# 仮想通貨技術と
# ブロックチェーン経済圏について

近畿大学
山崎重一郎

# 自己紹介

## 最近の著書


newton 仮想通貨とブロックチェー
山崎重一郎
2018年


ブロックチェーンプログラミング
（講談社）
山崎重一郎
安土茂亨
田中俊太郎
2017年


仮想通貨
（東洋経済新報社）
岡田仁志
高橋郁夫
山崎重一郎
2015年



FinTech革命
（日経BPムック）
ブロックチェーンの解説
2016年



インターネット白書2016
（インプレス）
ブロックチェーン技術の
仕組みと可能性
2016,2017年

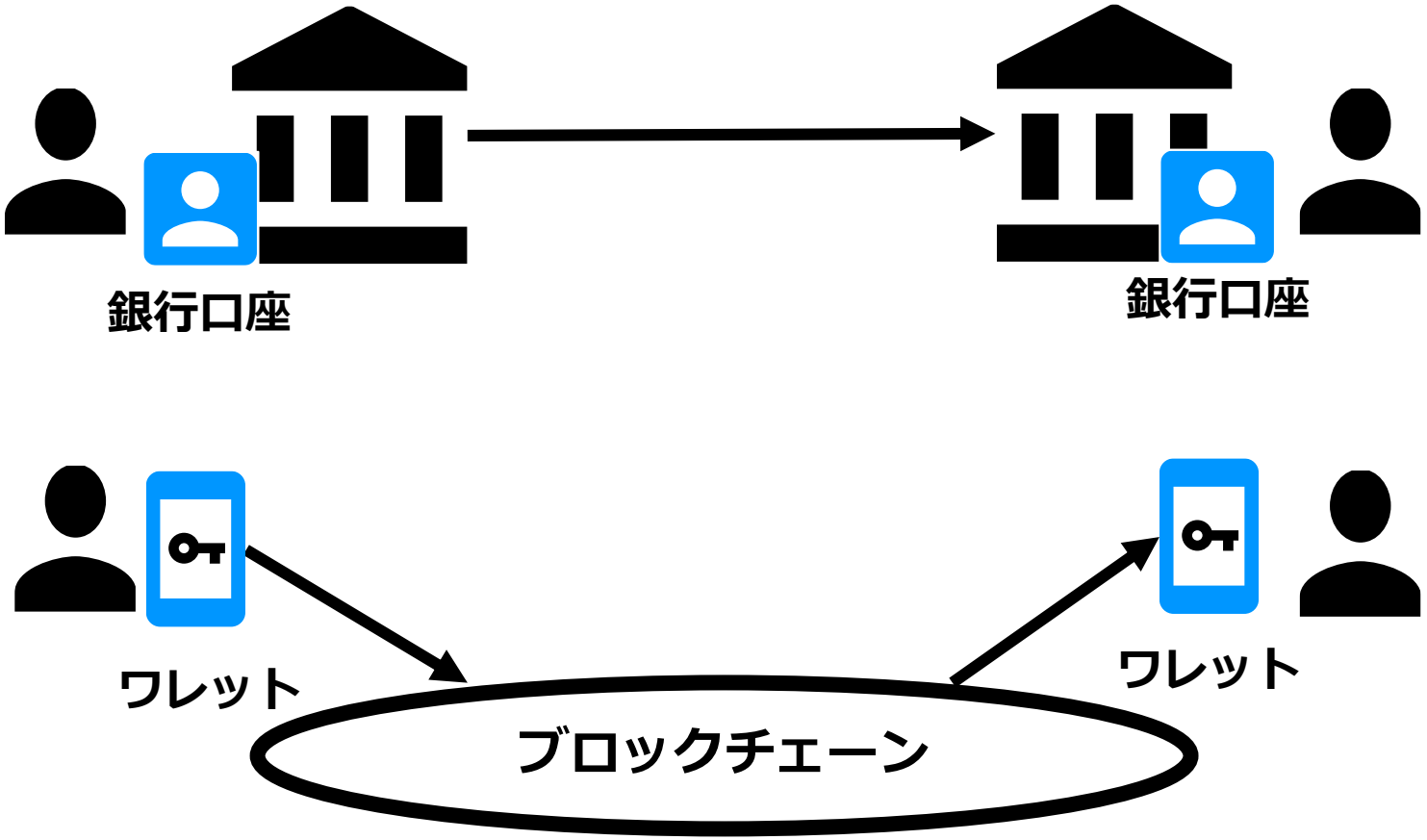



日経FinTech
2016-2018
（日経BP）
ブロックチェーン技術

# 「あちら側」から「自分たちの側」への
# ゲームチェンジ

# ブロックチェーンによるゲームチェンジ

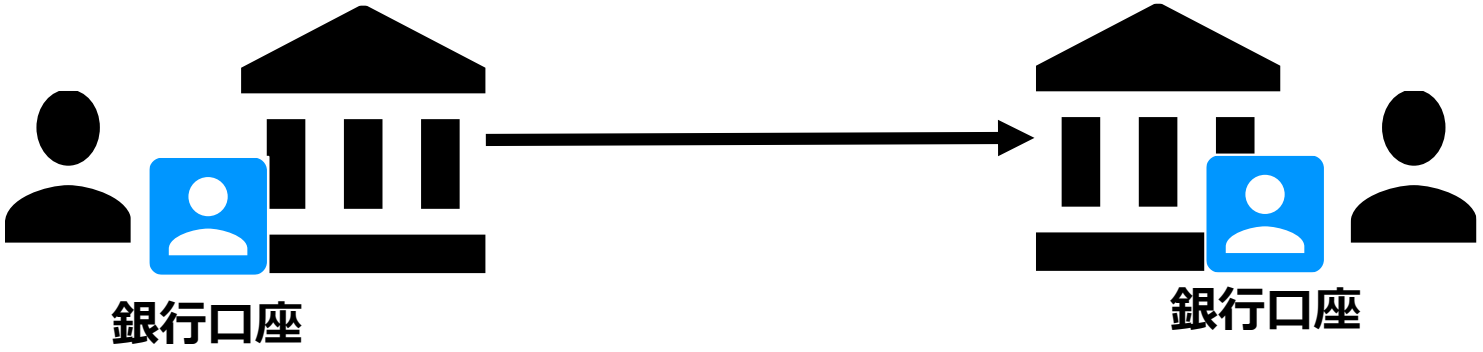
## 送金に銀行口座が不要になるから銀行は不要？



# ブロックチェーンによるゲームチェンジ

## 送金に銀行口座が不要になるから銀行は不要？

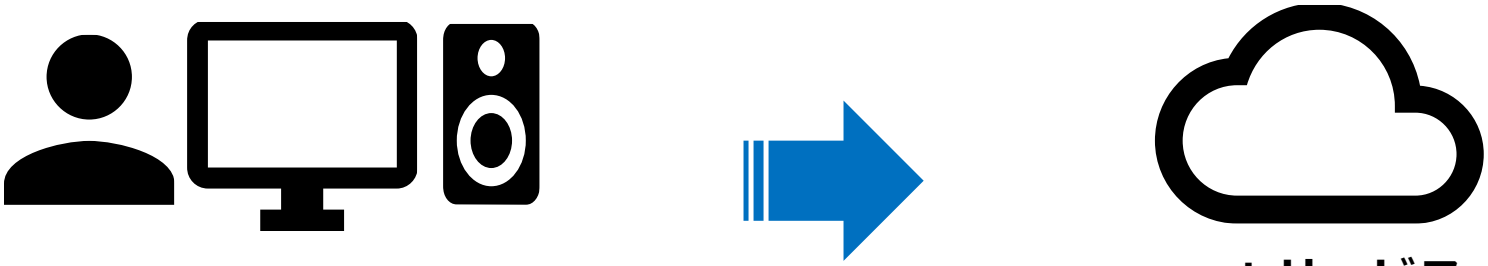
## それはたぶんない




# 2005年ごろのWeb 2.0 ブーム

ティム・オライリー

梅田望夫，著書：ウェブ進化論 「あちら側」



個人のパソコン
「こちら側」

webサービス
「あちら側」

不特定の個人がwebメディアを通じて
受動的なサービス享受者ではなく、能動的表現者になり、
Webは個人が価値を生み出す能力の増幅器になる

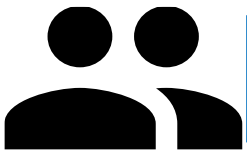
# それから14年後のWeb 2.0 の現実

webメディアの能動的表現者になりえた個人はごく少数

個人の日常的な活動履歴

- GAFAの莫大な収益の源泉になった

webメディアの
利用者

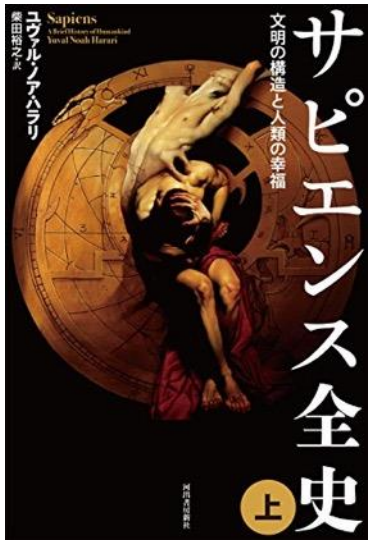



検索履歴、視聴履歴、購買履歴、
友人関係、つぶやき、「いいね」

# 共同幻想と人類

## ホモ・サピエンスは、共同幻想を武器にする生き物

- 「神」、「国家」、「通貨」などの幻想を信じることができる能力
- 知能、身体的に優れていたネアンデルタール人などを駆逐した能力





ユヴァル・ノア・ハラリ

# ジョン・レノンのイマジンの逆説

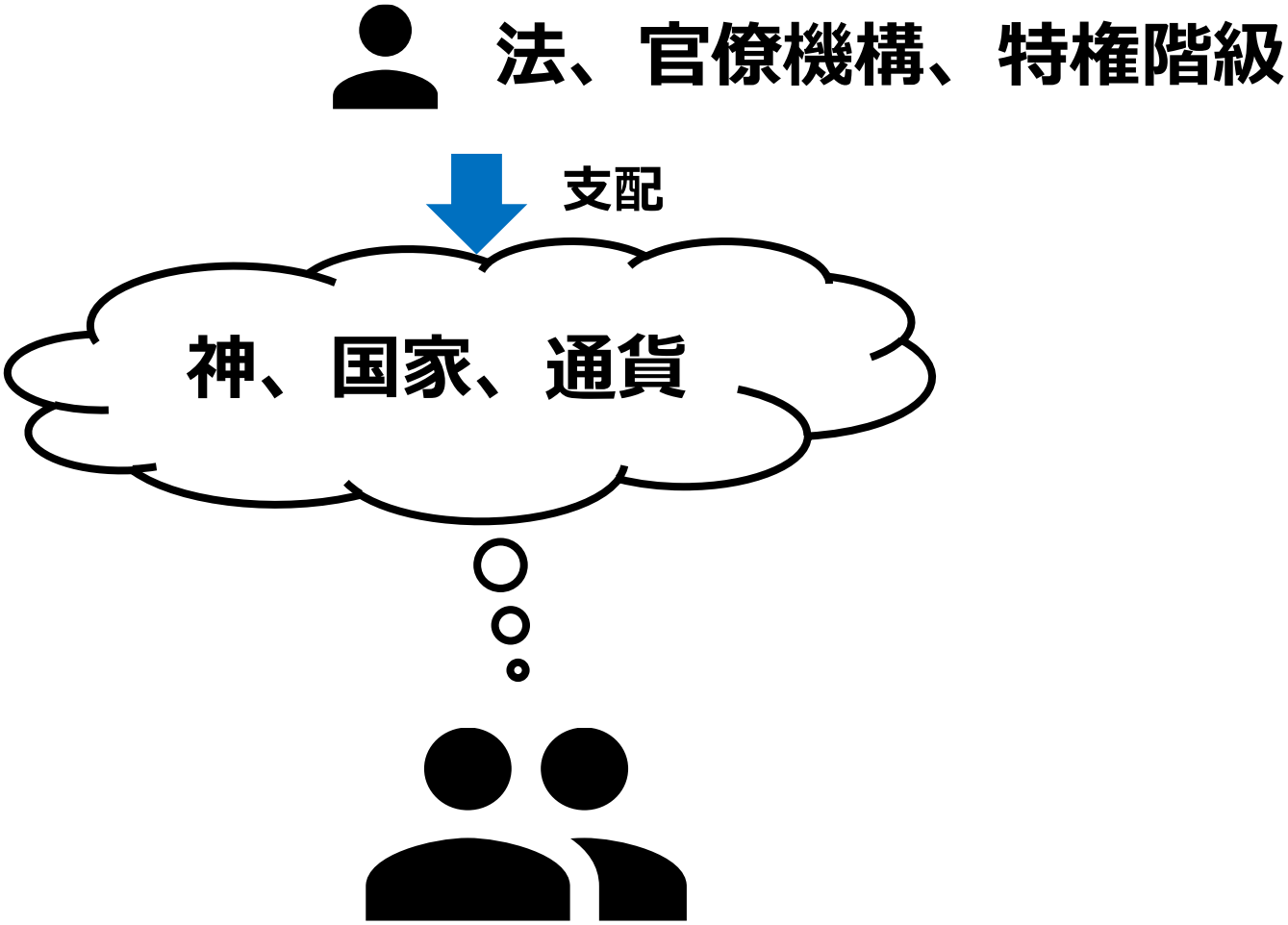
天国や国家を信じる人たちと信じない人たちが

戦争すると、どちらが勝利するだろうか？


天国、国家を信じない人たち

# 共同幻想の支配構造と闘争

## 天国、国、通貨を信じる人たちに対するガバナンス



# データとアルゴリズムの時代の到来

## 共同幻想の対象が交代する

- 神、国　→　データ、アルゴリズム

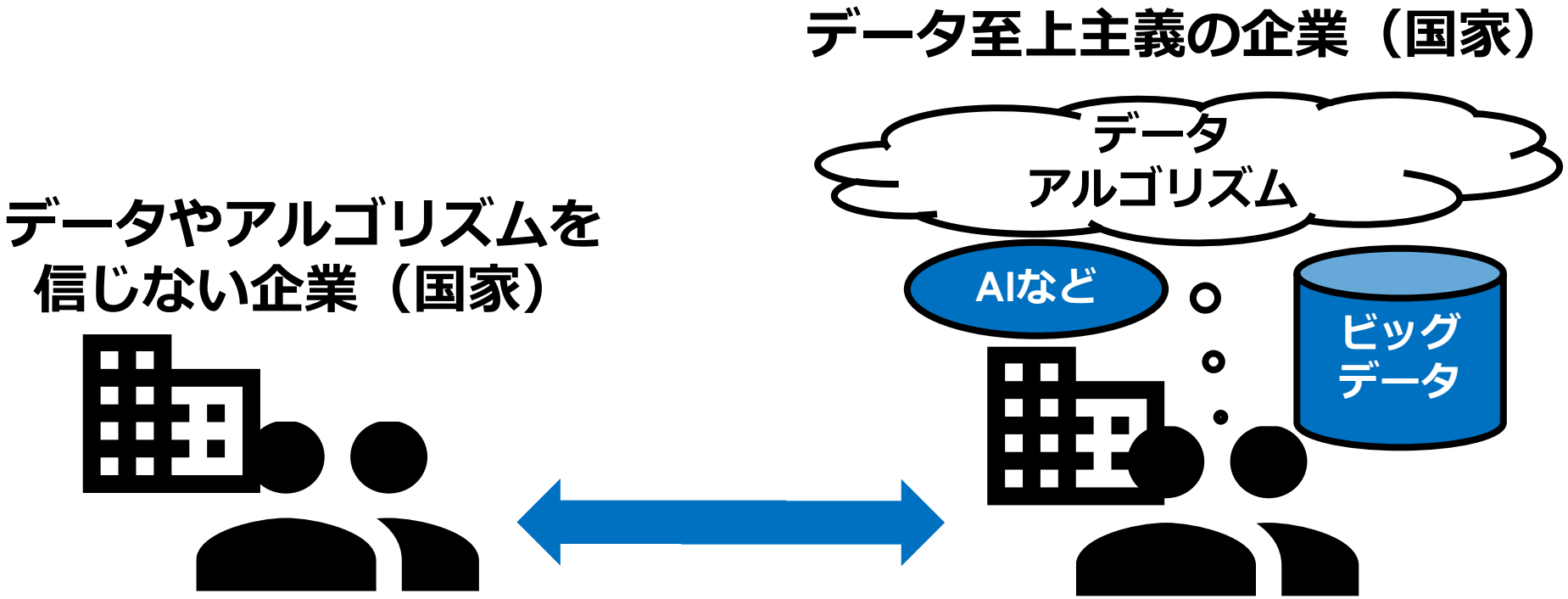
ビッグデータ 、 AI（アルゴリズム） などはその例


# データとアルゴリズムの時代は来るのか？

データ、アルゴリズム(機械学習、統計,...） を

信じる企業（国家）と、信じない企業（国家）が戦ったら

どちらが勝利するだろうか？



# データとアルゴリズムの支配への闘争

誰が「データ」「アルゴリズム」を支配するのか

GAFAによる「空気のような」支配が続くのか？

# GDPR（EU一般データ保護規則)

## EU域内の市民の個人データのコントロール（2018年5月）

- 個人データへのコントロールをGAFAから取り戻す

# 「あちら側」から「自分たちの側」に

## データとアルゴリズムの支配への闘争

## GAFAは空気のような存在ではなくなるかも（？）

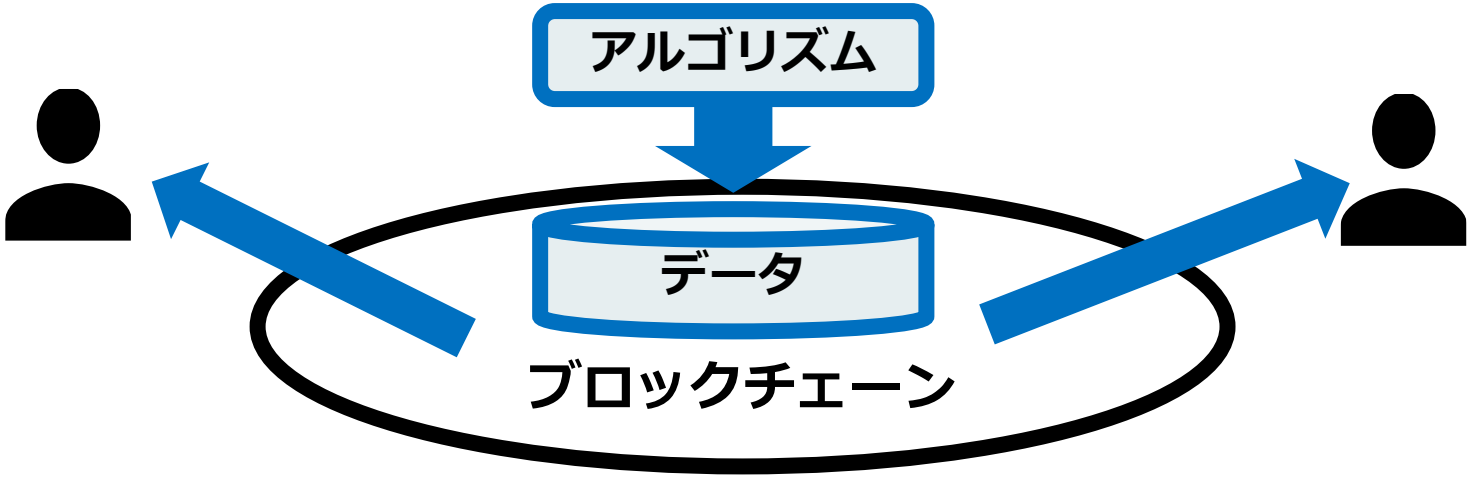
# ブロックチェーンによるゲームチェンジ

データとアルゴリズムの支配を

「あちら側」から「自分たちの側」にする技術

（これも楽観主義的予想かもしれないが…）

ブロックチェーンは
「自分たち」が主体的にデータとアルゴリズムを支配する場

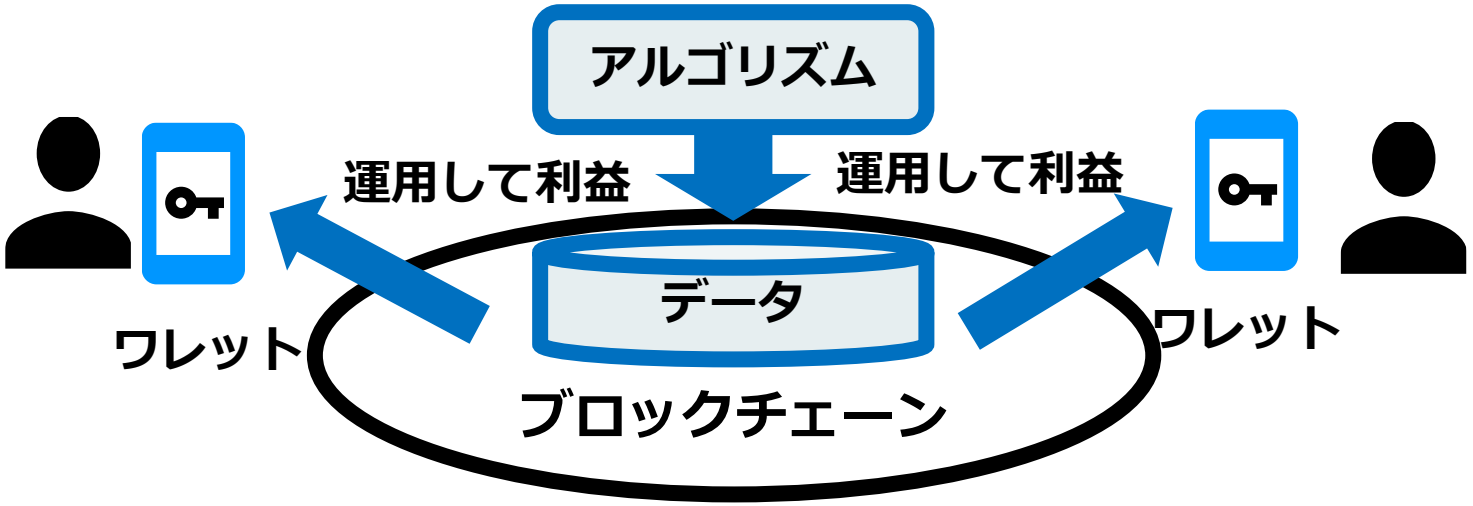


# ブロックチェーンによるゲームチェンジ

## ★楽観的な例

## アルゴリズムによるブロックチェーン上の金融

- ブロックチェーン上のアルゴリズムによって資金が運用される
- 資金の運用益は、ほとんど全額が出資者に還元される

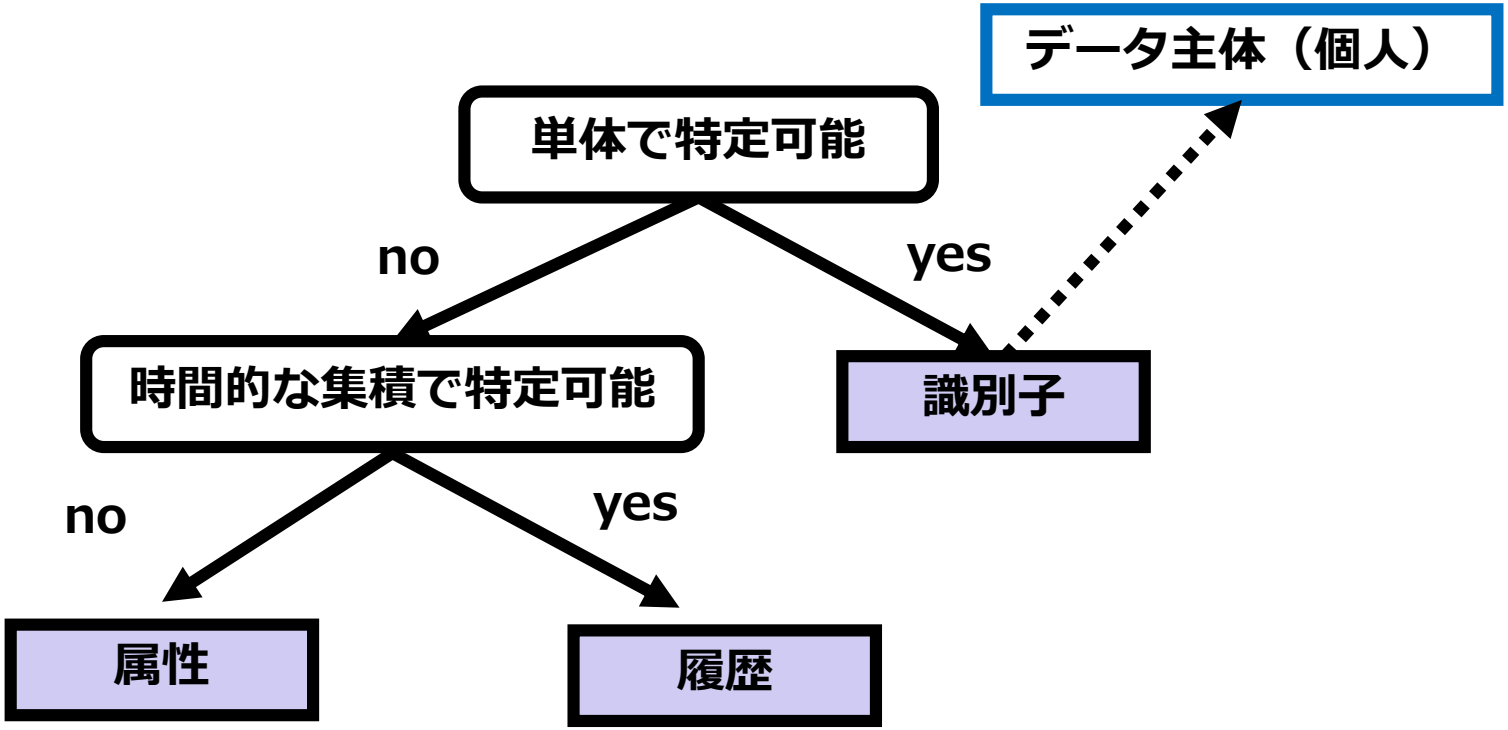


# 個人データの支配

# 個人データ

## 個人データの種類

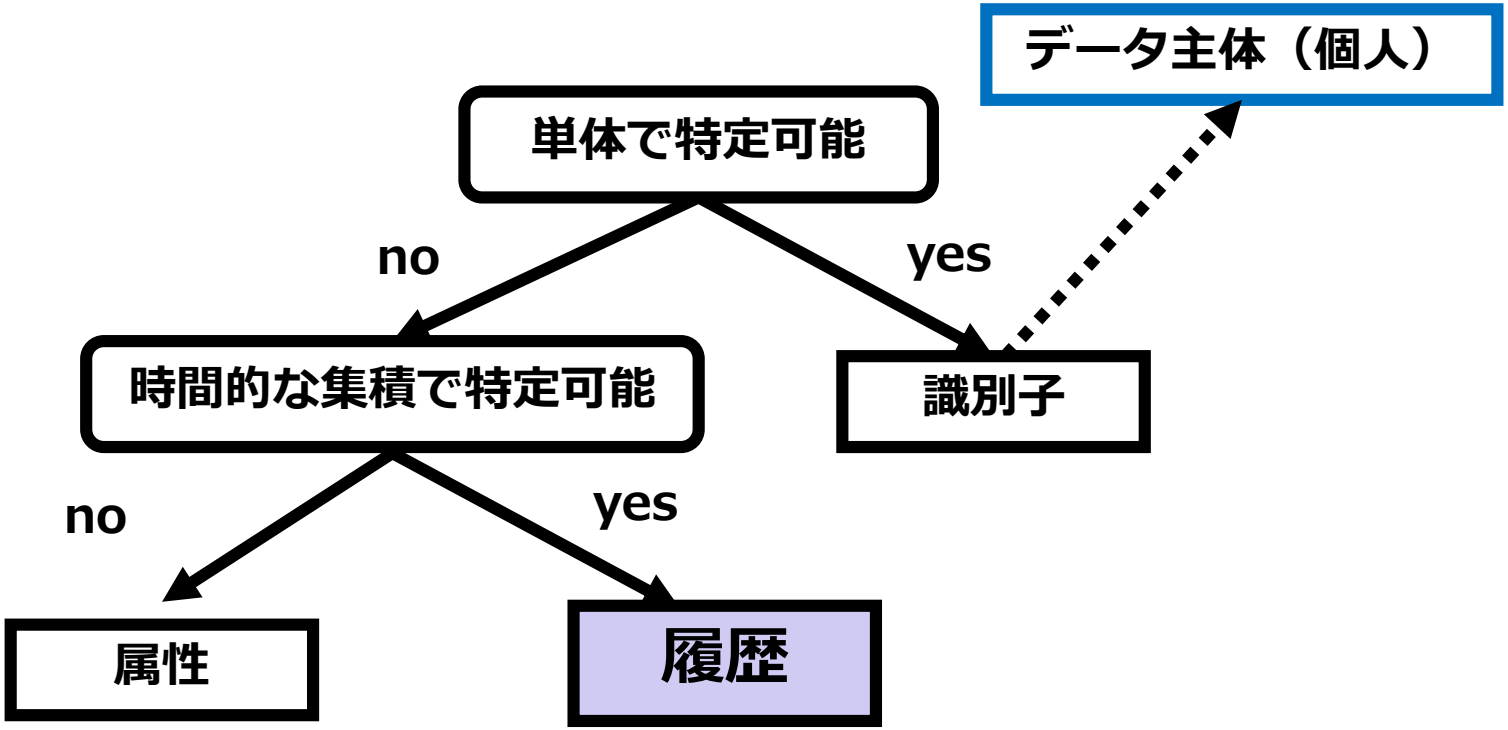
- 識別子（単体で個人「データ主体」を特定できる）
- 履歴（集積されると個人が特定可能）
- 属性（他の属性との組み合わせで個人が特定可能）



# 特に有用な個人データは履歴

## 個人データの種類

- 識別子（単体で個人「データ主体」を特定できる）
- 履歴（集積されると個人が特定可能）
- 属性（他の属性との組み合わせで個人が特定可能）



# 個人の履歴の例

## 個人ごとの映画の視聴履歴の表

- この人はこの映画を見たことがある→ 1
- この人はこの映画を見たことがない→ 0

| | 映画１ | 映画２ | 映画３ | 映画４ | 映画５ | 映画６ |
|---|---|---|---|---|---|---|
| 人１ | 1 | 0 | 1 | 0 | 1 | 0 |
| 人２ | 1 | 1 | 0 | 0 | 1 | 1 |
| 人３ | 1 | 1 | 1 | 1 | 0 | 0 |
| 人４ | 0 | 1 | 0 | 0 | 1 | 0 |
| 人５ | 0 | 0 | 1 | 1 | 1 | 1 |

# プログラミングIの授業で実施したアンケート

## 映画名の配列

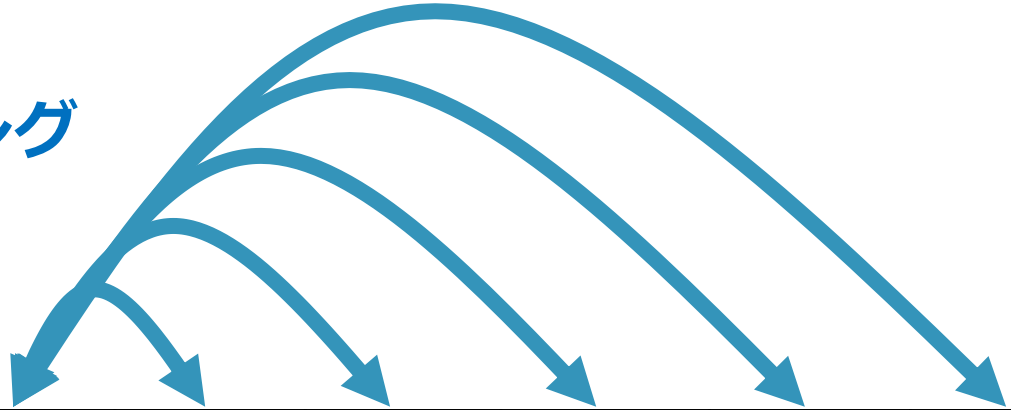
movies= ["グレイテストショーマン", "風の谷のナウシカ", "君の名は", "ノーゲイム・ノーライフ", "風立ちぬ", "ジョーズ", "紅の豚", "サマーウォーズ", "時をかける少女", "シンゴジラ", "ゼログラビティ", "アナと雪の女王", "ナルニア国物語", "タイタニック", "ベイマックス", "シェイプオブウォーター", "ミニオンズ", "美女と野獣", "少林サッカー", "探偵はbarにいる", "聲の形", "言の葉の庭", "マレフィセント", "アナコンダ", "ピンポン", "キングスマン", "羊たちの沈黙", "時計じかけのオレンジ", "シャイニング", "図書館戦争", "英国王のスピーチ", "プレデターズ", "猿の惑星", "寄生獣", "レッドクリフ", "アメリカン・スナイパー", "天使にラブソングを", "アルマゲドン", "フォレストガンプ", "インターステラー", "フルメタル・ジャケット", "ジョニーは戦場へ行った", "戦慄の楽譜", "アオハライド", "ララランド", "シックスセンス", "バタフライ・エフェクト", "はじまりのうた", "パシフィックリム", "セブン", "アントマン", "本能寺ホテル", "アイ、ロボット", "土竜の唄", "海猿", "デスノート", "インセプション"]

# この映画を見ている人は
# この映画も見ている

映画と映画の全ての組み合わせについて距離を求める

データから推薦アルゴリズムを生成する

協調フィルタリング



| | 映画１ | 映画２ | 映画３ | 映画４ | 映画５ | 映画６ |
|---|---|---|---|---|---|---|
| 人１ | 1 | 0 | 1 | 0 | 1 | 0 |
| 人２ | 1 | 1 | 0 | 0 | 1 | 1 |
| 人３ | 1 | 1 | 1 | 1 | 0 | 0 |
| 人４ | 0 | 1 | 0 | 0 | 1 | 0 |
| 人５ | 0 | 0 | 1 | 1 | 1 | 1 |

# 実験

"風の谷のナウシカ"を見ている人は？

```
e0=eiga_v[1]    # "風の谷のナウシカ"
p eiga_v.map.with_index{|e,i|[tanimoto(e0,e),movies[i]]}.sort


=>  [... [0.5510204081632653, "風立ちぬ"], [0.6229508196721312, "君の名は"], [0.6530612244897959, "紅の豚"], [0.6727272727272727, "サマーウォーズ"], [0.6730769230769231, "時をかける少女"], [1.0, "風の谷のナウシカ"]]
```

こういう映画も見ている

- 時をかける少女
- サマーウォーズ
- 紅の豚
- 君の名は

# 実験

"羊たちの沈黙"を見ている人は？

```
e0=eiga_v[26]    # "羊たちの沈黙"
p eiga_v.map.with_index{|e,i|[tanimoto(e0,e),movies[i]]}.sort


=>  [... [0.3333333333333333, "シャイニング"], [0.3333333333333333, "フルメタル・ジャケット"], [0.3333333333333333, "英国王のスピーチ"], [0.4, "ジョニーは戦場へ行った"], [1.0, "羊たちの沈黙"]]
```

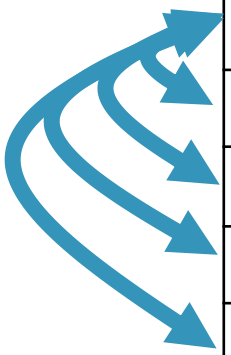
こういう映画も見ている

- ジョニーは戦場へ行った
- 英国王のスピーチ
- フルメタル・ジャケット
- シャイニング

# この人とこの人は
# 見た映画が似ている

## 人と人の距離

- 人と人の組み合わせについて距離を求める



| | 映画１ | 映画２ | 映画３ | 映画４ | 映画５ | 映画６ |
|---|---|---|---|---|---|---|
| 人１ | 1 | 0 | 1 | 0 | 1 | 0 |
| 人２ | 1 | 1 | 0 | 0 | 1 | 1 |
| 人３ | 1 | 1 | 1 | 1 | 0 | 0 |
| 人４ | 0 | 1 | 0 | 0 | 1 | 0 |
| 人５ | 0 | 0 | 1 | 1 | 1 | 1 |

# 無料視聴サービスの目的は？


hulu

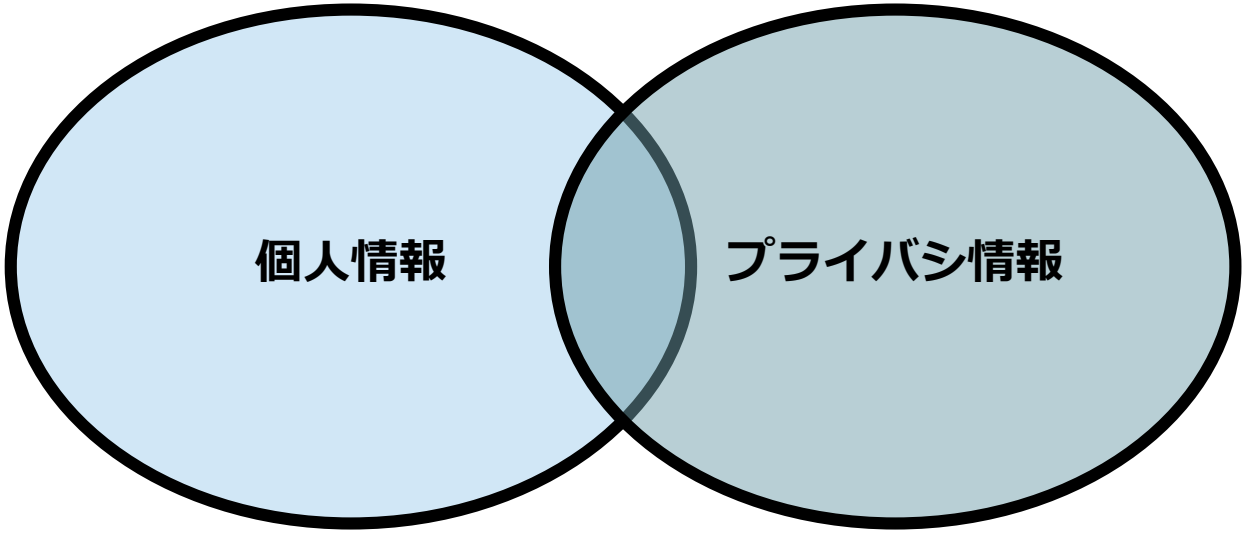
# 個人データの合法的利用

個人情報保護法は、個人情報の合法的利用法を規定した法律

改正個人情報保護法で匿名加工すれば個人情報ではなくなる

# 個人情報とプライバシ情報

## 両者は必ずしも一致しない




特定の個人を識別する情報（2条1項）

氏名、住所、生年月日、性別

個人識別符号（2条2項）

指紋データ、顔データ、個人番号、

免許証番号、保険証番号

個人の尊厳に関する情報（憲法13条）

好きな食べ物、好きな芸能人、

位置情報、通信履歴、購買履歴、

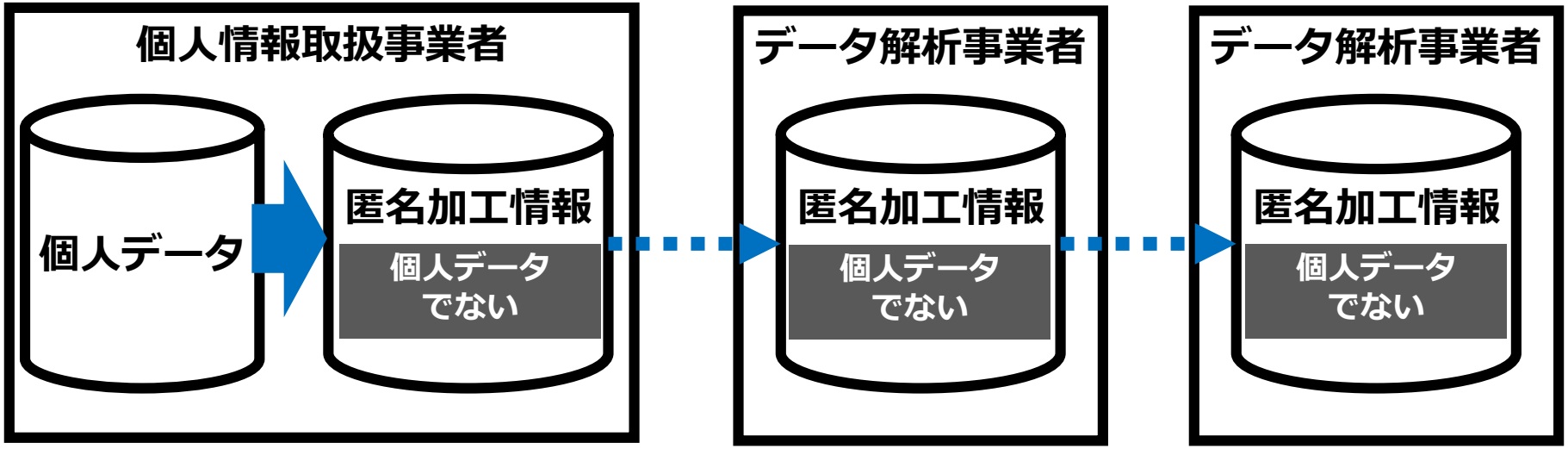
友人関係、診療記録

# 匿名加工情報

## 個人情報保護法第２条９項

- 匿名加工情報（データ主体とデータとの相関を取り除いた情報）
- 匿名加工情報は、データ解析目的で第三者に提供してよい

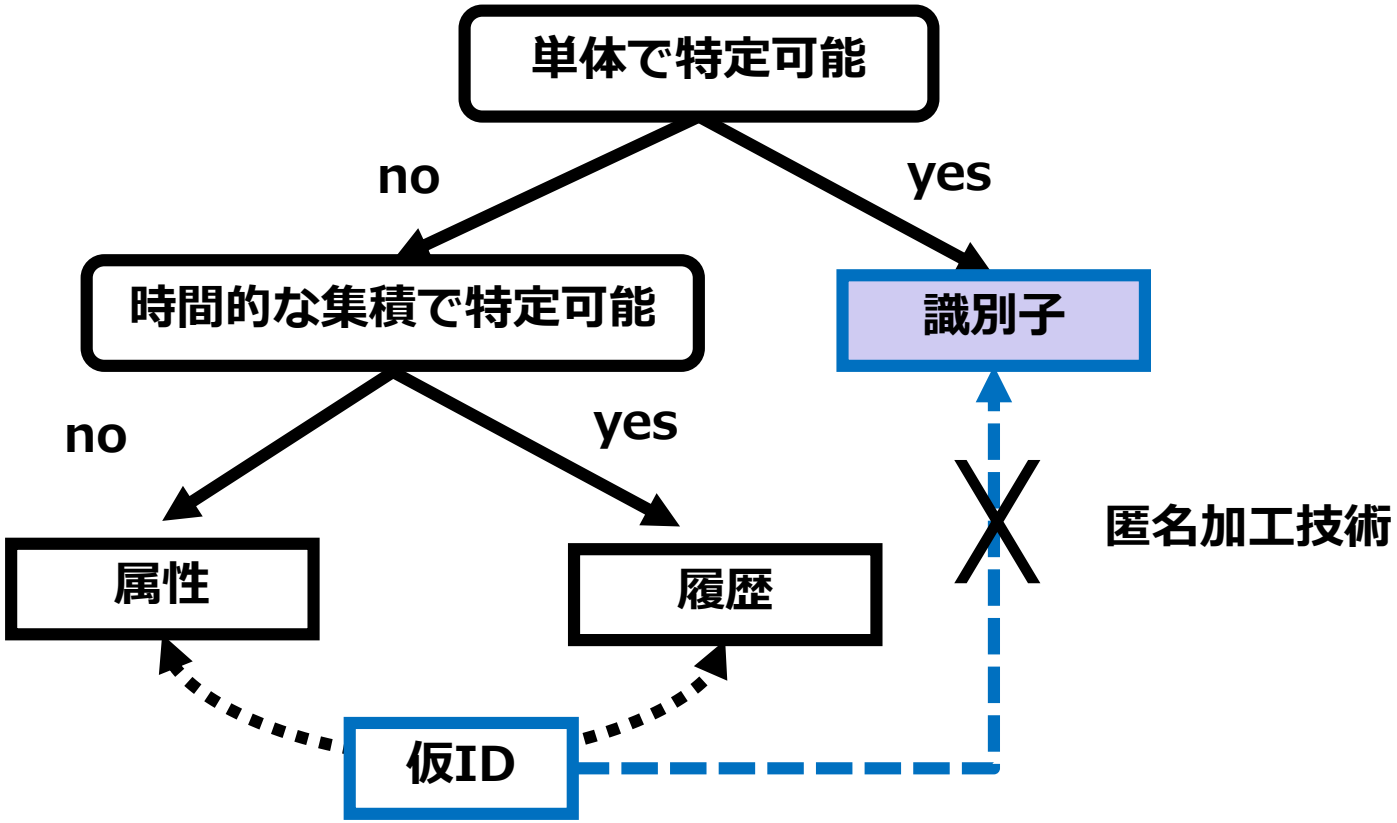
## 個人データを合法的に活用したビジネスを推進するのが目的



# 匿名加工

## 仮ID（仮名）から識別子を復元できなくする技術

- 仮名化だけでは識別子を復元できてしまう脅威がある



# 個人情報保護法と匿名加工情報のリスク

個人情報保護法は、匿名加工情報から「特定」と「照合」を試みることを禁じている

（属性推定などは禁じていない）

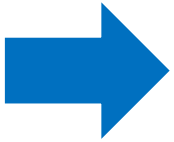
- 特定（再識別）
- 属性推定
- 本人連絡
- 照合

# k-匿名性

## 仮IDごとに少なくともk個のレコードが存在すること

- 仮ID：属性の組み合わせで作れられる識別子
- k はしきい値で、k が大きいほど安全

| 職業 | 性別 | 年齢 | 購買商品 |
|---|---|---|---|
| 大学生 | 男 | 20代 | 即席麺 |
| 社会人 | 女 | 30代 | 中華まん |
| 大学生 | 男 | 20代 | 即席麺 |
| 社会人 | 女 | 30代 | ワイン |
| 社会人 | 女 | 20代 | ワイン |
| 大学生 | 女 | 20代 | 中華まん |



| 職業 | 性別 | 年齢 | k |
|---|---|---|---|
| 大学生 | 男 | 20代 | 2 |
| 大学生 | 男 | 20代 | |
| 大学生 | 女 | 20代 | 1 |
| 社会人 | 女 | 20代 | 1 |
| 社会人 | 女 | 30代 | 2 |
| 社会人 | 女 | 30代 | |

# l-多様性

## （疑似）識別子ごとの履歴データの多様性の指標

- 多様性が小さいとk-匿名化で推定のリスクが増加する

例

- 20代男は全員大腸がん → A君は20代男だから大腸がん

A君

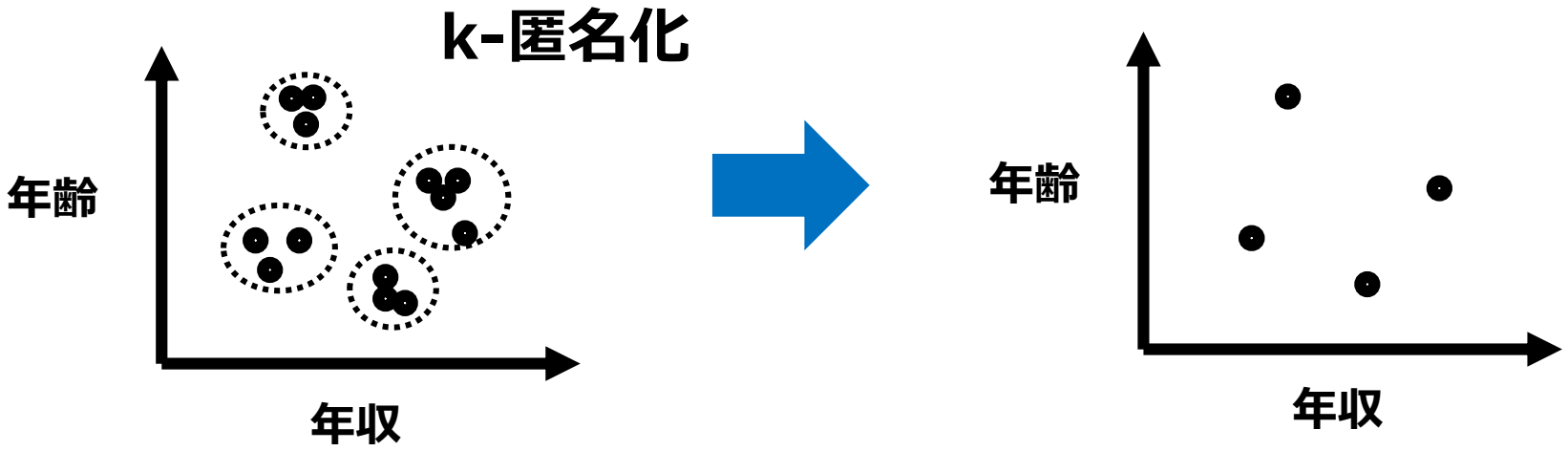
| 職業 | 性別 | 年齢 | 病気 |
|---|---|---|---|
| 大学生 | 男 | 20代 | 大腸がん |
| 社会人 | 女 | 30代 | 喘息 |
| 大学生 | 男 | 20代 | 大腸がん |
| 社会人 | 女 | 30代 | 大腸がん |
| 社会人 | 女 | 20代 | 喘息 |
| 大学生 | 女 | 20代 | 結核 |

| 職業 | 性別 | 年齢 | k | 病気 | l |
|---|---|---|---|---|---|
| * | 男 | 20代 | 2 | 大腸がん | 1 |
| * | 男 | 20代 | | 大腸がん | |
| * | 女 | 20代 | 2 | 結核 | 2 |
| * | 女 | 20代 | | 喘息 | |
| * | 女 | 30代 | 2 | 喘息 | 2 |
| * | 女 | 30代 | | 大腸がん | |

# 匿名加工技術の例
# マイクロアグリゲーション

数値属性に注目してグループ化して匿名化する手法

- グループごとの代表値（平均値など）に置き換える方法
- グループにしきい値を設定することで、k-匿名化が可能
- AIの機械学習データなどとして利用しやすい



# マイクロアグリゲーションの例

## 映画の視聴履歴を k-匿名化

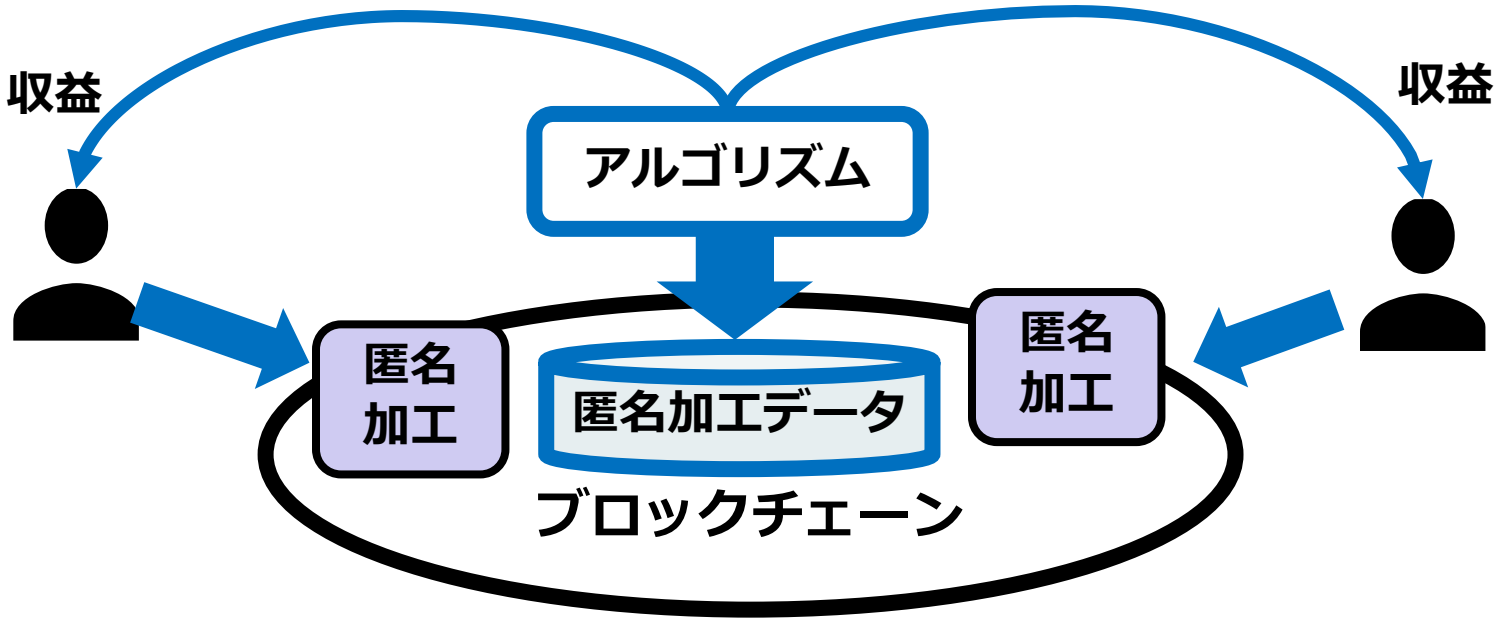
- k人分のレコードをまとめて平均をとる
- 仮IDをつけて１レコードにする
- 加工結果からの推薦精度が落ちないように工夫する

| | 映画１ | 映画２ | 映画３ | 映画４ | 映画５ | 映画６ |
|---|---|---|---|---|---|---|
| k人 人１ | 1 | 0 | 1 | 0 | 1 | 0 |
| k人 人２ | 1 | 1 | 0 | 0 | 1 | 1 |
| k人 人３ | 1 | 1 | 1 | 1 | 0 | 0 |
| k人 人４ | 0 | 1 | 0 | 0 | 1 | 0 |
| … | | | | | | |
| 人n | 0 | 0 | 1 | 1 | 1 | 1 |

# 匿名加工ブロックチェーン

## 「自分たち」の履歴を集積するブロックチェーン

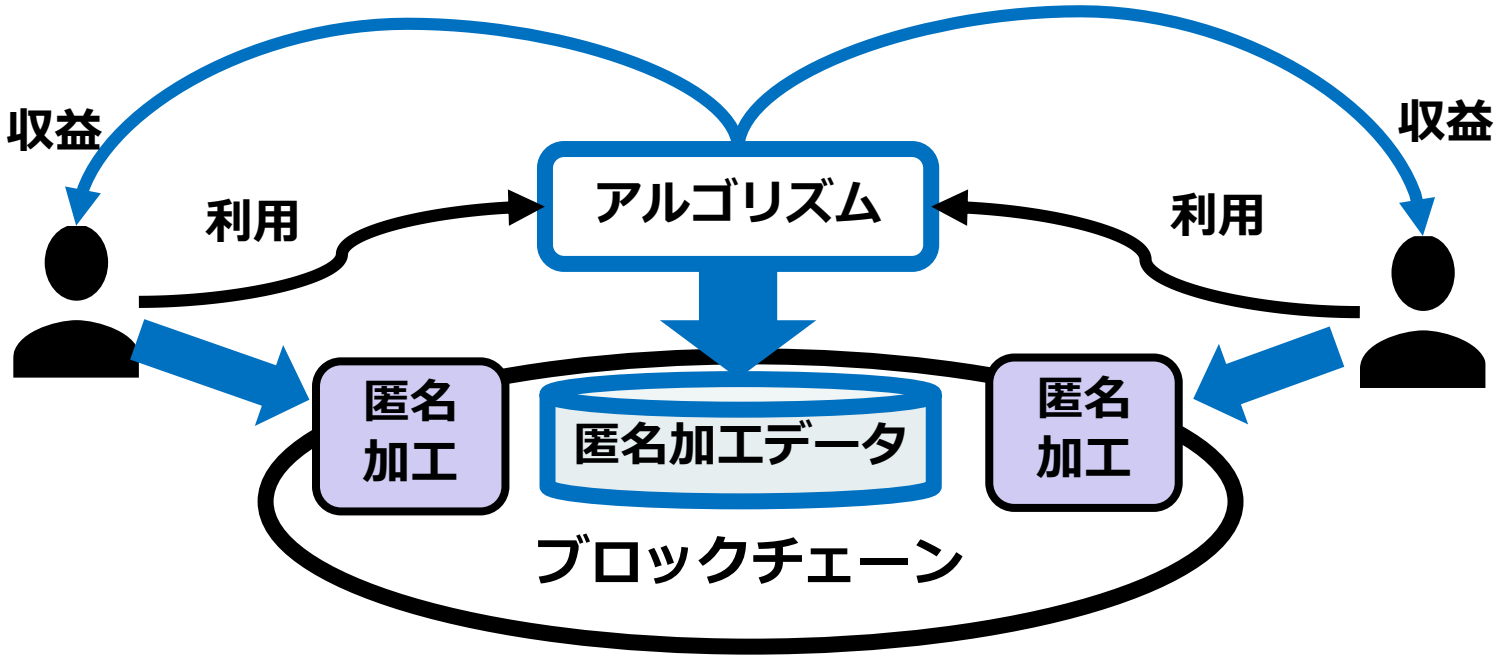
- 登録情報が自動的に匿名加工される機能を備える



# 匿名加工ブロックチェーンの有用性

「自分たち」でデータを自由に利用する（アルゴリズム）

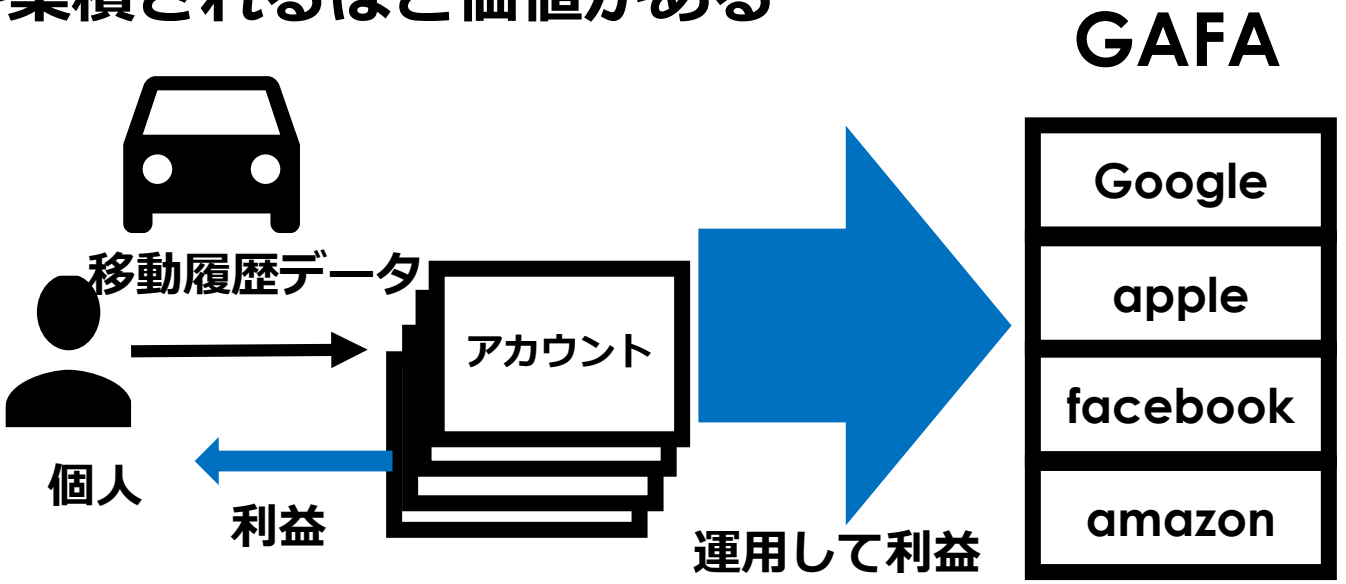
「自分たち」の収益源にできる



# 自動運転自動車が実現したら

## 自分の車の駐車場は不要になるかも

- 駐車している時間にタクシーのようなサービスで収益
- シェアエコノミー（個人の資産による収益）
- 地域における人やものの移動データが蓄積される
- データが集積されるほど価値がある

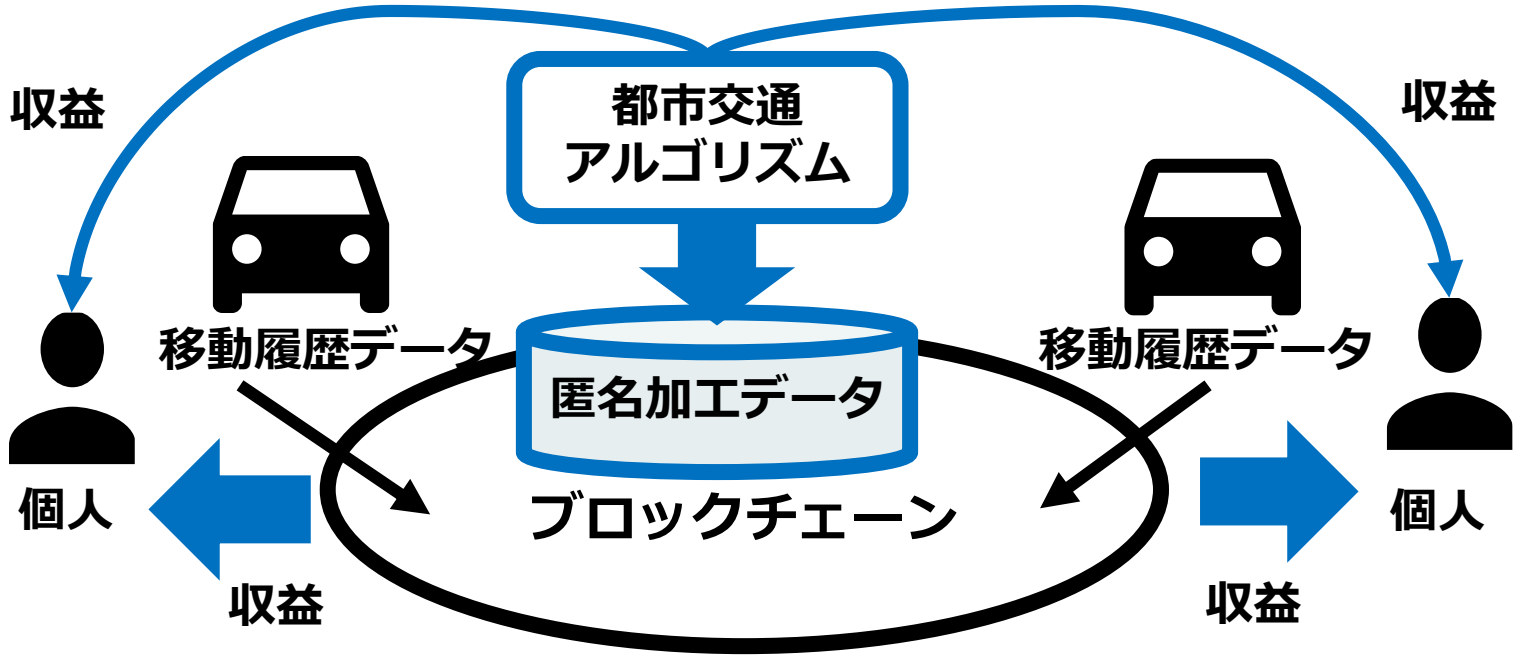


# 自動運転自動車が実現したら

GAFAに移動履歴データ集積するのではなく

匿名加工ブロックチェーンに集積すれば

「自分たちの側」が収益を得る



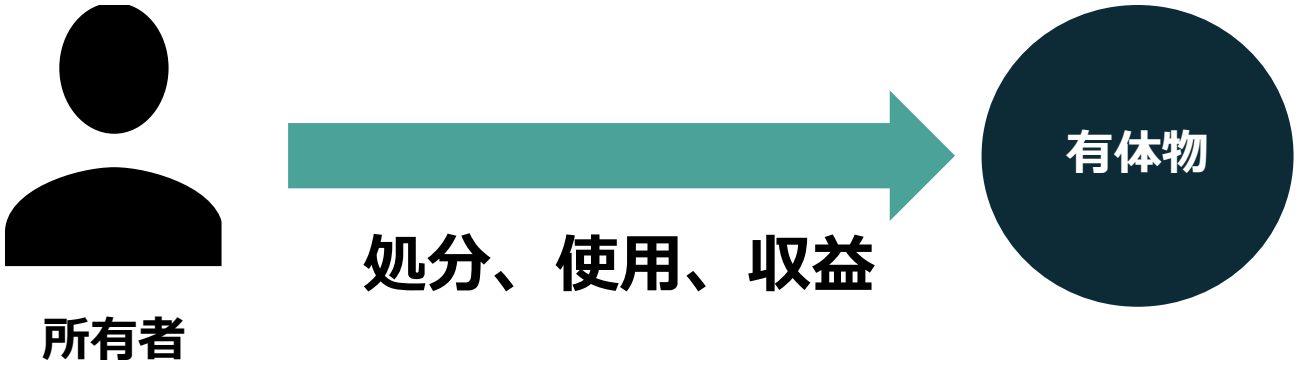
# ブロックチェーンと所有権

# 所有権

資産への排他的な支配

物権（有体物）に対する権利

- 処分する権利
- 使用する権利
- 収益を得る権利



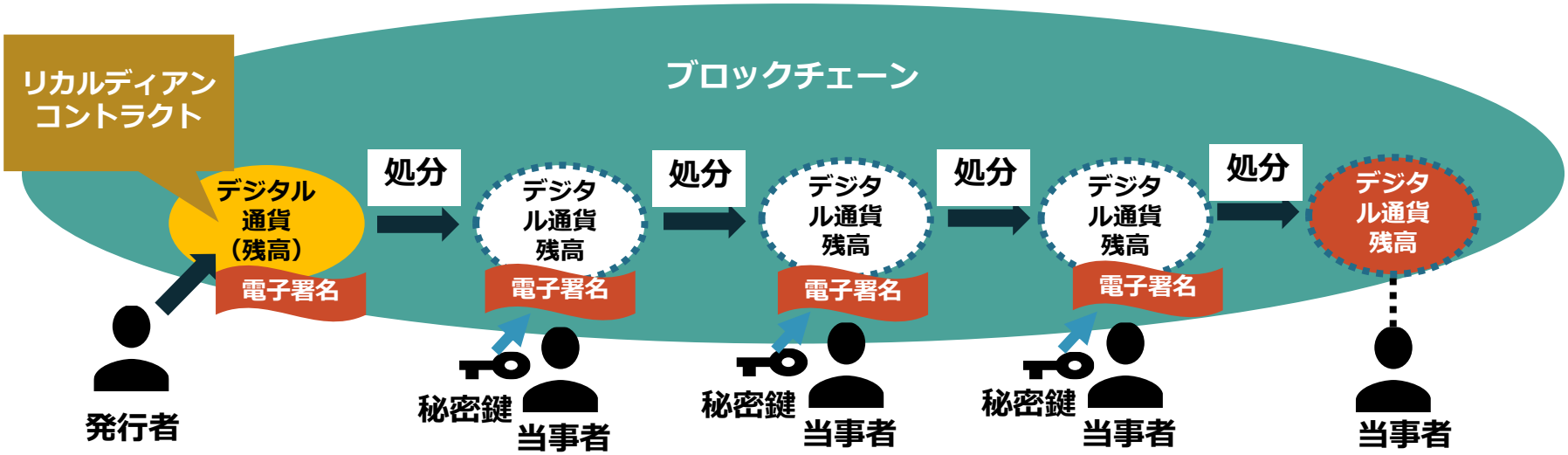
# ブロックチェーン上の資産の「所有」

## リカルディアン・コントラクトによる定義

- ≒　スマートコントラクト
- コントラクト　＝　アセットの移譲条件

  電子署名などによってアセットの「処分」を行う条件

  契約主体　＝　「公開鍵暗号基盤」による署名主体



# ブロックチェーン上で不動産登記を管理？

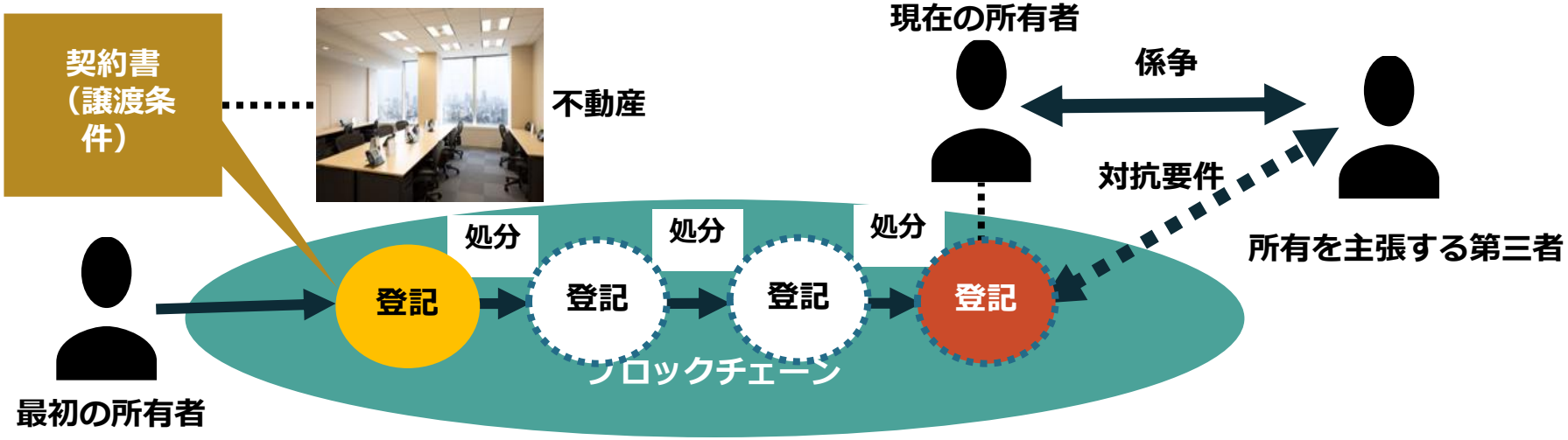
## Nick Szaboによるスマートコントラクトの提案

Secure Property Titles with Owner Authority , 2005年

- 不動産の登記が例として挙げられている

しかし、不動産登記は国家主権が前提：　尖閣諸島、竹島、北方領土？

★不動産登記簿をブロックチェーンで分散管理する必要性はない



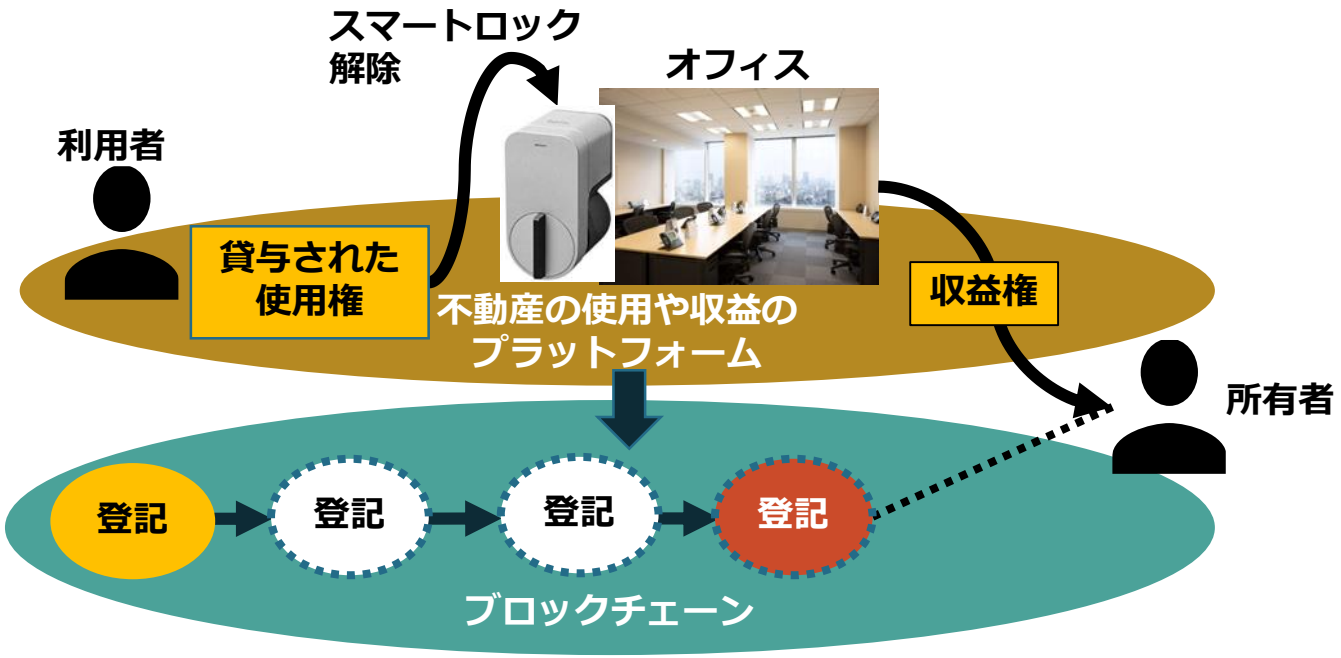
# 不動産の使用権や収益権の方が重要では？

## シェアリングエコノミー

- 個人や企業が自分の資産の活用によって収益を得る経済

## 不動産の「使用」や「収益」のためのプラットフォーム

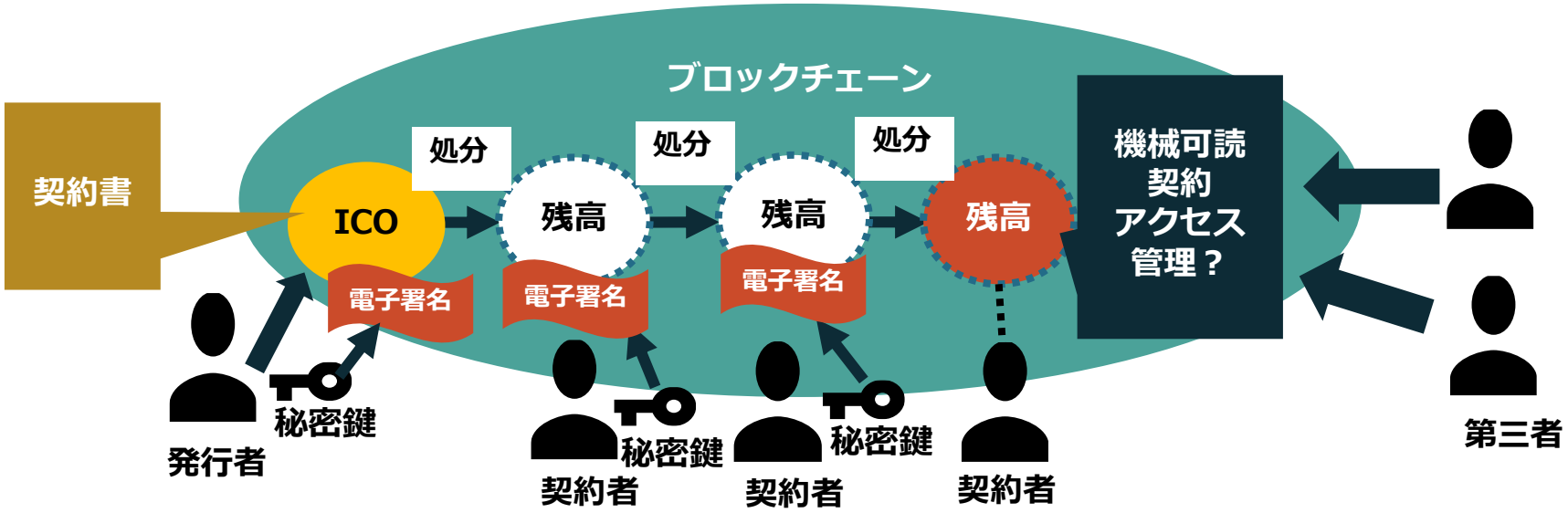
- シェアオフィス、民泊などのシェアエコノミーの基盤



# ブロックチェーン上の企業資産

## DAOやICOによる「仮想」企業の資産

- 基本的にリカルディアン・コントラクトであり、債権である
- 資金調達や投機の対象にはなり得る
- 第三者からの「使用」やそれによる「収益」を得る企業資産にはならない



# 中華人民共和国民法の改正のインパクト

## インターネット上のデジタル資産の法的保護 (民法総則第127条)

**2017年3月15日の全国人民代表大会で可決、2017年10月1日より施行**

**第一百二十四条**　自然人依法享有继承权。

自然人合法的私有财产，可以依法继承。

**第一百二十五条**　民事主体依法享有股权和其他投资性权利。

**第一百二十六条**　民事主体享有法律规定的其他民事权利和利益。

**第一百二十七条**　法律对数据、网络虚拟财产的保护有规定的，依照其规定。

**第一百二十八条**　法律对未成年人、老年人、残疾人、妇女、消费者等的民事权利保护有特别规定的，依照其规定。

**第一百二十九条**　民事权利可以依据民事法律行为、事实行为、法律规定的事件或者法律规定的其他方式取得。

**第一百三十条**　民事主体按照自己的意愿依法行使民事权利，不受干涉。

**第一百三十一条**　民事主体行使权利时，应当履行法律规定的和当事人约定的义务。

**第一百三十二条**　民事主体不得滥用民事权利损害国家利益、社会公共利益或者他人合法权益。

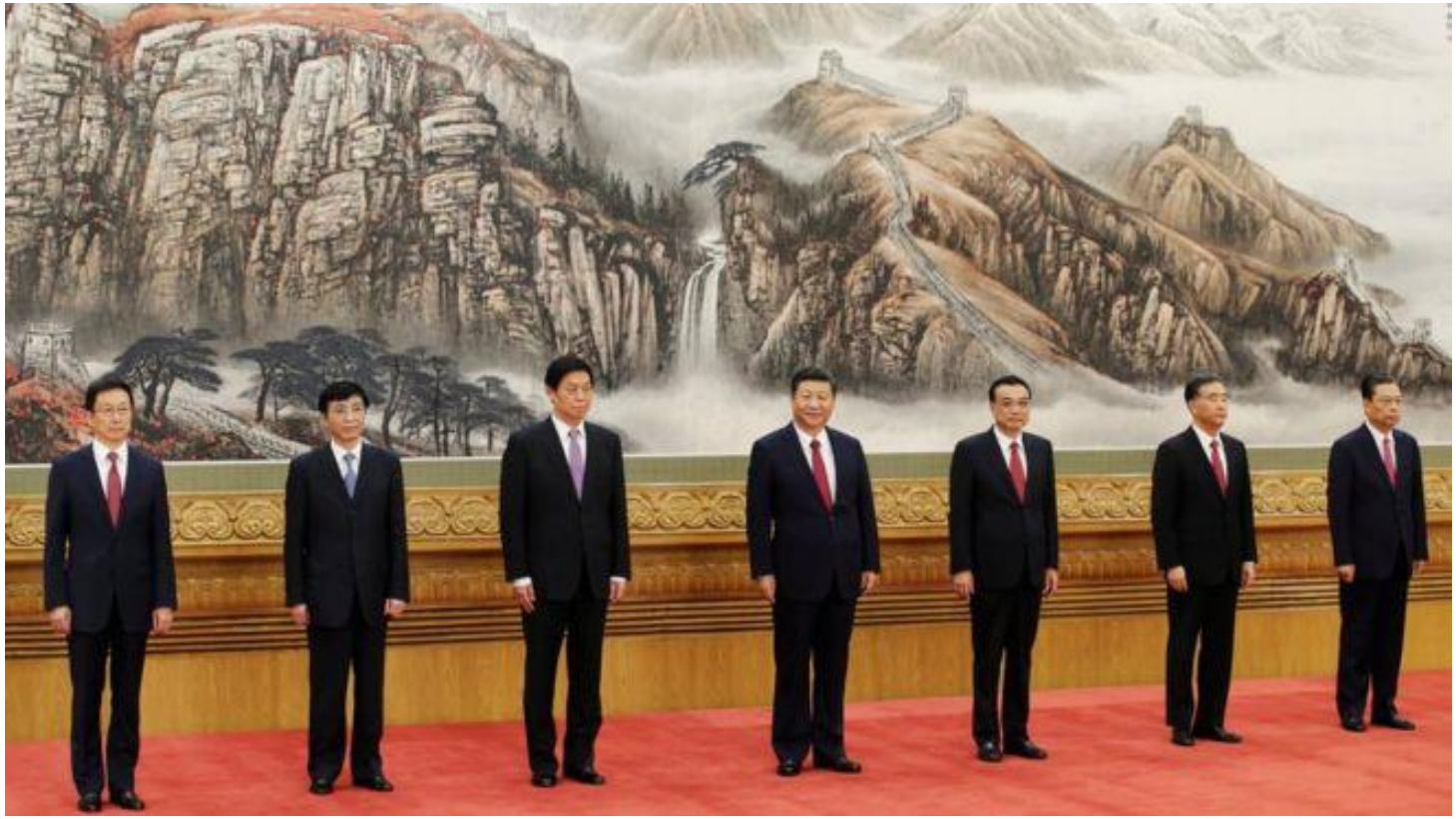


**google 翻訳の結果**

**第127条　データ及びオンライン仮想財産の保護を規定する法律は、その規定に従うものとする。**

**仮想通貨を財産として利用できる**
**無体物にも所有権を定義したのに近い？**

# 中国共産党大会　2017年10月



# 一帯一路の開発拠点とマイニング拠点の類似


習近平 一帯一路構想

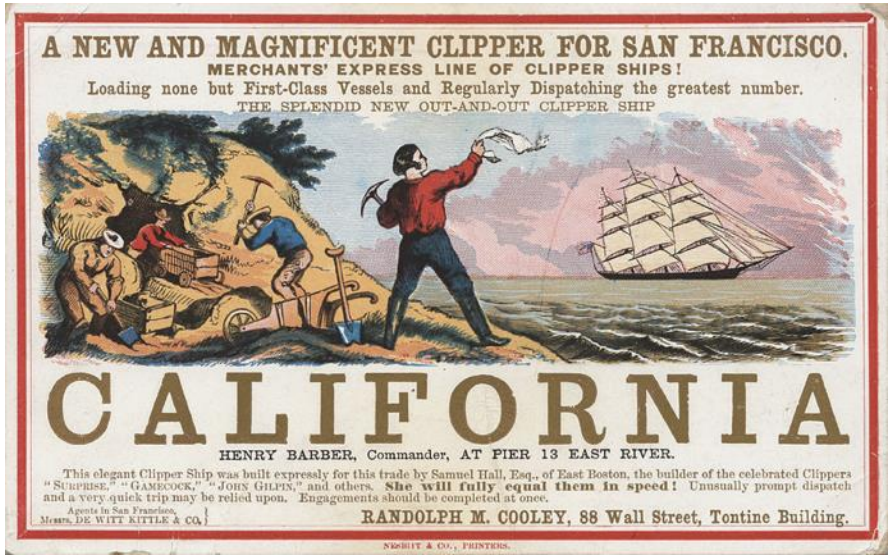

ケンブリッジ大学金融研究所報告書

# 1849年のアメリカのゴールド・ラッシュ

## 20万人が金を求めてカリフォルニアに移動

### 西部開拓の原動力

## 大陸横断鉄道の建設、海路の整備




# アメリカ独立戦争

イングランド銀行（世界の銀行）

イングランド銀行の支配からの独立が目的の１つ

- ボストン茶会事件 1773年
- アメリカ独立戦争 ~ 1783年

独立戦争後勝利後のアメリカの通貨発行

- アメリカの地域銀行券はまるで仮想通貨

# サフォーク銀行

自由放任主義の決済システム

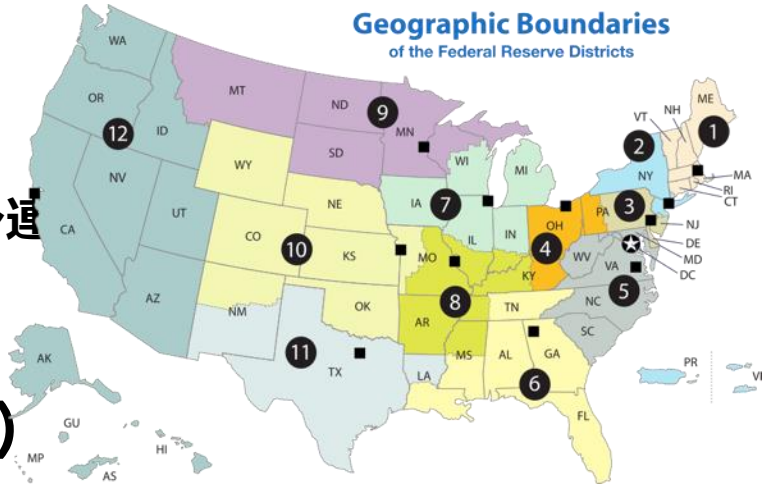
アメリカの地域銀行の親分銀行（地域ごと）

- 地方銀行券を一定率（1/3)預かり、価格調整
- 地方銀行券間の交換所

連邦準備銀行 (FRB) の前身

- 12主要都市のFRB

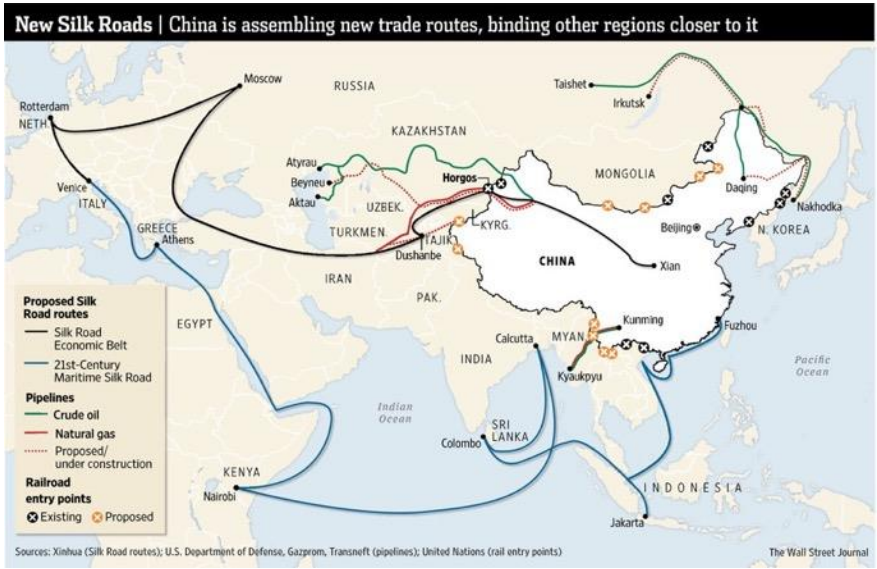
  シカゴ連銀、ニューヨーク連銀、ボストン連




カリフォルニアの金の発見後

- ドルによる支配へ（世界の通貨）

# 貿易金融のための仮想通貨




日常的な決済には使いづらい

- 完了までに時間がかかる
- 少額決済では手数料が割高

貿易決済通貨としては理想的

- 多数の国家を経由する商取引の決済

中国人民銀行発行のデジタル通貨構想

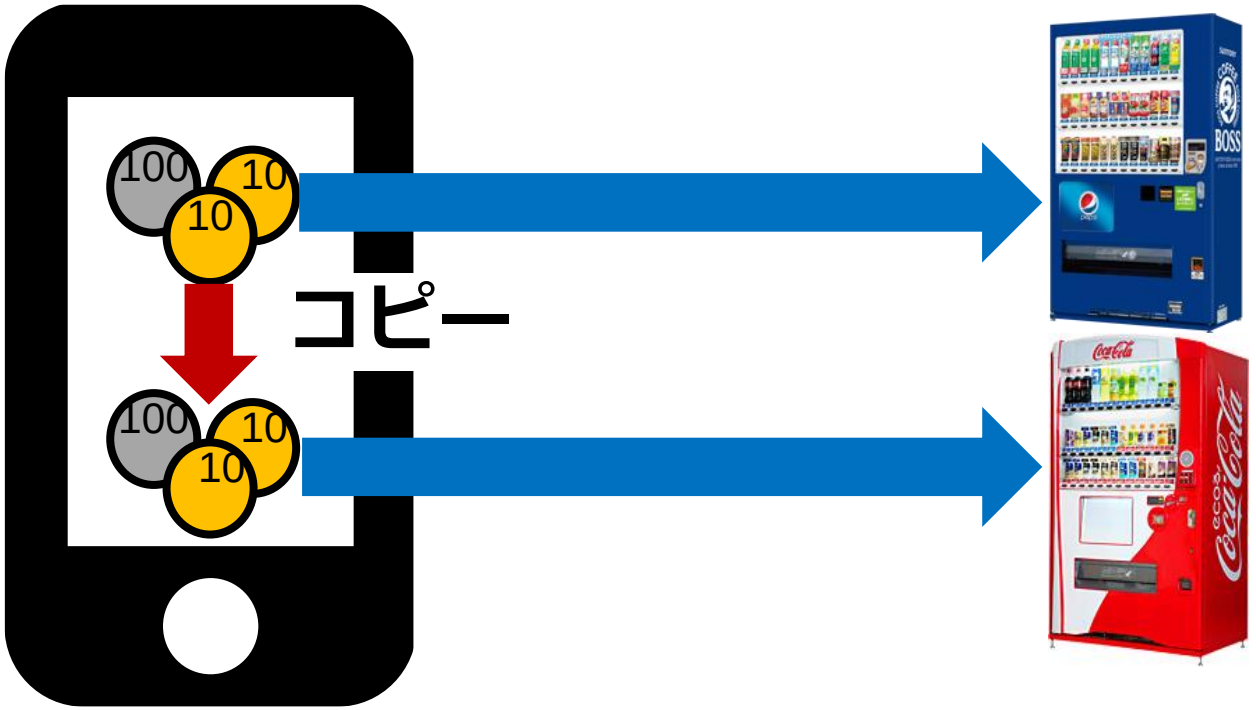
# bitcoinとブロックチェーンの仕組み

# 電子マネーの二重使用問題

「原子」でできてる現金は使用すると手元から消滅

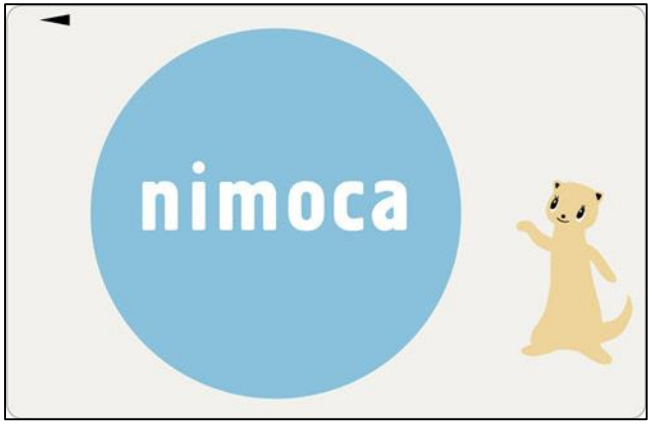
「情報」でできている電子マネーは原理的も消滅不可能

- データは削除できるが、「情報」は消すことができない

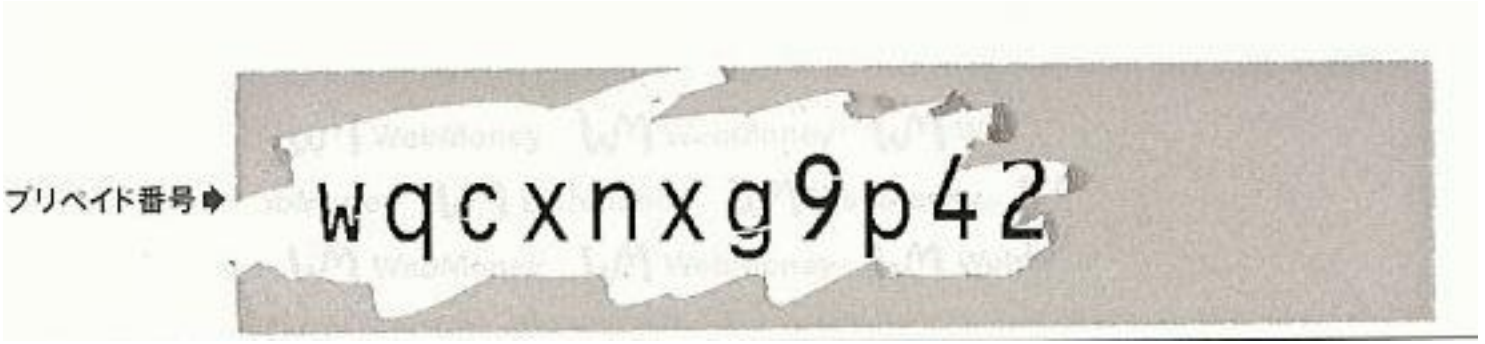


# 従来の解決策

## ICカード（耐タンパデバイス）

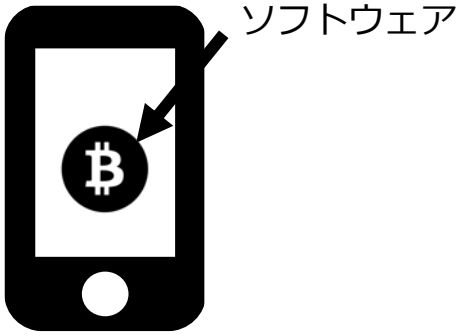



## 信頼できるネットワークサービス

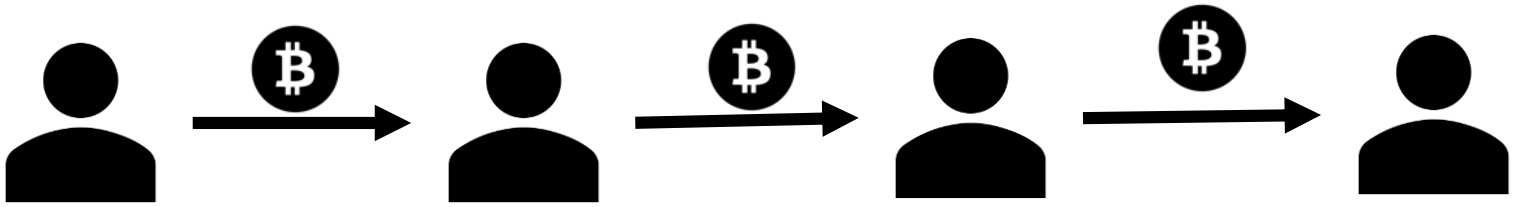


# Bitcoinによる二重使用問題の解決

## ソフトウェアだけで実現可能




## 信頼点を必要としない



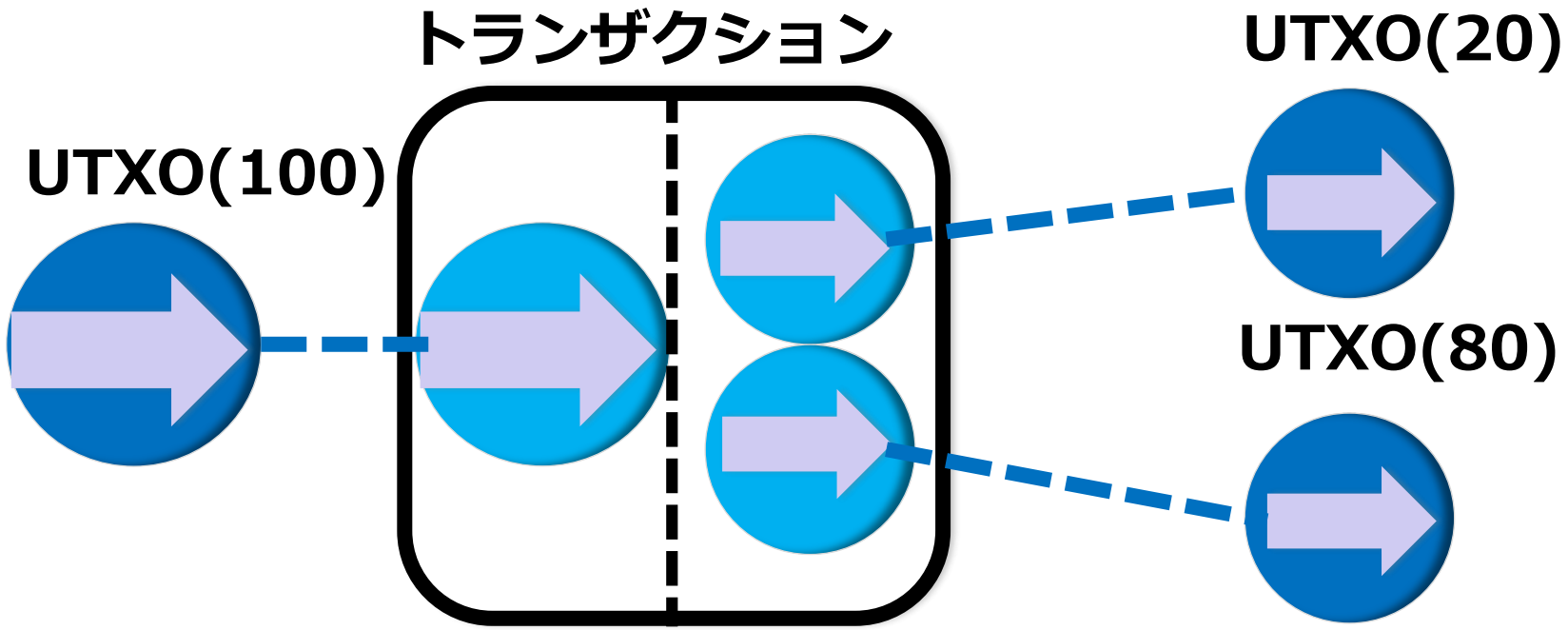
## 個人から個人への転々譲渡が可能

# bitcoinの二重使用問題の解決法

## 三式簿記と通貨的価値の保存則

## トランザクション：三式簿記の最小単位

- トランザクションによって通貨的価値の総量は増減しない

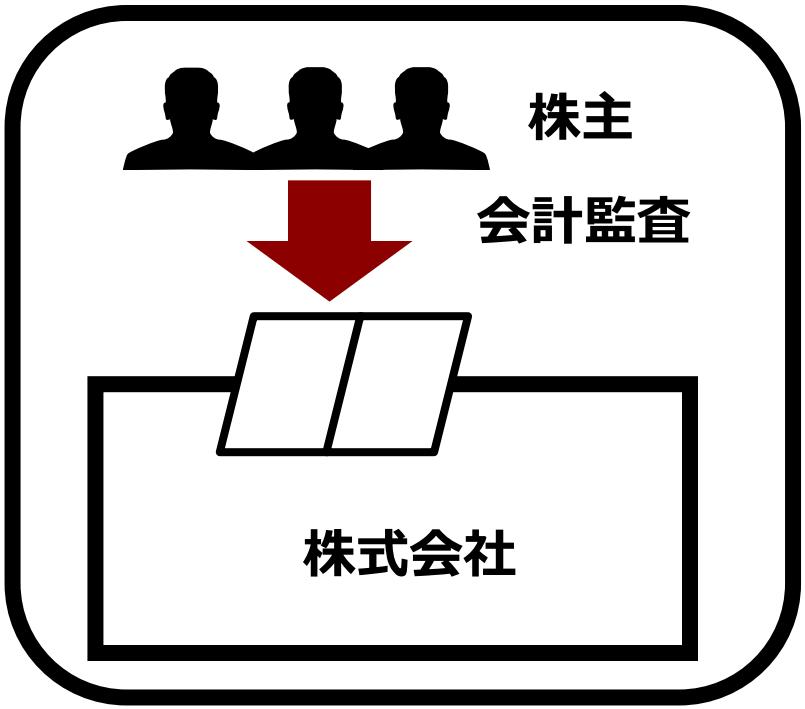


# 複式簿記

## 資本主義、株式会社の発達に貢献

## 会計監査

- 会社が株主に、資産、負債、費用、収益の整合性を証明
- クローズドシステム
- 会計期：１年

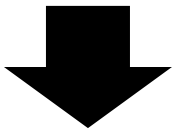


# 三式簿記

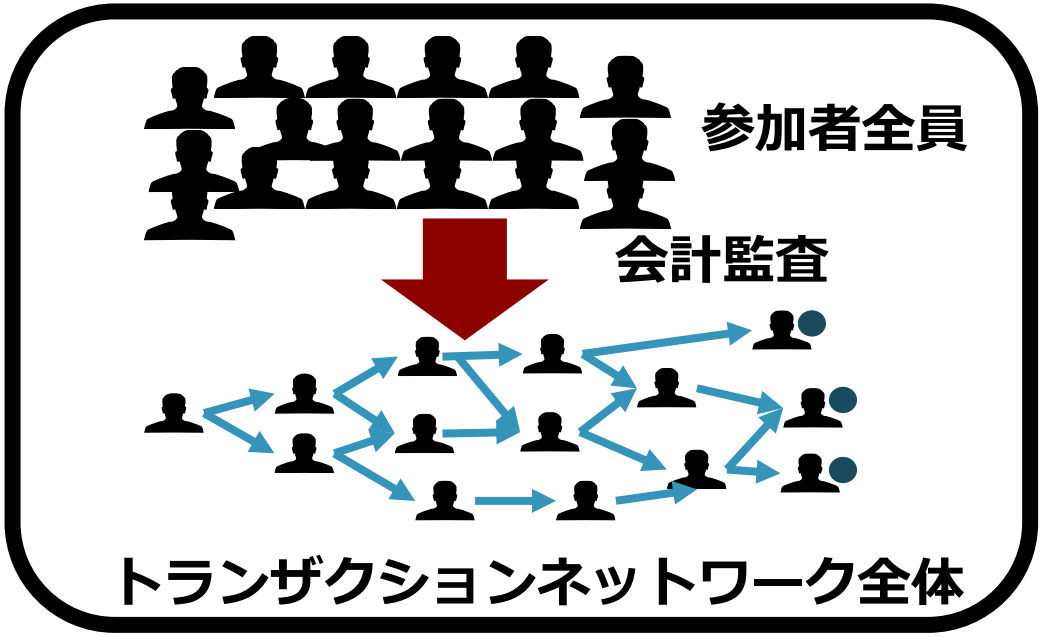
## bitcoinが最初に本格的に採用

## 送金内容の監査

- 送金の当事者が、参加者全員に送金内容の整合性を証明
- オープンシステム
- 会計期：約10分間



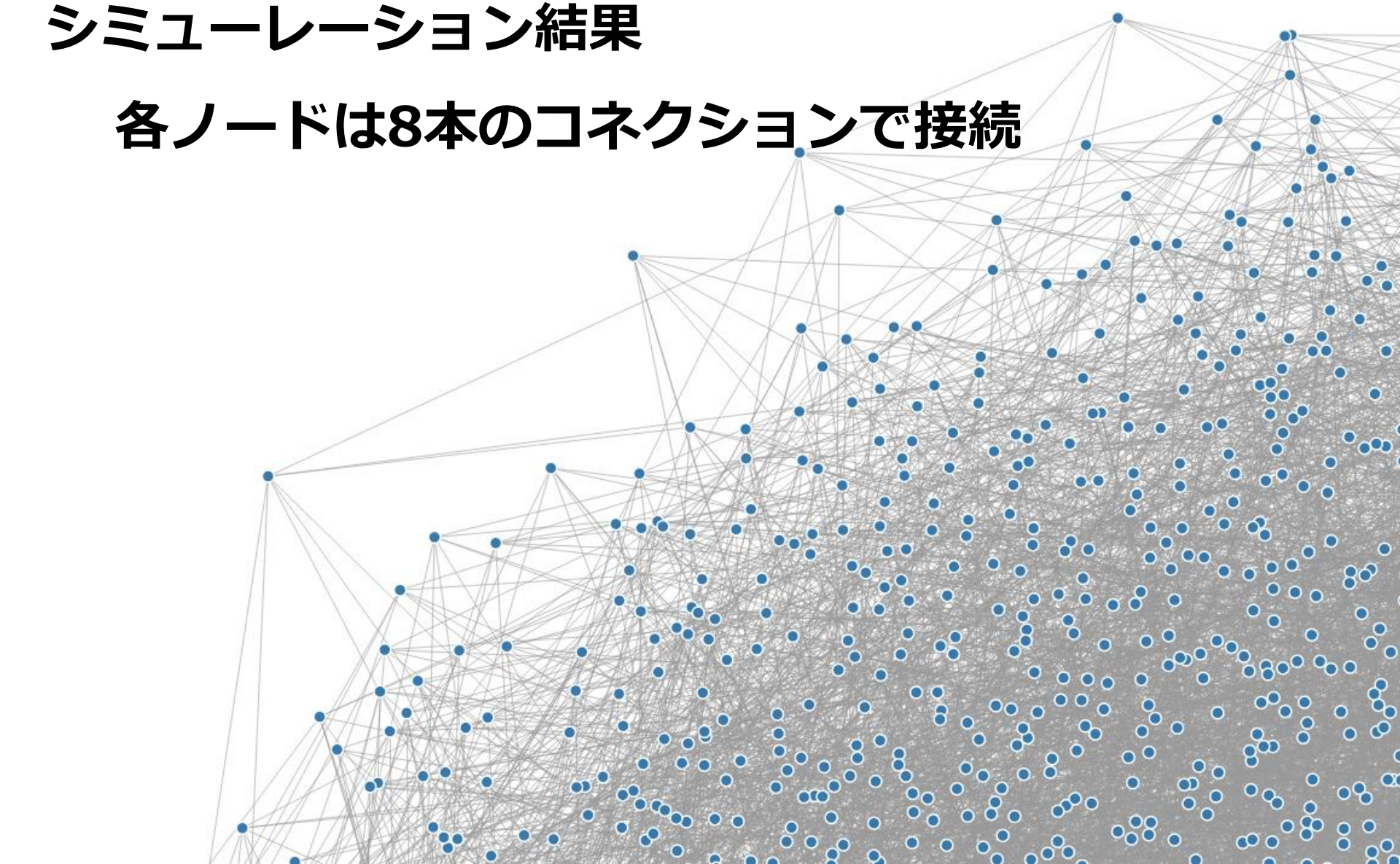
## 二重使用問題を解決!



# bitcoinネットワーク

## シミューレーション結果

各ノードは8本のコネクションで接続

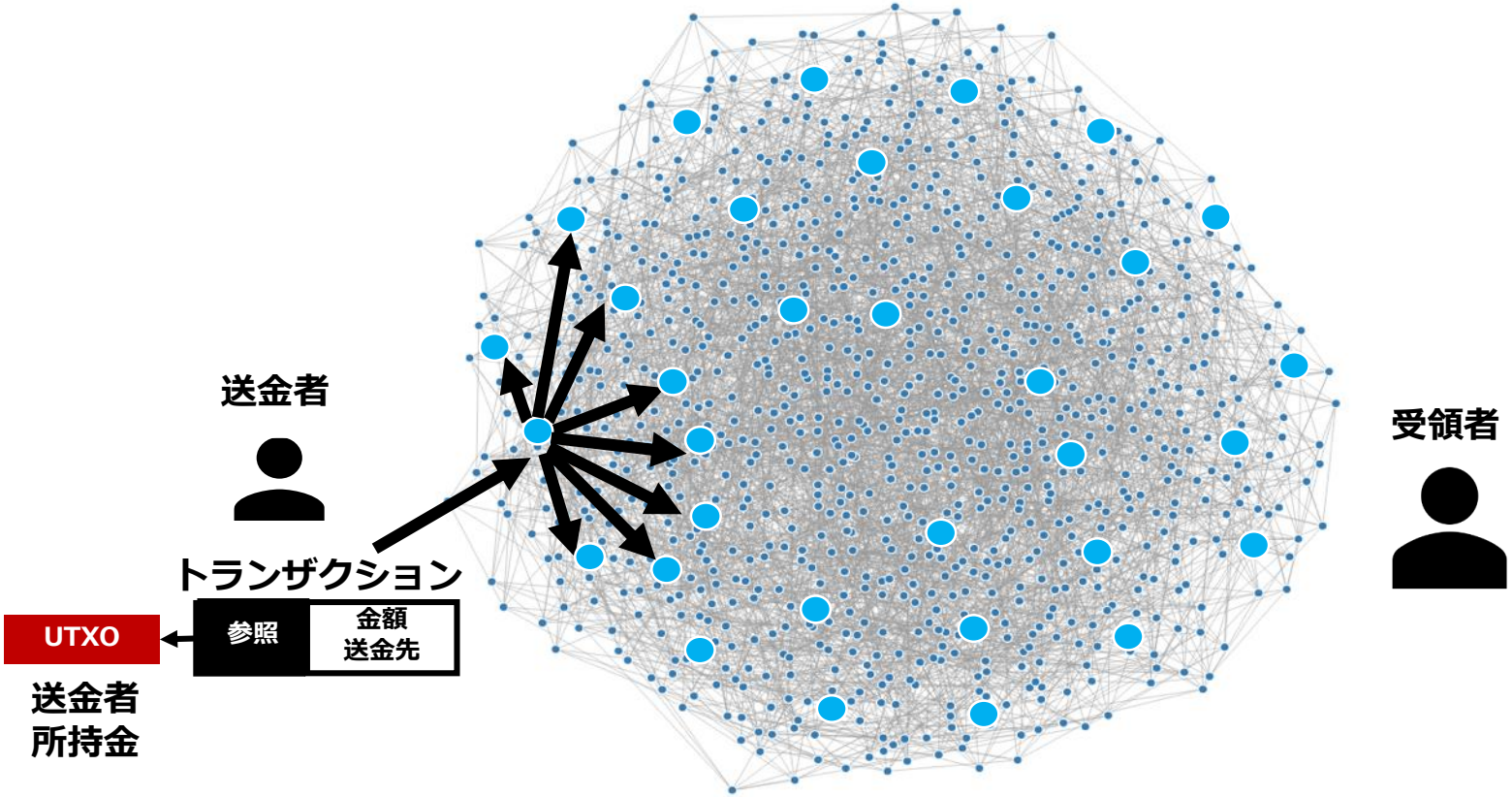


# ビットコインの送金開始

(1) 送金者は、送金用トランザクションを作成

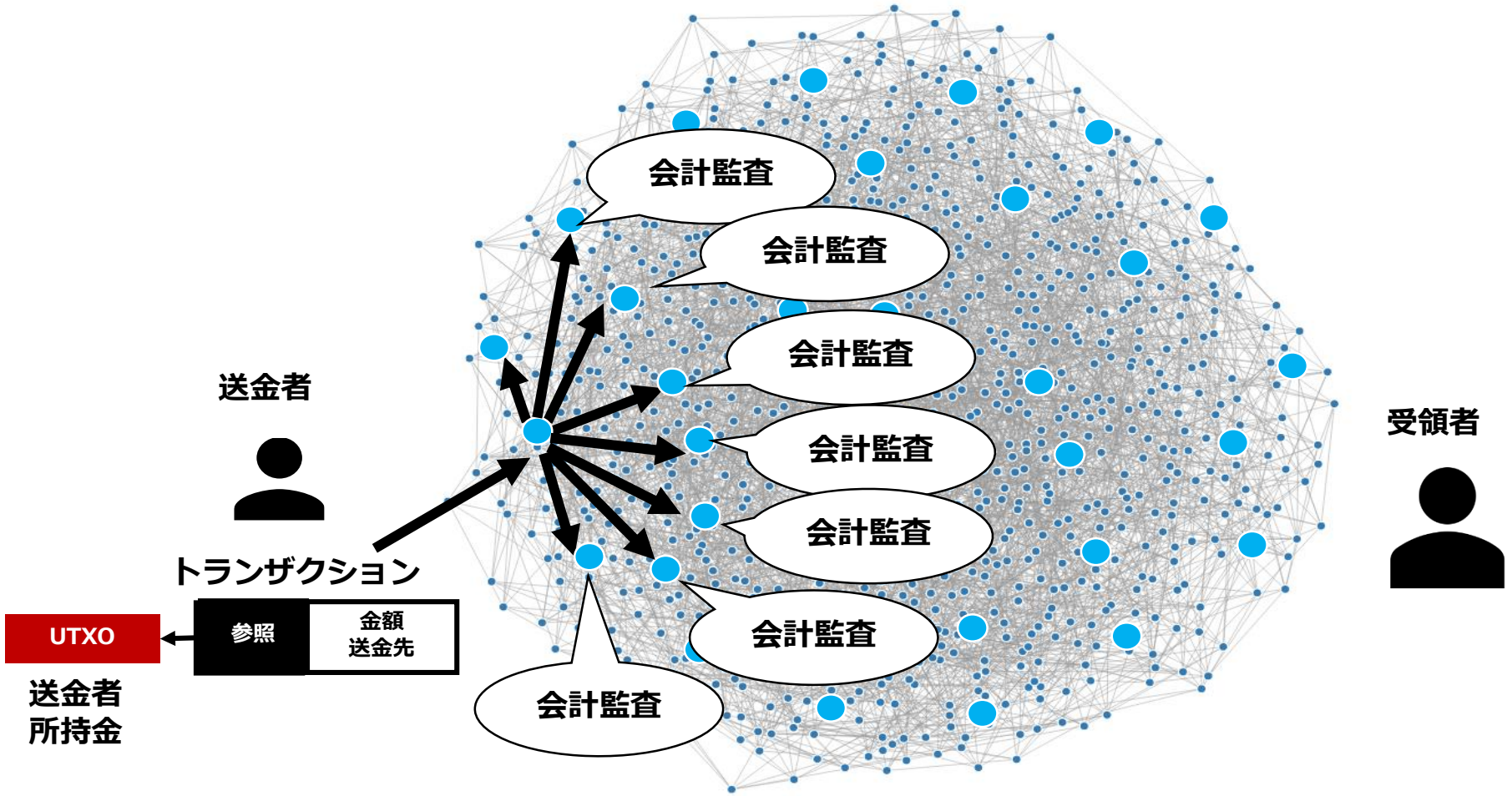
(2) トランザクションをbitcoinネットワークに送信

- 接続している８ノードに送信する



# ノードによるトランザクションの会計監査

## (3) 各受信ノードがトランザクションを検証（会計監査）する

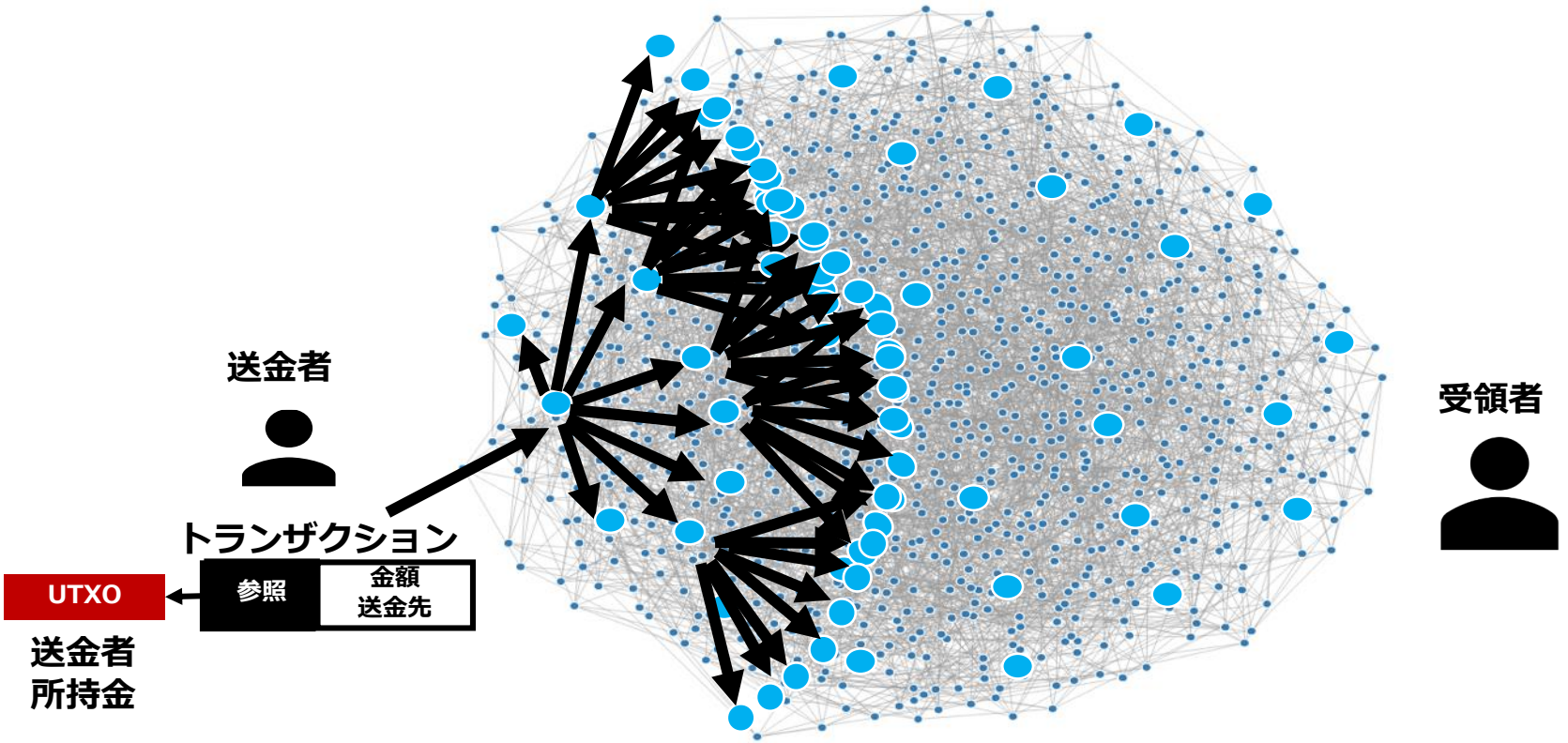


# 隣接ノードへのトランザクションのリレー

## (4) 会計参加の結果

- 問題がなければトランザクションを隣接する８ノードにリレーする
- 問題があればトランザクションは破棄される

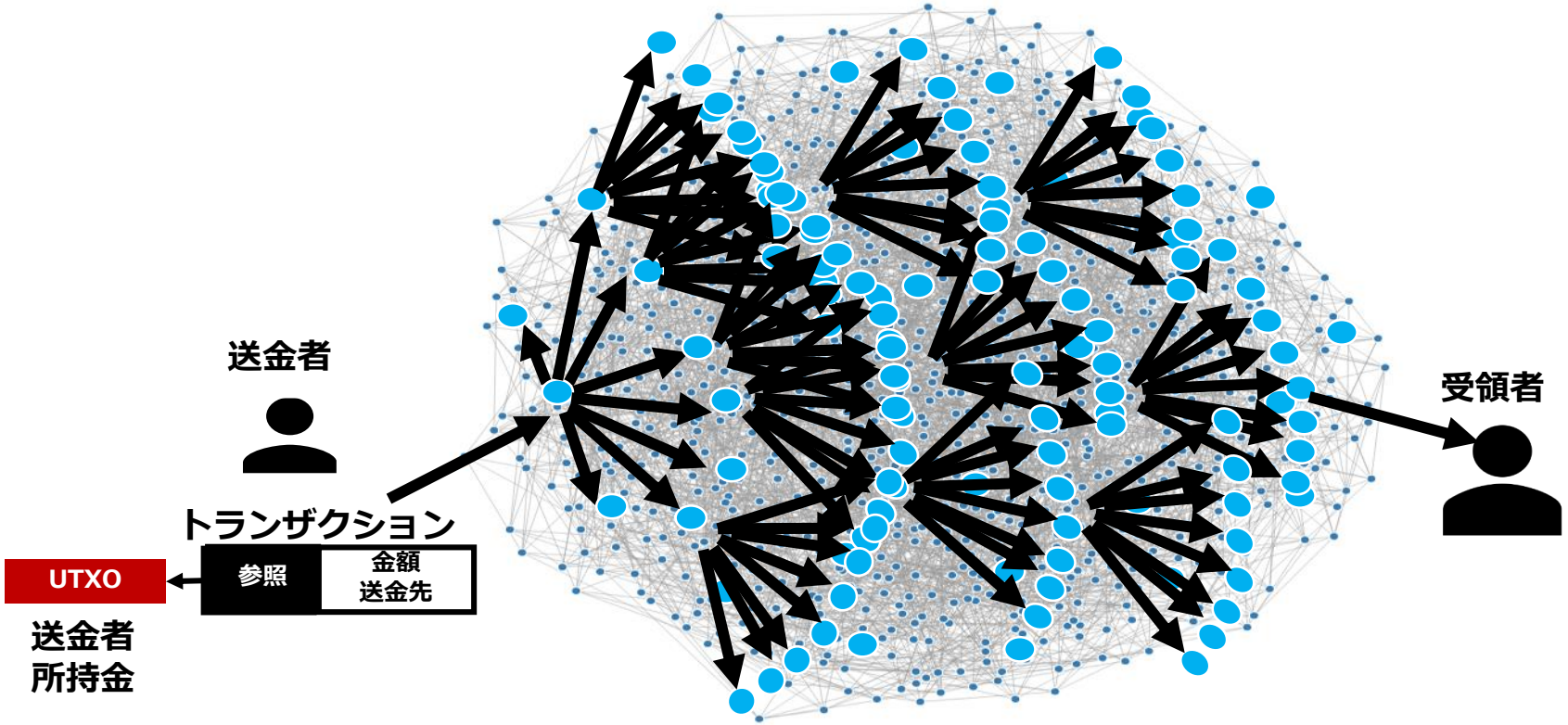
## (5) 会計監査とリレーが繰返される



# 全ノードにトランザクションが到達

## (6) 受領者にもトランザクションが到達する

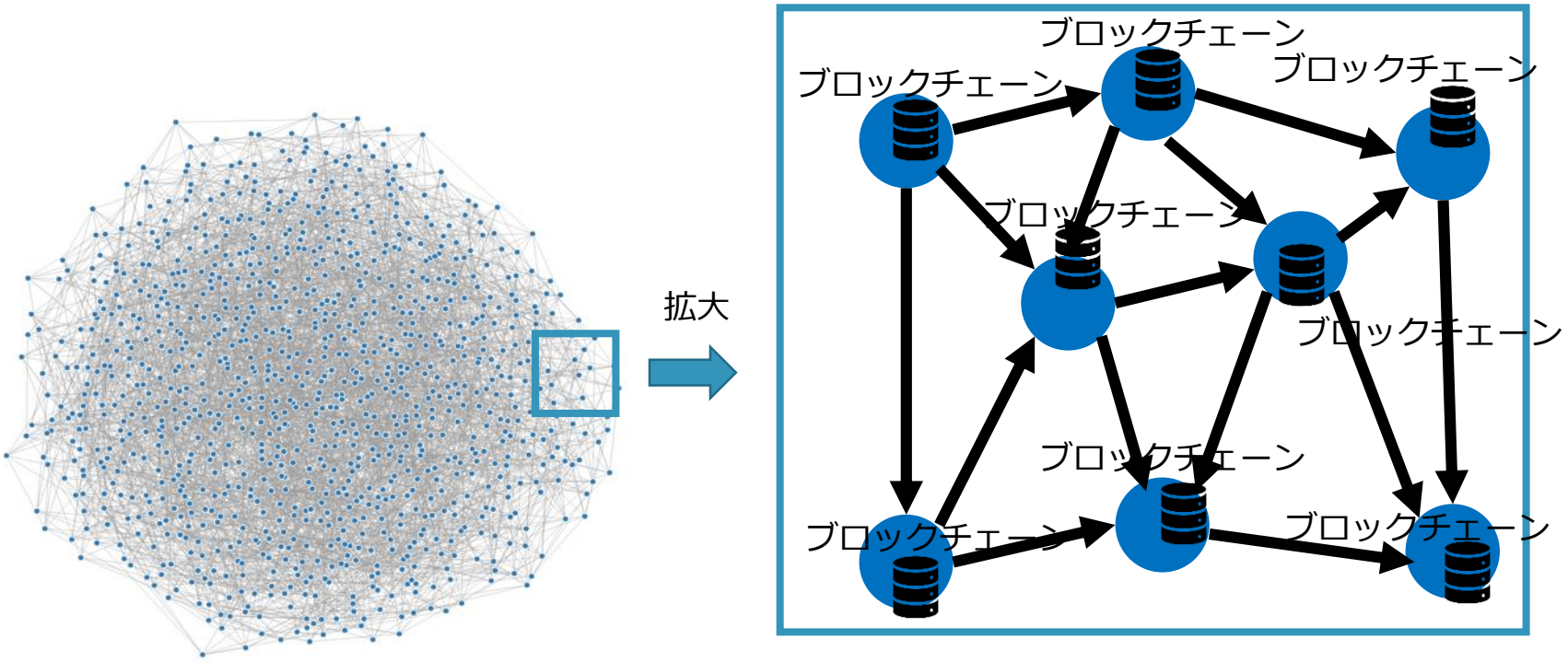
- 送金はまだ完了していない



# ブロックチェーンとは

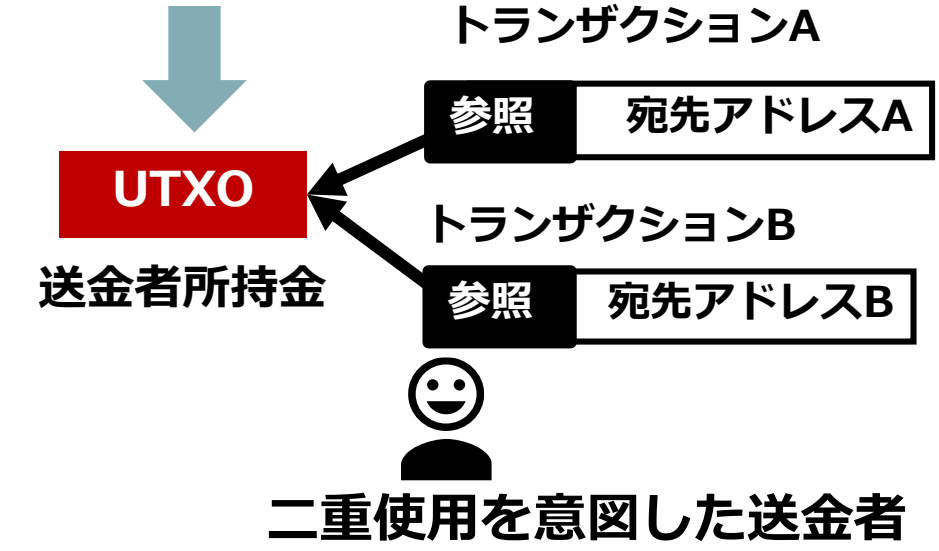
**Bitcoinネットワークの各ノードが保有している台帳記録**

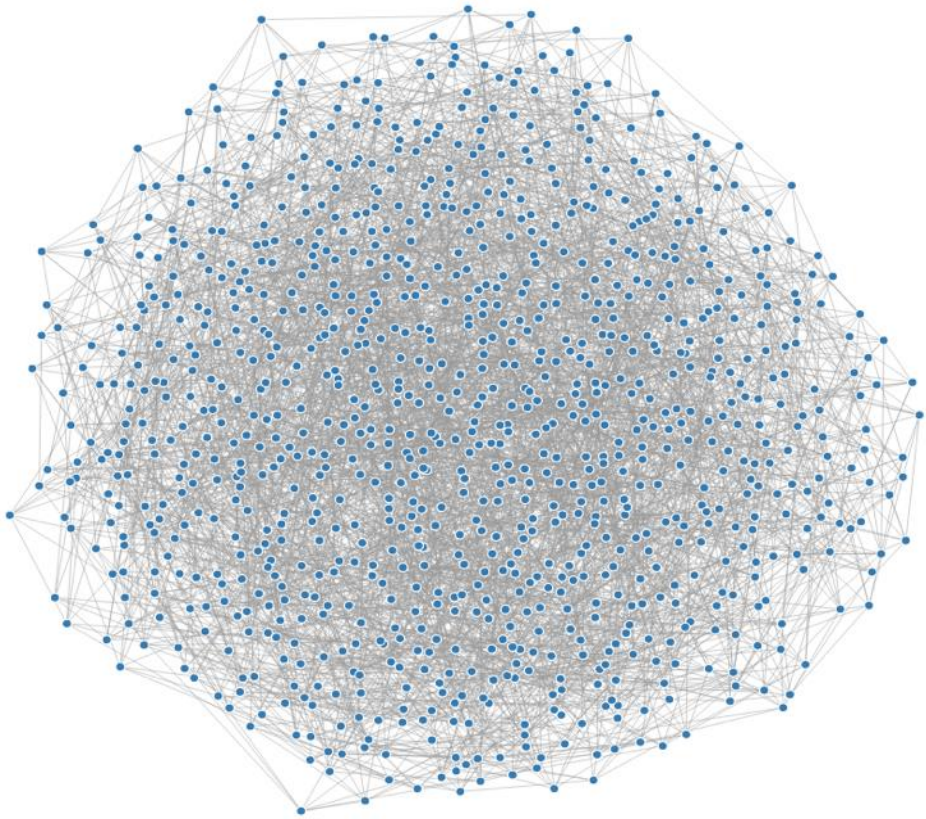
**正当なトランザクションが保管されている**



# 分散台帳による送金の二重使用の防止方法

## 同一のUTXOを二重に使用する不正を試みた場合

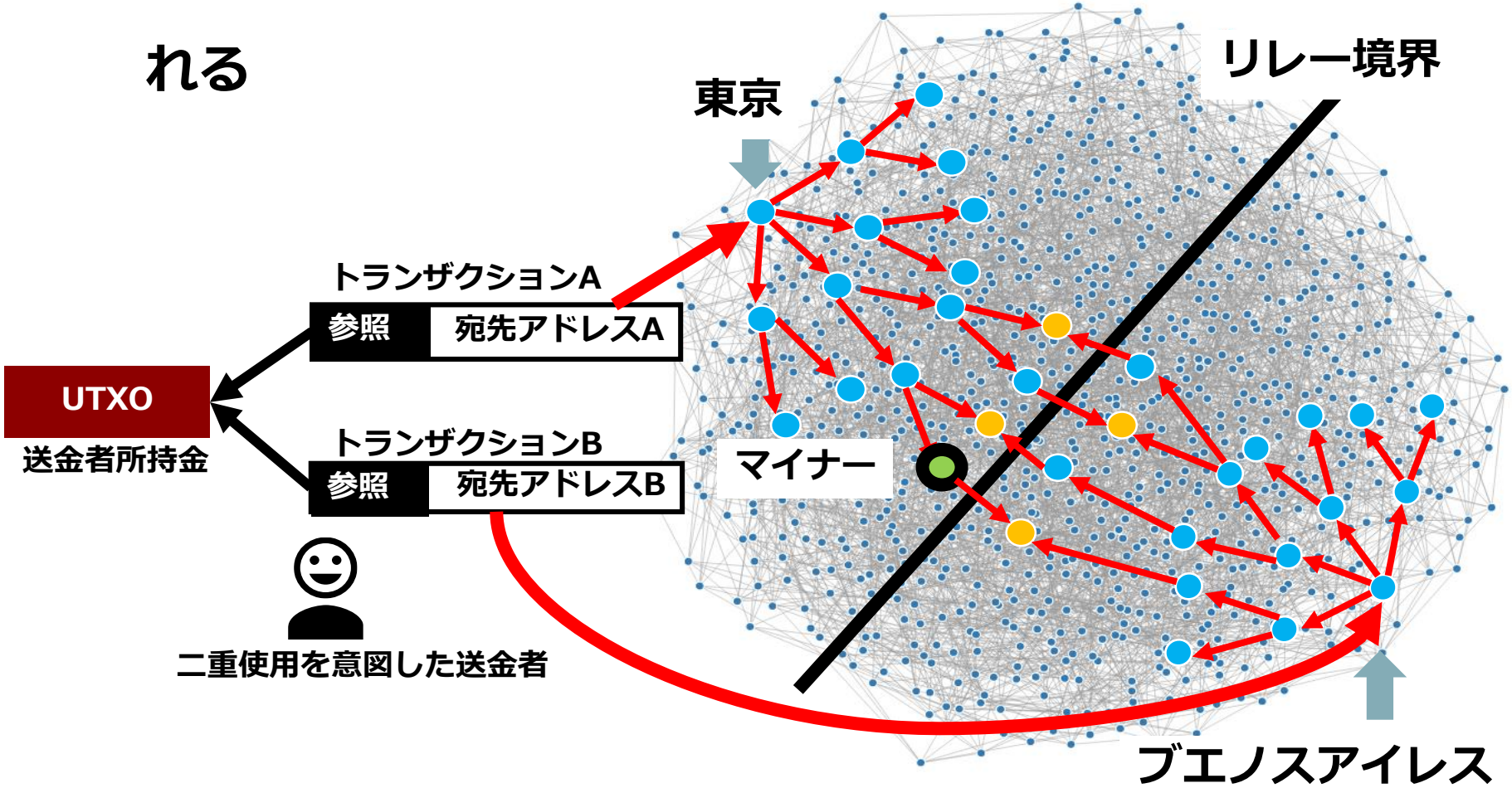


# 観測者（マイナー）を一つ定めると

## 正統な記録が一つ定まる

- UTXOを使用するの一方トランザクションのみが採用される

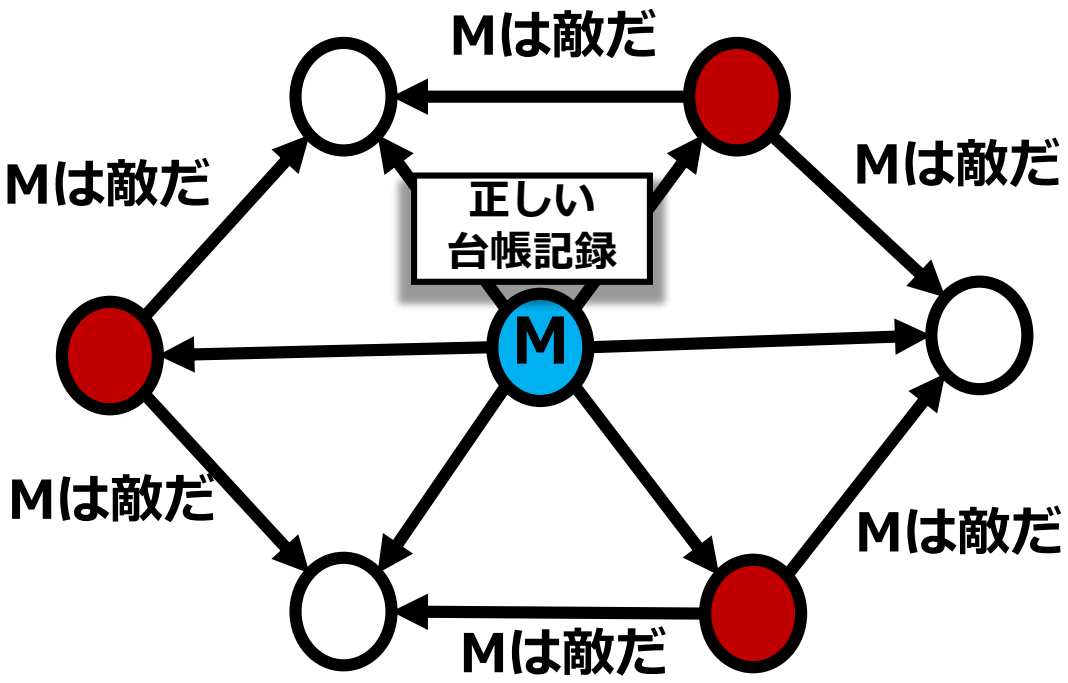


# ビザンティン合意問題

## 正常なノードすべてに同じ値を合意させる

## 1/3 以上の敵が結託すると合意は不可能

- 正常なノード
- 本当は正常なノード
- 結託しているノード

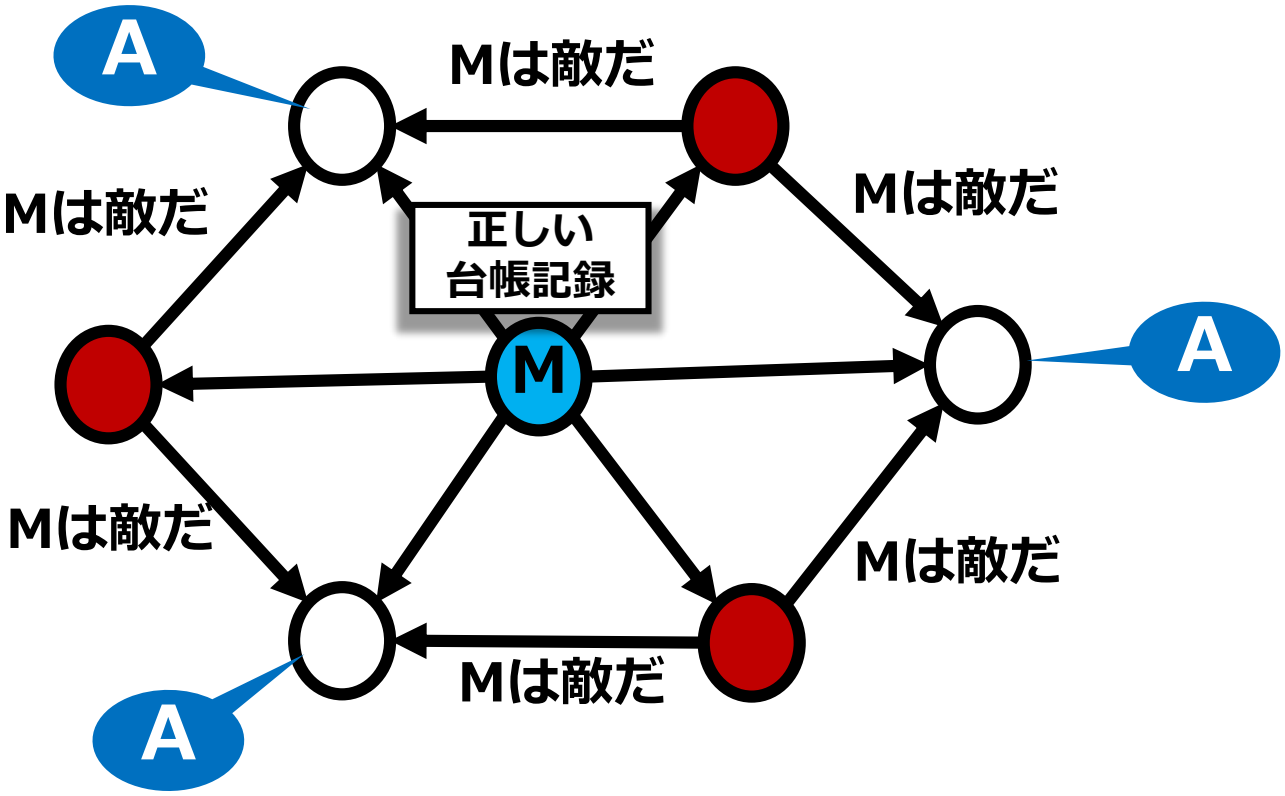


# コンセンサス・アルゴリズムとは

## 正常なノードの合意判定アルゴリズムのこと

A 合意アルゴリズム

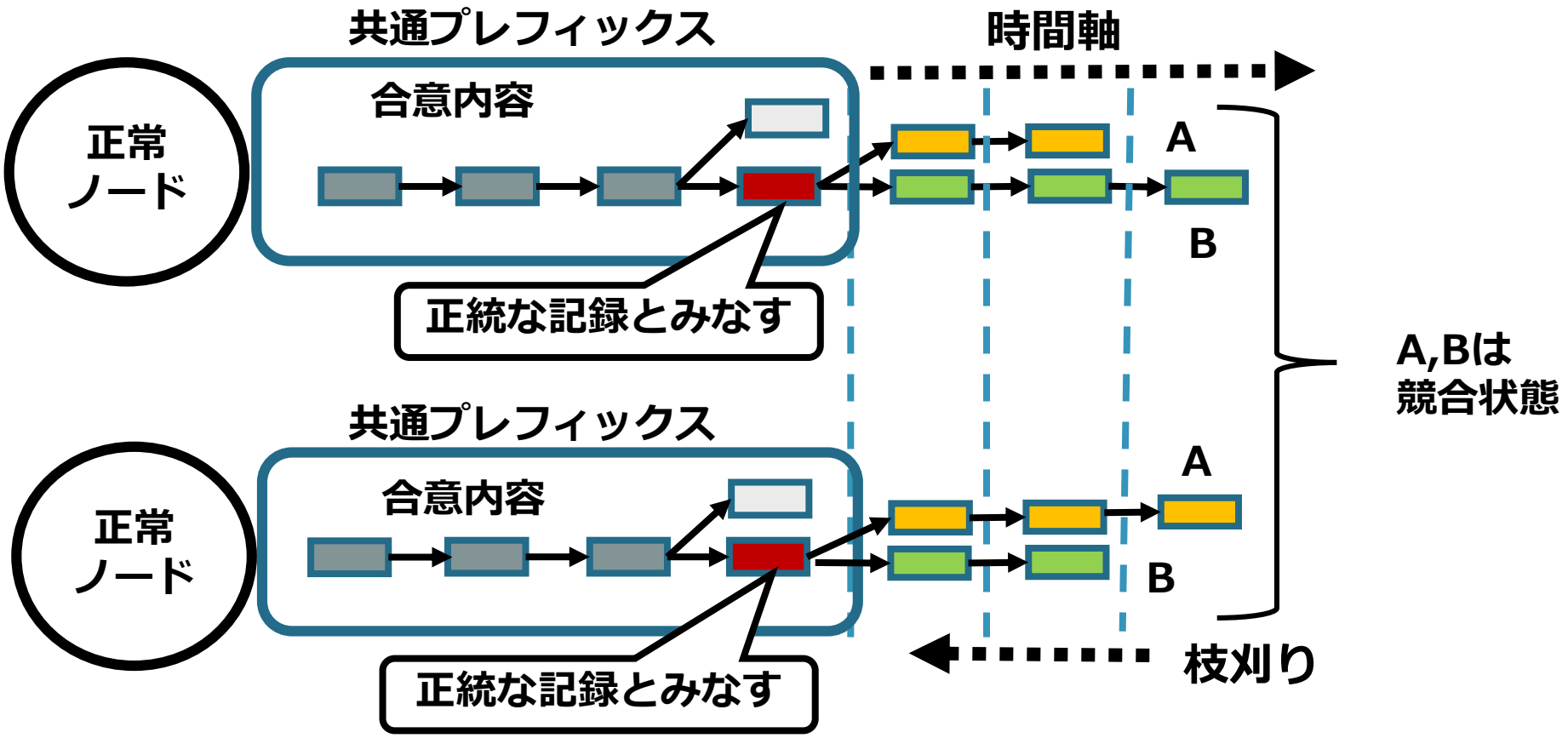
- 敵対ノードがいても正しい情報のみを台帳に記録する



# 共通プレフィックス法による合意

## 最長のチェーンの前半を確率的に合意内容とみなす

- 現在から過去方向にブロックチェーンを枝刈りする



# ブロックチェーンのガバナンスの課題

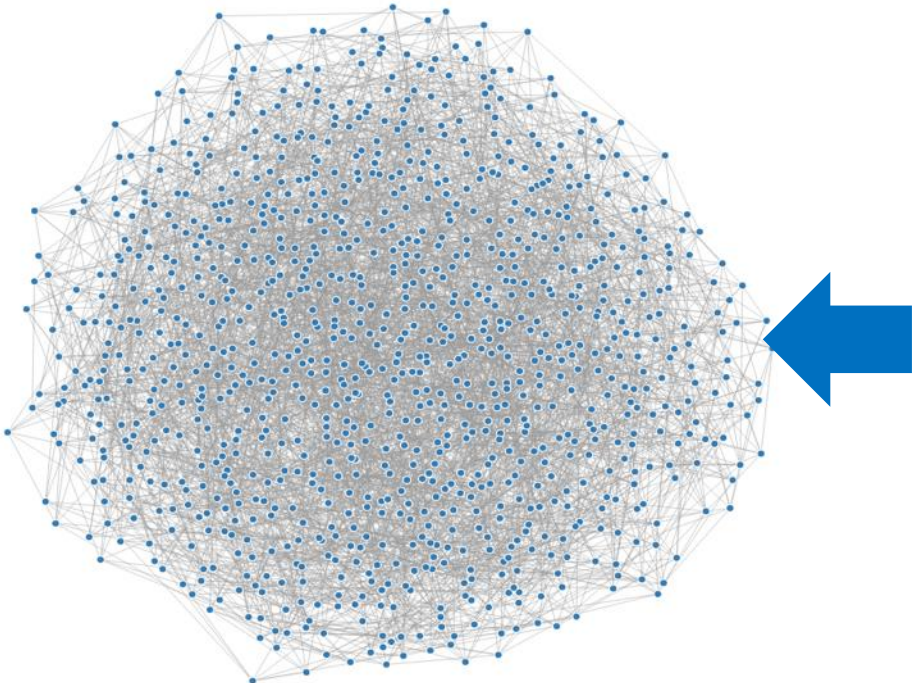
# ブロックチェーンの仕様のガバナンス

## P2P型システムのバージョンアップ方法

- サーバ型とは基本的に異なる

## コードの仕様変更　＝　経済圏のルールの変更

- 当事者の収益率への影響など、対立が生じうる



バージョンアップ
仕様変更

# Code (法律) = Code (プログラム)

ハーバート大学　ローレンス・レッシグ教授

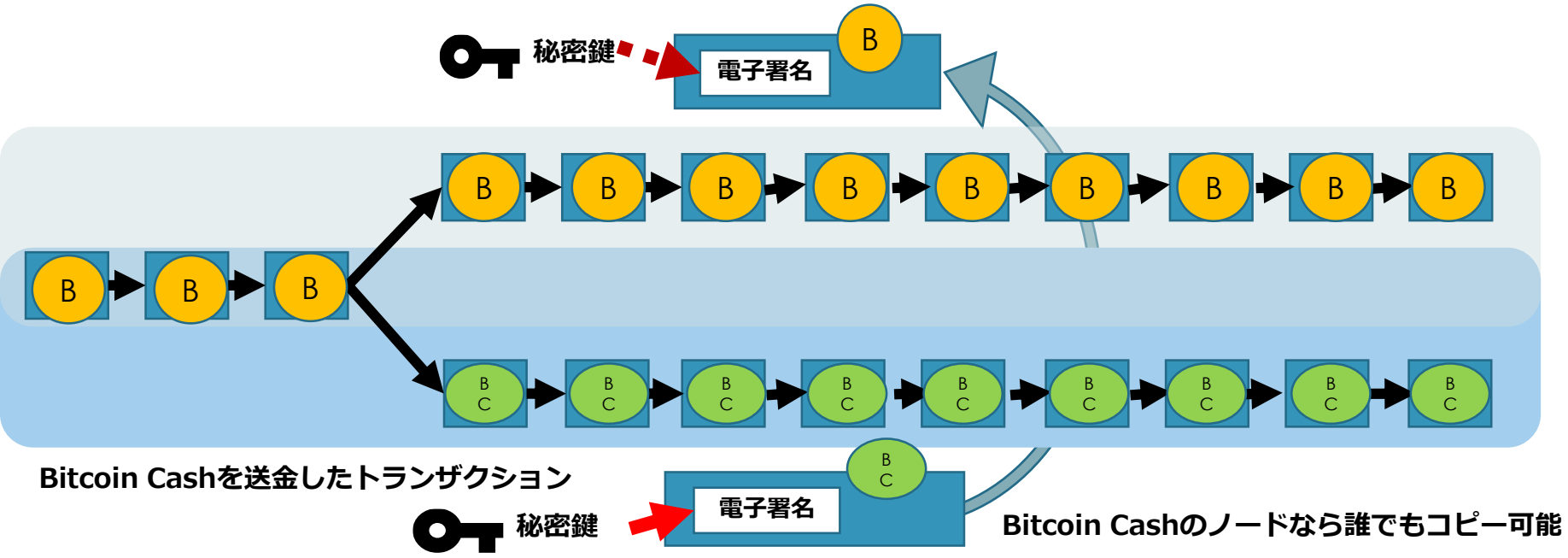
# ブロックチェーンの分裂問題

## ハードフォーク発生時の問題の例

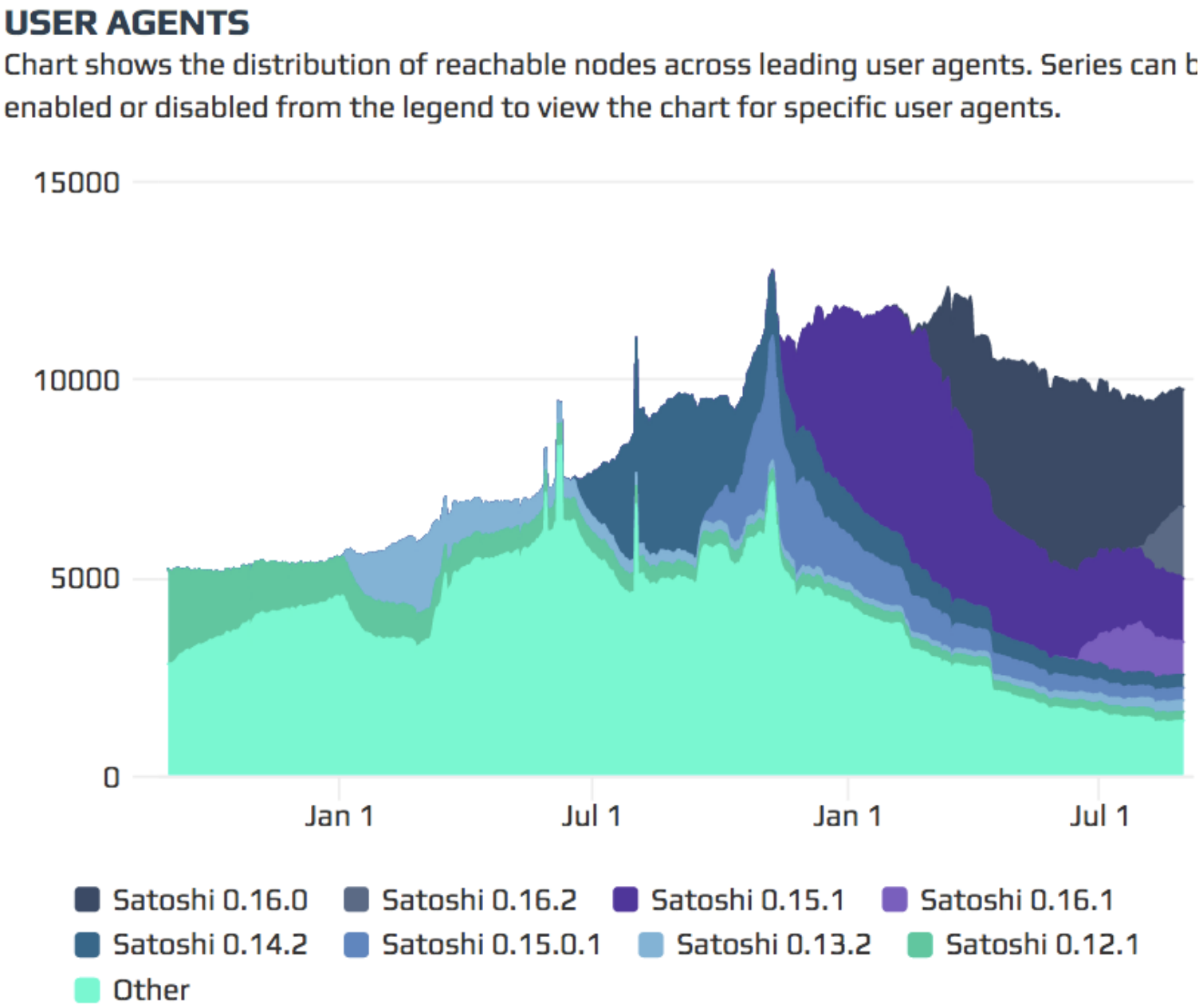
- トランザクションのリプレイ攻撃

  双方のチェーンの未使用の仮想通貨は，同じ秘密鍵で送金できる

  2-wayでプロテクトすれば回避可能だが、敵対的ハードフォークの場合はあえてプロテクトしない



# ビットコインノードのバージョン比率の時間的推移



# 全世界のビットコインフルノード

## GLOBAL BITCOIN NODES DISTRIBUTION

Reachable nodes as of Sat Mar 02 2019 13:48:44 GMT+0900 (日本標準時).

# 10508 NODES

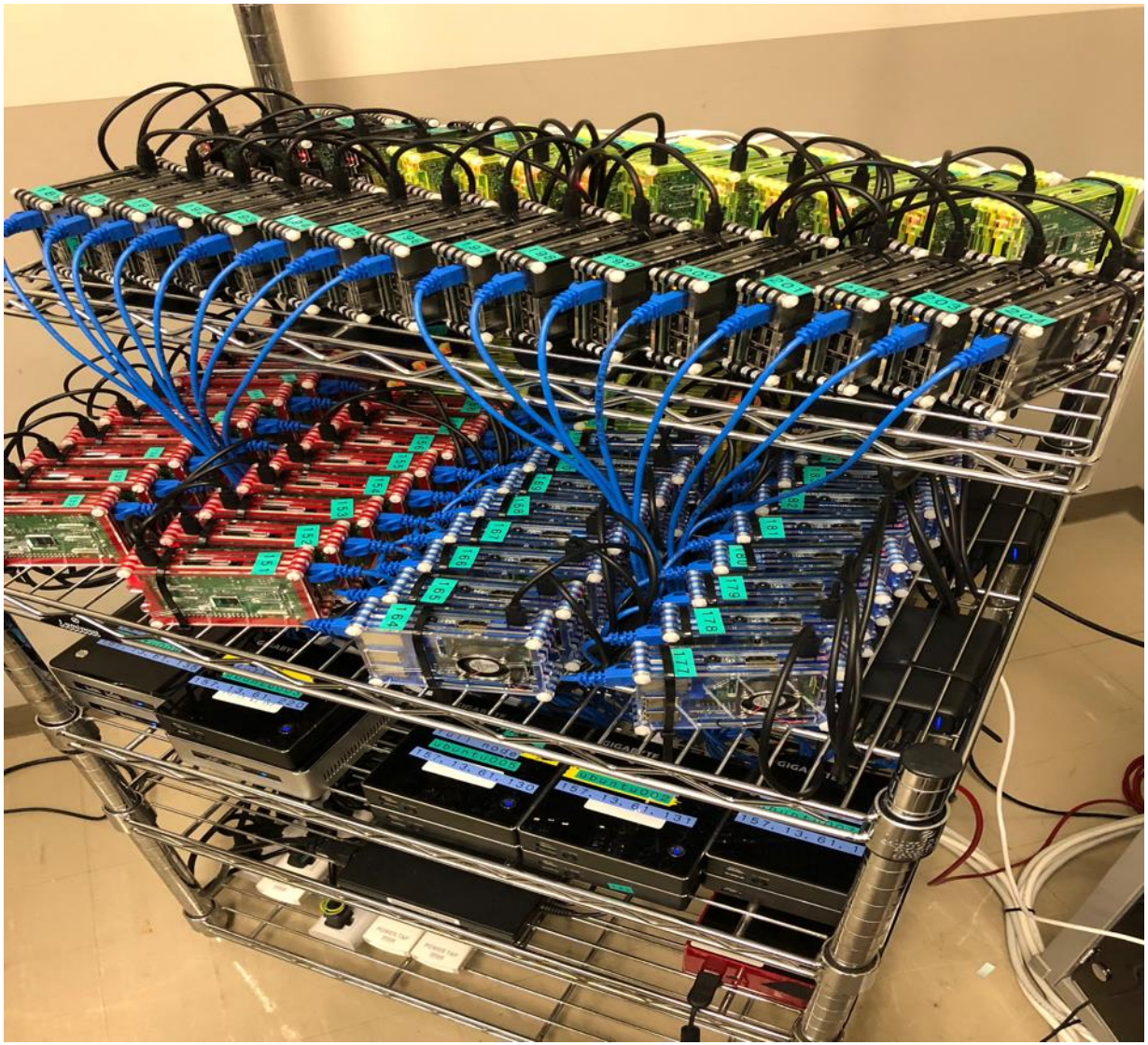
24-hour charts »

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

| RANK | COUNTRY | NODES |
|---|---|---|
| 1 | United States | 2635 (25.08% |
| 2 | Germany | 2009 (19.12% |
| 3 | France | 691 (6.58%) |
| 4 | Netherlands | 536 (5.10%) |
| 5 | Canada | 389 (3.70%) |
| 6 | China | 358 (3.41%) |
| 7 | United Kingdom | 355 (3.38%) |
| 8 | Singapore | 323 (3.07%) |
| 9 | Russian Federation | 272 (2.59%) |
| 10 | Japan | 249 (2.37%) |

# 近畿大学山崎研究室のフルノードクラスタ

## 2017年から90台稼働中（現在拡張中）



# 全世界のビットコインフルノード

## GLOBAL BITCOIN NODES DISTRIBUTION

Reachable nodes as of Sat Mar 02 2019 13:48:44 GMT+0900 (日本標準時).

# 10508 NODES

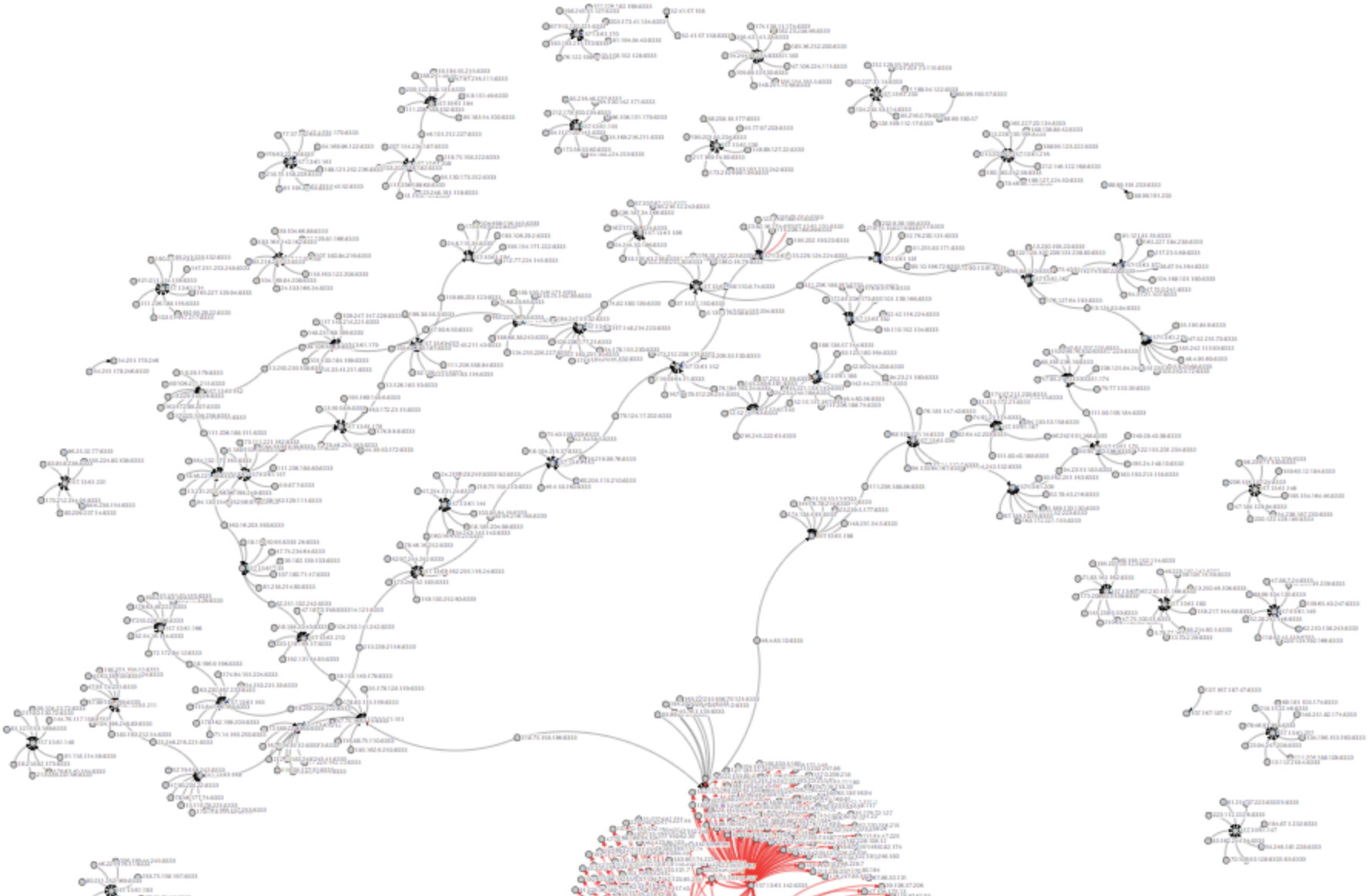
24-hour charts »

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

| RANK | COUNTRY | NODES |
|---|---|---|
| 1 | United States | 2635 (25.08% |
| 2 | Germany | 2009 (19.12% |
| 3 | France | 691 (6.58%) |
| 4 | Netherlands | 536 (5.10%) |
| 5 | Canada | 389 (3.70%) |
| 6 | China | 358 (3.41%) |
| 7 | United Kingdom | 355 (3.38%) |
| 8 | Singapore | 323 (3.07%) |
| 9 | Russian Federation | 272 (2.59%) |
| 10 | Japan | 249 (2.37%) |

# 山崎研から距離１の bitcoin ネットワーク

## 実際に８ずつ接続していることが確認できる

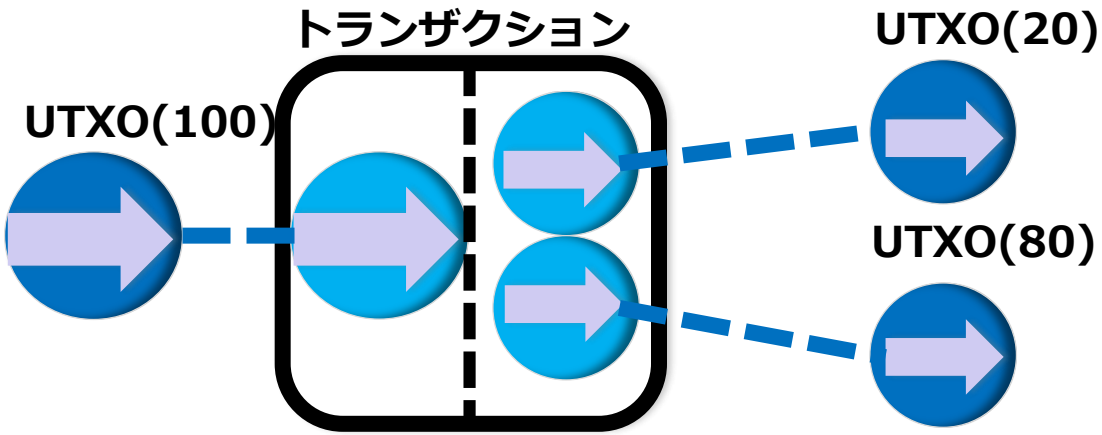


# 「物理世界」と「ビットの世界」の結合の必要性

# 仮想通貨以外でのブロックチェーンの利用

## 貨幣的価値以外で「総量保存則」を利用

- 製薬会社からの薬剤の流通の検証
- 廃棄物処分経路の管理
- …



# 物理世界とビットの世界の対応が不明

## 廃棄物の処分経路？

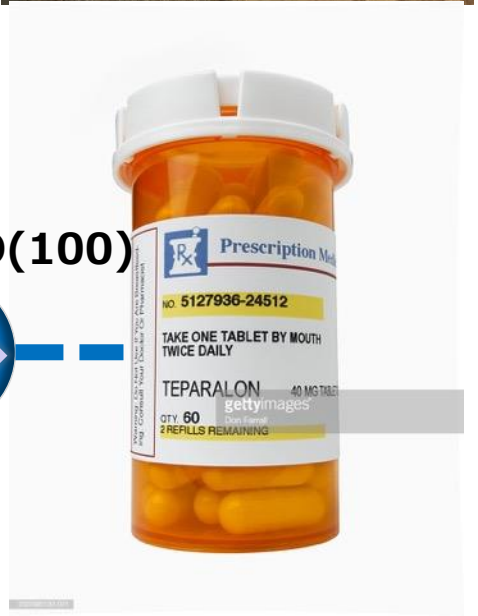
- ダンプカーが処分場に運搬した廃棄物の量
- 確認する方法は？

UTXO(100)

## 薬剤の流通？

- 調剤薬局の薬瓶の中身
- 確認する方法は？

UTXO(100)



# 物理世界とビットの世界の対応が不明

## 廃棄物の処分経路？

- ダンプカーが処分場に運搬した廃棄物の量
- 確認する方法は？

## 薬剤の流通？

- 調剤薬局の薬瓶の中身
- 確認する方法は？

UTXO(100)

UTXO(100)


**信頼できる主体が検証**

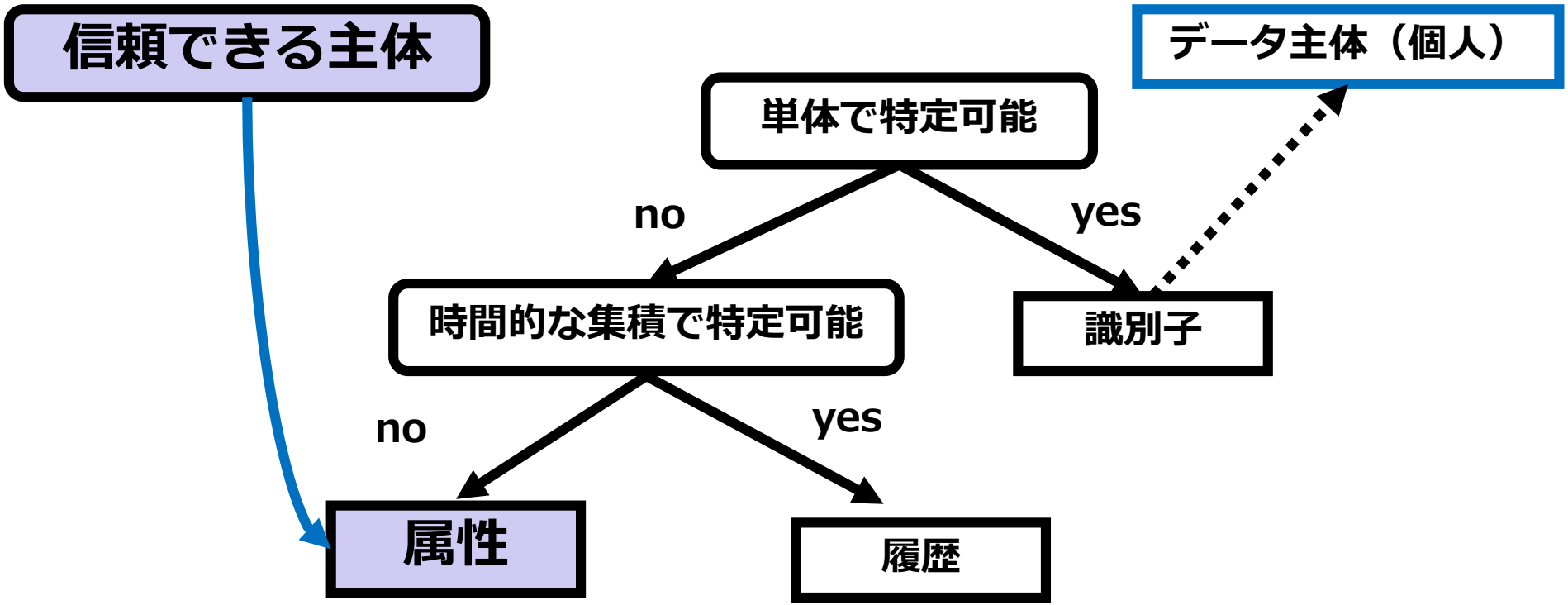
## 集中管理の方が合理的

- データベースの方が低コストで高性能

# 個人の属性の証明は？

## 学歴、資格、免許などの管理

- 信頼できる主体が認証しなければ無意味
- ブロックチェーンで管理する意味は無い



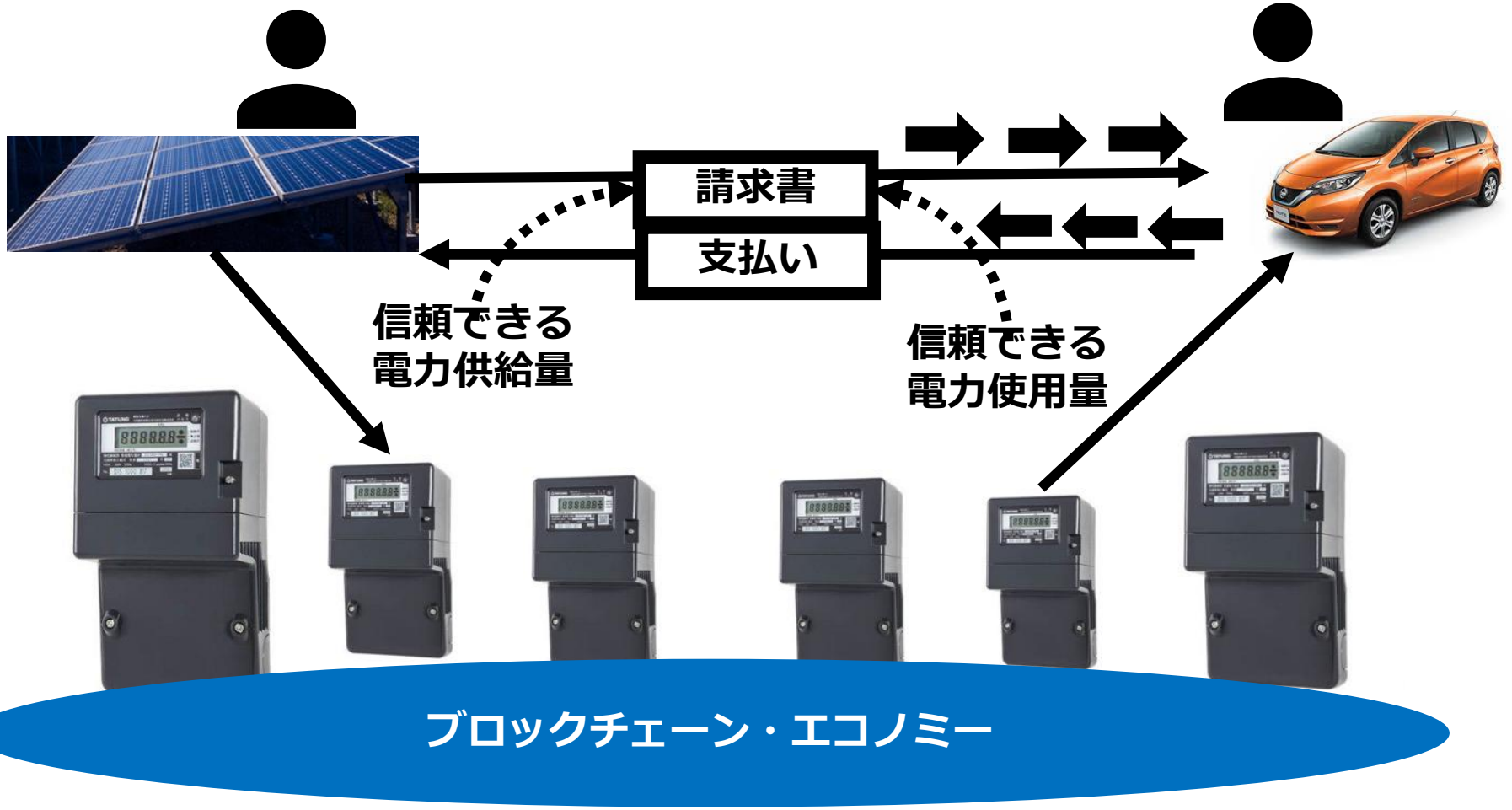
# 「物理」と「ビット」が結合している分野

## 電力消費量（物理量）と電力料金（ビット）

- みんなが電力メータを信じているから
- 日本には夥しい数の電力メータが存在している

# 電気メータというユビキタスな信頼点の存在

- ブロックチェーン経済圏が構成可能
- 電力供給者と電力消費者のプラットフォーム



# 電力会社は電力メータの企業として再定義？

## データの信頼点を維持管理する主体は支配者側

- ブロックチェーン経済圏の基盤を支える企業

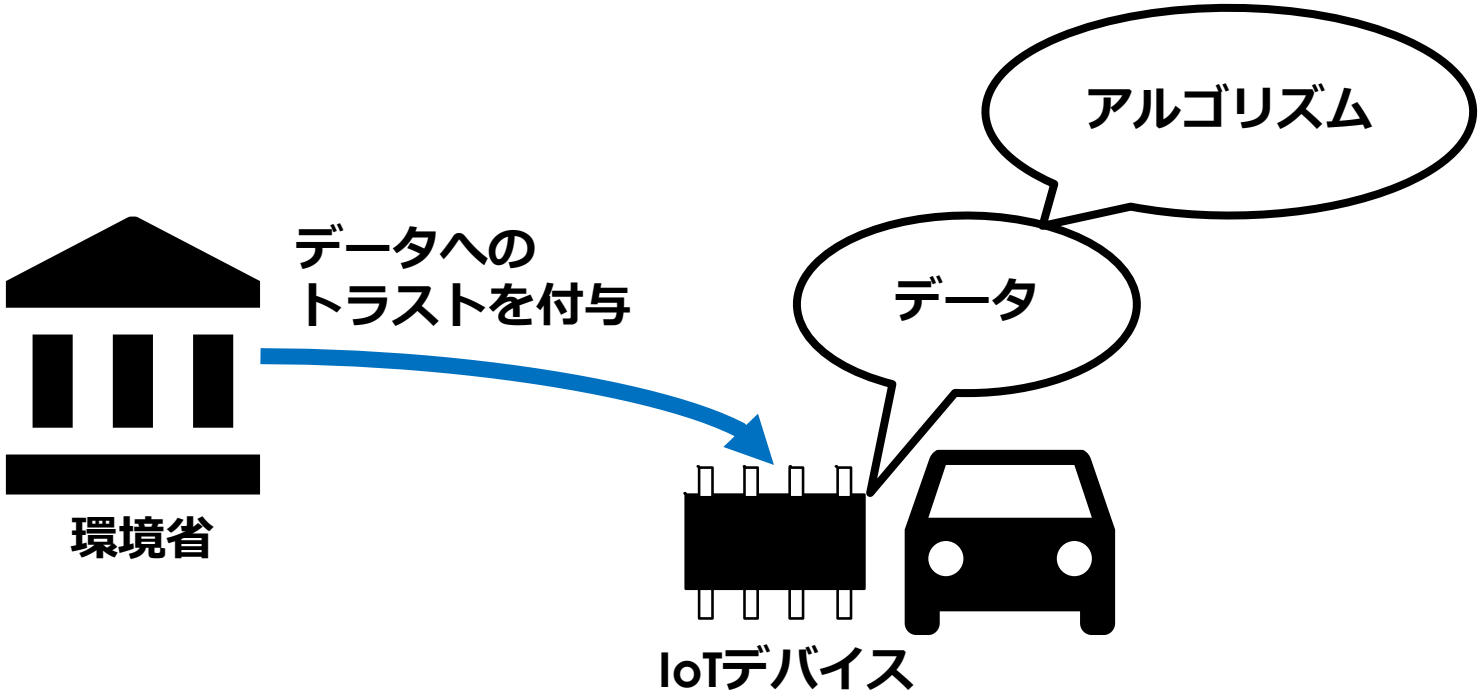
信頼できるデータを支配

# データの分散的なトラスト基盤

## データとアルゴリズムの支配戦略

### もしすべての日本車にCO2排出量装置が装備されたら？

- 環境省指定のIoT装置を組み込み、適切に匿名加工してデータ収集
- 全世界に輸出された日本車から信頼できるデータがとれる



# 5G とP2P

## 通信速度の改善と体感速度

3G ＜ 4G LTE ＜ 5G

15倍 10倍

- 本当に体感している？

## クラウド型サービスの限界

- エッジ型サービス、P2P型サービスへの潮流
- 高機能、大容量のスマートフォンの時代

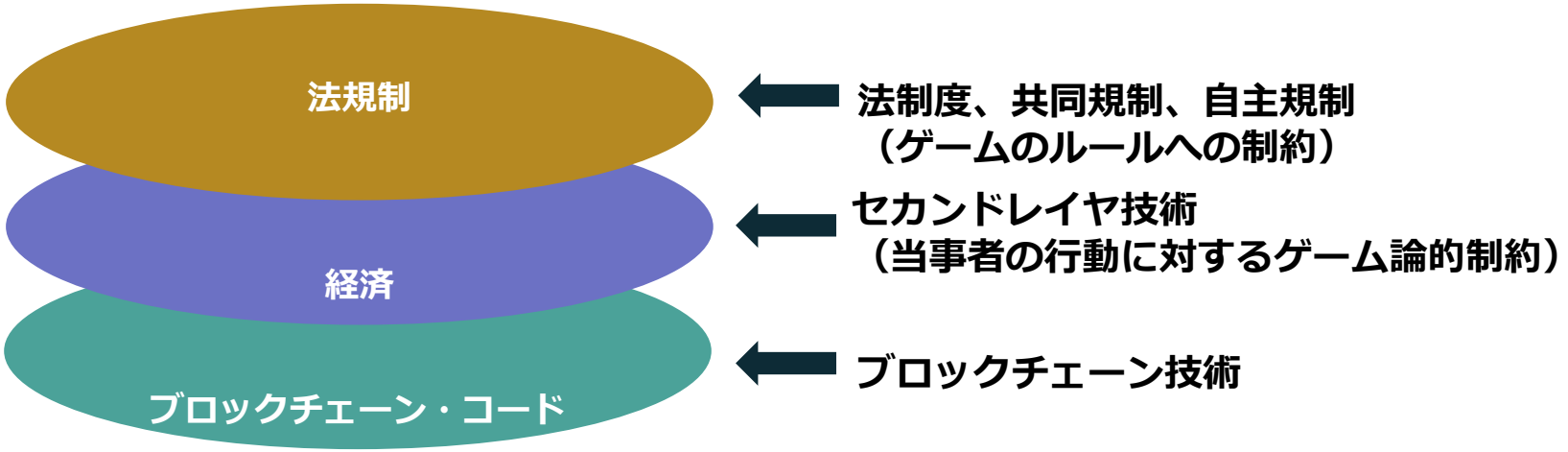
  500GBのストレージがあればbitcoin のフルノードになれる

# コード、ゲーム、法規制の三層モデル

# ブロックチェーンエコノミーの三層モデル

ブロックチェーン・コード、経済、法規制の三層で構成

ブロックチェーン技術だけで問題を解決しようとしない

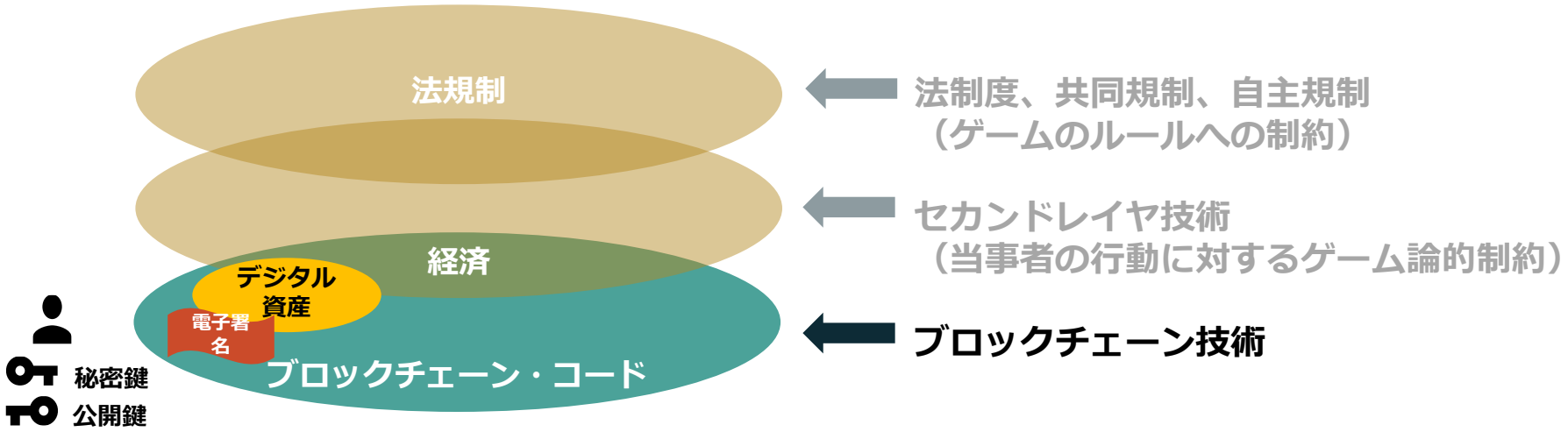


# ブロックチェーン・コードのレイヤ

## 公開鍵暗号基盤による当事者

- 公開鍵による識別と秘密鍵による署名能力）

## リカルディアンコントラクトによる資産の転々譲渡



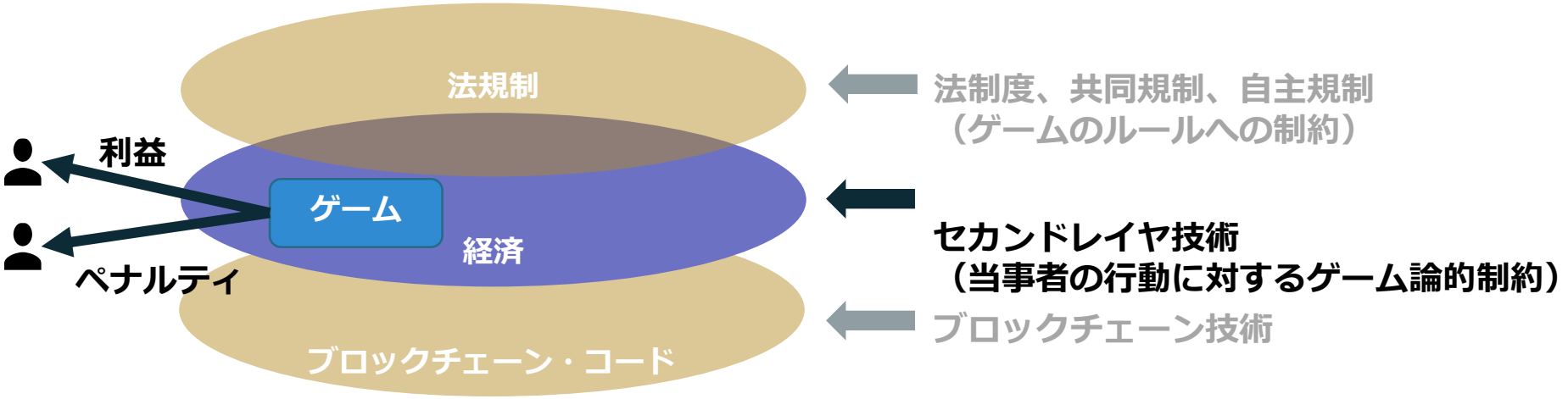
# 経済のレイヤ

## ブロックチェーン・エコノミーのプラットフォーム

- ゲーム論的制約（不正を行うと確実にペナルティが課せられる仕組みなど）

## ブロックチェーンのセカンドレイヤ技術で実現

- ライトニングネットワーク、データベース技術、プライベートチェーンなど



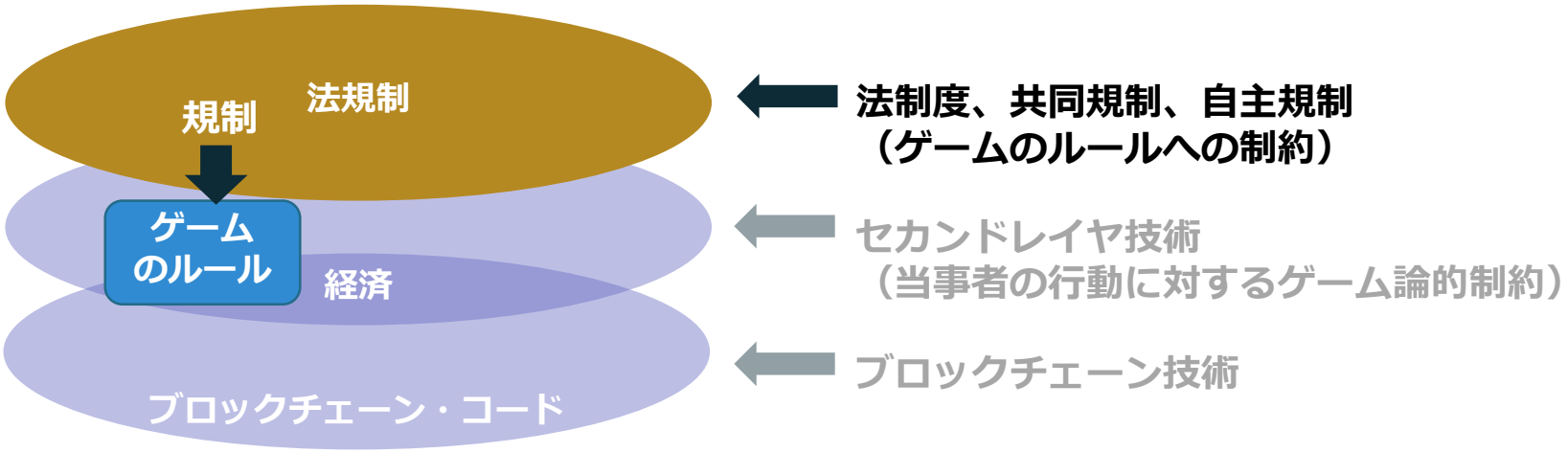
# 法規制のレイヤ

## 経済レイヤのゲームのルールを正義に基づくものに規制する

- 経済圏の発展と成熟に依存する

## 規制は無い方が自由なのか？

- 自主規制　→　共同規制　→　法的規制

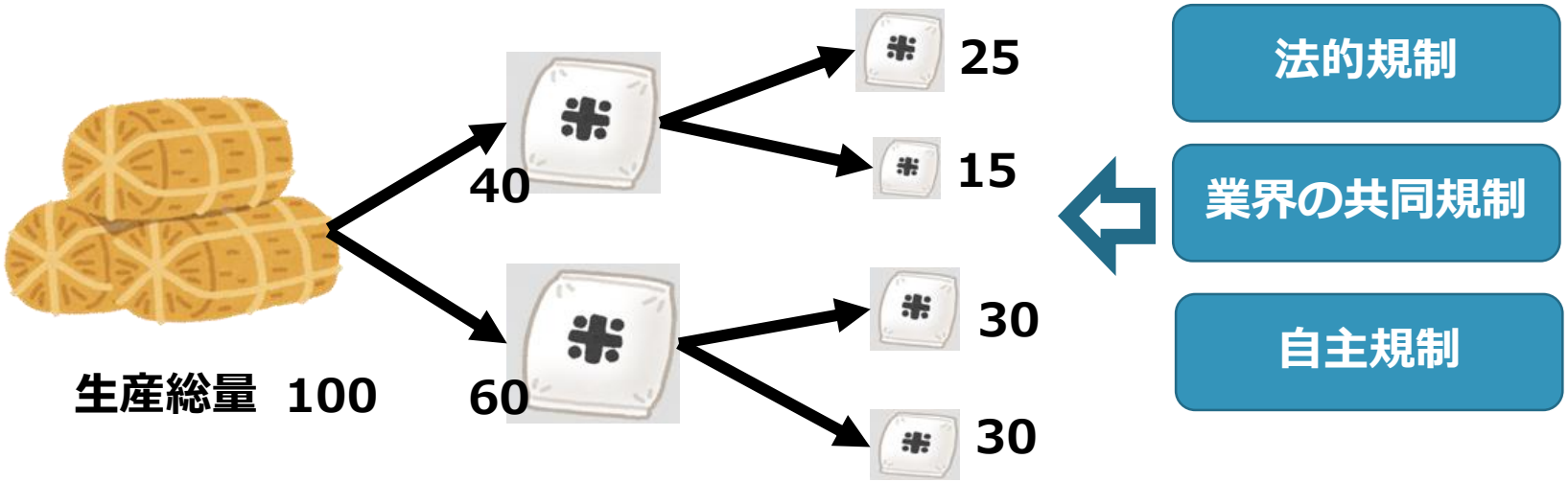


# 共同規制

## 業界による自主規制の問題

- 業界にとって都合のよい規制
- 参入障壁としての規制

## 中立性、実効性、透明性（業界に任せない中立的規制）



# 法規制と国際的な戦略

## 所有権の対象は有体物だけ (民法85条)

- データなどの無体物は対象外
- 著作権、債権、個人情報保護法などで対処
- 電磁的記録の媒体や装置は有体物として扱える（データベースなど）

## ブロックチェーン上のデジタル資産は？

- 分散的に管理される抽象的なデータ

## 日本では改正資金決済法で「仮想通貨」という法律用語が定義された

# 法整備の国際的な協調

## 2015年6月エルマウ・サミットの首脳宣言

## 2016年5月の伊勢志摩サミット

- 「情報通信技術の進展等の環境変化に対応するた めの銀行法等の一部を改正する法律案」が成立し、2017年4月から施行
- ノウ・ユア・カスタマールール(KYC)

# レイヤ２技術による
# ブロックチェーン技術の進展

# レイヤ２技術

## ブロックチェーン技術の課題の解決

- スループットの改善
- スケーラビリティの実現

  ライトニング・ネットワーク

  サイドチェーンなど

## 当事者の行動へのゲーム論的制約

- ブロックチェーン・エコノミーの（経済）秩序の形成

法制度、社会正義、秩序との整合性

# レイヤ２技術

## ブロックチェーン技術の課題の解決

- スループットの改善
- スケーラビリティの実現

  ライトニング・ネットワーク

  サイドチェーンなど

## 当事者の行動へのゲーム論的制約

- ブロックチェーン・エコノミーの（経済）秩序の形成

法制度、社会正義、秩序との整合性

# 「仮想通貨」から「通貨」へ
# その戦略的布石の段階

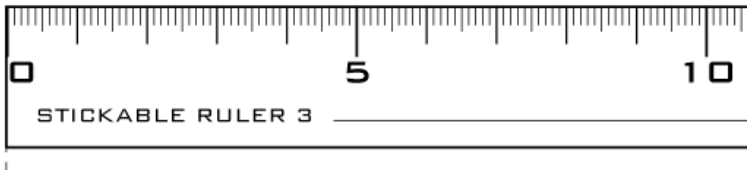
# 「仮想通貨」に欠けている機能

## 仮想通貨には市場価値の安定化装置が存在しない

- 全く制御できないシステムが「神の見えざる手」などによって自律調和的に安定するというのは幻想
- 事実、市場価値は暴騰と暴落を繰り返している

## 「通貨」には価値の尺度機能が必須

- モノの価格の単位になりえるのか（例 BTC)




# ブロックチェーン「通貨」の洗練

## 2018年6月アント・フィナンシャル社の送金実験

- ブロックチェーンによる国際送金（香港からフィリピン）
- フィリピンのGキャッシュ社に（SWIFT非経由で）送金
- ８億7000万人にのぼるアリペイのアクティブユーザー
- 中国の中小企業1500万社にこのサービスを提供



# facebookのバスケット型「通貨」

## FB coin

- ブロックチェーンによる複数の国民通貨のバスケット通貨
- ソーシャルな価値（「いいね」など）の通貨価値化
- ソーシャルな基盤を使った流通性

# SDR（特別引出権）の仮想通貨化？

## SDR（特別引出権）

- ドル、ユーロ、円などの引き出し権
- 金利もある
- 価格：世界貿易において1%以上のシェアを持つ16通貨を元にSDR価格を評価
- 通貨単位(ISO4217) は XDR

# 「暗号資産」

## 2018年3月ブエノスアイレスG20の声明

- 国際的な基準や規制の策定を表明
- しかし同年7月と11月のG20では審議先送り
- 2018年12月、金融庁は「仮想通貨」を「暗号資産」に呼称を変更する案を発表

## 審議先送りの背景

- 米中の対立
- 対立軸の中には基軸通貨を巡る問題も含まれる

# EBA（欧州銀行監督機構）の定義

## 2019年1月9日に公開された

- Report with advice for the European Commission on crypto-assets
- 「暗号資産」の定義や仮想通貨がEUに影響を及ぼす可能性とリスクを評価
- EBAの報告書では、「暗号資産」と「仮想通貨」は異なる概念として定義されている
- 「暗号資産」という用語は「仮想通貨」などを含む広い概念としても使われているようである

# 幻滅期のブロックチェーンの今後

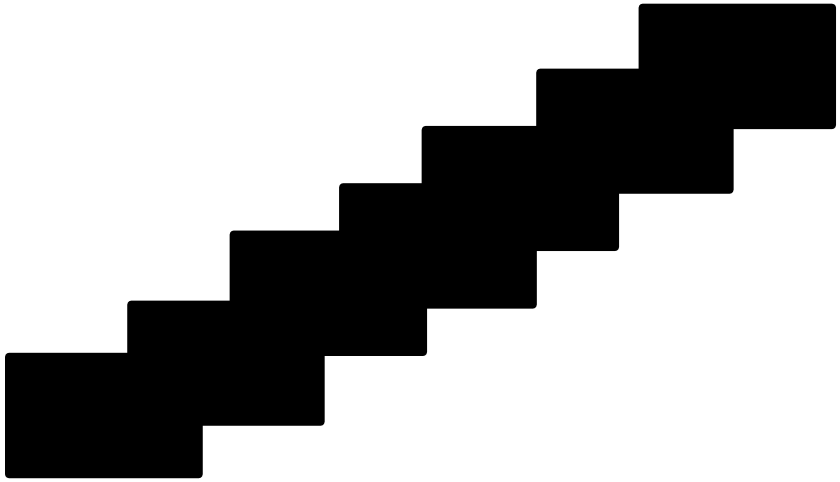
# 事故や攻撃と技術の成熟

事故や攻撃の経験は、技術の成熟にとって不可欠

暗号技術やセキュリティ技術に「完璧なシステム」は無い

幾多の事故や攻撃を耐えて生き残ったものだけが実用に耐える

技術的成熟への道を一歩ずつ登るしかない



# オッカム主義の台頭

## マッキンゼーの報告書

### 「Blockchain's Occam problem」(2019年1月)

- 数十億ドルの投資、ブロックチェーンの実用的用途はまだ無い
- 投資家の視点からは、ブロックチェーンの技術的進歩は緩慢で幼稚な段階から抜け出せない
- ブロックチェーンのPoCとして離陸したプロジェクトがDBベースで着地する

# ブロックチェーンの適切な用途

## NIST (アメリカ国立標準技術研究所) による指針

- NISTIR 8202 Blockchain Technology Overview

## 6要件（以下の条件が全部 true でなければDBなどを使え）

- 一貫性の維持が必須なデータ共有が必要か？
- 複数の主体がデータの提供者になりえるか？
- 書き込まれた記録への修正や削除が不可能でよいか？
- 機微な個人情報が記録されることがないか？
- データ提供主体に書き込み権限を与えるために信用などの管理は不要か？
- 改ざん不可能な追跡可能な記録がどうしても必要か？

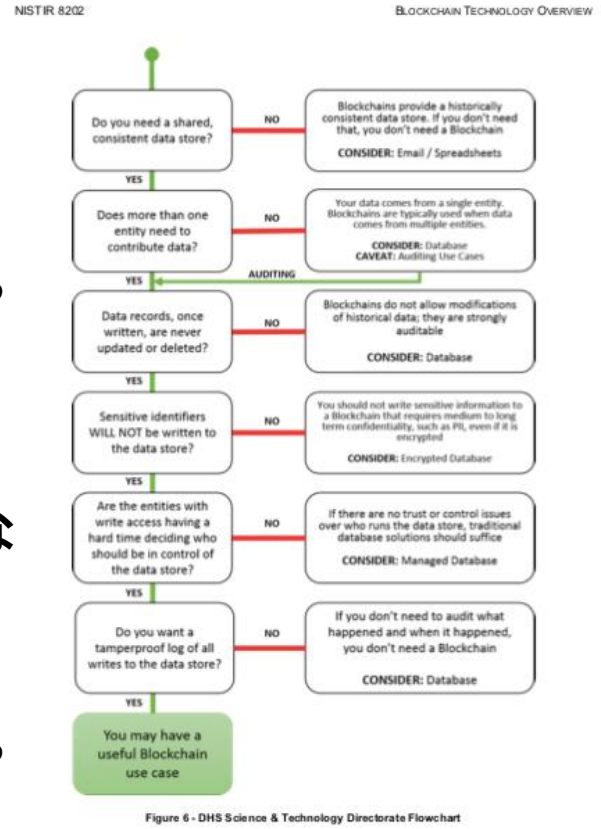


Figure 6 - DHS Science & Technology Directorate Flowchart

# PoC（概念検証）段階の投資は終焉

## ブロックチェーンによるゲームチェンジを
## 具体的に考えるステージに移行

# 日本ではまだPoCレベルの投資が継続中

**PoCへの投資はもうやめよう**

**ブロックチェーンの適切な用途への深い理解が必要**

**幻想ではなく、技術に対する着実な投資の継続が必要**

# まとめ

## データ至上主義の視点

- データとアルゴリズムの支配をめぐる闘争への戦略的アプローチ

## 「あちら側」から「自分たちの側」へのゲームチェンジ

- （ユビキタスな）トラストの基盤の構築主体が鍵になる

## セカンドレイヤ技術は多方面に発展

- スケーラビリティ、スループットだけでない

## 「暗号資産」？

- 「仮想通貨」から「通貨」へ至る緻密な戦略

## ブロックチェーンのPoCは終焉

- PoCへの投資はやめ、適切な用途に対する着実な投資の継続を