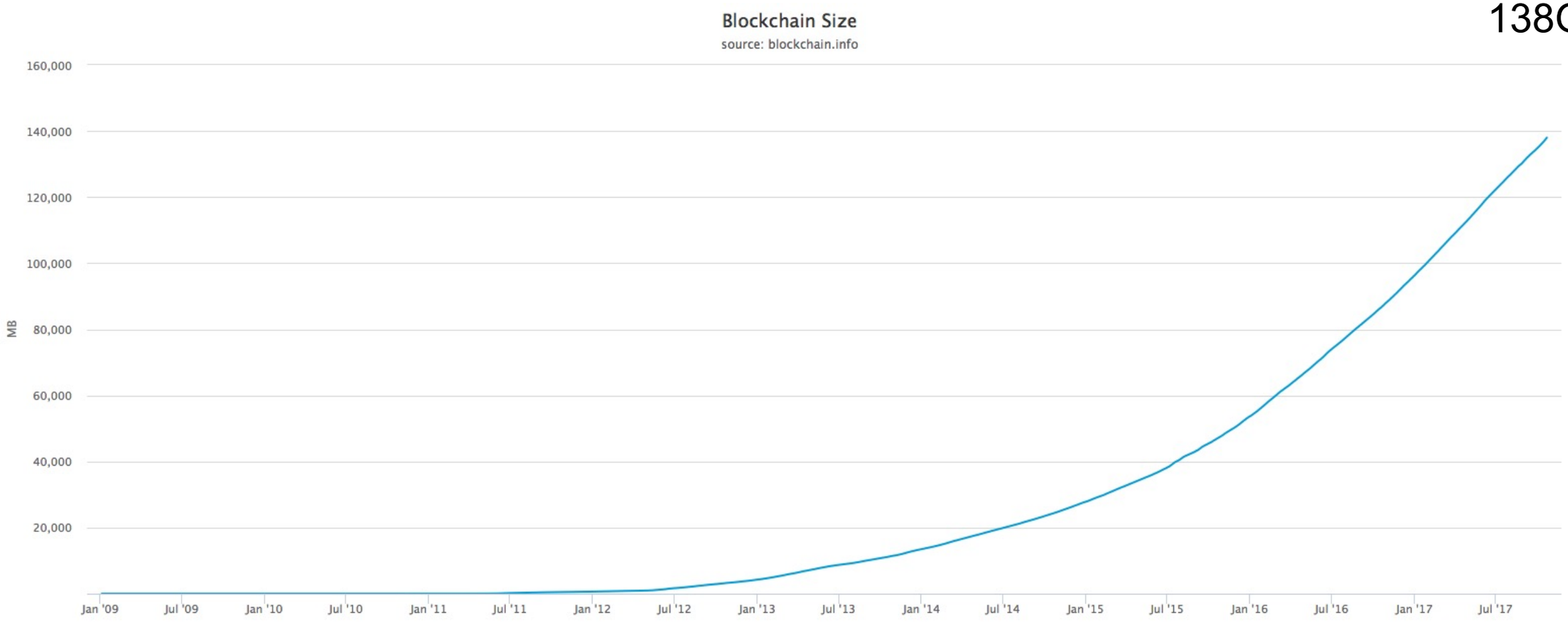
Market Price

5983/1BTC

https://blockchain.info/en/charts/market-price?timespan=all

Blockchain Size

138GB



https://blockchain.info/ja/charts/blocks-size?timespan=all

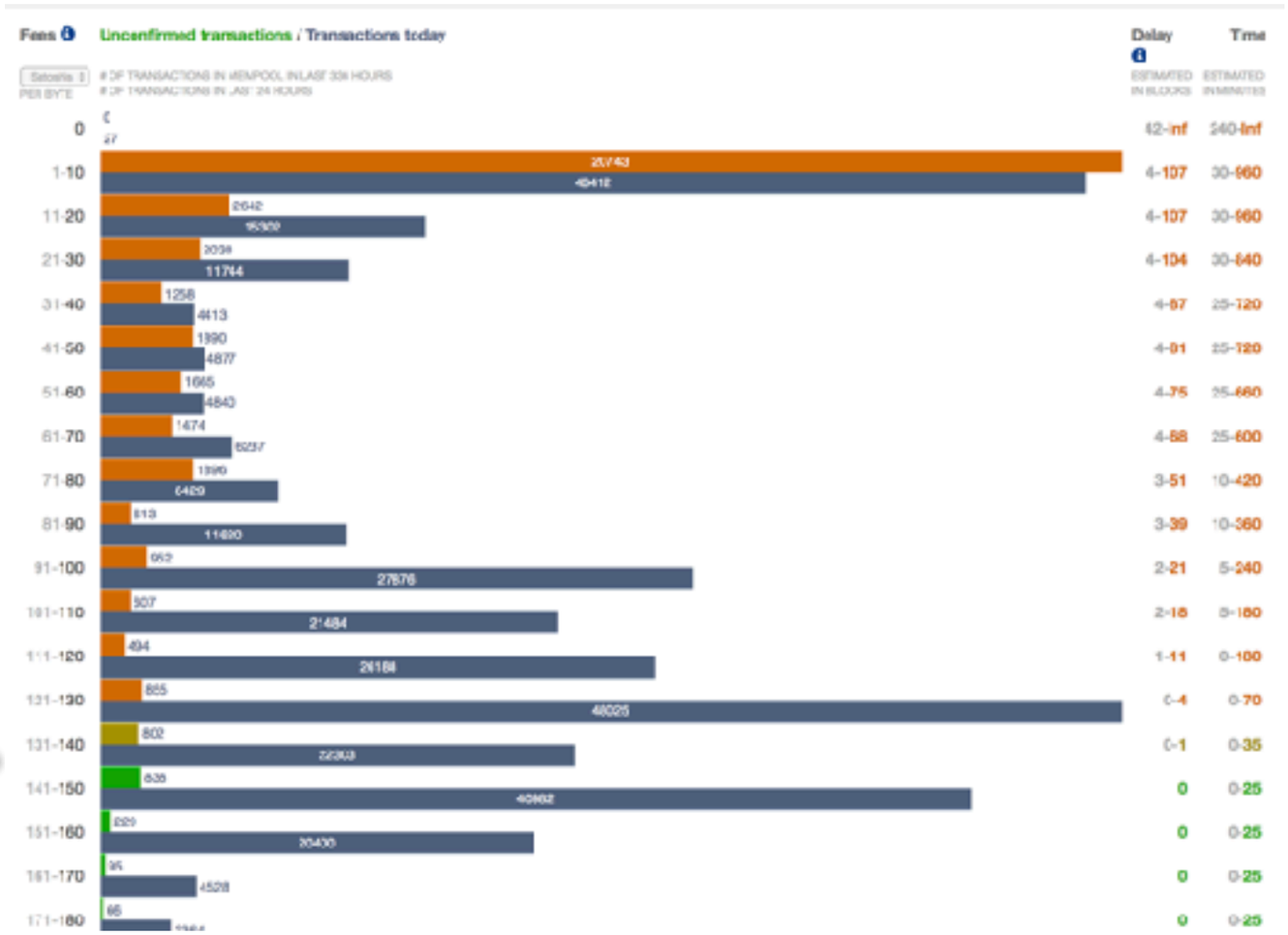
Hash Rate

10EH/s

Source: https://blockchain.info/en/charts/hash-rate?timespan=all

Transaction Fees

- Quest for the fastest cheapest transaction
  at median transaction size: 226 bytes



Source: https://bitcoinfees.21.co

2017/4/24
180 satoshis/byte * 226 bytes
→ 40680 satoshis/transaction
→ 0.45USD (1BTC =~ 1248USD)

2017/7/7
360 satoshis/byte * 226 bytes
→ 81360 satoshis/transaction
→ 2USD (1BTC =~ 2544USD)

2017/10/24
150 satoshis/byte * 226 bytes
→ 33900 satoshis/transaction
→ 2USD (1BTC =~ 5855USD)

ブロックチェーン利用における
ごく個人的見解

良く言われること

- マイナーのインセンティブは？
- ブロックチェーンに何でも入れるの？
  - 非公開情報は、Permissioned ブロックチェーンでないとダメなんでは？

マイナーのインセンティブ

- マイナーにインセンティブが無いとブロックを作れない
  - Yes

- 乗っているアプリケーションのインセンティブとの合致は必要か
  - No

- ブロックチェーンと、それに乗るアプリケーションのインセンティブが一致している必要は無い
  - 暗号通貨は、一気通貫で、マッチしているにすぎない

ブロックチェーンには何を入れるのか

- ブロックチェーンに入れないとデータの検証は出来ない → NO
- 署名検証には、データが揃っている必要がある → YES

- 一方、いつ署名検証をするかによって、署名対象のデータを揃えるためのアクセス制御やタイミングに柔軟性を持たせられる
  - 署名検証するときに揃っていれば検証可能
  - 署名したあと、署名対象のデータや署名それぞれ（細分化も可能）通信路、保存場所は、検証したい時に揃っていれば、問われない

- Public ブロックチェーンをプライベートデータと組み合わせてうまく使う

Bitcoinの分岐: ハードフォーク

人によるコンセンサス

- Bitcoin を運用するための「コンセンサス」とは
  - ある修正の適用の可否の判断をどう決定するか

フォーク

- フォークにはいくつか種類がある
  - フォーク
    - 同一コンセンサスルールで動作する複数のBitcoinネットワーク上のノードでブロックが同時に採掘されたときに起きる
  - ハードフォーク
    - コンセンサスルールが変更されたソフトウエアが実行されるようになり、新ルールによるブロックが古いノードによって不正と解釈されるように、後方互換性が無い形で完全に分岐してしまう状態
  - 説明略: ソフトフォーク

なぜハードフォークが起きるのか

- 後方互換性の無い修正が入るため

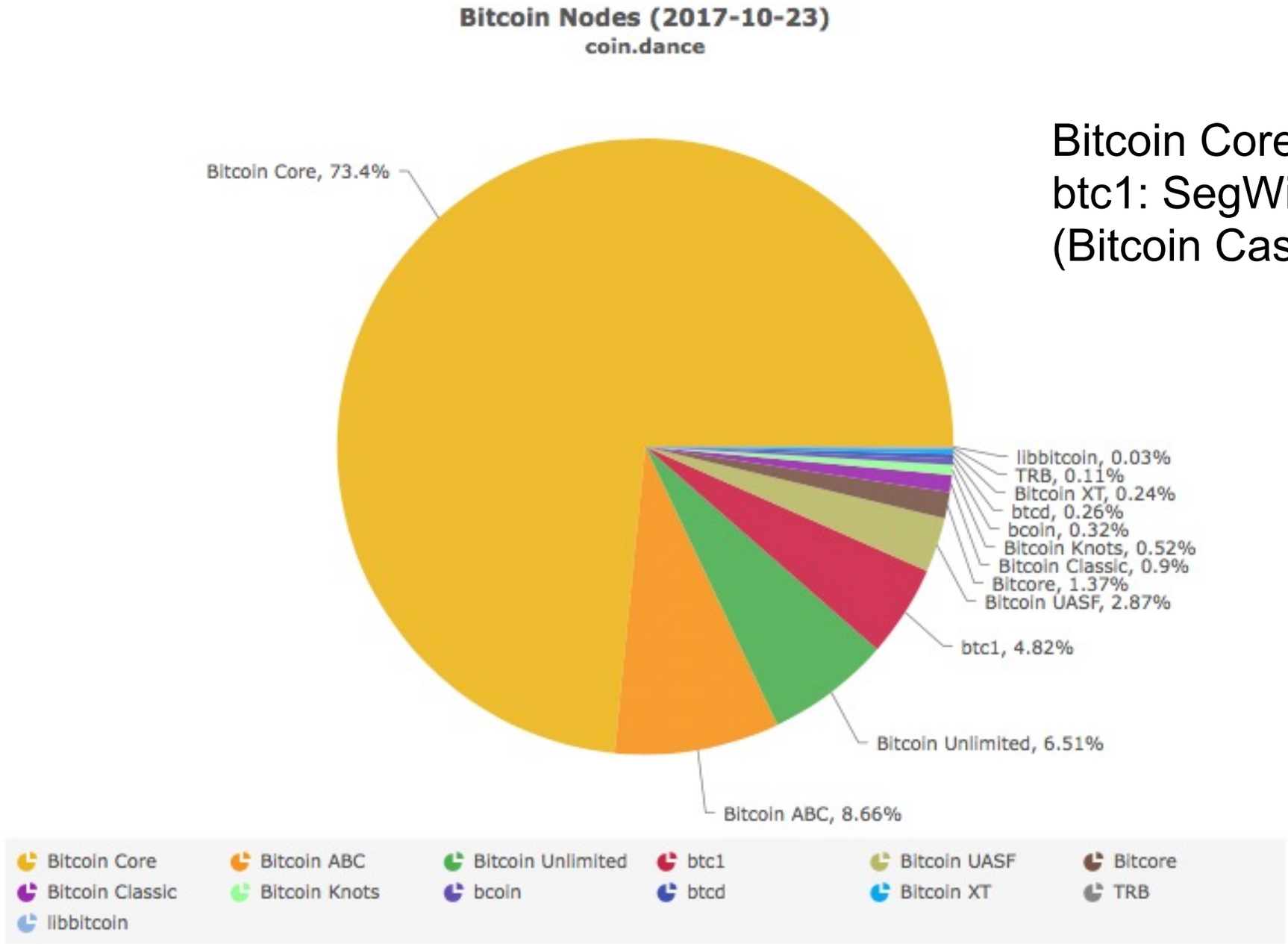
- Bitcoin Cash: ブロックサイズ 1MB → 8MB [2017/8/1]
  - ASICboost hack 可能

- SegWit : 署名データを分離することでブロックの効率化 [2017/8/24]
  - オマケ: Transaction Malleability Attack の対策になる

- Bitcoin Gold: Equihashへのアルゴリズム変更 [2017/10/25 頃]
  - ASIC採掘対策。GPUで採掘できる

- SegWit2x : SegWit + ブロックサイズ 1MB → 2MB　[2017/11/19 頃]

Bitcoin コード別ノード数比率



Bitcoin Core: SegWit
btc1: SegWit2x
(Bitcoin Cashはこのグラフには無い)

https://coin.dance/nodes/share

Bitcoinな論文

Routing Attack

BGP Hijacking

Hijacking Bitcoin: Routing Attacks on Cryptocurrencies

https://btc-hijack.ethz.ch

Maria Apostolaki
ETH Zürich
apmaria@ethz.ch

Aviv Zohar
The Hebrew University
avivz@cs.huji.ac.il

Laurent Vanbever
ETH Zürich
lvanbever@ethz.ch

***Abstract*—As the most successful cryptocurrency to date, Bitcoin constitutes a target of choice for attackers. While many attack vectors have already been uncovered, one important vector has been left out though: attacking the currency via the Internet routing infrastructure itself. Indeed, by manipulating routing advertisements (BGP hijacks) or by naturally intercepting traffic, Autonomous Systems (ASes) can intercept and manipulate a large fraction of Bitcoin traffic.**

This paper presents the first taxonomy of routing attacks and their impact on Bitcoin, considering both small-scale attacks, targeting individual nodes, and large-scale attacks, targeting the network as a whole. While challenging, we show that two key properties make routing attacks practical: *(i)* the efficiency of routing manipulation; and *(ii)* the significant centralization of Bitcoin in terms of mining and routing. Specifically, we find that any network attacker can hijack few (<100) BGP prefixes to isolate ~50% of the mining power—even when considering that mining pools are heavily multi-homed. We also show that on-path network attackers can considerably slow down block propagation by interfering with few key Bitcoin messages.

We demonstrate the feasibility of each attack against the deployed Bitcoin software. We also quantify their effectiveness on the current Bitcoin topology using data collected from a Bitcoin supernode combined with BGP routing data.

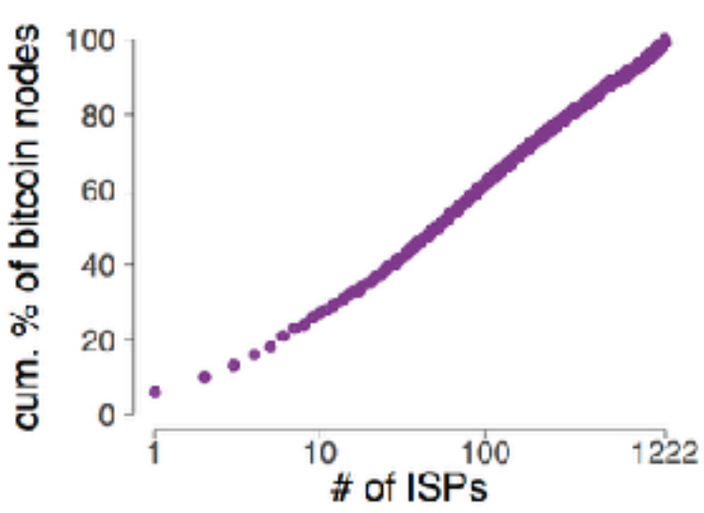
The potential damage to Bitcoin is worrying. By isolating parts of the network or delaying block propagation, attackers can cause a significant amount of mining power to be wasted, leading to revenue losses and enabling a wide range of exploits such as double spending. To prevent such effects in practice, we provide both short and long-term countermeasures, some of which can be deployed immediately.

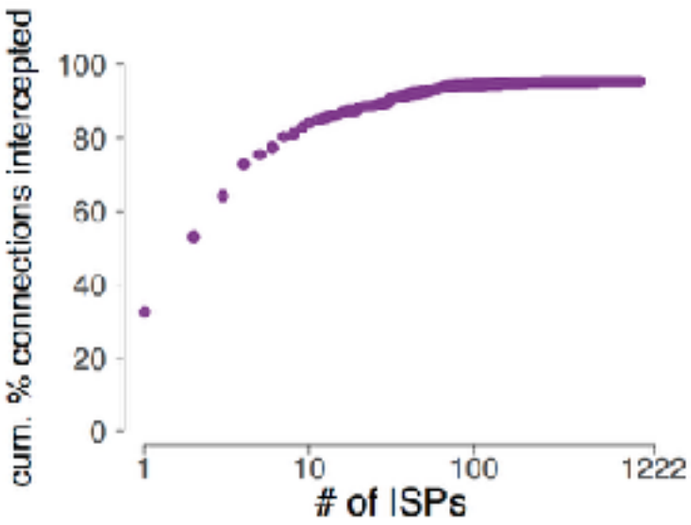
One important attack vector has been overlooked though: attacking Bitcoin via the Internet infrastructure using *routing attacks*. As Bitcoin connections are routed over the Internet—in clear text and without integrity checks—any third-party on the forwarding path can eavesdrop, drop, modify, inject, or delay Bitcoin messages such as blocks or transactions. Detecting such attackers is challenging as it requires inferring the exact forwarding paths taken by the Bitcoin traffic using measurements (e.g., traceroute) or routing data (BGP announcements), both of which can be forged [41]. Even ignoring detectability, mitigating network attacks is also hard as it is essentially a human-driven process consisting of filtering, routing around or disconnecting the attacker. As an illustration, it took Youtube close to 3 hours to locate and resolve rogue BGP announcements targeting its infrastructure in 2008 [6]. More recent examples of routing attacks such as [51] (resp. [52]) took 9 (resp. 2) hours to resolve in November (resp. June) 2015.

One of the reasons why routing attacks have been overlooked in Bitcoin is that they are often considered too challenging to be practical. Indeed, perturbing a vast peer-to-peer network which uses random flooding is hard as an attacker would have to intercept many connections to have any impact. Yet, two key characteristics of the Internet's infrastructure make routing attacks against Bitcoin possible: *(i)* the efficiency of routing manipulation (BGP hijacks); and *(ii)* the centraliza-

Hijacking Bitcoin: Routing Attacks on Cryptocurrencies

- The author's opinion:
  - Attack#1: Routing attacks can partition Bitcoin into pieces
  - Attack#2: Routing attacks can delay block delivery by 20 minutes





Source: https://btc-hijack.ethz.ch/

Stability

Stability of Blockchain

- "One presenting one of our articles released last February where we review and correct Satoshi's calculations of the probability of double-spending in the Bitcoin founding paper. For the first time, we proved a fact, often stated but never proved before in the literature, that this probability decreases exponentially to zero in terms of the number of confirmations."

- "Our second proposal is a novel study of blockchains stability where we discuss the convergence between private and public interests by highlighting possible cases of instability never really studied so far."

- Cyril Grunspan (ESILV, France)
Ricardo Perez-Marco (CNRS, U. Paris VII, France)

https://medium.com/@CGrunspan/open-letter-to-stanford-universitys-president-and-to-the-bitcoin-community-7ea56239ed5e

慶應における活動

Activities at Keio

- ブロックチェーンラボの共同研究
  - ブロックチェーンの活用戦略についての共同研究
  - ブロックチェーン技術の特定領域に特化した研究

- アプリケーション
  - ファブ技術との連携によるアプリ研究開発
  - 医療関係者との連携によるアプリ研究開発

- BSafe.Networkとの連携

ブロックチェーンラボ

ブロックチェーンラボ

- ブロックチェーンについての研究をすすめる
- 暗号通貨に止まらない応用を検討

- アプリケーション
  - 医療系システムへの適用
  - センシングデータへの応用
  - デジファブ

- ブロックチェーン自身
  - 挙動についての研究
  - 運用
  - 開発: 新たな独自実装

BASE Alliance

BASE ALLIANCE

24 July 2017

オープンな議論

研究開発

実証実験

コミュニティ形成

活動概要

- ブロックチェーン技術全般についての研究開発
- ブロックチェーンを用いたアプリケーションの研究開発
- 既存および実装したブロックチェーン技術を用い、実験実証するテストベットの構築、運用、および、その研究
- 国際的産学連携コミュニティの醸成

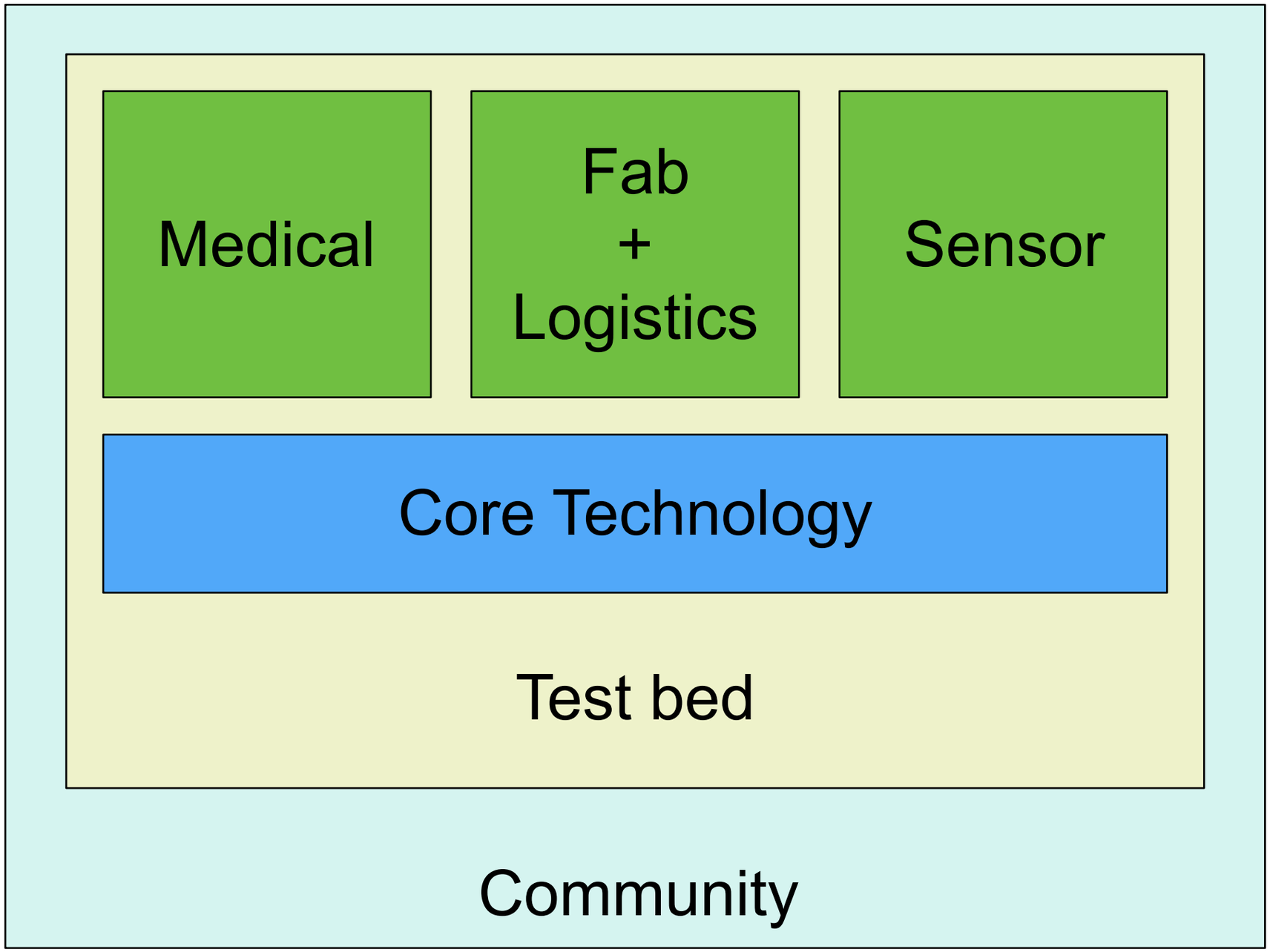
現在の参加者のトピック

- アプリケーション
  - 医療系システムへの適用
  - センシングデータへの応用
  - デジファブ
- ブロックチェーン自身
  - 挙動についての研究
  - 運用
  - 開発: 新たな独自実装
- コミュニティ
  - BSafe.Networkとの連携
- 標準化

運営・研究メンバー

- 伊藤 穣一　　慶應義塾大学 SFC研究所 主席所員 / MIT メディアラボ所長
- 松浦 幹太　　東京大学 生産技術研究所 教授
- 村井 純　　慶應義塾大学 環境情報学部 教授
- 松尾 真一郎　　慶應義塾大学大学院 政策・メディア研究科 特任教授 /
  東京大学 生産技術研究所 リサーチフェロー /
  MITメディアラボ 所長リエゾン（金融暗号）
- 岸上 順一　　室蘭工業大学大学院 教授 / 慶應義塾大学 訪問教授 /
  W3Cアドバイザリーボード
- 鈴木 茂哉　　慶應義塾大学 大学院 政策・メディア研究科 特任准教授
- 林 達也　　慶應義塾大学SFC研究所所員 ブロックチェーンラボ 研究員

BASE Alliance Activity Overview



BSafe.Network

BSafe.Network

- BSafe.Network[BSAFE][BSAFEW] is a testing platform for Blockchain among academia for experimenting new codes, etc
  - Currently, Bitcoin Blockchain (with Segregated Witness patch)

- 18 Universities at this moment:
  - Boston University(USA), Cambridge Centre for Alternative Finance at the Judge Business School(UK), EPFL(Switzerland), ETHZurich(Switzerland), Imperial College London(UK), Imperial College London(UK), Indian Statistical Institute(India), Keio University(Japan), Massachusetts Institute of Technology(USA), Newcastle University(UK), Ritsumeikan University(Japan), SIM University(Singapore), Toho University(Japan),
    Univ. of Cape Coast(Ghana), Universitat Autonoma de Barcelona(Spain), University of British Columbia(Canada), University of Cambridge(UK), University of Illinois Urbana-Champaign(USA), University of Nicosia(Cyprus), The University of Tokyo(Japan)

監査付き通信路としてのブロックチェーン

(Blockchain as an Audit-able Communication Channel)

鈴木 茂哉, 村井 純

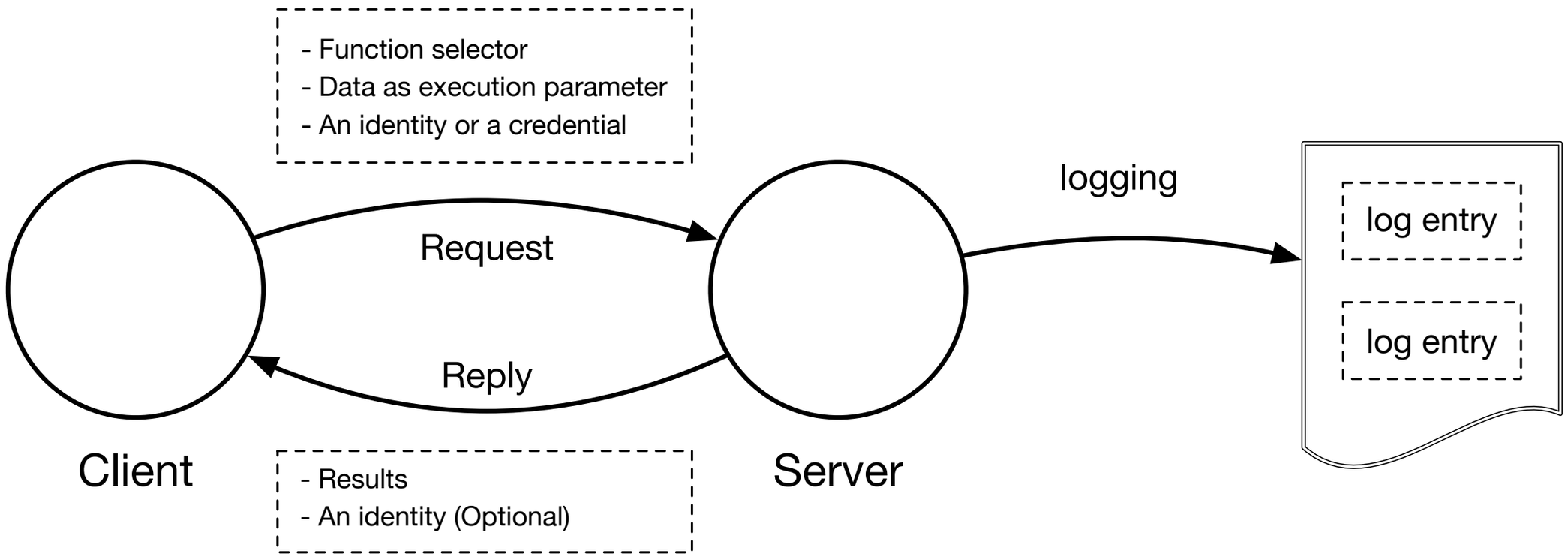
Blockchain as an Audit-able Communication Channel

- Author
  - Shigeya Suzuki, Jun Murai

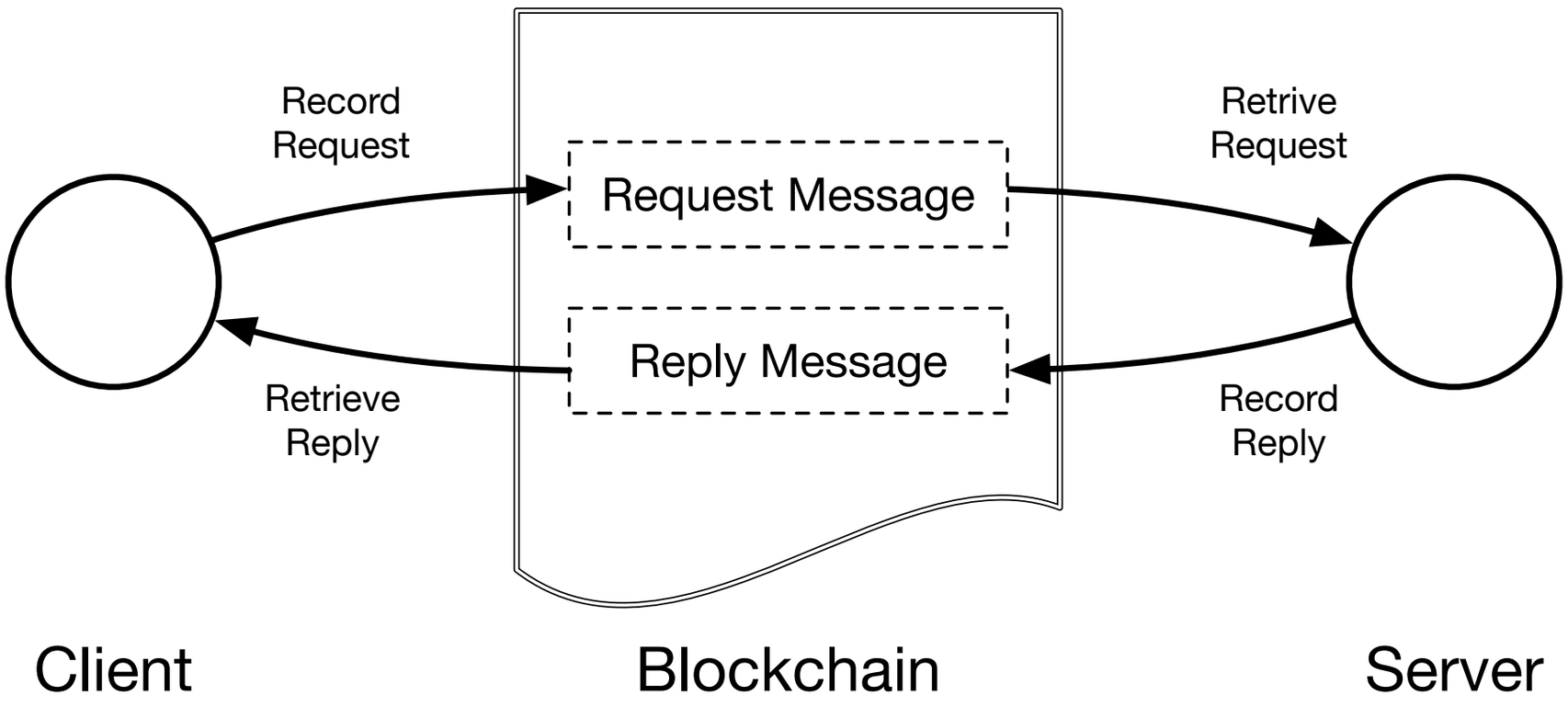
- Abstract
  - Applications requiring strict access control, such as medical record query, often require auditing of the query. The current typical design relies on server side logging. However, logging on server-side do not provide strict means of auditing, since the server can be tampered with attackers, and also anybody who has permission to write can modify the log. We propose a scheme using blockchain technology, as a request-response channel for a client-server system, to record both client request and server reply in an audi-table manner. We have implemented a proof-of-concept system on top of a publicly available blockchain testbed. By using a blockchain as a client-server request-response channel, the request-response sequence can be verified by anybody who has access to the blockchain, providing a way to implement audit log for strictly controlled resources.

`http://ieeexplore.ieee.org/document/8029983/`

クライアント-サーバシステムとログ



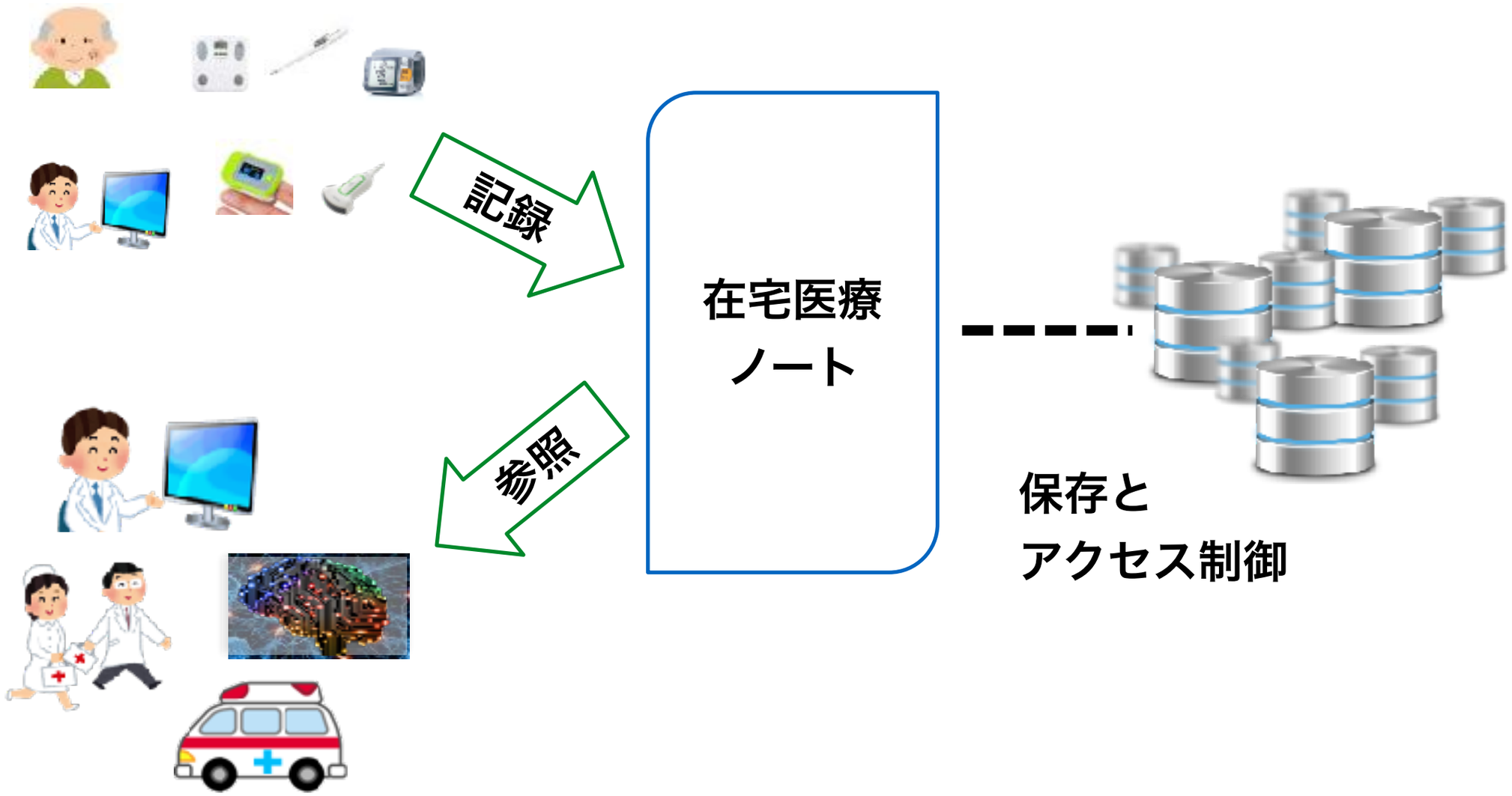
提案方式:
監査付き通信路としてのブロックチェーン



ブロックチェーンの在宅医療への活用

在宅医療ノート

・特定の患者に結びついた、様々な在宅医療にまつわる情報をひとまとまりとして、ワンストップで扱うコンセプト



在宅医療ノートの要件

- 情報の記録
- 情報の参照
- 情報の保存とデータモデル
- アクセス制御の必要要件

情報の記録

- 情報のソース
  - 患者
  - 医療従事者
  - センサ

- 要件
  - データの出自の確かさを担保できる仕掛け
  - 異なる患者の情報が、正しく記録できる仕掛け
    - 例: 同じ血圧計を使っていても、患者毎に正しく記録されること

情報参照

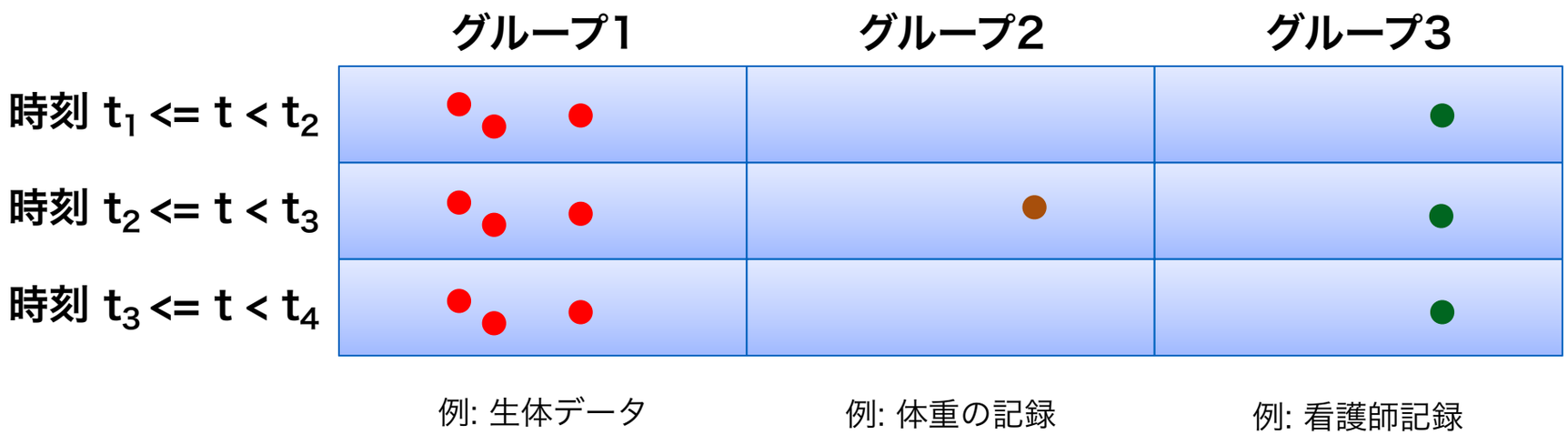
- 情報の参照者
  - 医療従事者
    - 医師、看護師、救急対応
  - AI

- 要件
  - 対象に応じたアクセスの付与、限定化

保存とデータモデル

- 実装の詳細に非依存な、メタなデータモデルだけ規定する

- 記録の最小単位
  - タイムスタンプを打たれた情報群
- 情報群のグループ化
  - 適切なグルーピングをする。グループ単位でアクセス制御する



アクセス制御の必要要件

- 情報を保持するサーバ
  - アクセス制御機構

- 情報:
  - 対象の指定 (時間範囲、グループ)
  - アクセス者のID
  - アクセス制御のための情報
    - 時間範囲 x グループ x アクセス者ID

- 操作
  - 認証による、アクセス者とIDとの結びつきの提示

ブロックチェーンの活用

- ブロックチェーンの活用により、在宅医療ノートに記録された情報の真正性を確認できるようにする

- 在宅医療ノートにおいては、情報に アクセスできる者が、**アクセスできる範囲の情報のみを対象としても** 検証可能とする必要がある
  - すなわち、検証対象となる情報は、その単位（グループ）でアクセス可能でなければならない

アクセス制御と署名・署名検証の関係

- 情報の真正性を証明するためには、対象情報へのアクセスし、署名を作成する必要がある
  - 署名を作成するには、対象となる情報に対するハッシュが必要

- 情報の真正性を確認するためには、対象情報へのアクセスが必要である
  - 署名を検証するために、検証情報のハッシュが必要である

- アクセスできる範囲に対するハッシュを作成できなければ、検証が成り立たない

プライベート情報からの
パブリックブロックチェーン活用

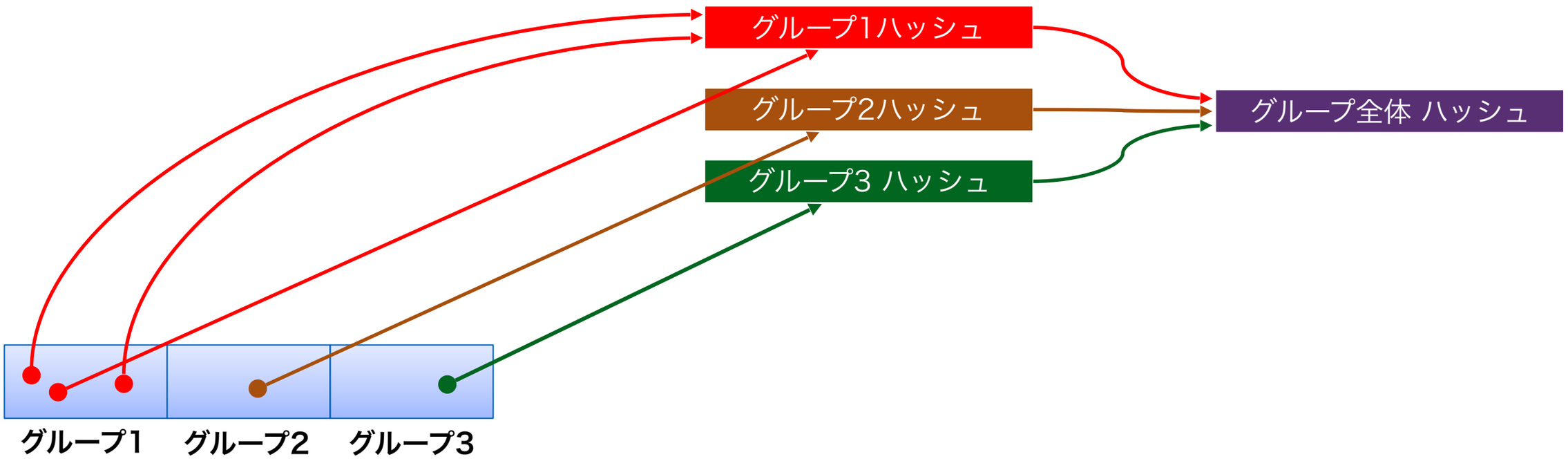
- データの真正性の確保が目的である一方、対象となるデータはプライベート情報が含まれる

- データの真正性を確認するために必要なのは、ハッシュのみであり、ハッシュのみがブロックチェーンに記録すべき情報である

- 一方、ハッシュが記録されることだけを必要とするのであれば、記録対象がプライベートブロックチェーンか、パブリックブロックチェーンかを問わないシステム設計は可能である
  - 前提: 対象患者のアイデンティティが表に出ていないこと

時系列・グループ単位のハッシング

- 時系列上のブロックと記録グループの固まりを対象としてハッシュを求める
- さらに、時系列上で並列するグループ群のハッシュをまとめてハッシュを求める



ブロックチェーンへの記録

- ブロックチェーンへの記録は二つの手段がある
  - グループ毎のハッシュのみを記録する
  - グループ毎のハッシュと、全体のハッシュ双方を記録する

- 前者の場合は、グループ毎のハッシュと全体のハッシュを取り出せるデータベースを参照可能としておく必要がある

References (1)

- Dai, W. b-money http://www.weidai.com/bmoney.txt
- Nakamoto, S. (2009). Bitcoin: A Peer-to-Peer Electronic Cash System, 1–9.
- Wood, G. (2014). Ethereum: A secure decentralised generalised transaction ledger. Ethereum Project Yellow Paper.
- [SEGWIT] Segregated Witness : the next steps https://bitcoincore.org/en/2016/06/24/segwit-next-steps/
- Ethereum White Paper https://github.com/ethereum/wiki/wiki/White-Paper
- Buterin, V. (2014a, June 19). On Mining - Ethereum Blog. Online March 16, 2017, from https://blog.ethereum.org/2014/06/19/mining/

References (2)

- [POS] Buterin, V. (2014b, July 5). On Stake - Ethereum Blog. Online March 16, 2017, from https://blog.ethereum.org/2014/07/05/stake/
- [LIGHT] Poon, J., & Dryja, T. (n.d.). The Bitcoin Lightning Network. Lightning.Network.
- [HYPER] Hyperledger Projects https://www.hyperledger.org/community/projects
- [PBFT] Practical byzantine fault tolerance and proactive recovery http://dl.acm.org/citation.cfm?doid=571637.571640
- [HLS]IBM unveils Blockchain as a Service based on open source Hyperledger Fabric technology https://techcrunch.com/2017/03/19/ibm-unveils-blockchain-as-a-service-based-on-open-source-hyperledger-fabric-technology/amp/
- [BSAFE] http://bsafe.network/
- [BSAFEW] BSafe.Network The Research Network for Blockchain Technology — White Paper http://bsafe.network/WhitePaper_BSafe_20170101_v102.pdf