地域におけるブロックチェーン活用の可能性

近畿大学 山崎重一郎

ブロックチェーン技術はまだ黎明期

- webが登場していないインターネットくらいの状況
- にもかかわらず、FinTechブームのせいで世界中で莫大な投資が集中

誤った情報が氾濫している

- 怪しい技術や明らかな詐欺も存在（玉石混交）

ブロックチェーン技術の可能性は本物だが

- 自分でしっかり理解し、自力で開発しなければ確実に騙される
- 外国の技術への投資、東京からの投資話などは、強く引き止めます

  シリコンバレー、イスラエル、エストニア、ロシア、...

福岡のFinTech企業動き

ハウ・インターナショナル（飯塚市）

NAYUTA（福岡市）

日本経済新聞

2017年8月15日（火）

Web刊 速報 ビジネスリーダー マーケット テクノロジー アジア スポーツ マネー ライフ 朝刊・

トップ 紙面連動 連載 社説・春秋 特集 映像 ＦＴ オピニオン 統計 トランプ政権

有料会員限定 記事 今月の閲覧本数： 3 本 登録会員の方は月 10 本まで閲覧できます。

Ｎａｙｕｔａ、先端分野のデータ取引 ブロックチェーン活用

2017/5/1付 | 日本経済新聞 朝刊

共有 保存 印刷 その他

ＩＴ（情報技術）ベンチャーのＮａｙｕｔａ（福岡市、栗元憲一社長）は兵庫県と組み、インターネットでデータを低コストで安全に取引する仕組み「ブロックチェーン」を先端研究分野に活用する。県内にある大型放射光施設「ＳＰｒｉｎｇ－８」を使う企業数社と協力し、電子材料などの解析データを流通させる仕組みをつくる。

2016.07.10

三井住友FGとハウインターナショナルがブロックチェーン技術を協同で研究へ

Fintech ブロックチェーン 金融ITニュース 銀行

三井住友フィナンシャルグループはブロックチェーン技術の研究のため、近畿大学とハウインターナショナルと提携している。ハウインターナショナルは福岡県飯塚市のITベンチャーでブロックチェーンに関するノウハウを持っており、金融サービスへの活用を目指す。

ハウインターナショナルとＦＦＧ（福岡銀行グループ）が日本初のブロックチェーン実証環境「Chaintope」を利用した 金融サービスの共同研究を開始！

Tweet Share G+ +1 B! Hatena

いいね！ 19 シェア ツイート G+ B! 0 Pocket LINEで送る

ハウインターナショナルは、株式会社ふくおかフィナンシャルグループ(以下 FFG)と、ブロックチェーン技術を活用した金融サービスの共同研究を開始した。

地域におけるブロックチェーン活用には

まず人材育成が最初の一歩

- 技術、経済、制度のすべての視点を持つ人材が必要
- コンサルや海外製品の宣伝文句は無視

教育機関は大学だけではない

- 地域の勉強会
- ブロックチェーンはアカデミアは参加しにくい分野

  例：暗号の専門家の多くは、ブロックチェーンの本質的価値を理解できない
- 教育プログラム付きのコンテスト

  （賞金だけでは地域企業や学生への教育的効果は小さい）

インターネットとブロックチェーン

多くの技術者が類似性を感じている

類似点の分析からブロックチェーンを見る

ビットコインの衝撃

20年以上も未解決だった問題を鮮やかに解決

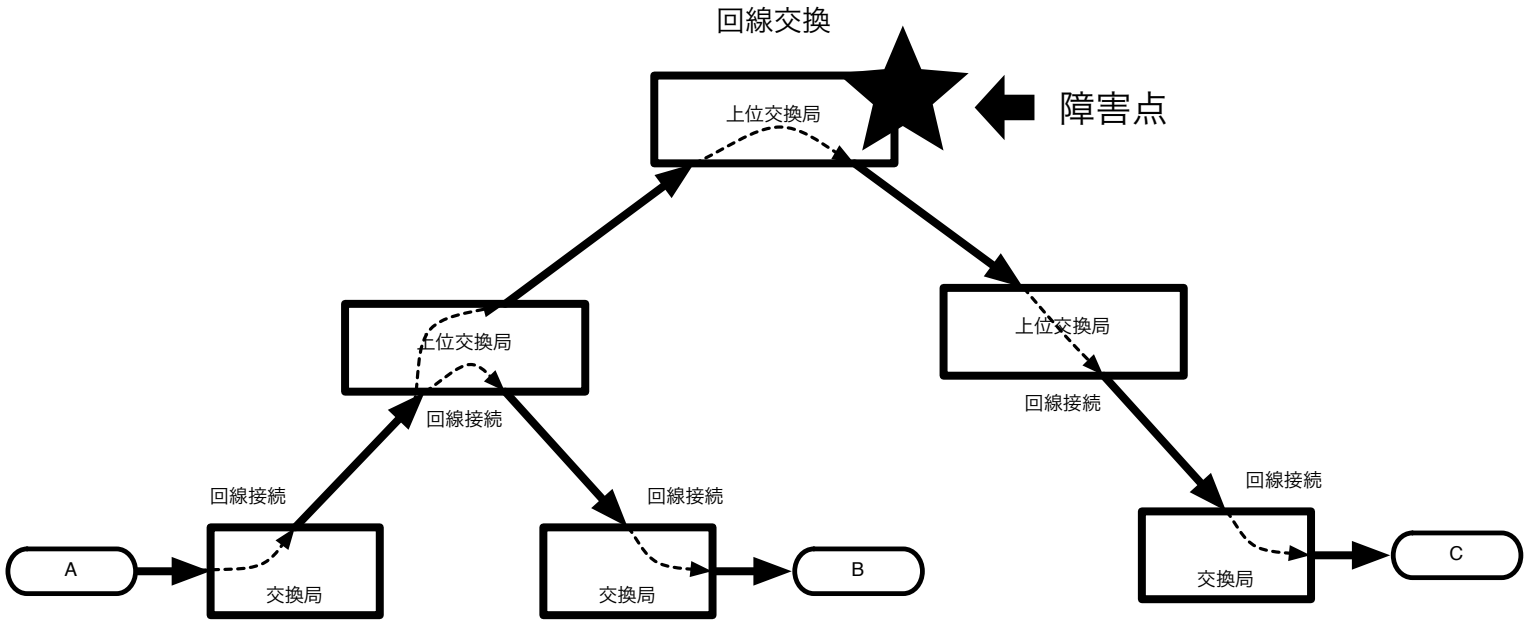
- ICカードなど物理媒体に依存しない
- 信頼できるサービス不要
- 個人から個人への転々流通が可能

… 岡本、太田の6条件のうち5条件を達成

インターネットの発明（俗説）

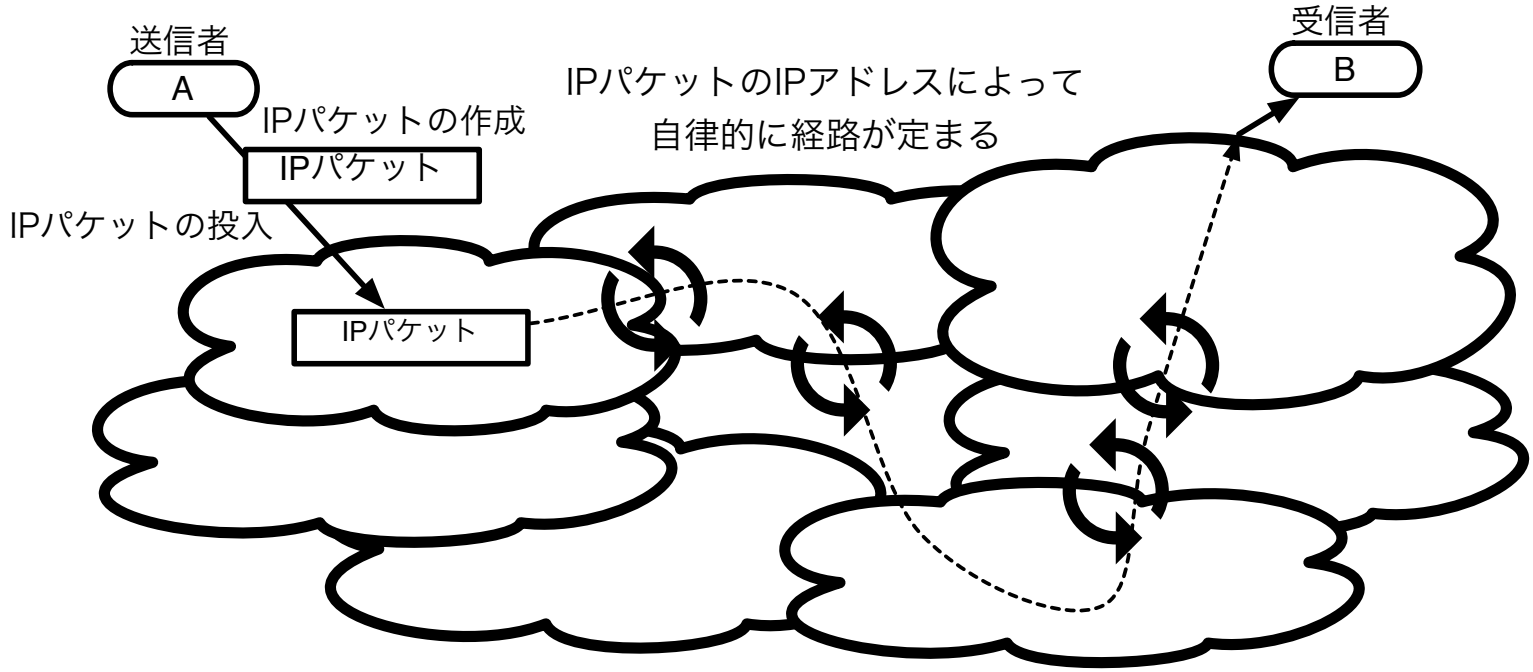
インターネットは核戦争の恐怖の下で発明された

- 回線交換方式：回線を専有する（一時的に）
- 全米の回線網は、交換局が核攻撃を受けると全身不随に陥る



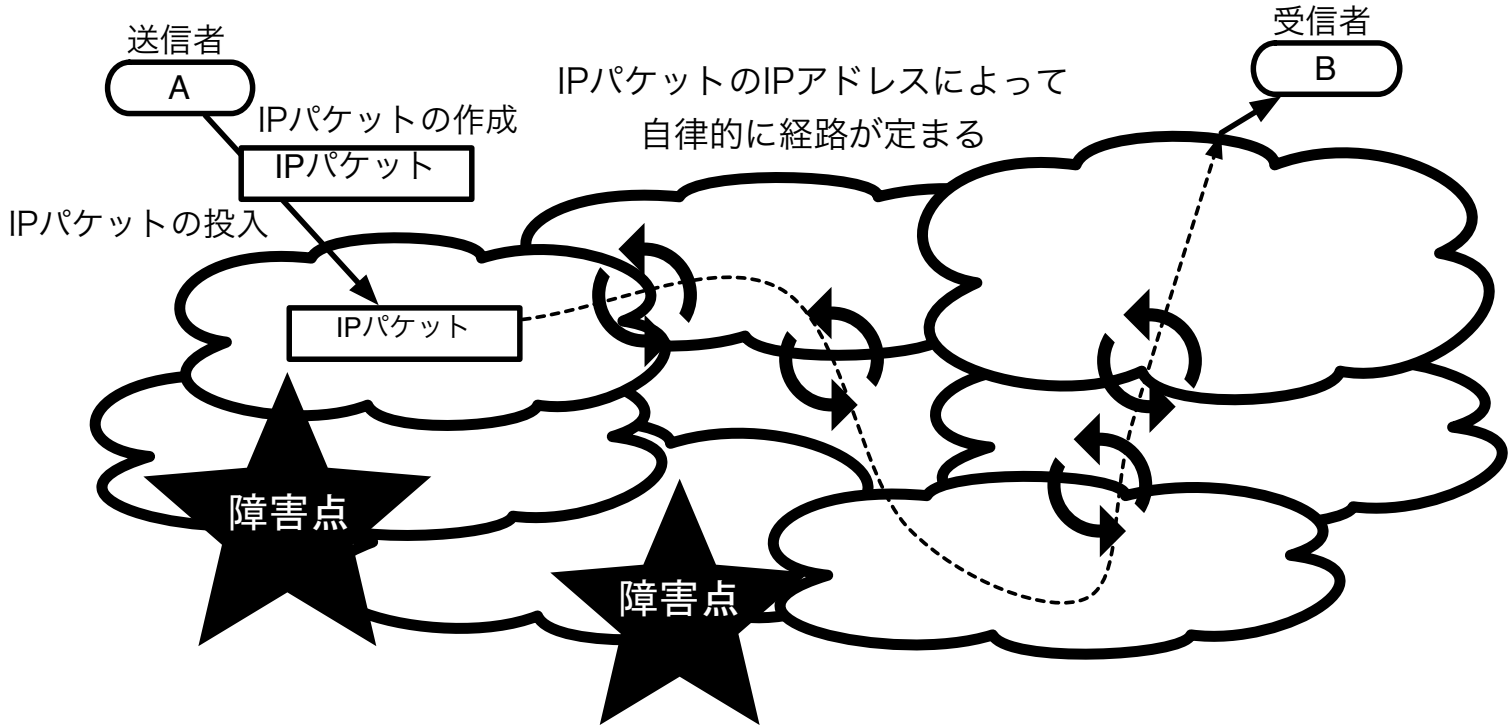
インターネット

IPパケット(宛先IPアドレスを持つデータ)
ネットワークは共有財（パブリックなネットワーク）



IPパケットによる自律的な通信

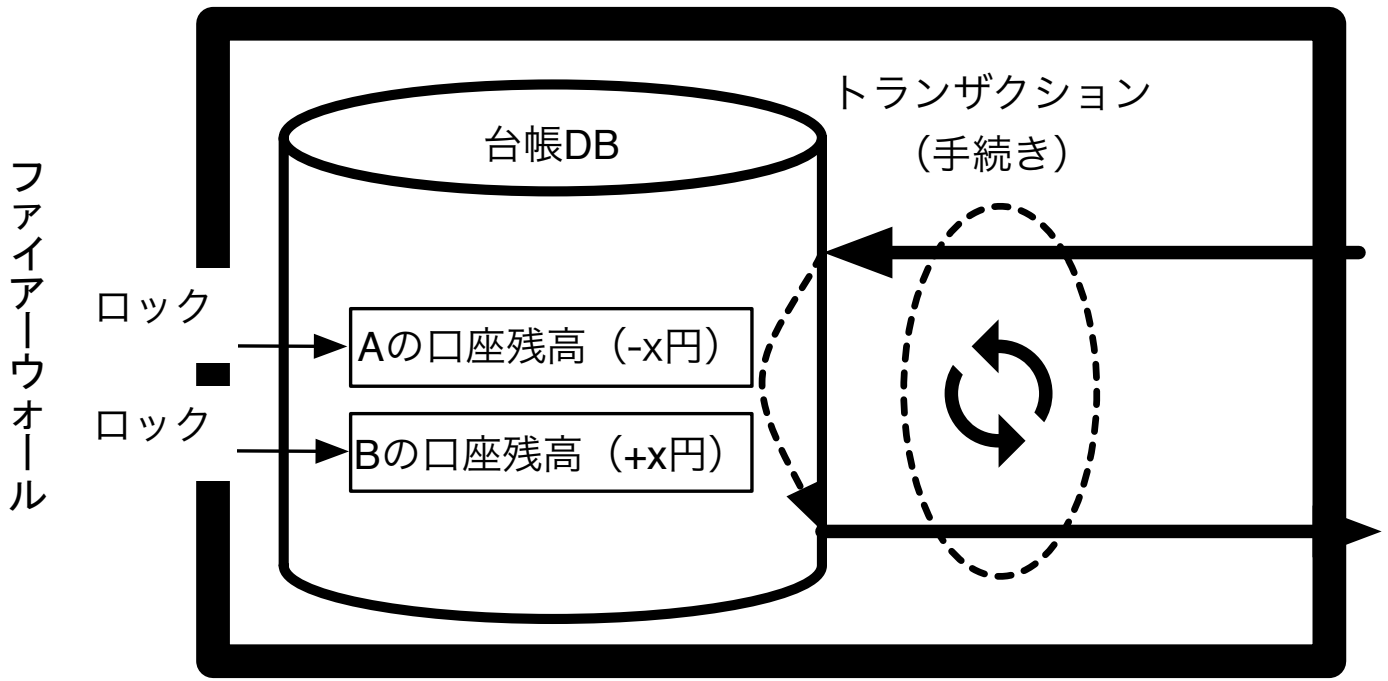
ネットワークに故障があれば、IPパケットは迂回する
障害点がない
回線を専有しない、共有資源のコストを互恵的に負担



データベースの「トランザクション」

データベースへの処理の最小単位

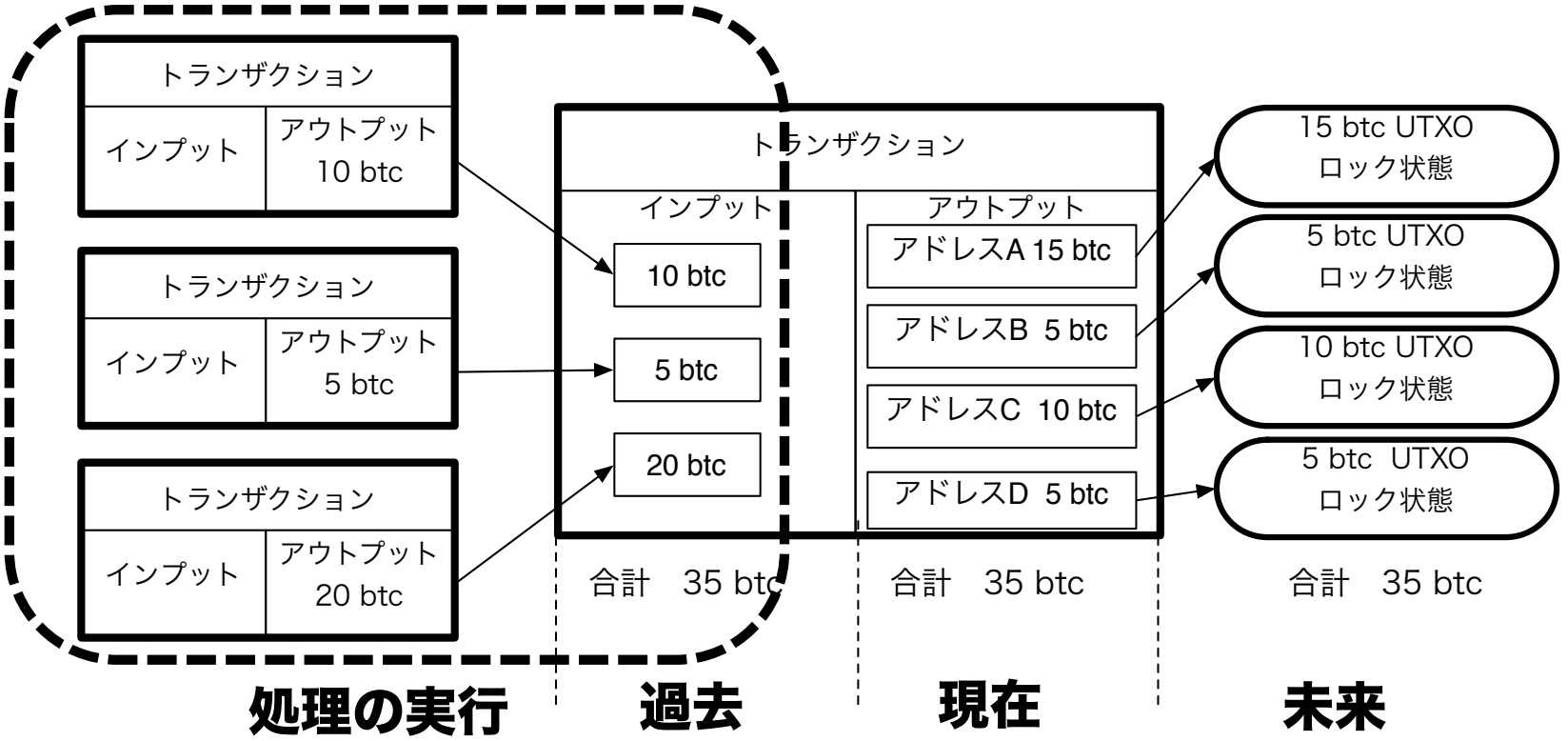
- 銀行の振込手続きはトランザクションになる
- ファイアーウォールの中の処理



ビットコインのトランザクション

トランザクションのrepresentation

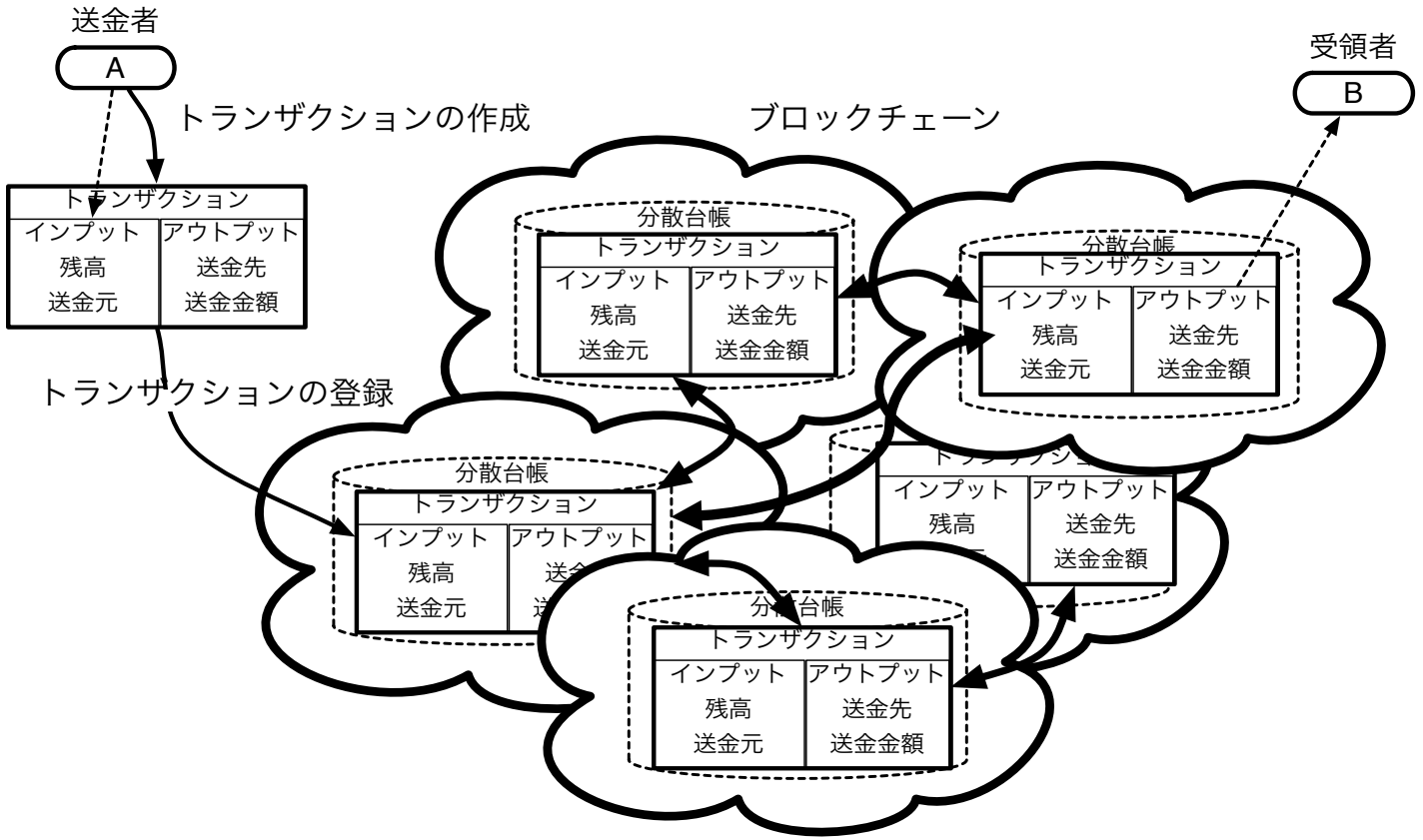
時制式三式簿記形式　＋　スクリプトによる処理



ブロックチェーンのトランザクション

送金先アドレスと処理の「表現」となる自律的データ

送金：トランザクションの作成、登録、複製の連鎖、合意

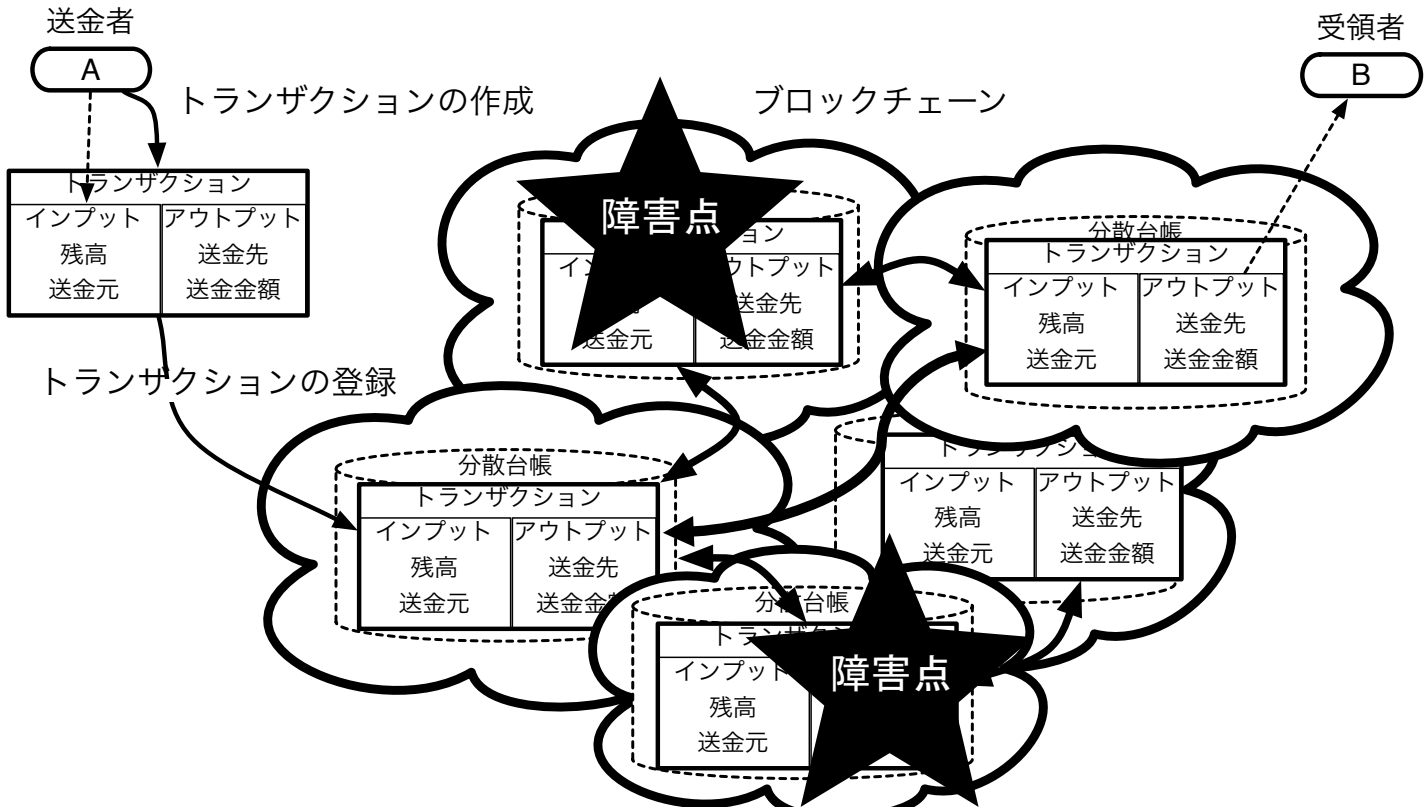


ブロックチェーンとインターネットの類似性

トランザクション＝IPパケット　（転送／送金の「表現」）

障害点がない、頑強性

資源を専有せず、互恵的に共有資源のコストを負担

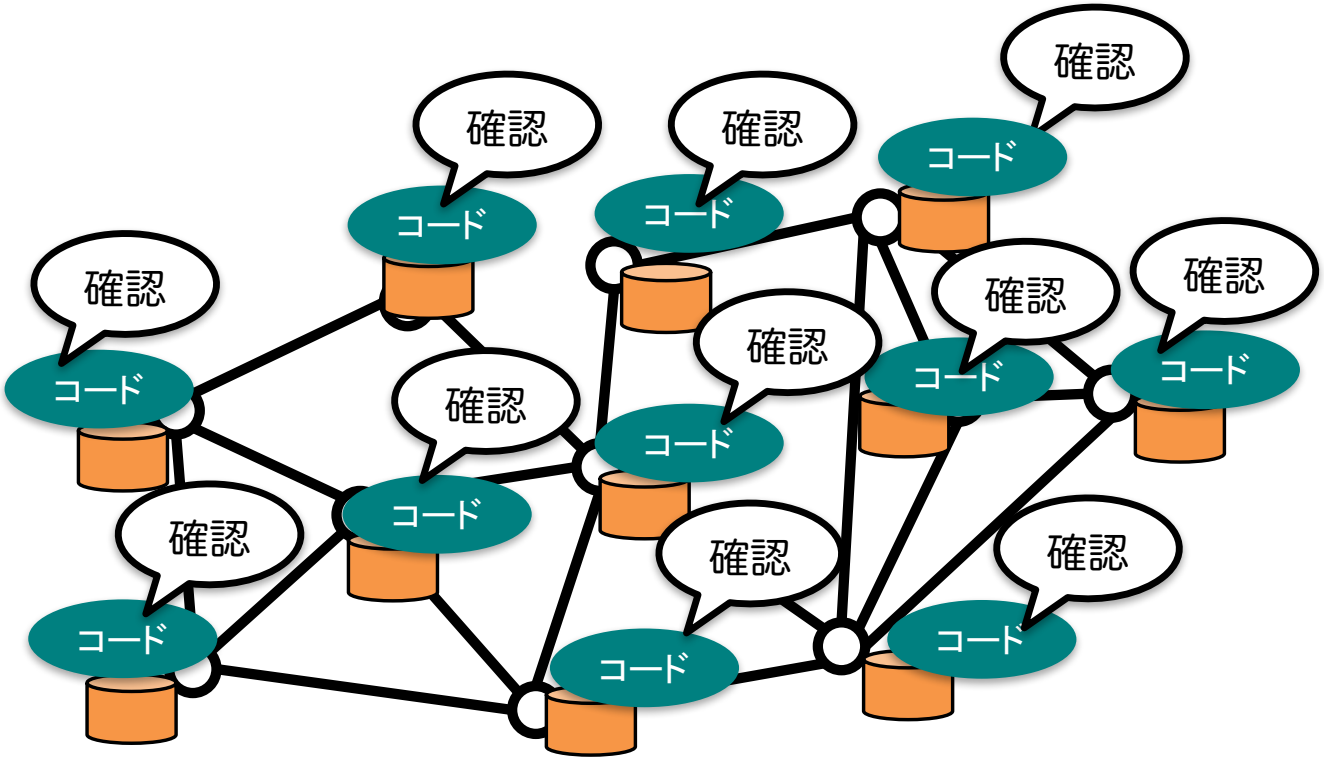


台帳監査の分散的ガバナンスとコスト

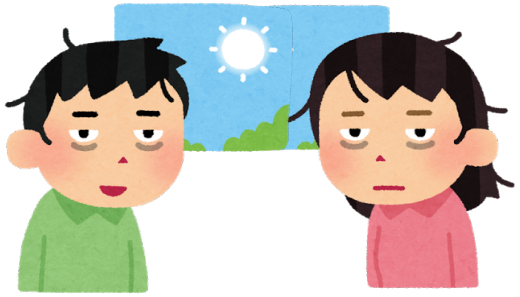
すべての記録の正当性を全員で確認し保存

互恵的なコスト分散

- 見かけのコスト削減の効果



ぜにさし（銭緡）



早起きして

前日の売上の銭を紐で通して

ぜにさしを作った

１００文として流通

早起きは３文の得

なぜ得をするのか？

お金の実体は見えないけど

民間人による暗黙の通貨発行が
行われている

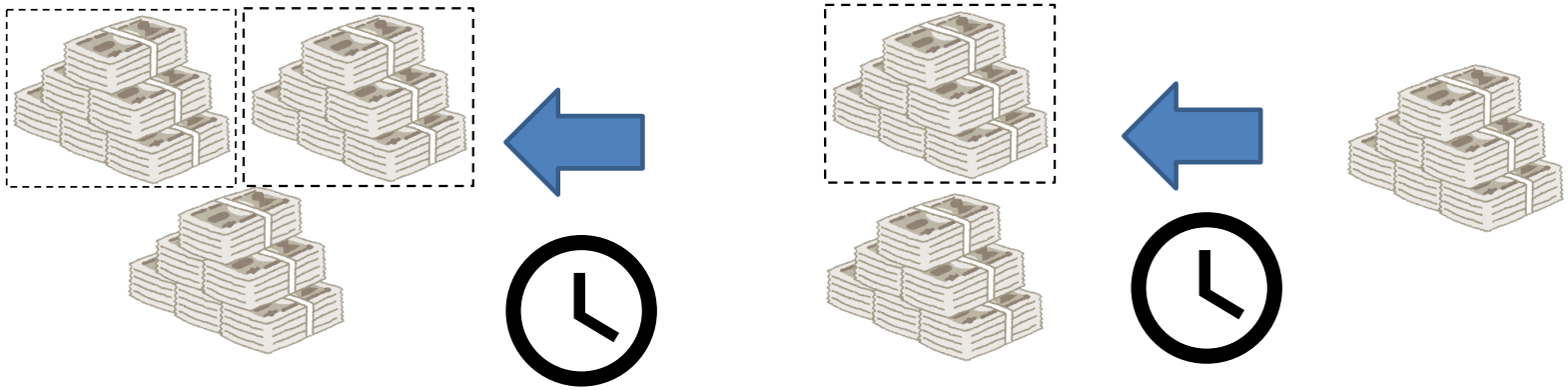
通貨発行益（シニョレッジ）＝王様／国家の特権

金利の発明

時間を利用した

民間人による暗黙の通貨発行

コシモ・デ・メディチ



ビットコインの通貨発行

消費電力が問題なる計算競争で記録の代表者を決定

プルーフ・オブ・ワーク＝莫大な計算の結果

ブロック

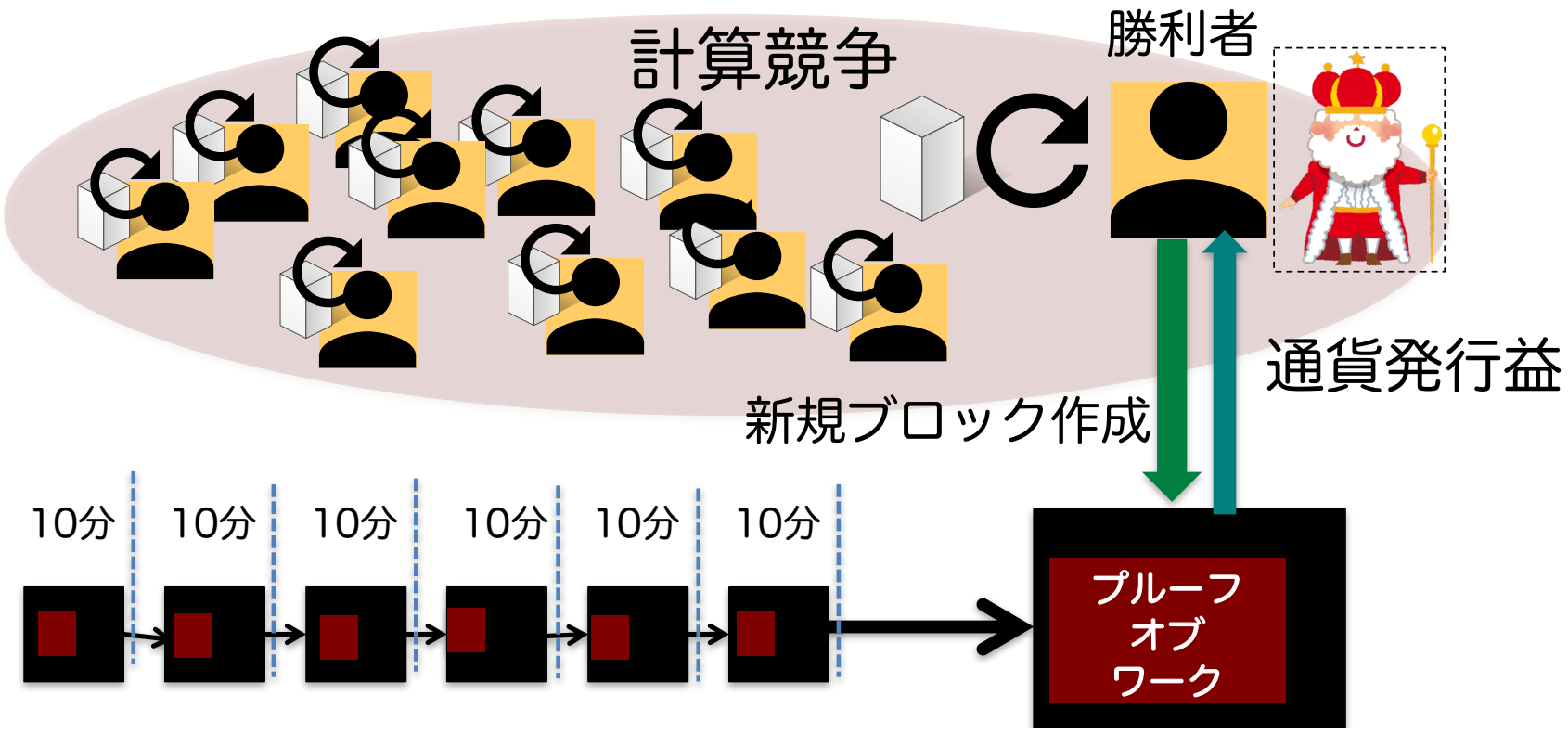
プルーフ・オブ・ワーク

報酬
取引
取引

マイニング競争

プルーフオブワークの計算競争の勝利者

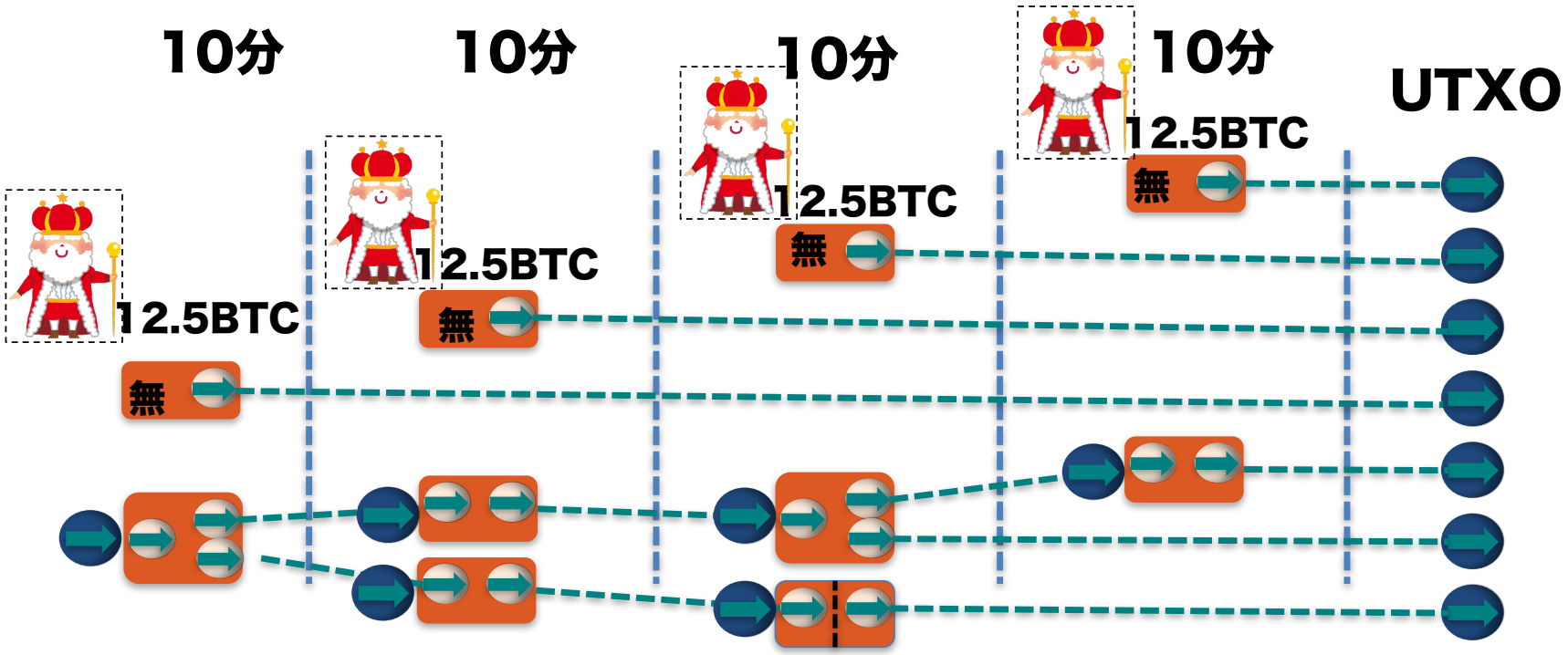
- 新しいブロックを作成し、報酬（通貨発行益）を得る



経済圏全体の「貨幣的量」は単調増加

10分ごとに一定量増加（マイナーが通貨発行）

- 増加量は（4年周期で半減）



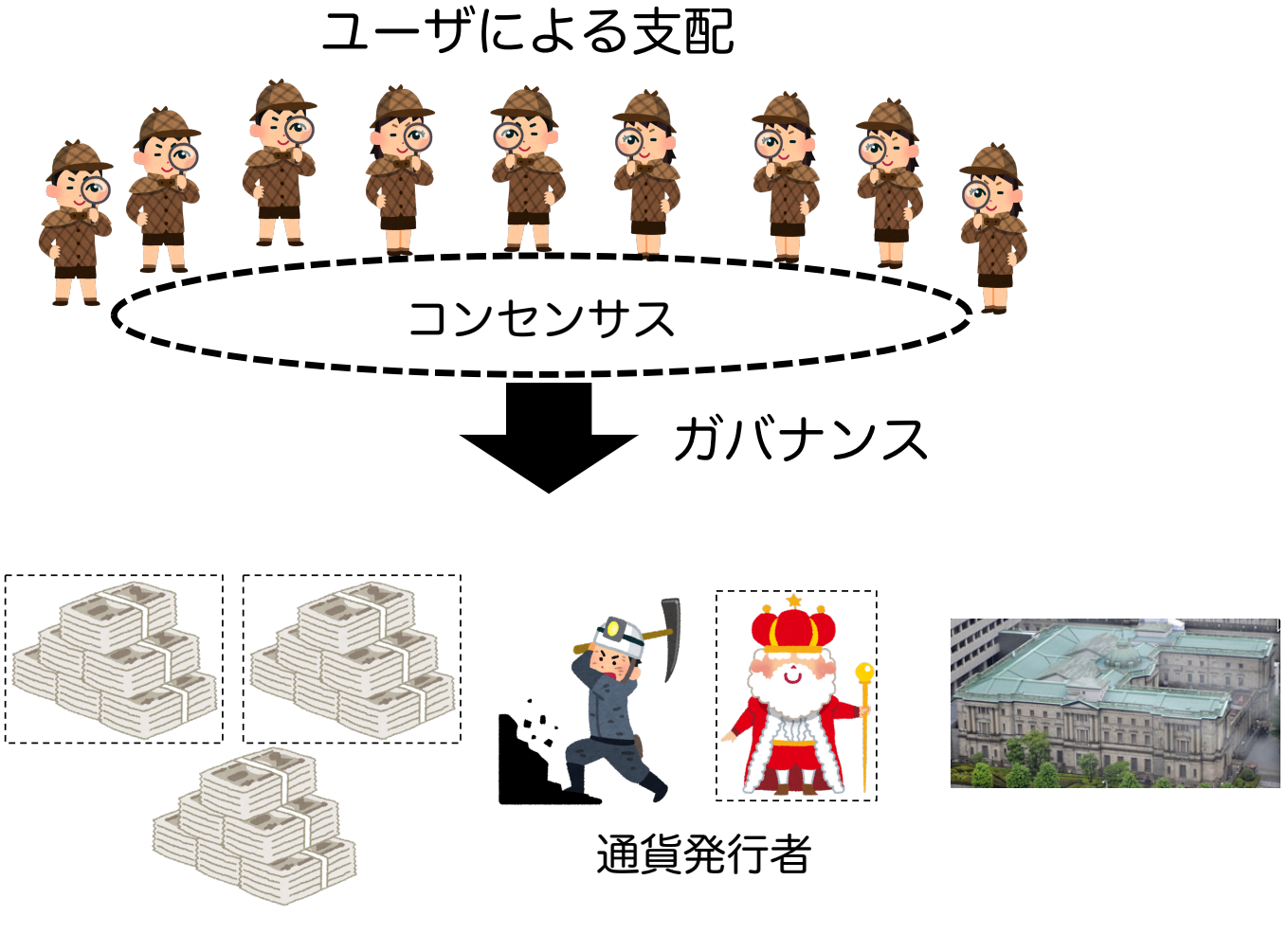
信用に基づかない通貨システム

人間の欲望によって価値が維持される通貨

企業、銀行や国家の破綻と運命をともにしない

ブロックチェーンには仮想通貨の存在が必要

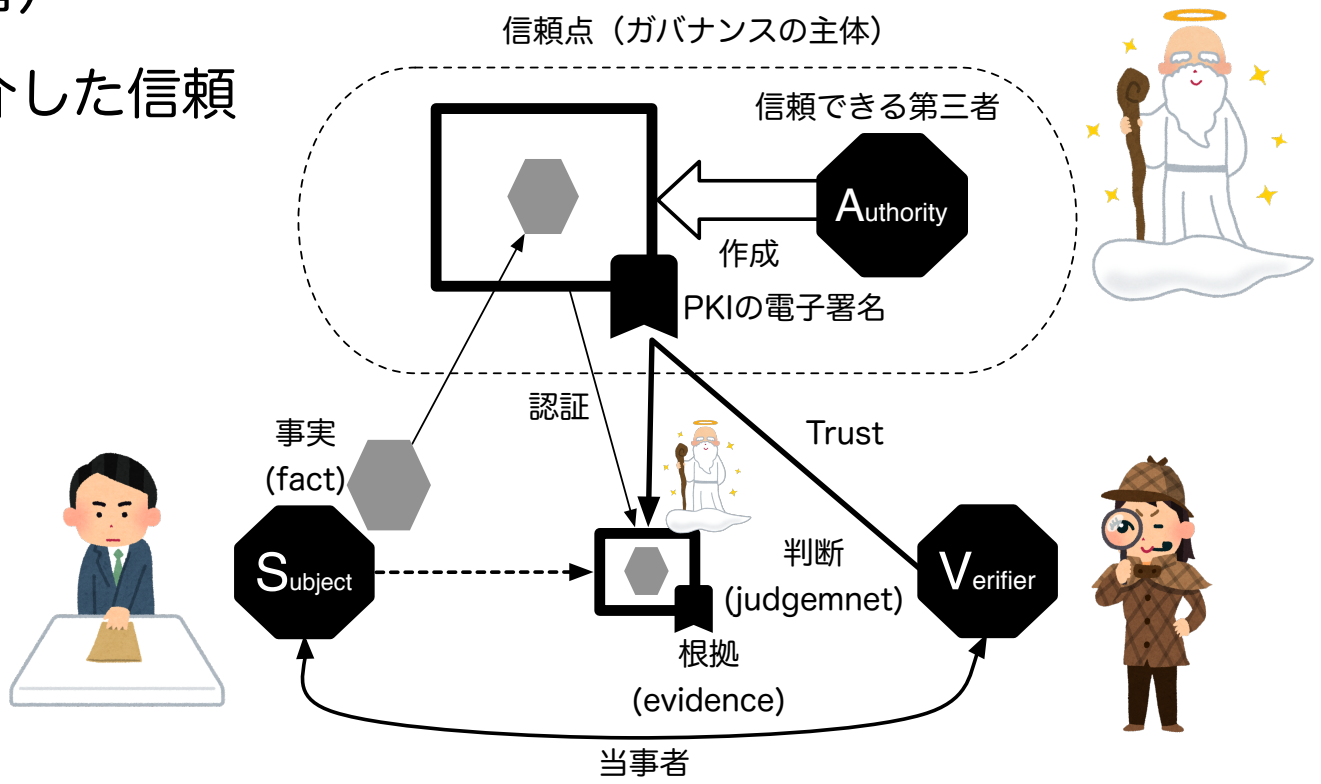
王様（通貨発行者）へのガバナンスとコンセンサス



PKIのガバナンス

信頼点が存在するモデル（信頼点がガバナンスの主体）

- 当事者（主体、検証者）
- 信頼できる第三者を介した信頼



ブロックチェーンのコンセンサスによるガバナンス

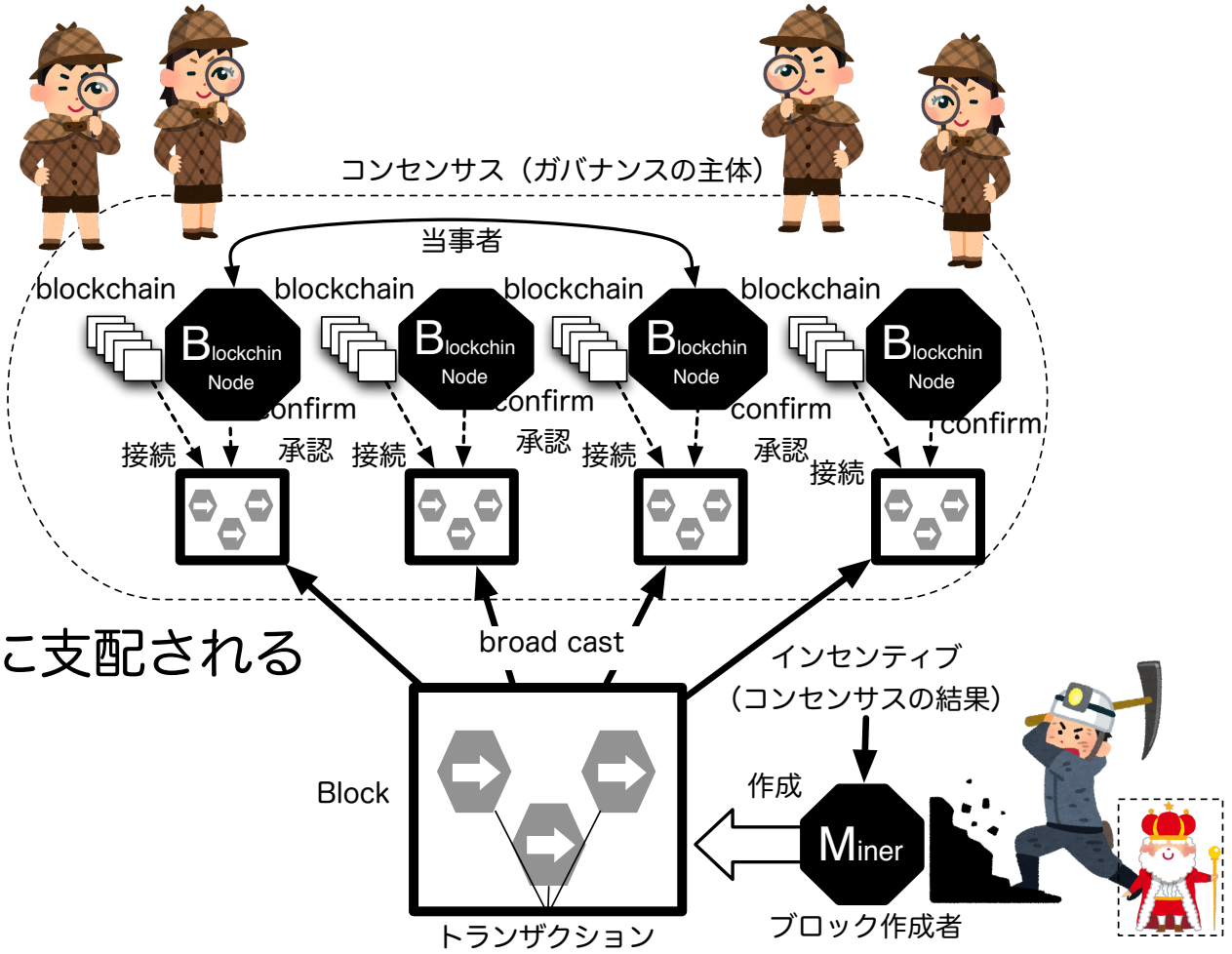
ブロックチェーンノード

- コンセンサスの主体
- ブロックを承認する

ブロック作成者(マイナー)

- 信頼点ではない
- コンセンサスの結果（承認）に支配される

PKIとは上下が反転

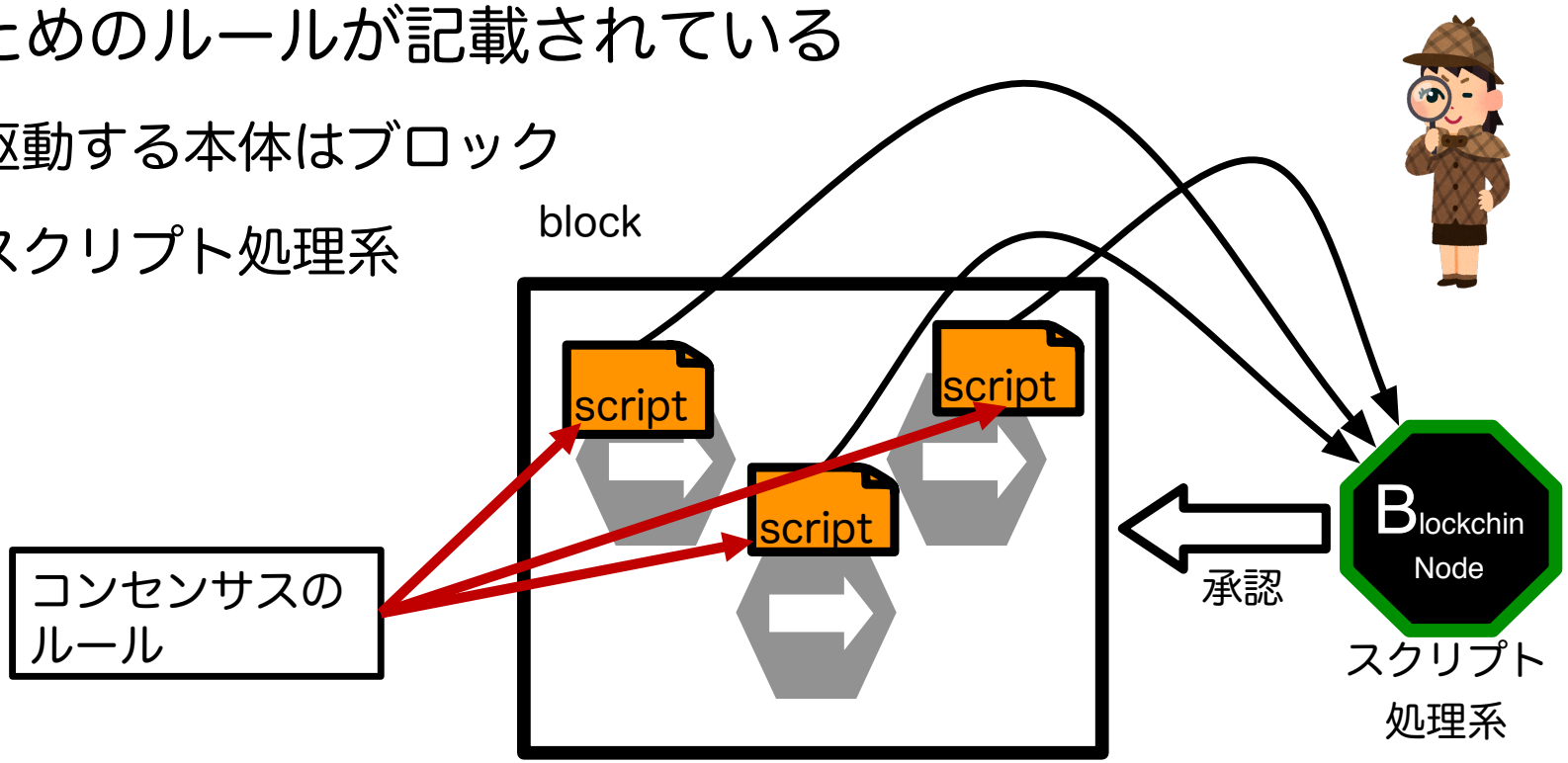


ブロックチェーンにはなぜブロックが必要か？

台帳記録にはブロックは必須要素ではない

ブロックに承認のためのルールが記載されている

- コンセンサスを駆動する本体はブロック
- ノードは単なるスクリプト処理系



ブロックとコードの仕様変更のガバナンス

ソフトフォークとハードフォーク

- ソフトフォーク

  古いバージョンのプログラムと互換性がある修正

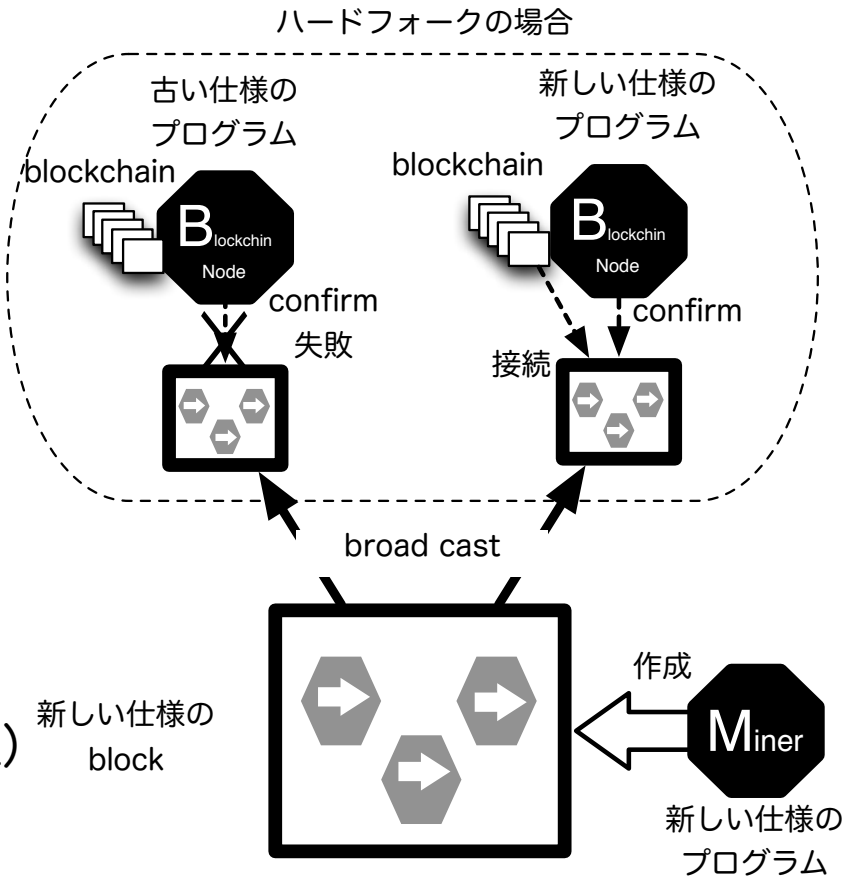
  複数バージョンの混在状態、段階的移行が可能

- ハードフォーク

  古いバージョンのプログラムと互換性がない修正

  全ノードがすべて新バージョンになる必要がある

  （さもなければ、複数のblockchainが並立する可能性）



マイナー達によるソフトフォークの支配

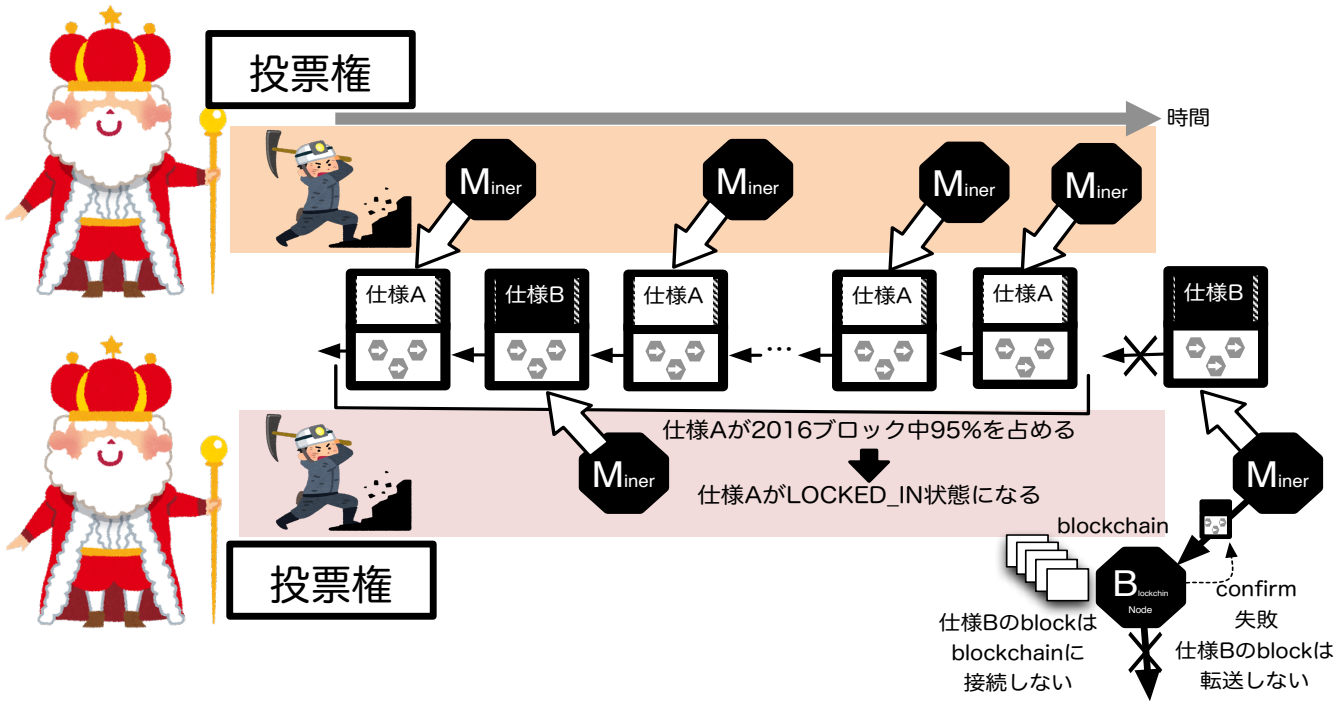
新仕様が多数派になると、旧仕様のブロックは承認されなくなる

- 95%ルール

  過去2016ブロックの95%が

  新仕様なら状態が遷移

  旧仕様のマイナーは労力が無駄



仕様変更への投票の問題

- マイナーだけが投票権を持つ

ブロックのコンセンサスと立場が逆転

先日の「ビットコイン分裂」騒動とは

マスコミの報道はほとんどが不正確だった

- 立場によって説明内容が偏るのはしかたがない
- しかし、中国のマイナーの（誤った）主張をそのまま一方の意見として報道

SegWit（ソフトフォークの例）

重要な技術（ビットコインの課題をことごとく解決する）

- トランザクション・マリアビリティの問題を本質的に解決
- 「未署名のトランザクション」という新しい技術要素が登場

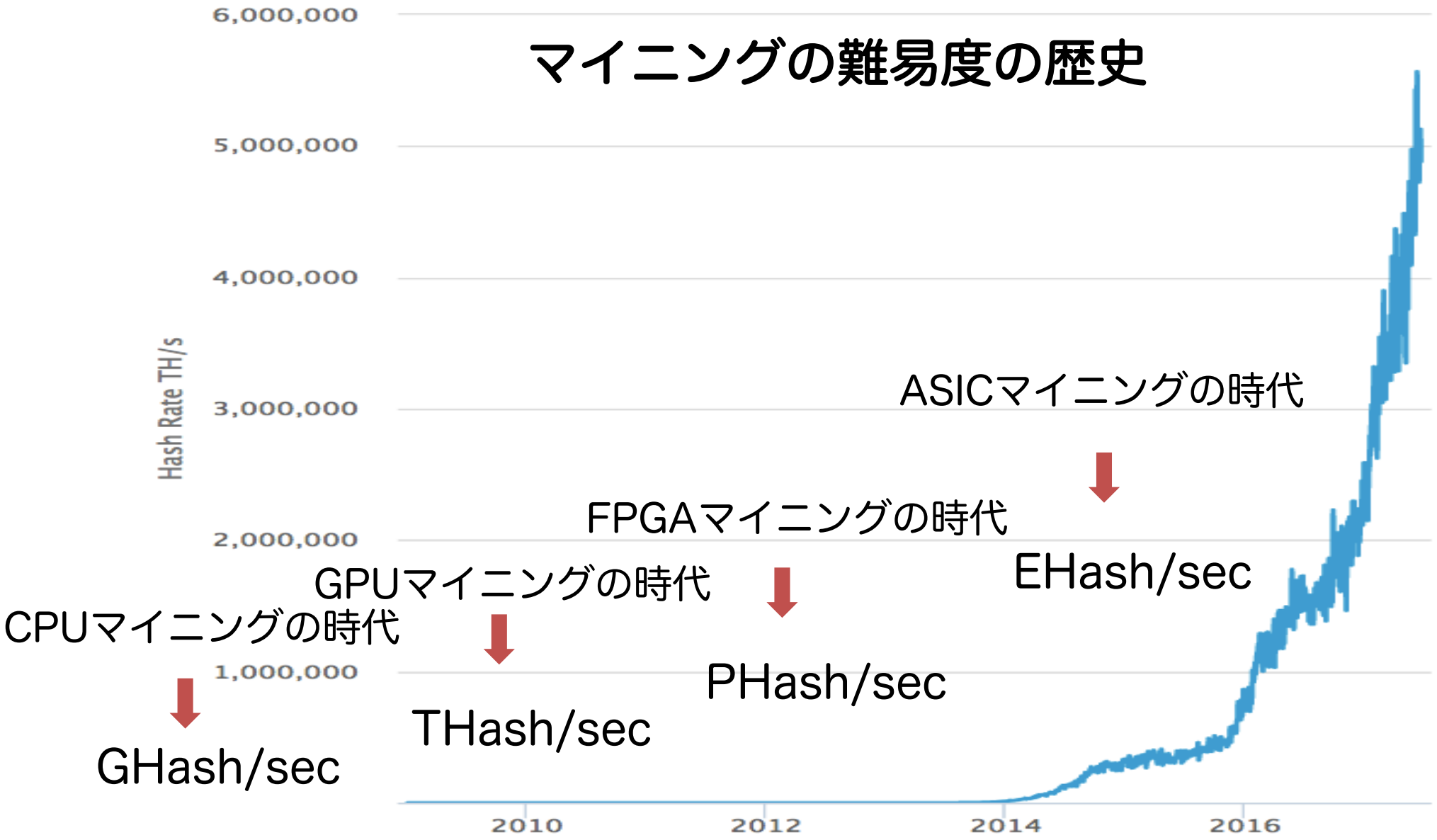
  オフチェーンスケーリングやサイドチェーンが可能になる

    高速取引、取引数の上限が無くなる、取引のプライバシの確保

SegWit有効化以降の
ビットコイン価格の高騰

１BTC　20万円　→　50万円

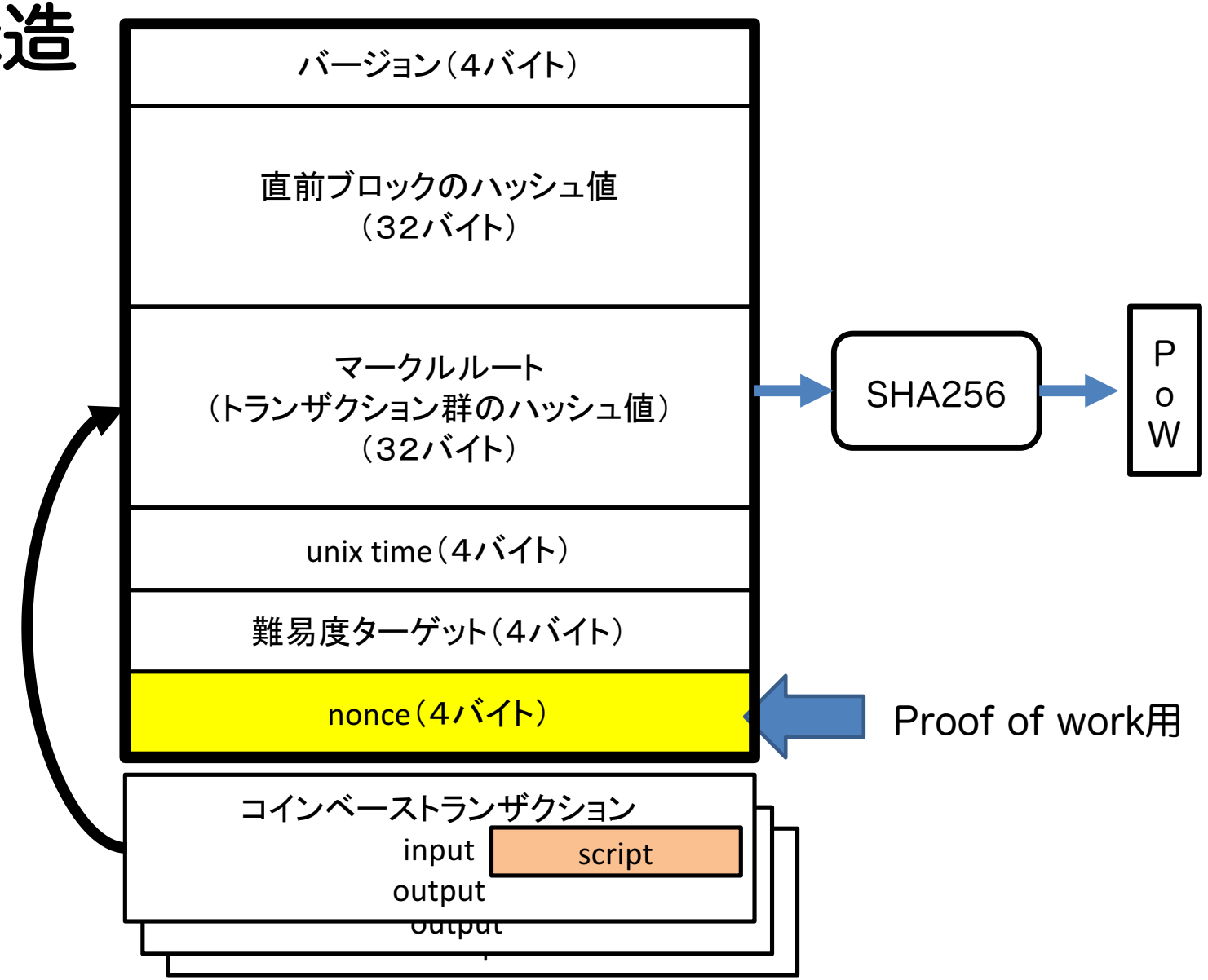
マイニングの難易度の歴史



ブロックの構造
80バイト

proof of work

ブロックヘッダの
sha256ハッシュ値が
難易度ターゲットより
小さいもの



ブロックの構造
80バイト

ハッシュレートが向上

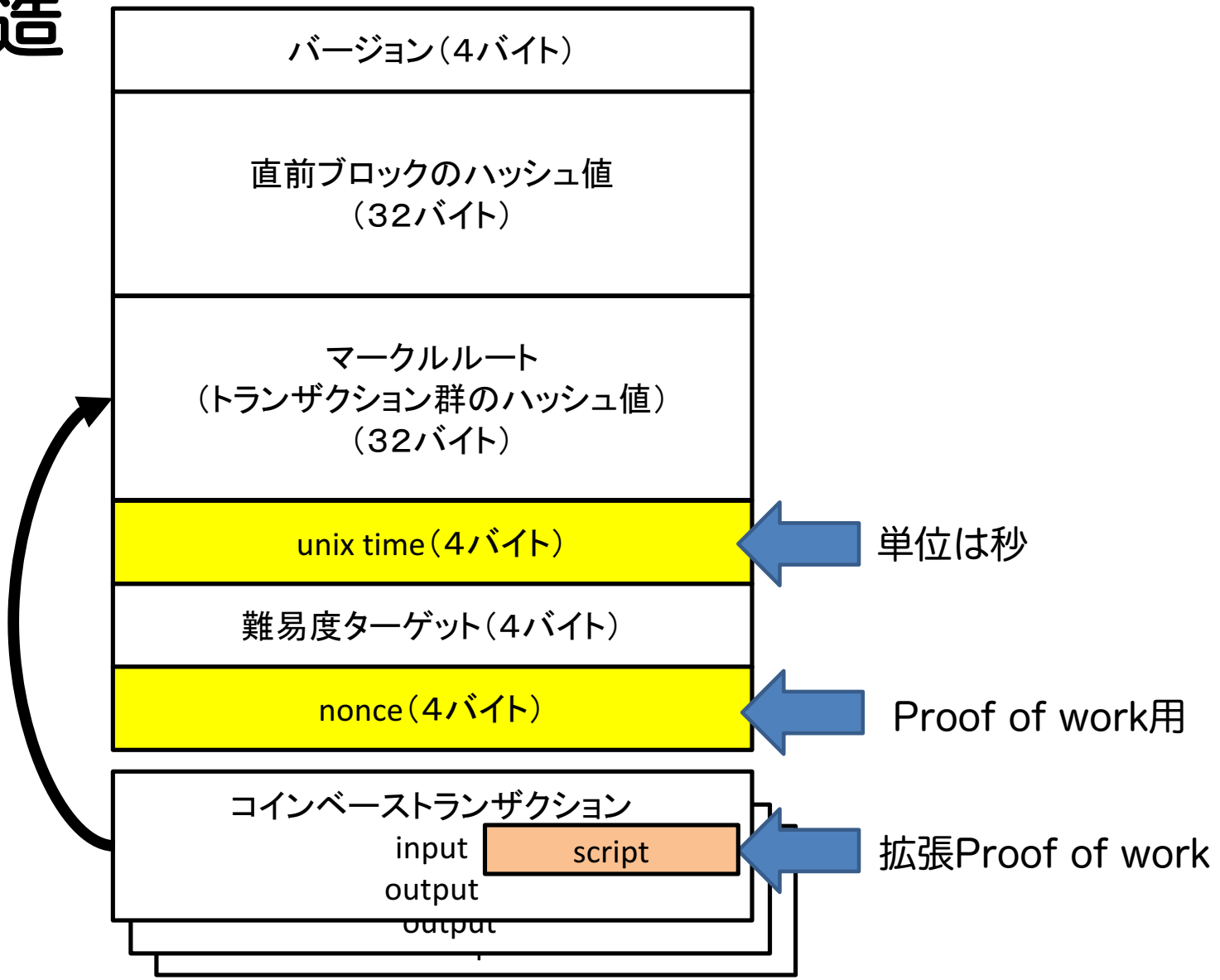
10分以内に4バイト

全部終了

タイムスタンプを利用して

nonceをリセット

4.3 GHash/sec



ブロックの構造
80バイト

ハッシュレートが向上

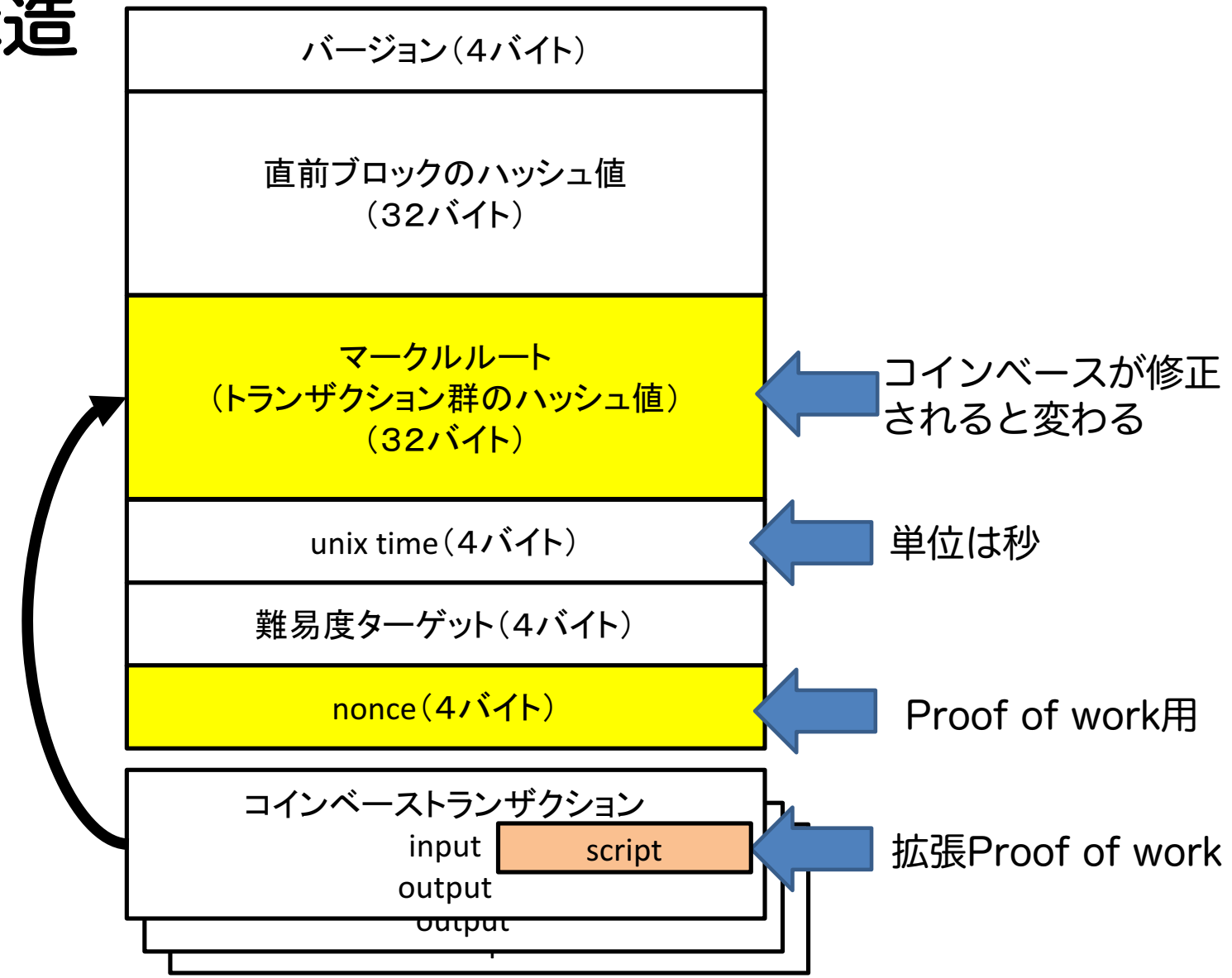
10分以内に4バイト

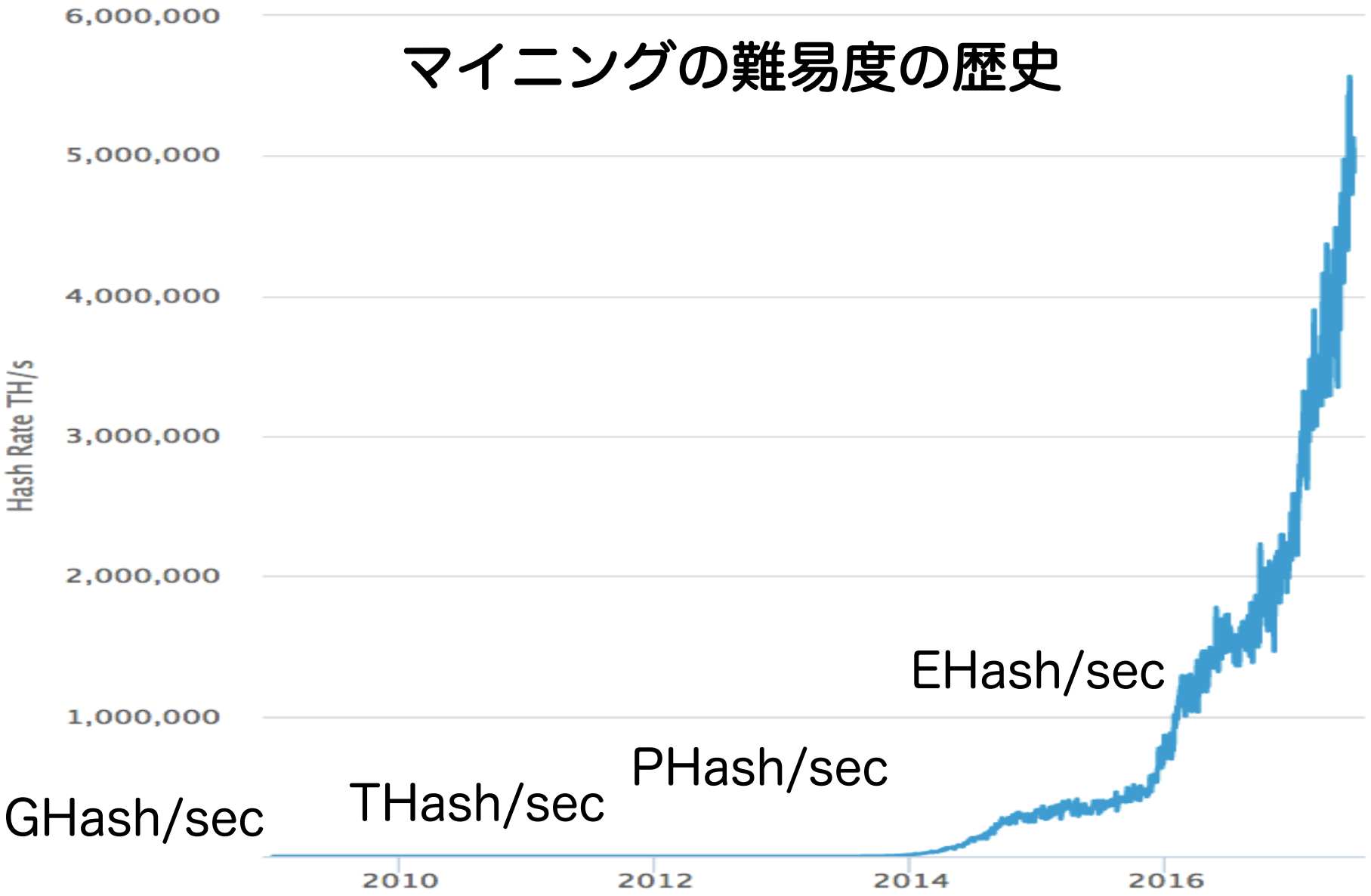
全部終了するのが

1秒以内になった

タイムスタンプは

利用できなくなった




マイニングの難易度の歴史
6,000,000
5,000,000
4,000,000
3,000,000
2,000,000
1,000,000
Hash Rate TH/s
2010
2012
2014
2016
GHash/sec
THash/sec
PHash/sec
EHash/sec

ブロックの構造
80バイト

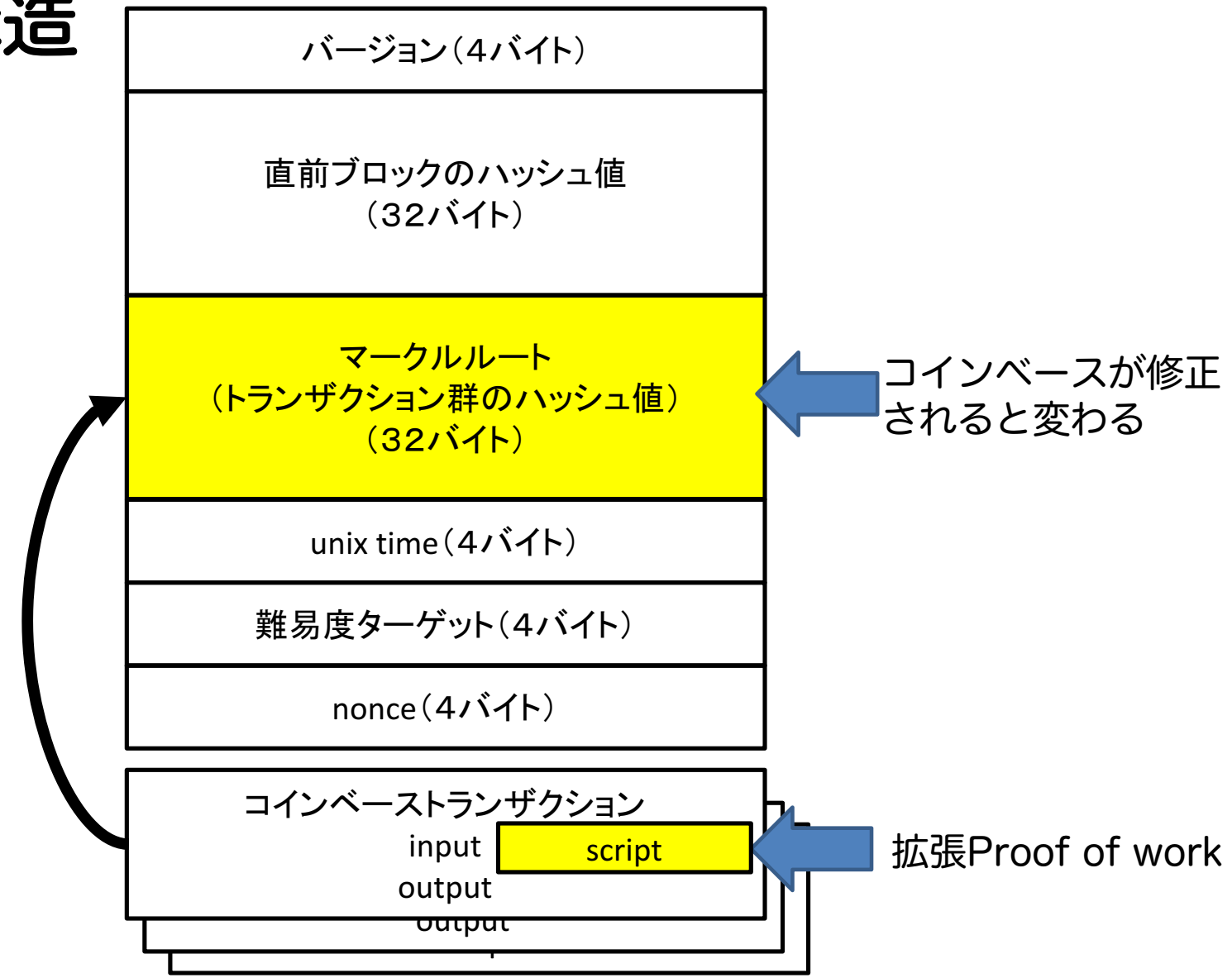
コインベースの

インプットスクリプトを

修正する

⇩

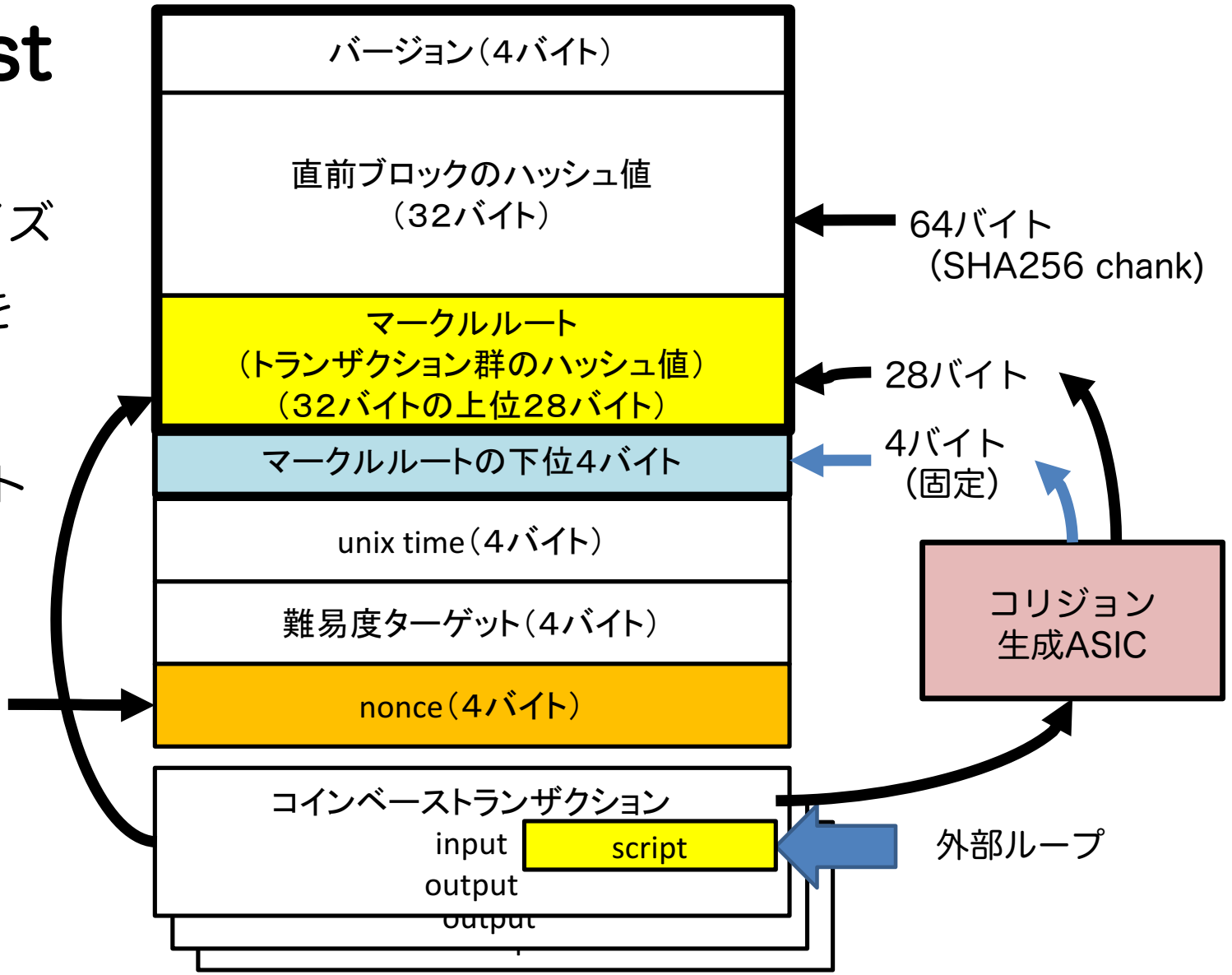
マークルルートが変わる



ASIC boost

SHA256のチャンクサイズが64バイトであることを利用して、マイニング領域を4バイト減らす攻撃

マイニング計算のASIC内部ループで利用



中国のマイナーがSegWitに反対した理由

Asic Boostができなくなる

結局、別の仮想通貨をスタートさせた　→　bitcoin cash

世界のフルノード数

約９０００　（7月になって急激に増加）

GLOBAL BITCOIN NODES DISTRIBUTION

Reachable nodes as of Wed Aug 09 2017 13:57:26 GMT+0900 (JST).

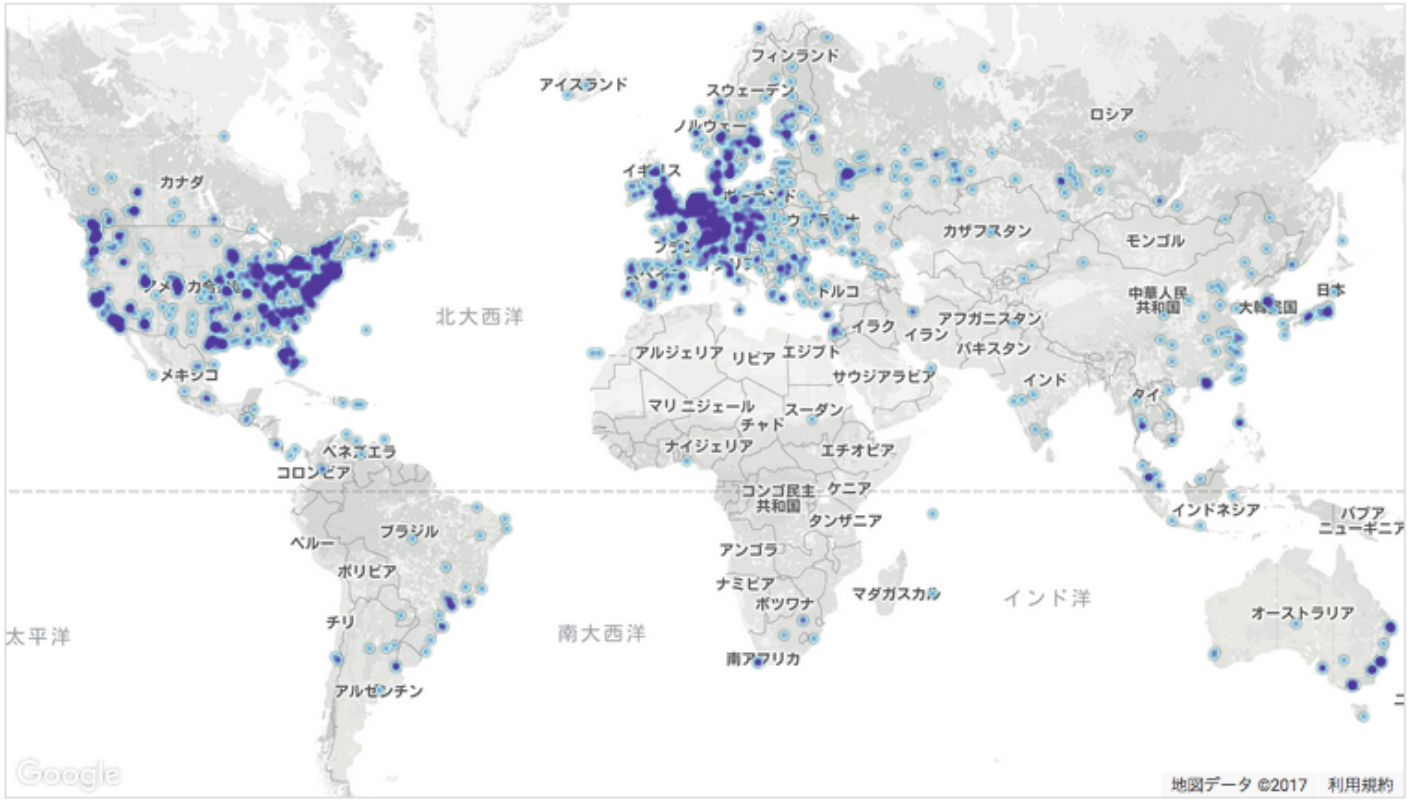
8959 NODES

24-hour charts »

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

RANK	COUNTRY	NODES
1	United States	2616 (29.20%)
2	Germany	1585 (17.69%)
3	France	593 (6.62%)
4	Netherlands	449 (5.01%)
5	China	401 (4.48%)
6	Canada	356 (3.97%)
7	n/a	317 (3.54%)
8	Russian Federation	315 (3.52%)
9	United Kingdom	309 (3.45%)
10	Singapore	176 (1.96%)

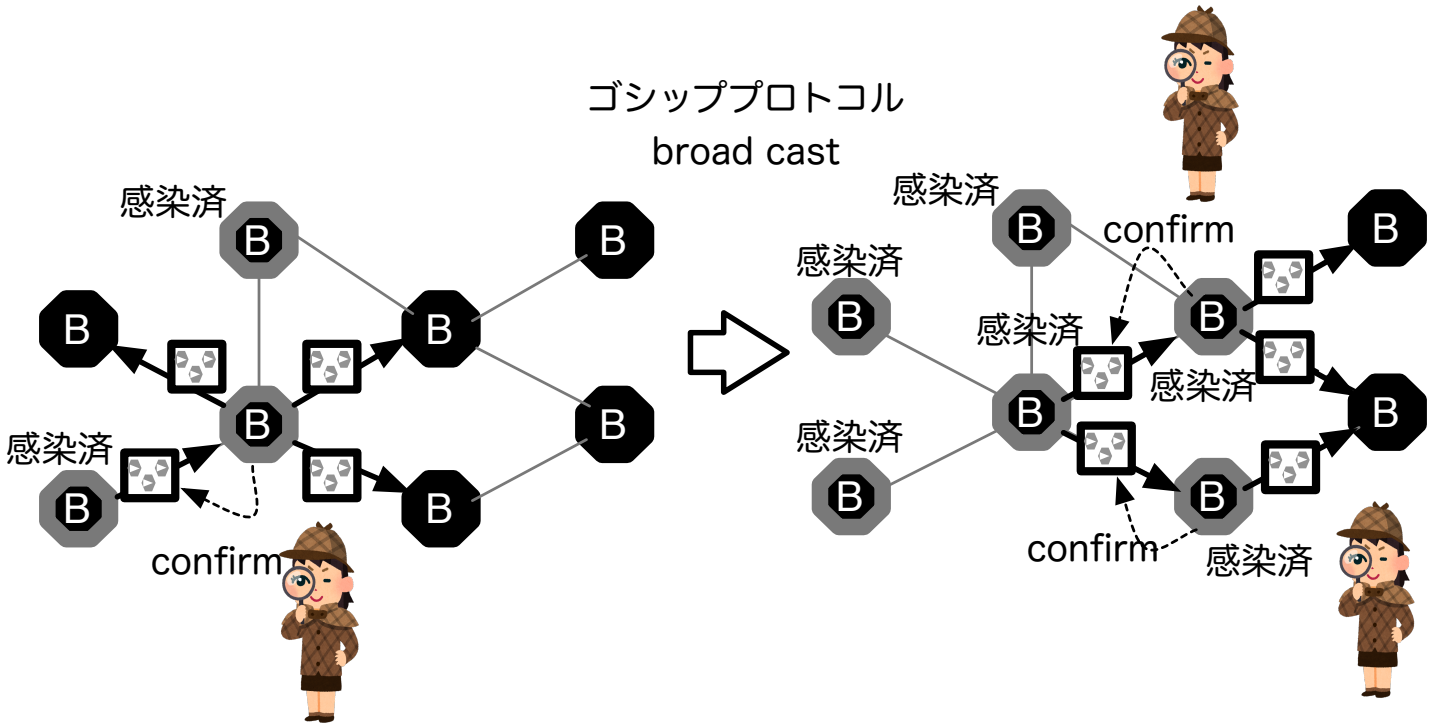
More (89) »



ブロックのBroadcast にも承認処理がある

ゴシッププロトコル（感染プロトコル）

- 自分のノードに隣接する未感染のノードにブロックを転送する
- 受信したノードは、感染状態になり、同じことを行う



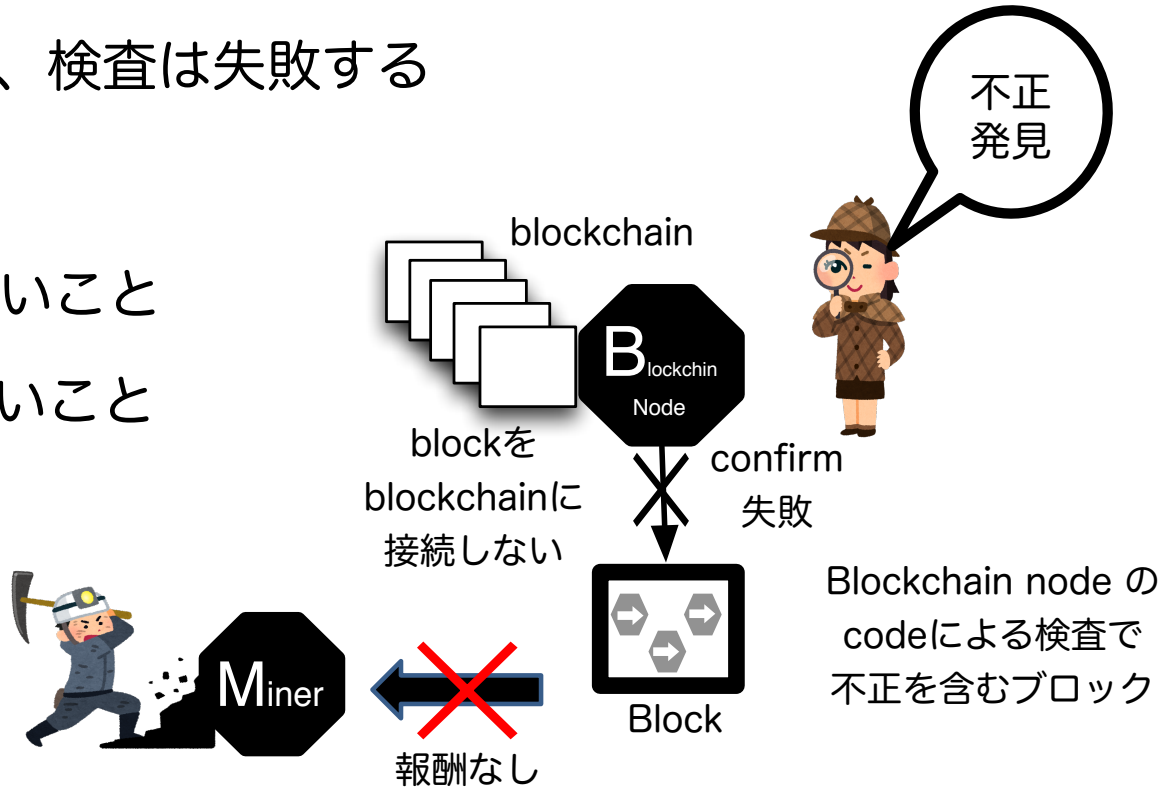
Bitcoin nodeがブロックを承認しない場合

Bitcoinのブロックは、必ず承認されるわけではない

- Bitcoin node は、codeの仕様に沿ってブロックを検査する
- ブロックが不正を含んでいた場合、検査は失敗する

ブロックを承認しないとは？

- ブロックをblockchainに接続しないこと
- 隣接ノードにブロックを転送しないこと

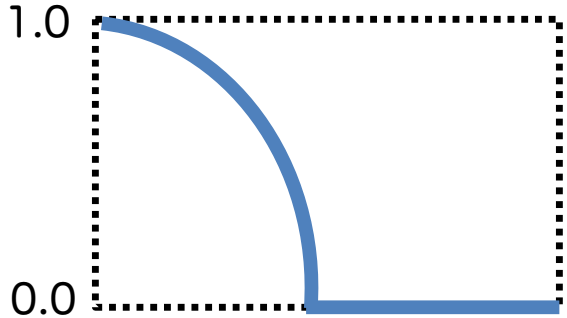


economic majority（経済圏の相転移）

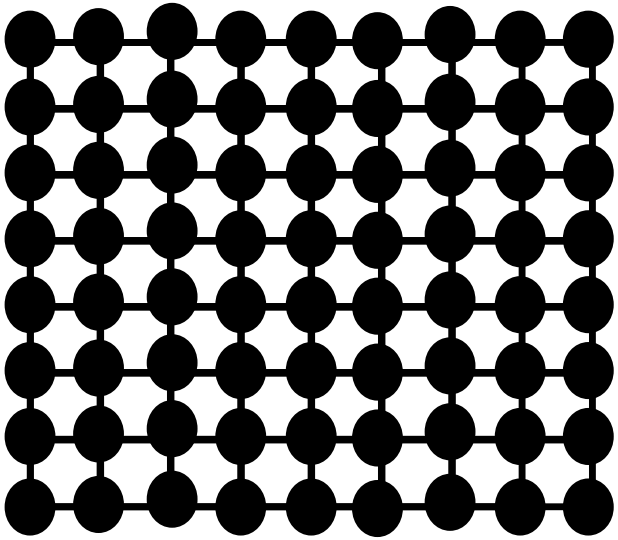
P2P型ブロードキャストの成功確率

●古い仕様も承認するノード

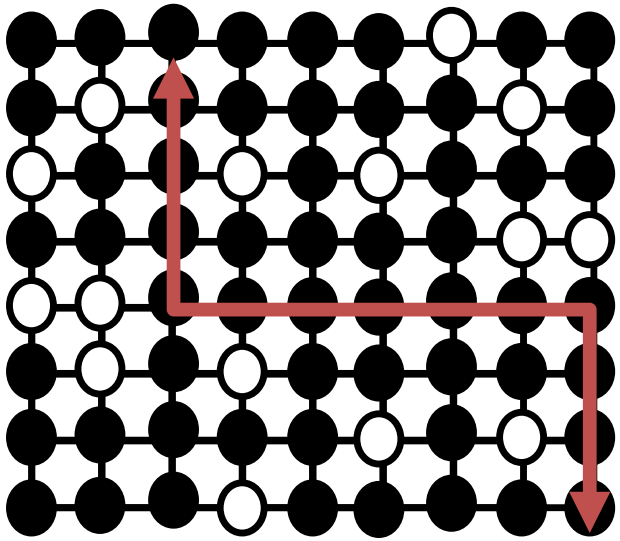
◯新しい仕様だけを承認するノード



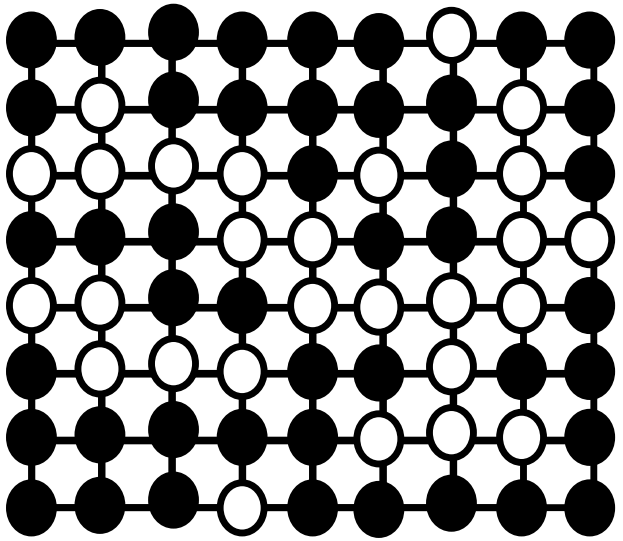
旧仕様相
すべてのノードで送金可能



旧仕様相
旧仕様のノードへは送金可能



新仕様相
旧仕様の送金はほぼ失敗する



近畿大学山崎研究室のフルノード

９０台稼働予定(今年の夏)

- ラズベリーパイ（８０台）、PC（１０台）

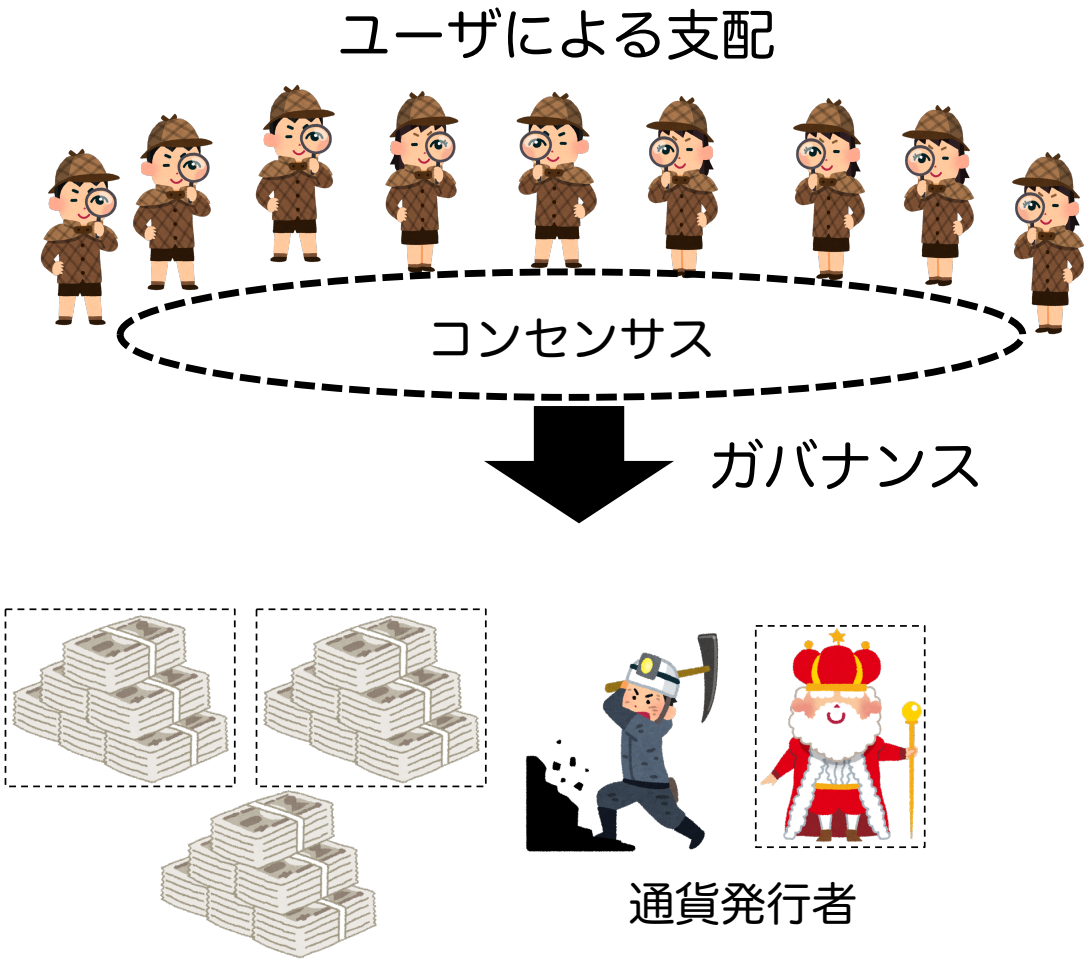
全世界のユーザノード、シグナリングの１％を支配する予定

- 相転移の確率をシミュレーションする予定

UASF（ユーザ主体のソフトフォーク）

コンセンサスのルールを支配するのはユーザ

- マイナーを適切に管理する方法はまだ良くわからない
- ユーザによるガバナンスにも経済原理が働く必要がある？



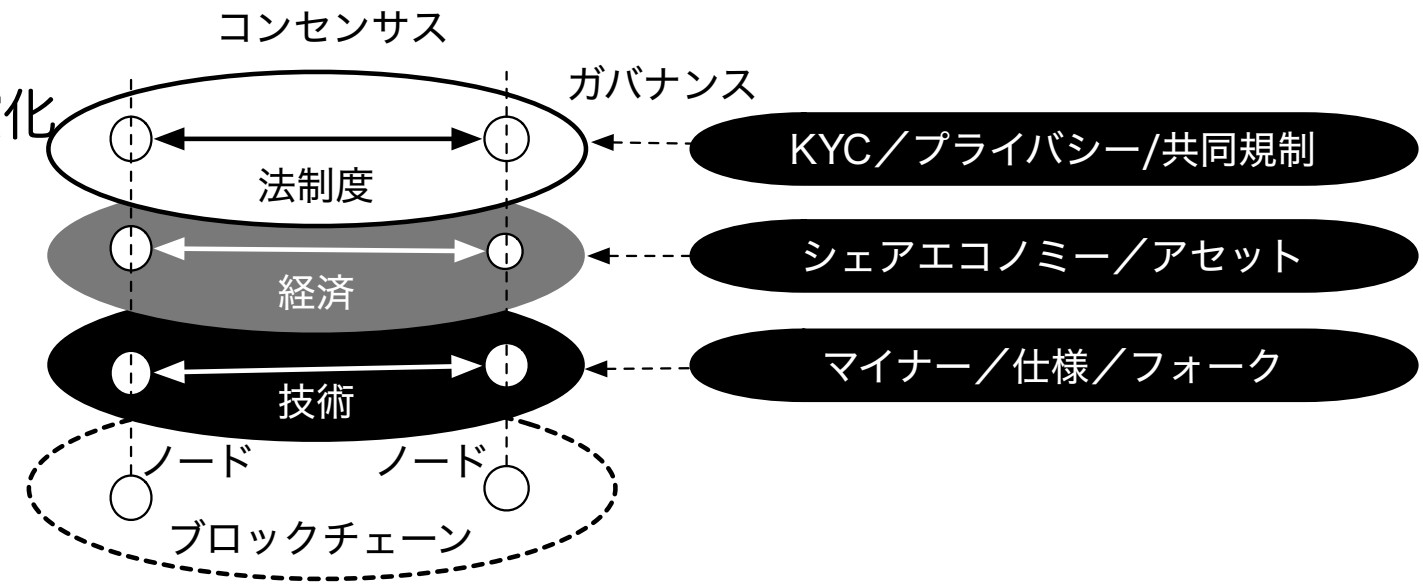
ブロックチェーン・エコノミーの三層モデル

仮想通貨は特殊な応用

- コンパクトに自己完結

仮想通貨以外への応用　→　利害関係者やエコシステムが急に複雑化

- レイヤ化による整理
- ステークホルダの明確化
- ガバナンス



規制は無い方が自由なのか？

無法地帯は、とてもコストがかかる

安全と水はタダではない

規制のない世界での経済活動はとてもコストが高い

ブロックチェーン・エコノミー

新しい仕事を創り出すプラットフォーム

- AI（人工知能）は人間から既存の仕事を奪っていく技術
- ブロックチェーンは、人間の仕事を創出を支援する技術

- シェアリングエコノミー
- （個人が雇用者から事業者なる経済）

  所有資産の商材化の支援、創作物や二次創作物の利益を得やすい流通

ブロックチェーン・エコノミー
経済レイヤの例（スマートプロパティ）

仮想通貨に通貨以外の価値を付与する

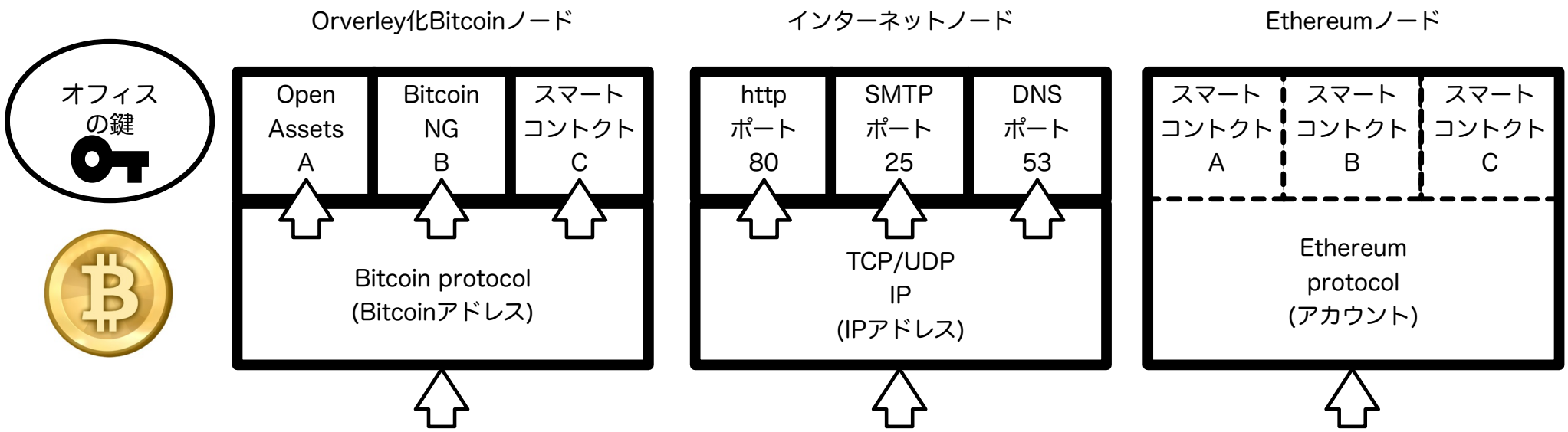
- 偽造できない、
- 二重使用できない、
- 個人から個人へ転々譲渡できるという性質を引き継ぐ

ブロックチェーン・アプリケーション

ビットコインアドレス　~　IPアドレス

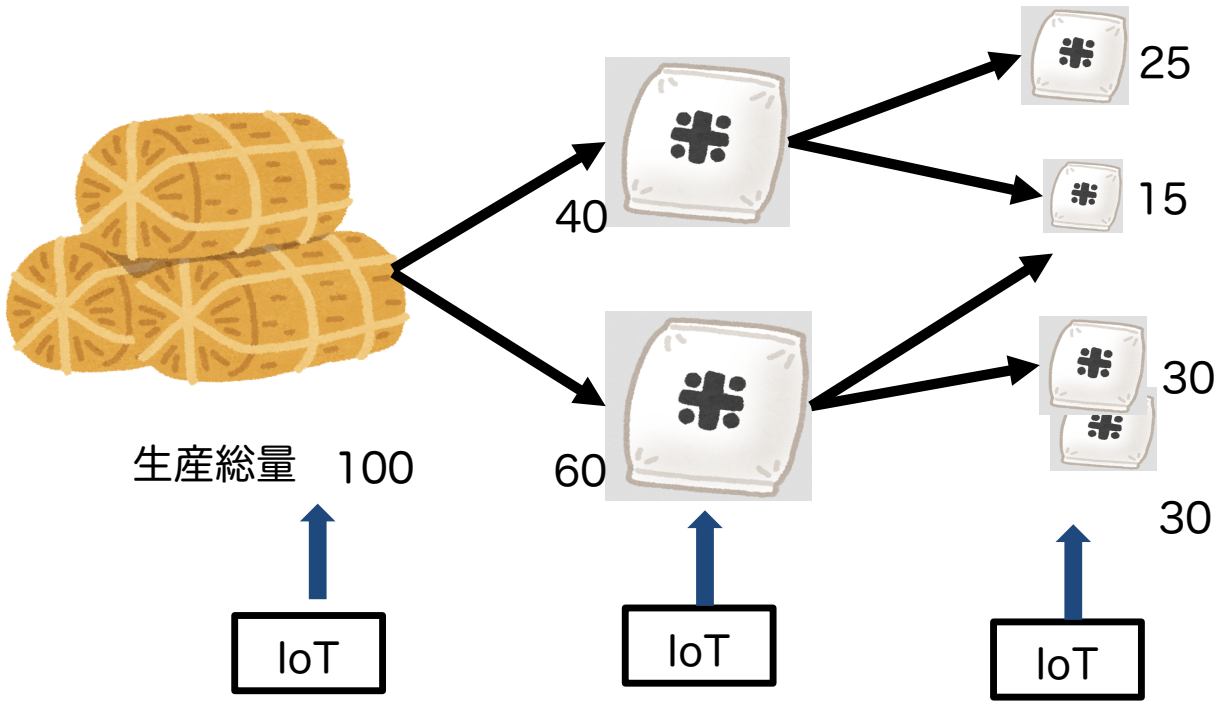
ビットコインの上位層としてアプリケーションレイヤを追加する

ワレットのアーキテクチャとして定義可能



ブロックチェーン・エコノミーに適した例

総量保存則の利用（流通の途中で増減しない）



法的規制

業界の共同規制

自主規制

ブロックチェーン・エコノミー

新しい仕事を創り出すプラットフォーム

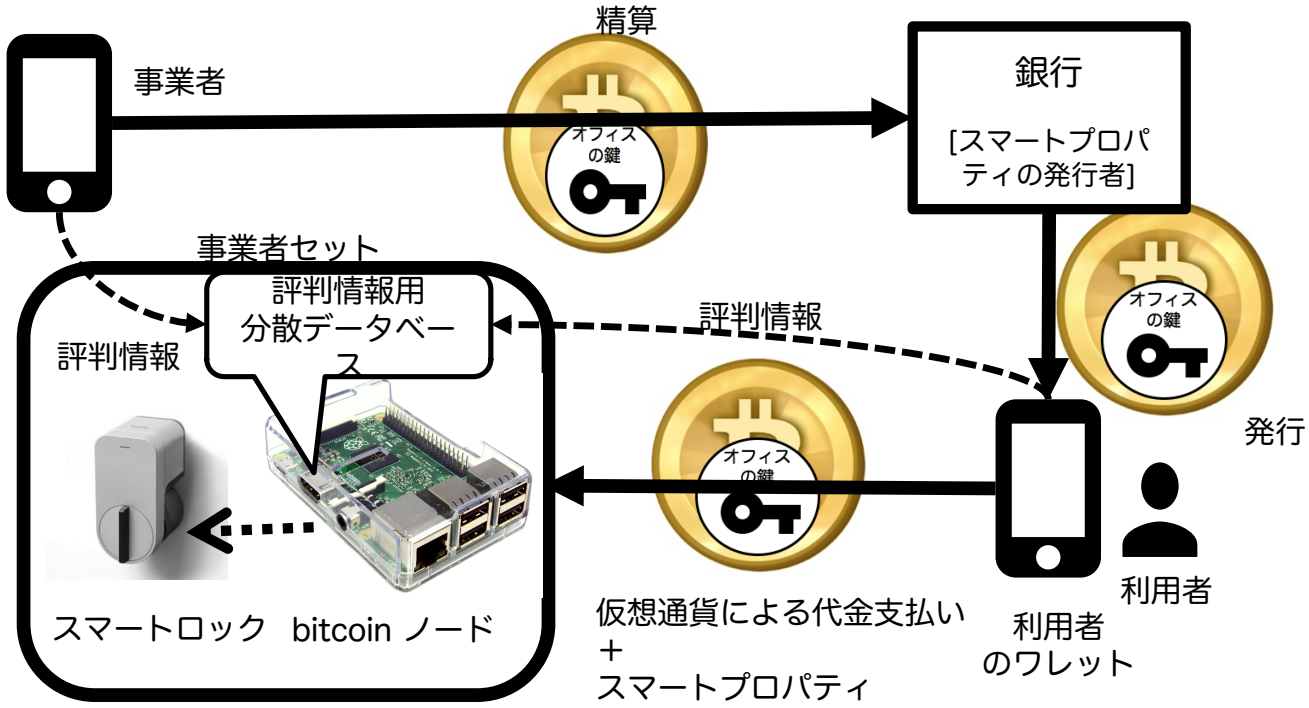
- AI（人工知能）は人間から既存の仕事を奪っていく技術
- ブロックチェーンは、人間の仕事を創出を支援する技術

- シェアリングエコノミー
- （個人が雇用者から事業者なる経済）

  所有資産の商材化の支援、創作物や二次創作物の利益を得やすい流通

スマートロックによるシェアオフィスの例

スマートプロパティの経済圏



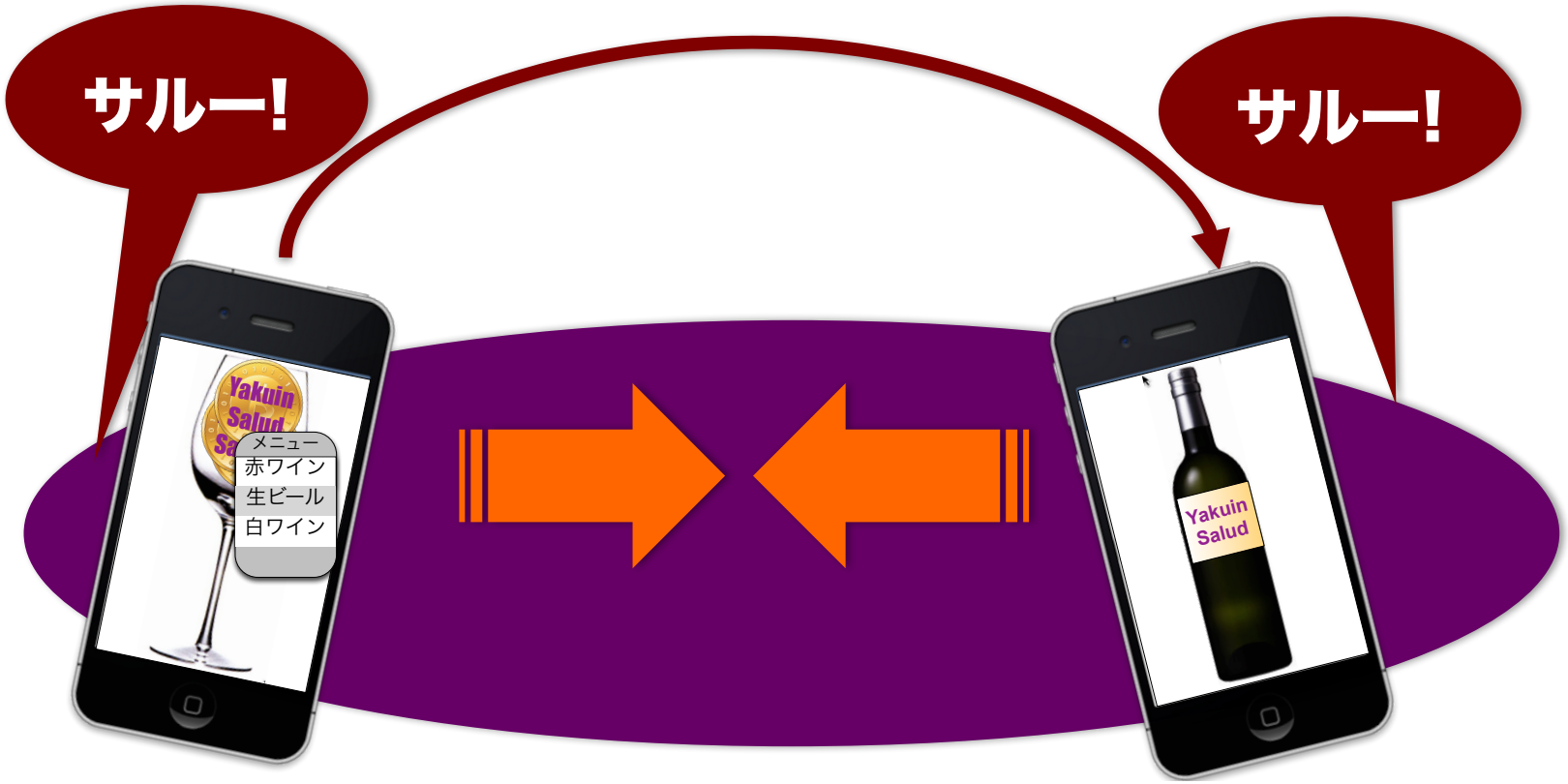
薬院サルーでの実験

福岡市薬院地区のはしご酒イベント

マイグラス片手に薬院のお店をハシゴする

スマートフォンでコインを転々譲渡

加速度と位置と時刻が一致ならコインを渡す



サルー！の位置と時刻

決済履歴をリアルタイムでモニタできる

協調フィルタリング

商品１を買っている人は商品３や商品６も買っている

商品とユーザの購買行動の表

	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11
商品1	1	1	0	0	0	1	1	0	1	0	1
商品2	0	1	0	1	1	0	0	1	0	1	1
商品3	1	1	0	0	0	1	1	0	1	0	1
商品4	0	0	0	1	0	1	0	0	1	0	0
商品5	0	1	0	1	0	0	1	0	1	1	1
商品6	1	0	0	1	0	1	1	0	0	0	1

商品組み合わせごとの距離を求める

$$\sqrt{\sum_{i=1}^{n}(x_i - y_i)^2}$$

商品１との距離

(5)商品２：2.8
(1)商品３：0
(4)商品４：2.2
(3)商品５：2.0
(2)商品６：1.7

ユーザベースの協調フィルタリング

商品とユーザの購買行動の表

	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11
商品1	1	1	0	0	0	1	1	0	1	0	1
商品2	0	1	0	1	1	0	0	1	0	1	1
商品3	1	1	0	0	0	1	1	0	1	0	1
商品4	0	0	0	1	0	1	0	0	1	0	0
商品5	0	1	0	1	0	0	1	0	1	1	1
商品6	1	0	0	1	0	1	1	0	0	0	1

ユーザの組み合わせごとの距離を求める
クラスタリングなどで類似したユーザを見つける

推薦すると買うかもしれない

リアルタイムの
リコメンデーション

それまでどの店で何を飲んできたか、

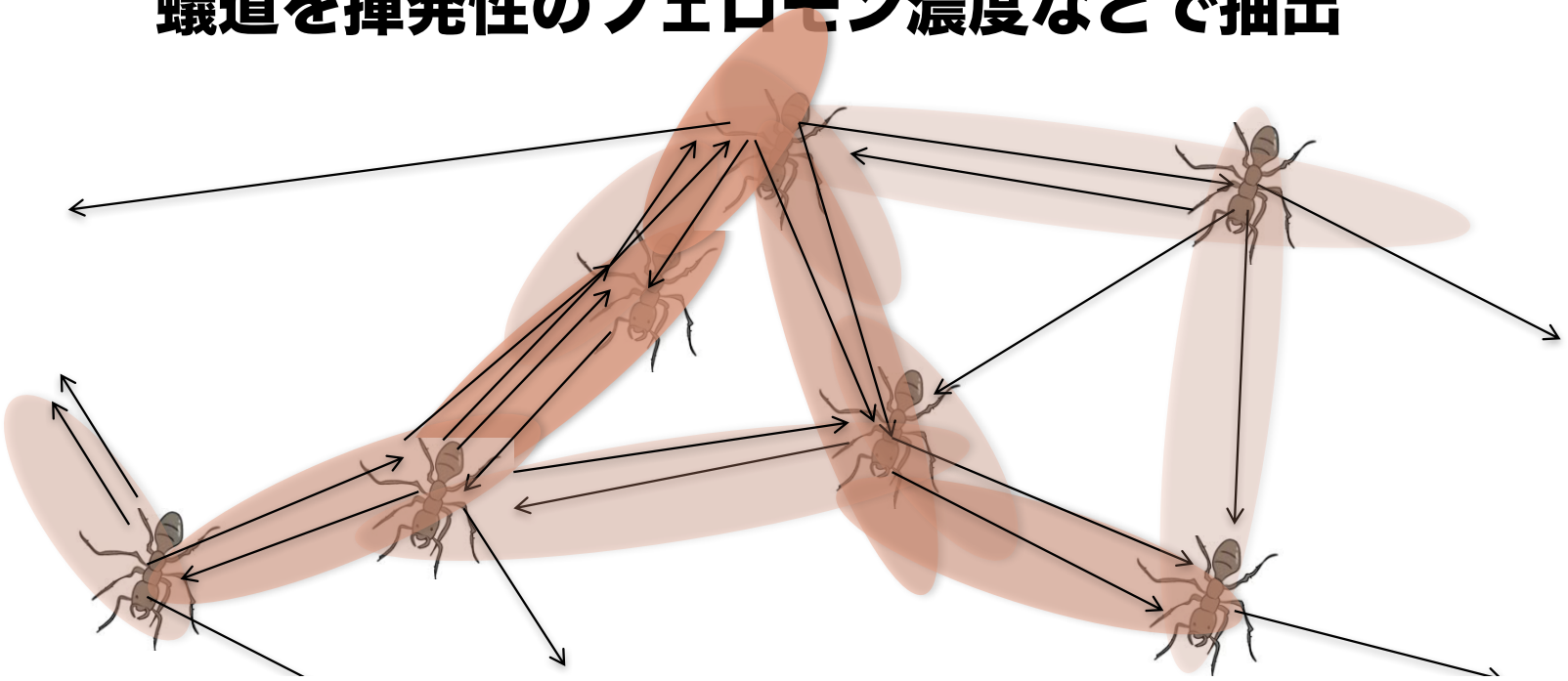
**この店で
赤ワインを
飲んだ人は
次にこの店に
行っています**

**サルー！
で注文した30分後**

繰り返される決済から
Nexus （結合体）を抽出

アントコロニー法など

蟻道を揮発性のフェロモン濃度などで抽出



投票システムには政府を超越した中立性が必要

ビットコインは、国家を超越した通貨を実現した

- 国家や政府を超越した投票システムも作れるのでは？

投票とは？

ルソーの社会契約論

- 個人は利害を超えた「社会契約」を結ぶ「一般意志」を持つ
- 投票は、一般意志の表明

ボルダ、コンドルセ

- 投票の問題分析と数学的基礎の精緻化

投票システムの問題

紙の投票システム

- 開票作業、集計作業の不正の可能性を払拭できない

電子投票システムの運用の透明性

- 選挙管理委員会に加えて開発ベンダー、運用者が存在
- 第三者が検証可能な投票用紙も存在しない

多数決の問題

リンカーンは少数派だった　(William Riker)

共和党：リンカーン	**奴隷開放（40%)**
北部民主党：ダグラス	**奴隷制肯定**
南部民主党：ブレッキンリッジ	**奴隷制肯定**
立憲連合党：ベル	**奴隷制肯定**

カレー店の人気投票の問題

票の割れによる優勝者は、投票結果の信頼と評判に影響する

カレー店１	**独特の味**	**(20%)**	**優勝してしまう**
カレー店２	**多くの人が好む味**	**(15%)**	
カレー店３	**多くの人が好む味**	**(13%)**	
カレー店４	**多くの人が好む味**	**(12%)**	
カレー店５	**多くの人が好む味**	**(10%)**	
カレー店６	**多くの人が好む味**	**(10%)**	
カレー店７	**多くの人が好む味**	**(10%)**	
カレー店８	**多くの人が好む味**	**(10%)**	

クイズ・ミリオネアの正答率

自分で回答できないときに補助手段が使える

●専門家に聞く　→　正解率60%

●オーディエンスに聞く　→　正解率96%

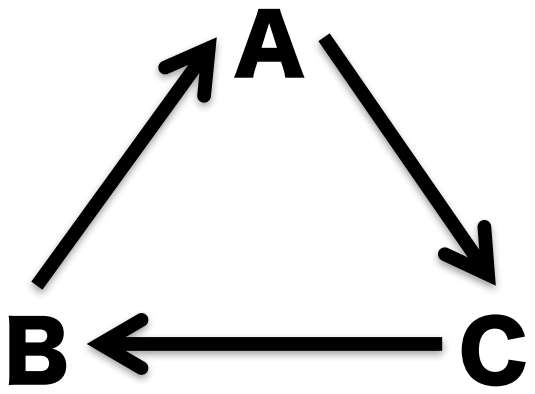
数学的に説明可能 →　コンドルセの陪審定理

複数選択投票を2択投票に変換する

A,B,C　の候補者に対して

AB, AC, BC のペアについてそれぞれ判断を投票する

順序が巡回しても矛盾とはみなさない



コンドルセ表とヤングの最尤法による集計結果

投票結果を表にする（この例は、従来の人気投票ではA,B,Cともに10票）

	A	B	C
A	-	4	6
B	9	-	1
C	5	5	-

AはBよりも美味しい：4票
AはCよりも美味しい：6票
BはAよりも美味しい：9票
BはCよりも美味しい：1票
CはAよりも美味しい：5票
CはBよりも美味しい：5票

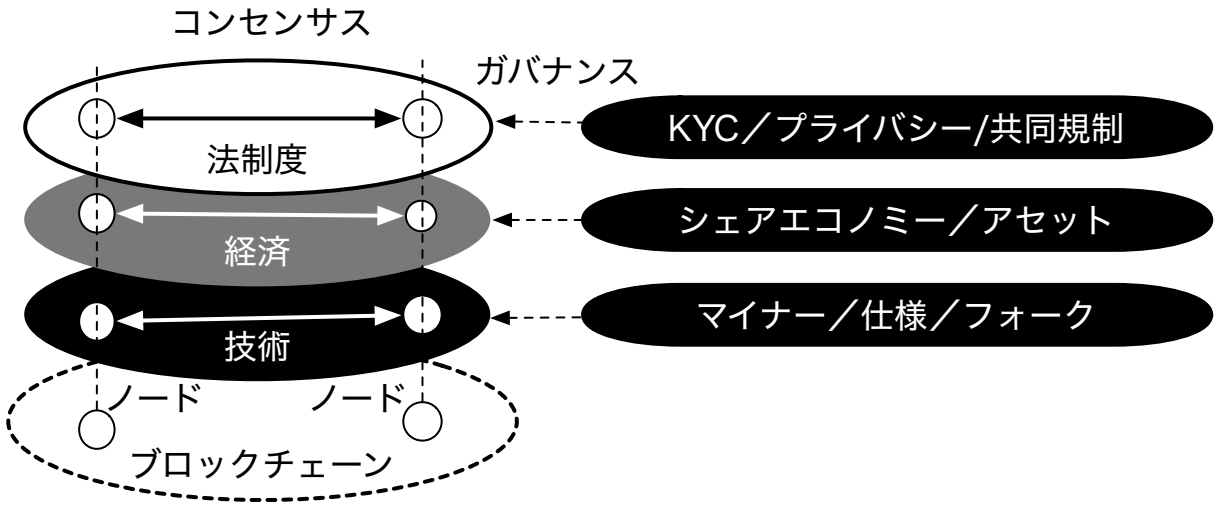
A>B>C (A>B,B>C,A>C)　4+6+1=11
A>C>B (A>C,C>B,A>B)　4+6+5=15
B>A>C (B>A,A>C,B>C)　9+1+6=16
B>C>A (B>C,C>A,B>A)　9+1+5=15
C>A>B (C>A,A>B,C>B)　5+5+4=14
C>B>A (C>B,B>A,C>A)　5+5+9=19 ←最尤順序

ものすごく面白い時代です

技術と経済と法律のすべてが必要

空想では何も進まない

実際に手を動かしてシステムをつくり、実験して知恵を集積する



地域におけるブロックチェーン活用には

まず人材育成が最初の一歩

- 技術、経済、制度のすべての視点を持つ人材が必要
- コンサルや海外製品の宣伝文句は無視

教育機関は大学だけではない

- 地域の勉強会
- ブロックチェーンはアカデミアは参加しにくい分野

  例：暗号の専門家の多くは、ブロックチェーンの本質的価値を理解できない
- 教育プログラム付きのコンテスト

  （賞金だけでは地域企業や学生への教育的効果は小さい）