オラクルのトラストモデルとブロックチェーン連携

近畿大学
山崎重一郎

- 2021/10/08 BASEアライアンス

自己紹介

●最近の主な著書

ブロックチェーン技術概論
理論と実践
1章～６章，付録を担当
（講談社）
山崎重一郎
安土 茂亨
金子 雄介
長田 繁幸
2021年

ブロックチェーンの技術と革新~
ブロックチェーンが変える信頼の世界
（ニュートンプレス）
ケビン・ワーバック（著），
山崎 重一郎（監修），
山﨑 裕貴（翻訳）
2021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

newton
仮想通貨とブロックチェーン
山崎重一郎
2018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
2016-2022
（日経BP）
ブロックチェーン技術

何が（現在の）ブロックチェーンではないか？

- **分散データベース**
  - ブロックチェーンはデータ管理の冗長性が高い（ロバストネスは高いが）
  - 大量データの管理手段としては従来のDB技術の方が合理的
- **業界横断EDI／サプライチェーンのための基盤**
  - スケーラビリティに限界（日本の金融機関だけでも955社)
  - ステークホルダー関係の複雑性に限界（スマートコントラクトの性能と安全性）
- **トレーサビリティの保証手段**
  - ブロックチェーンのトラストはオラクル（外部情報）の偽造や改ざんには無力

ブロックチェーンの再定義への動機

期待の実像が見えてきたのなら，それを実現する技術にまで育てればいい

- **大規模な信頼性のある共有ストレージは必要**

  GAFAのようなTSP型ではない，信頼可能な共有ストレージのインフラ

- **スケーラブルで複雑化が可能な業界EDI／サプライチェーンの基盤は必要**

  アマゾンレベルのe-コマース
  自動車産業のサプライチェーンが実装できるスケーラビリティ

- **信頼できるトレーサビリティ保証システムは必要**

  オラクル（ブロックチェーン外の情報）へのトラスト

トラストのアーキテクチャの視点で

ブロックチェーンの定義にアプローチしてみます

- コンセンサス
- 分権的（decentralized)
- オラクル

ブロックチェーンとトラスト

「ビットコインには管理者がいない」

では，どうして，

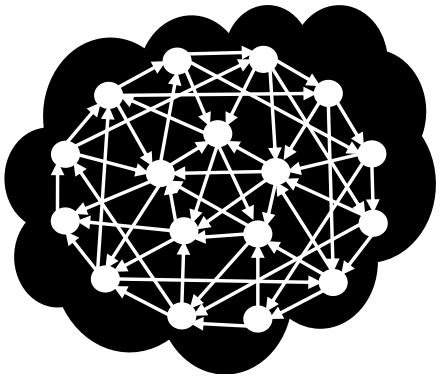
ビットコインは仮想通貨／暗号資産として機能しているのか？

トラストレス（なトラスト）

- **LinkedInの創設者のリード・ホフマンがビットコインのトラストを表現するために作った造語**
  - 管理者がいないだけでない
  - 誰も他のどの参加者（ノード）も信じてはいない
  - 送金の当事者も互いに相手を信じていない
  - しかし「トラストが無い」のではなく確実に存在している

    それも金融機関なみに信頼できる

リード・ホフマン

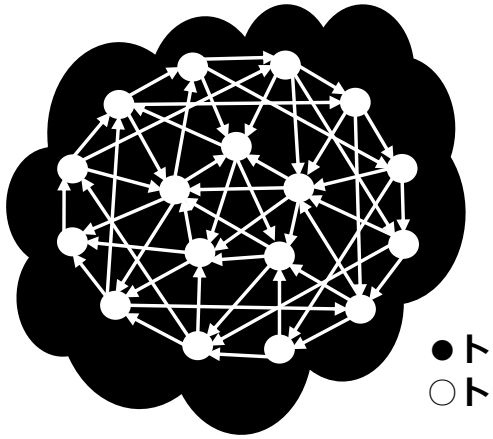


●トラストされている主体／基盤

○トラストされていない主体

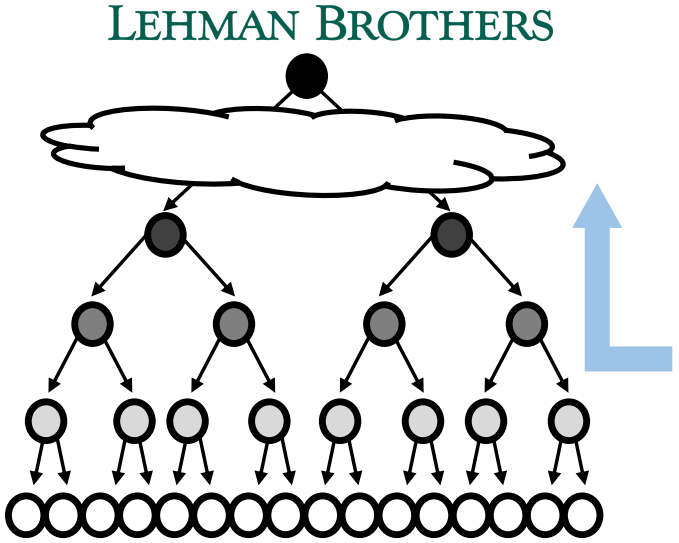
サトシ・ナカモト論文とリーマンショック

- **サトシ・ナカモト論文の投稿　2008年10月31日**
- **リーマン・ブラザーズの破綻　2008年9月15日**
  - 世界金融トラストの単一障害点の破壊　→　全世界の金融システムの連鎖的崩壊



会計監査によるトラスト

●トラストされている主体／基盤
○トラストされていない主体



破綻直前まで
４大監査法人の
格付けはAAAだった

Deloitte. デロイト トーマツ
EY Building a better working world
pwc
KPMG

トラストとは？

人が，リスク（ヴァルネラビリティ）への恐怖と向き合い前向きな行動を行うために必要な信念

- 新しいワクチンを接種する
- 金融商品を購入する
- ハンドルもブレーキも付いていない自動運転車に乗る

共同幻想としてのトラスト

●通貨の価値は共同幻想

- 逆ー裸の王様
- 「一万円札は紙じゃない」

●ブロックチェーンにはトラストが創発される土壌の機能

- トラストが芽生え，育つ苗床

●ブロックチェーンは本質的にソシオテクニカルなシステム

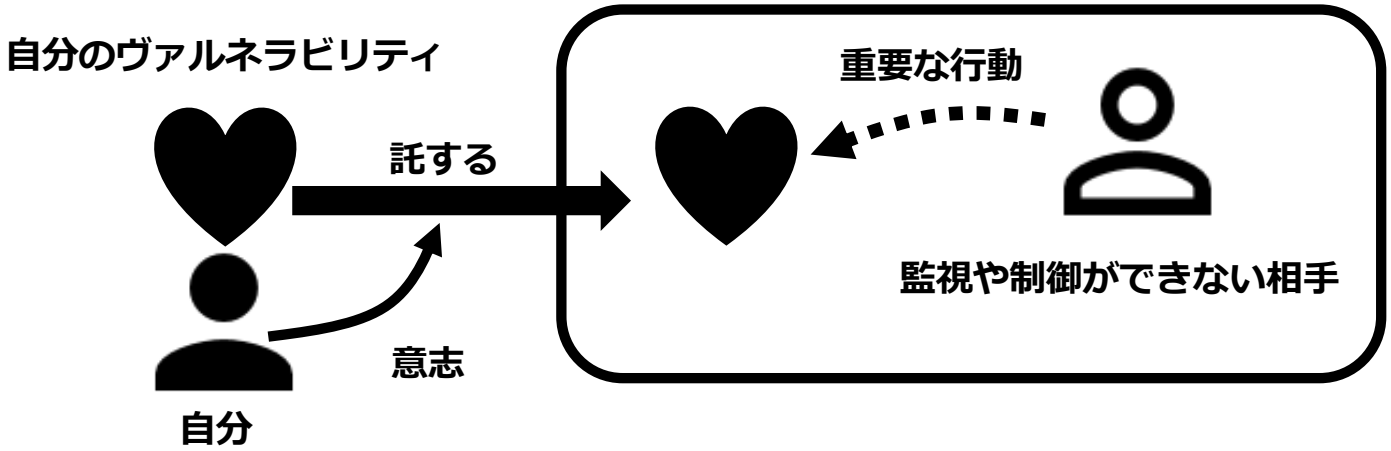
- 人間の存在（共同幻想）が不可欠なシステム

トラストの定義

ロジャー・メイヤー

●組織行動学者 ロジャー・メイヤーの定義

- 自分の「ヴァルネラビリティ」を託する意志
- 対象：監視や制御が可能でない相手
- 期待：自分のヴァルネラビリティに対する重要な行動



トラストのアーキテクチャの分類（ケビン・ワーバック）

人類の文明はこれまで様々なトラストのアーキテクチャを発明してきた

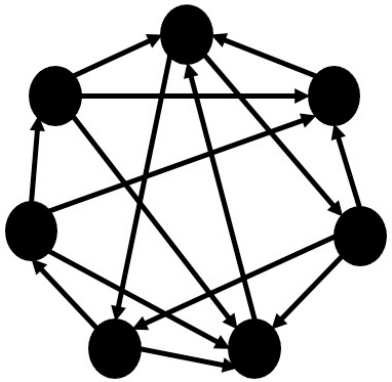
- P2P型（person to person)トラスト
- リバイアサン型トラスト
- 仲介者型トラスト（TSP)
- トラストレス型トラスト（ブロックチェーン）

Kevin Werbach

（ニュートンプレス）
ケビン・ワーバック（著），
山崎 重一郎（監修），
山﨑 裕貴（翻訳）
2021年

P2P型(person to person)トラスト

- **血縁や部族の絆によるトラスト**
  - 属人的な信頼
  - 集団の掟による制裁
  - 集団主義的倫理観
- **例**
  - 日本の村社会（会社社会）
  - マグリブ商人の掟
  - オープンソース開発コミュニティ
- **コミュニティの掟や他人からの信頼に束縛される**

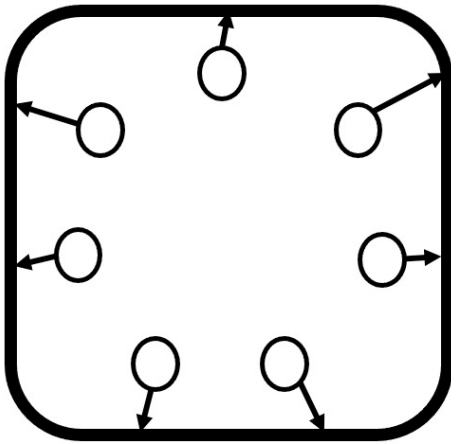


●Trusted Subjects
○Untrusted Subjects

マグリブ商人

リヴァイアサン型トラスト

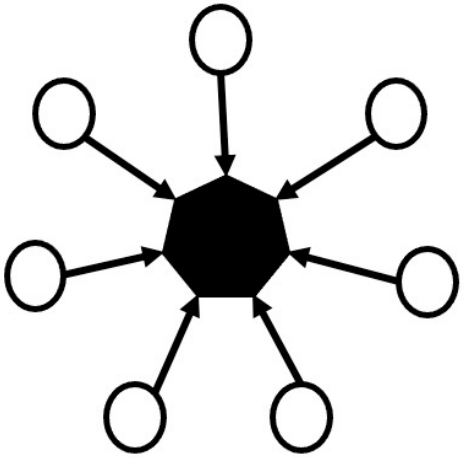
- **トマス・ホッブスの著書**
  - 国民国家の概念
- **ヴァルネラビリティ**
  - 暴力によって自分の財産や生命が奪われる危険性
  - 自然状態は「万人の万人に対する闘争」
- **国家が暴力を独占（警察，軍隊）**
  - 国家の暴力を背景とした権力と強制力
  - 官僚機構と法制度による社会の安定
- **個人は自由を放棄することになる**



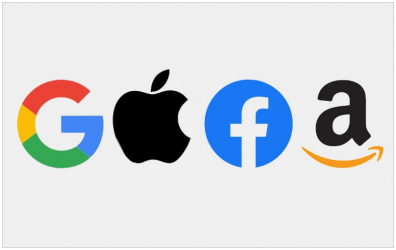
● Trusted Foundation
○Untrusted Subjects

仲介者型トラスト（TSP型）

- **トラスト・サービス・プロバイダ（TSP）**
  - 金融機関
  - GAFAなどのプラットフォーマ
- **TSPに託する個人のヴァルネラビリティ**
  - 金融資産
  - 個人データ（SNSのログ，購買履歴，…）
- **TSPはユーザへの責任と権限を持つ**
  - アカウント停止などが可能



●Trusted Subjects
○Untrusted Subjects



トラストレスなトラスト

●人類史に登場した新しいトラストのアーキテクチャ

- 他の参加者（ノード）の誰も信じていない（P2P型でない）
- 国家による強制力や法規制が不要（リヴァイアサン型でない）
- 信頼できる第三者が存在しない（仲介者型でない）

●トラストレスなトラストの特徴

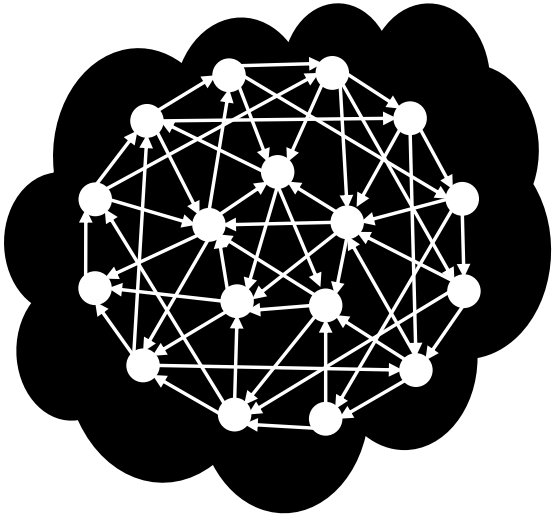
- 自由が制限されない

  コミュニティの掟，倫理観からの自由

  国家による法規制からの自由

  TSPによる規制（コード）からの自由

- しかも金融機関レベルのトラストの恩恵（リスクに対する安全性，信頼性）は得られる



●Trusted Foundation

○Untrusted Subjects

ヴラド問題

Vlad Zamfir

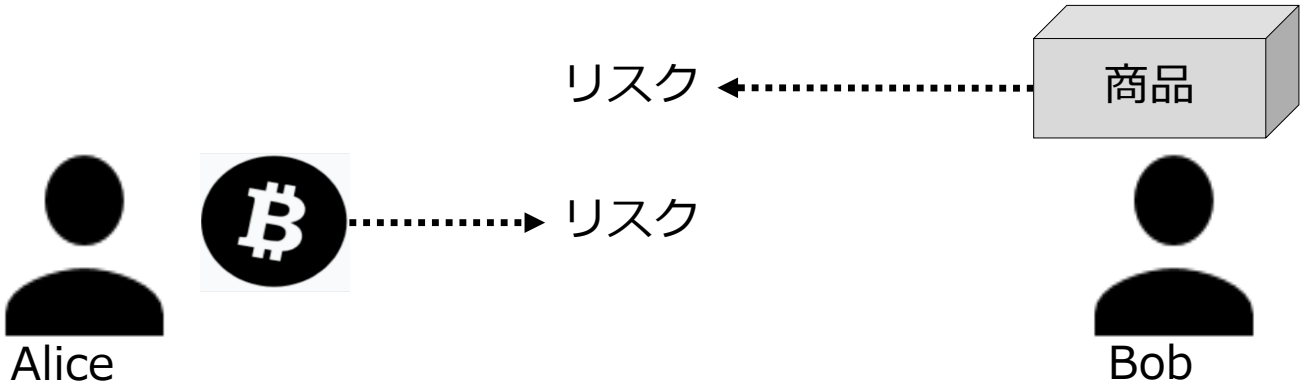
- **法規制とトラストレスによる自由の対立**
- **ヴラド・ザンフィル**
  - イーサリアムのコア開発者
  - 2017年のTwitter投稿

    「多くの政府に採用されている政策目標とブロックチェーンの真の成功の間には直接的な対立があるように思われる」

  - 経済制裁，AML，テロ資金規制，脱税回避，資本規制，著作権保護，情報公開規制など
  - ほとんどの政府にとって，どの政策も曖昧にはできない種類のもの

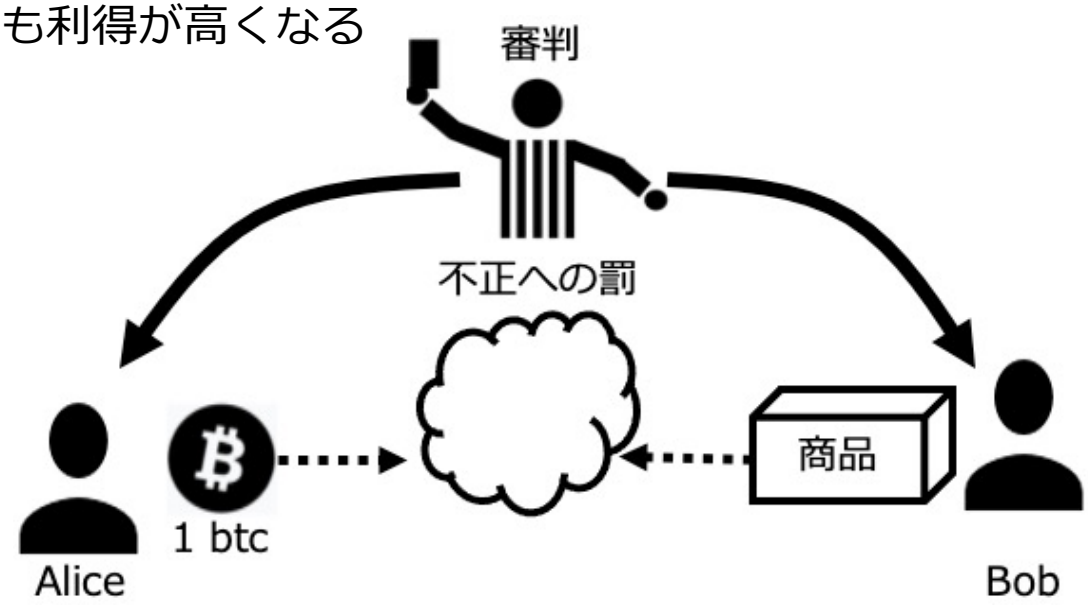
トラストが無い社会ではビジネスはできない

- **ゲーム理論的に見た「万人の万人に対する闘争」の状態**
  - 商品を発送したのに代金が得られないリスク
  - 代金を送金したのに商品が発送されないリスク
- **ナッシュ均衡（非協力ゲームの解）は**
  - 「送金しない」「商品を発送しない」



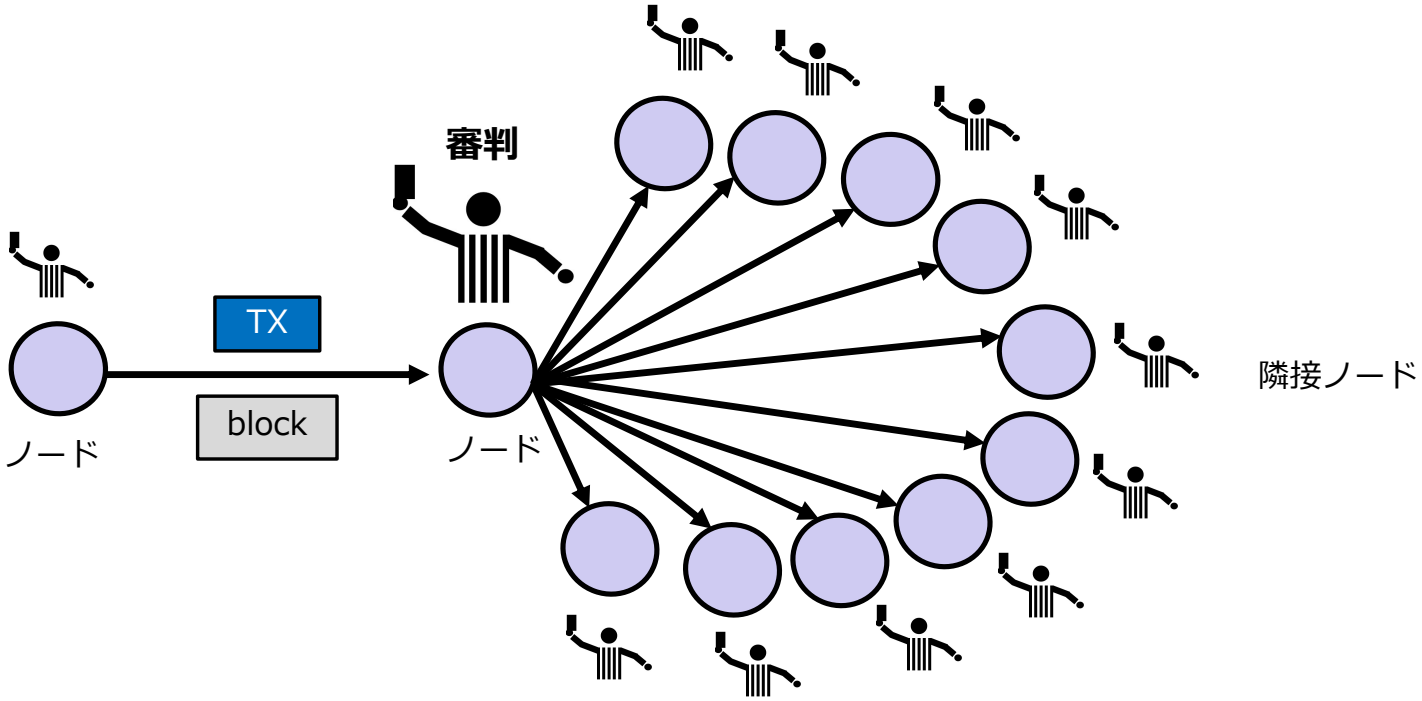
ブロックチェーンのトラストには審判が存在する！

- **ゲーム理論的な罰則の存在**
  - ルール違反者には，罰が与えられる＝利得が減少する
- **その結果，健全なビジネスが可能になる**
  - 「送金する」「商品を発送する」が最も利得が高くなる
  - ナッシュ均衡　＝　パレート最適
- **トラストレスなトラストの原理**



ビットコインでは全員（フルノード）が審判になる

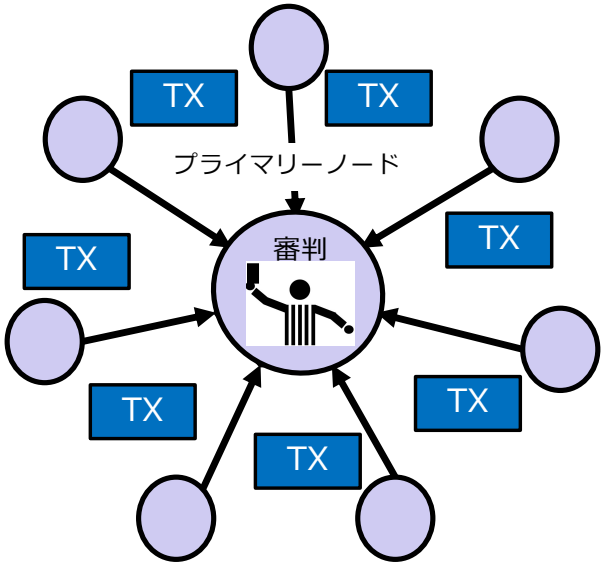
- 全員がトランザクションやブロックへの監査を行う
- 不正への罰　＝　不正なトランザクションを破棄し，ブロードキャストしない



必ずしも全員が審判である必要はない

Brian Behlendorf

- **ブライアン・ベーレンドルフ**
  - Hyperledger のエグゼクティブディレクター
- **メッセージの中継ノードが審判（神）として振る舞えばよい**
  - 中継の停止によって罰が与えられる



ブロックチェーンのトラスト＝審判への合意

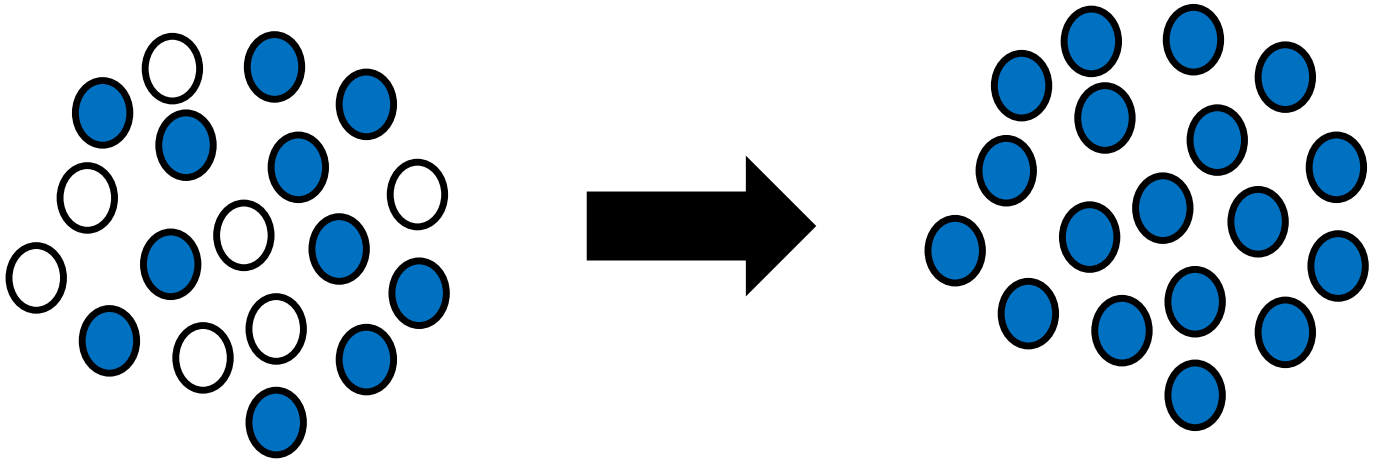
（神）を信じるための仕組み

コンセンサスの問題

コンセンサス

●全体の状態を一つに統一する仕組み

- 少数派は多数派の状態へ強制的に状態遷移させられる



●少数意見を尊重する「民主主義」とは対立する

ブロックチェーンの本質は「コンセンサス・マシーン」である

- **コンセンサス機構によって強制的に矛盾状態を解消するシステム**
- **例：二重送金のトランザクションが発生した場合**
  - （何らかのアルゴリズムで）一方のトランザクションのみを正統なものと判定する
  - ネットワーク全体に対して，判定への合意を強制する

二重送金状態が解消される

ただし，コンセンサスとは単なる「アルゴリズム」ではない

- **ブロックチェーンの「共同幻想」としてのトラストとコンセンサス形成方法の整合性**
  - 「トラストの創発」という重要な機能を殺してしまわないようにしなければならない
  - ブロックチェーンは本質的にソシオテクニカルなシステムである

- **コンセンサスはブロックチェーンの適用領域の「社会のエントロピー」とも関連する**
  - 社会のエントロピー（独裁制社会　＜　平和で繁栄した社会　＜　紛争や犯罪が頻発する社会）

    PoW, PoS, PoA, …

コンセンサスが機能する条件とトラスト

●ワクチン接種の義務化からのアナロジー

- 集団免疫の形成，変異株の出現抑制には，全国民（全人類）のワクチン接種が必要
- 民主主義国家では，少数意見も尊重しなければならない

分権化 (decentralization)

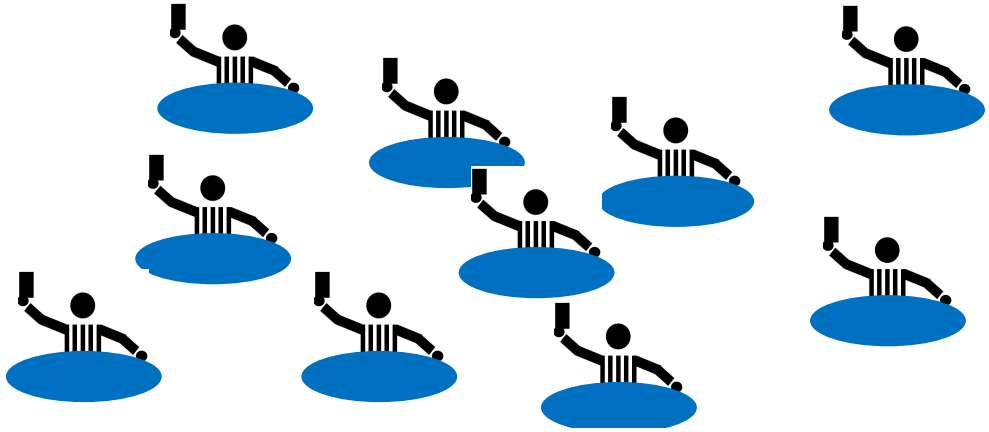
中央政府

●分権化＝自分に判断権限があること

- 判断のためにいちいち中央にお伺いをたてなくてよい
- 地方分権，三権分立と基本的に同じ意味

●審判としての判断権限の構造

- したがってやはりトラストの構造が本質
- トラストレス＝審判の構造が分権的であること



ヴィリのパラドクス

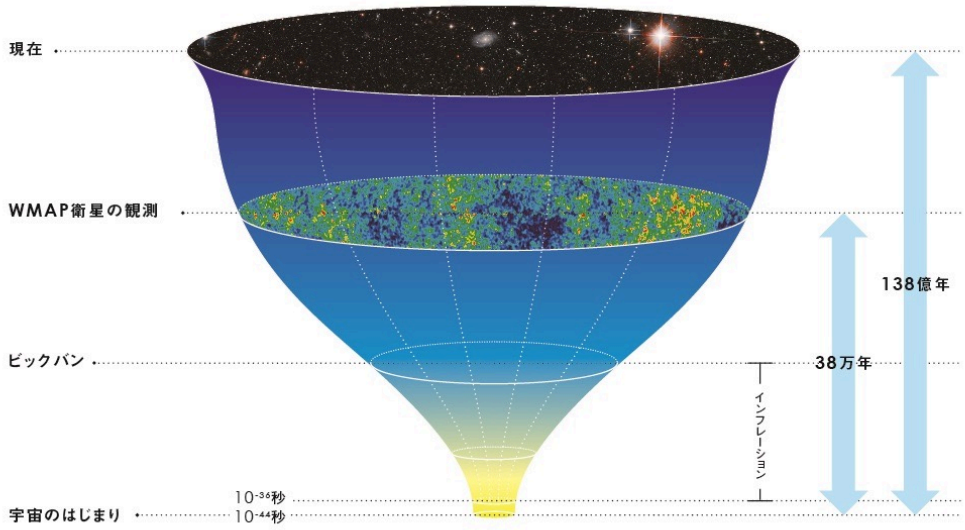
- **分権化とガバナンスの間には矛盾が存在する（ヴィリ・レードンヴィルタ）**
  - ブロックチェーンにガバナンスを導入した瞬間に分権的ではなくなる
  - しかし分権的システムの運用にはガバナンスが不可欠（パラドクス）
- **ヴィリの意味での「ガバナンス」**
  - ブロックチェーン・システムの仕様決定
  - （ハード／ソフト）フォークなど
- **イーサリアムのガバナンス**
  - ヴィタリック・ブテリンが統治者になっている（彼へのお伺いが必要）

Vili Lehdonvirta

オラクルとは

ビッグバン理論と観測可能な宇宙

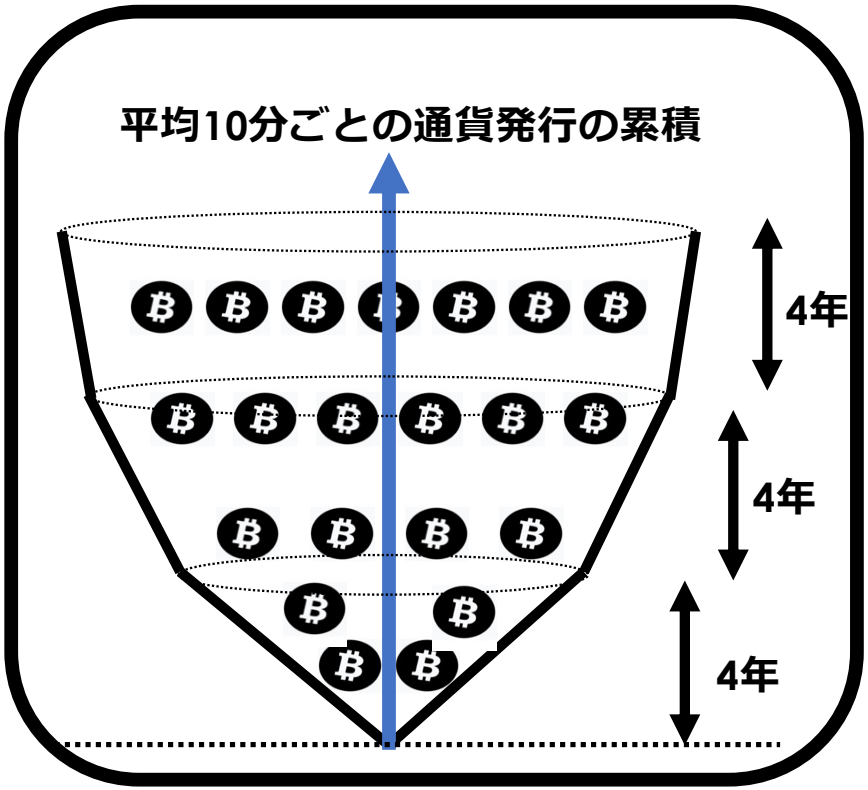
- 光速で膨張する宇宙
- 観測可能な宇宙は限られている
- 「外側」の情報を知ることはできない



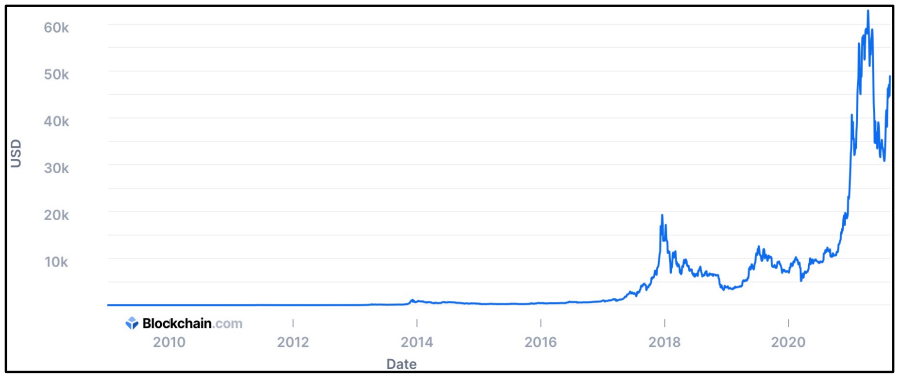
東京大学 https://www.u-tokyo.ac.jp/focus/ja/features/f_00066.htmlより引用

Bitcoin は外側の情報を観測できない閉鎖システム

- Bitcoin のブロックチェーンの世界



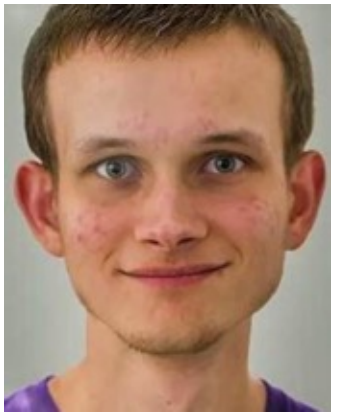
外部世界の情報
ビットコインの市場価格など



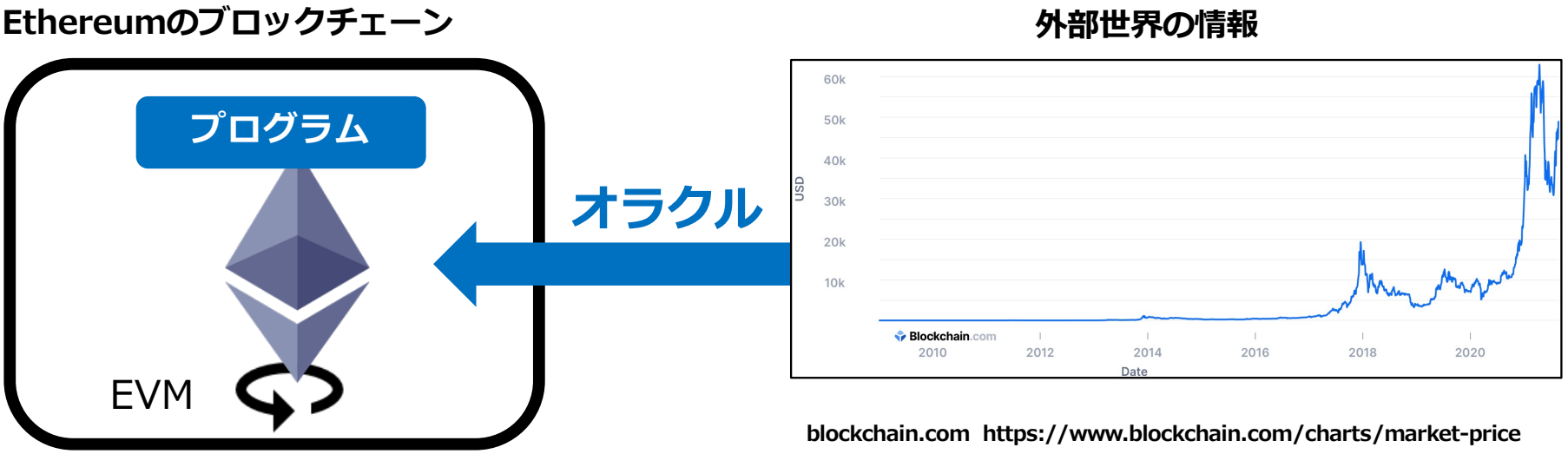
blockchain.com https://www.blockchain.com/charts/market-price

Ethereum の white paper (2013)

- **当時19歳のヴィタリック・ブテリンの提案**
  - ブロックチェーンの「外側の情報」を観測可能なブロックチェーン
- **オラクル（神のおつげ）：ブロックチェーンの外部世界の情報**



Vitalik Buterin



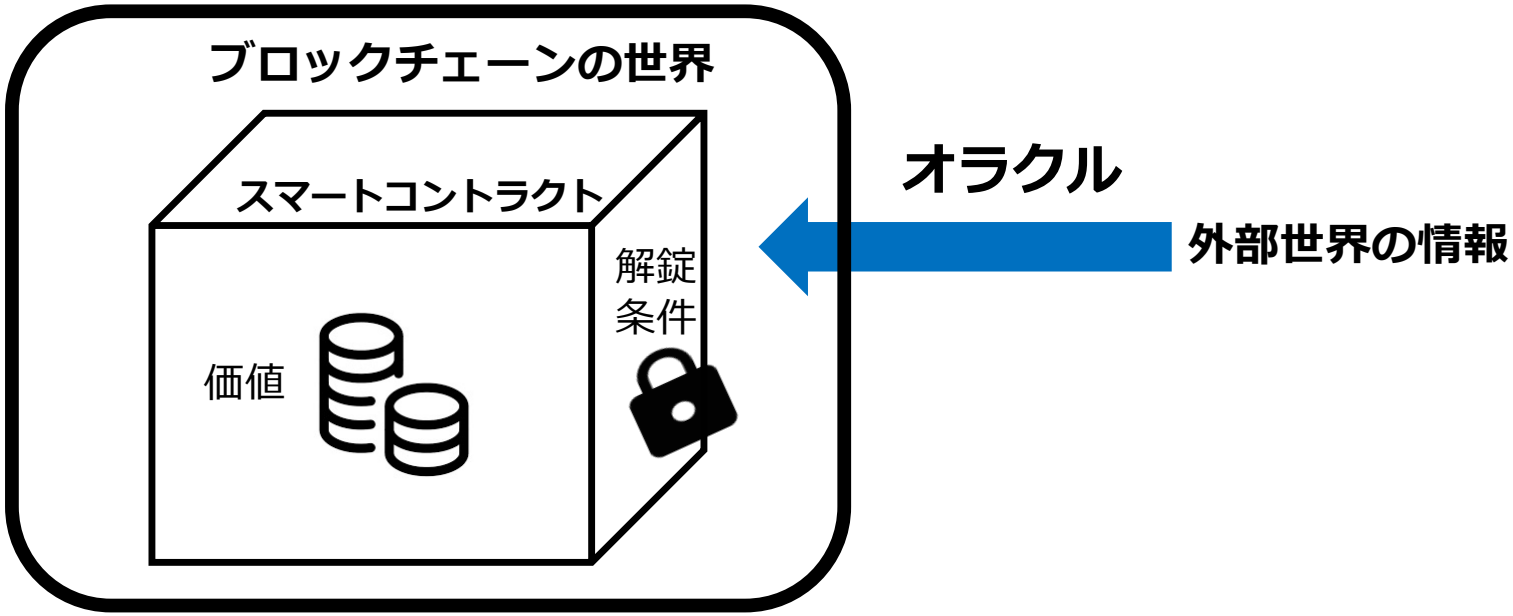
blockchain.com https://www.blockchain.com/charts/market-price

ヴィタリック・ブテリンのスマートコントラクト

- **「条件に適合したときのみに解錠される，価値を格納した暗号学的箱」**

  （2013年の white paper におけるヴィタリック・ブテリンによる定義)

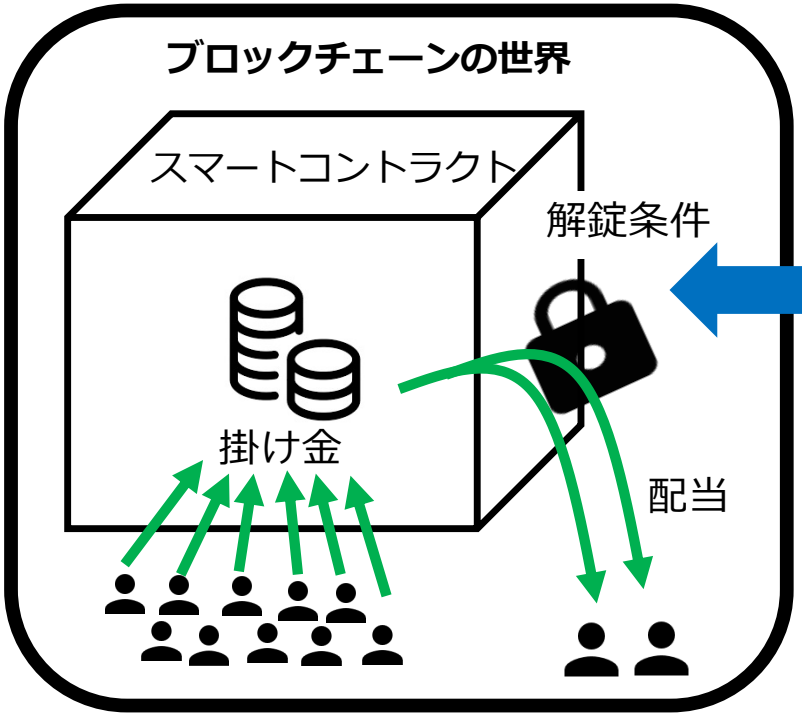
  - オラクルを入力として駆動されるアプリケーション



ヴィタリック・ブテリンのスマートコントラクトの例

- **サッカーの試合結果によるギャンブル**
  - スマートコントラクトに格納されている価値：集めた掛け金
  - オラクル：サッカーの試合結果

    解錠条件：勝利チームに賭けた人への配当



オラクル

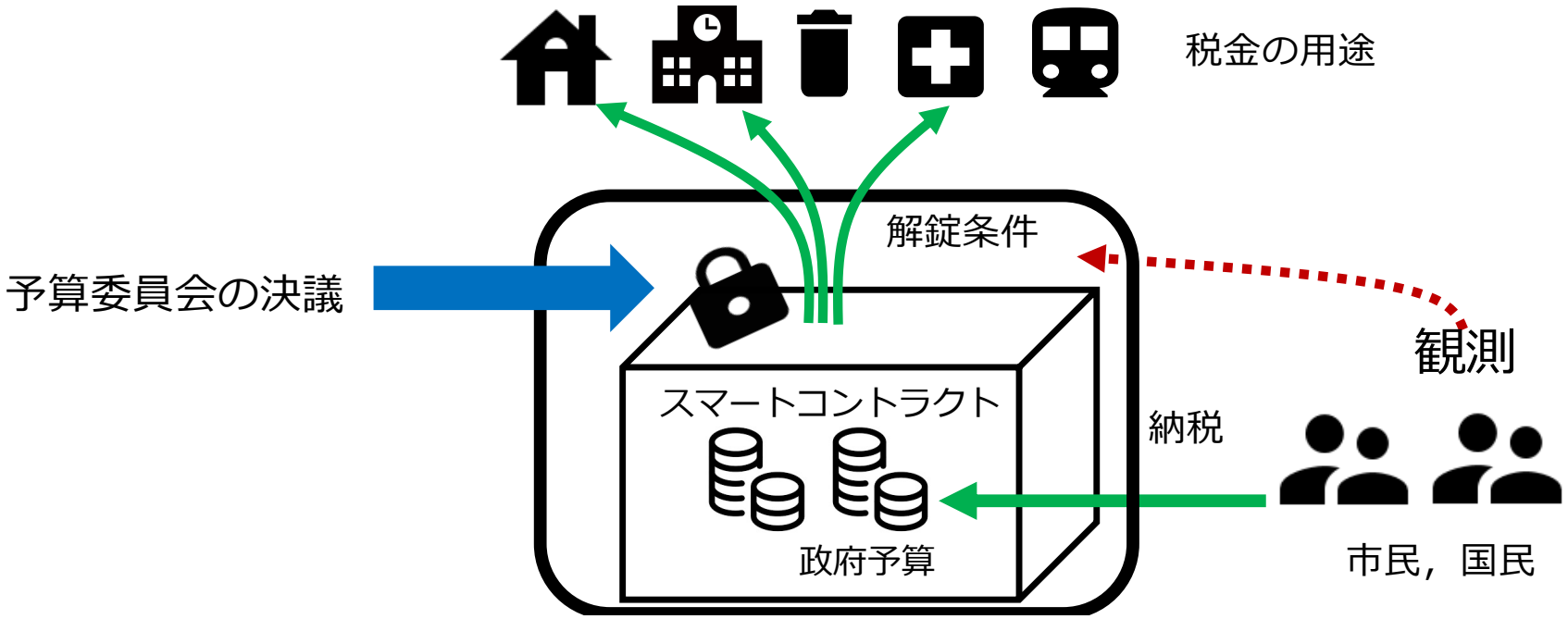
試合結果

現実世界のサッカーの試合

スマートコントラクトによる政府予算配分

- **ギャンブルの掛け金の配当と同じ**
  - スマートコントラクト：予算の執行条件
  - 検証可能性（市民も契約の当事者）

スマートコントラクトを備えたCBDC
(central bank digital currency)



オラクルへのトラスト

●ランダム・オラクル・モデル（HTLC)

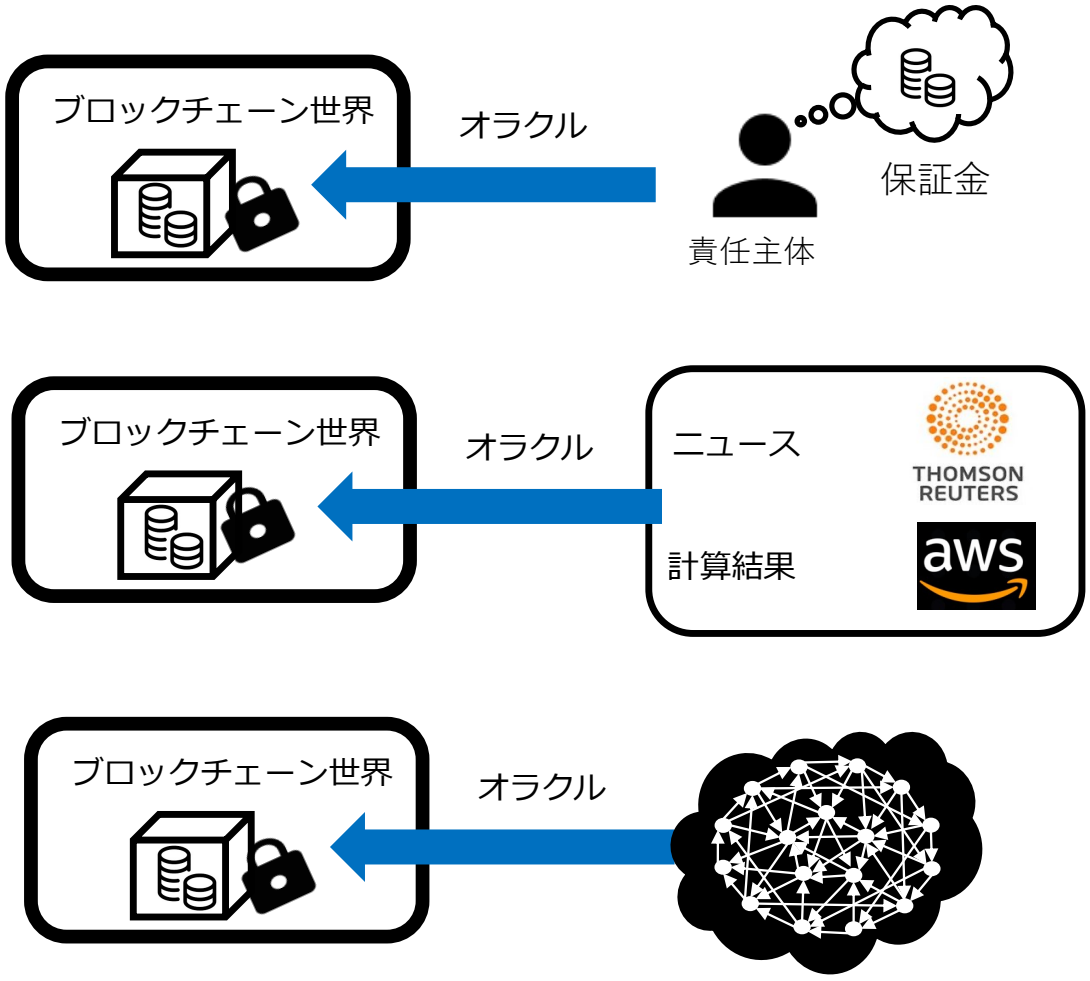
- 保証金をデポジットした責任主体の創出

●集中管理型オラクル

- TSP型オラクル
- 計算処理オラクル

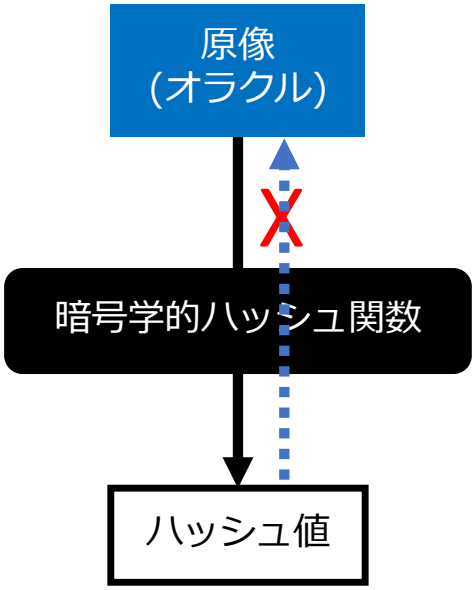
●分権型オラクル

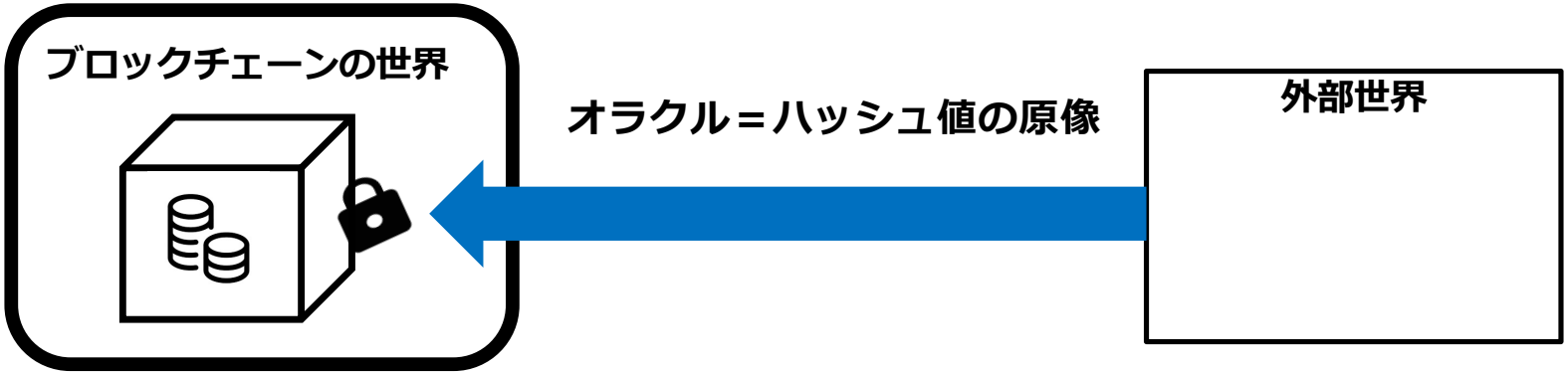
- オラクルへのトラストレスなトラスト基盤



ランダムオラクルモデル

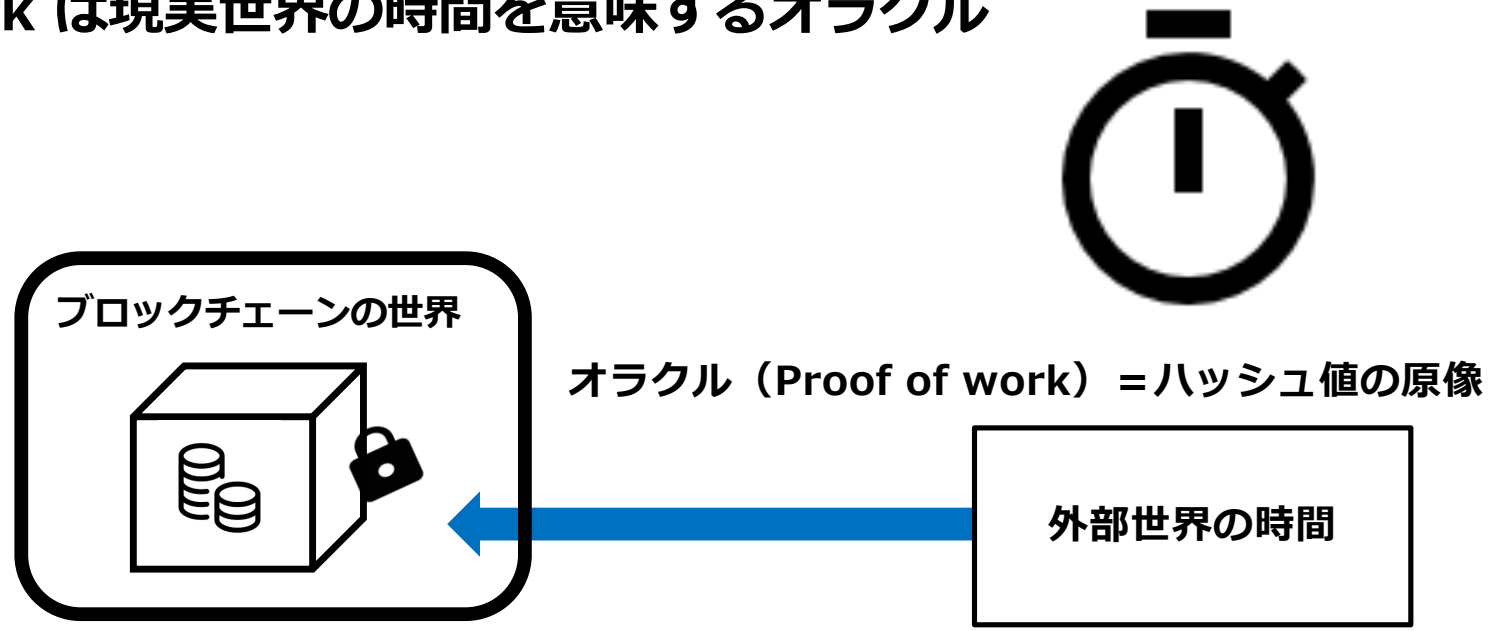
- **暗号学の安全性仮定の一つ**
  - 暗号学的ハッシュ関数を理想的なランダムオラクルとみなすという仮定
  - 理論的安全性との間にはギャップがあるが安全性の証明が単純化される
- **オラクル＝ハッシュ値の原像**
  - ハッシュ値の原像は直接計算できない（しらみつぶしに試すしかない）





ランダムオラクルモデル

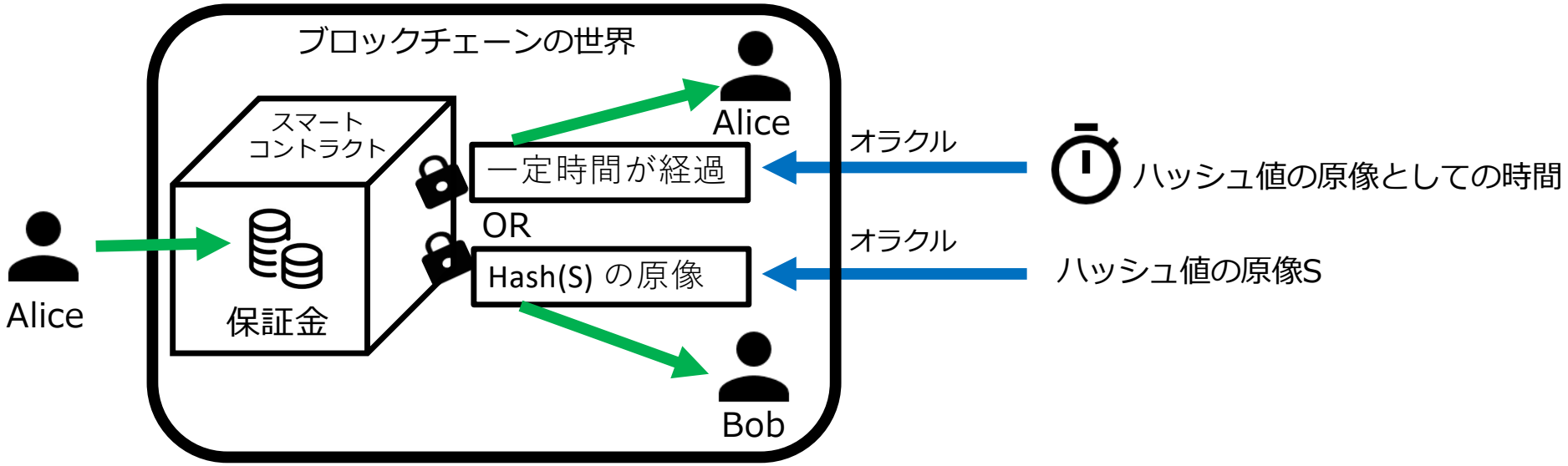
- **Proof of work (Hashcash法)**
  - ハッシュ値の原像 (を求める計算時間)　＝　「外部世界の時間」を意味するオラクル
  - Proof of workの計算は「マイニング」と呼ばれる
- **Proof of work は現実世界の時間を意味するオラクル**



HTLC (Hashed Time Lock Contract)

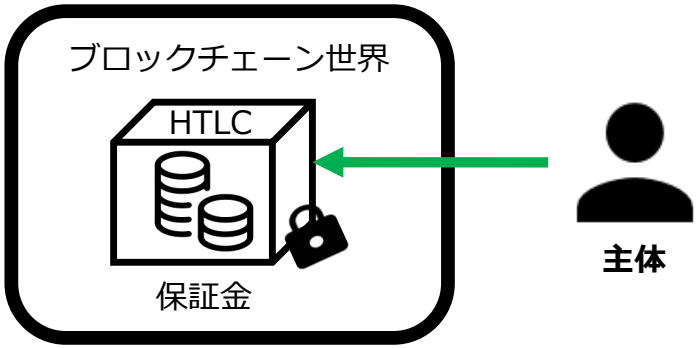
●HTLCでロック状態になっている保証金を解錠する条件

- カウンターパーティリスク（当事者の失踪など）の回避が動機だった
- 「ハッシュ値の原像を示す」　OR　「一定時間が経過する」

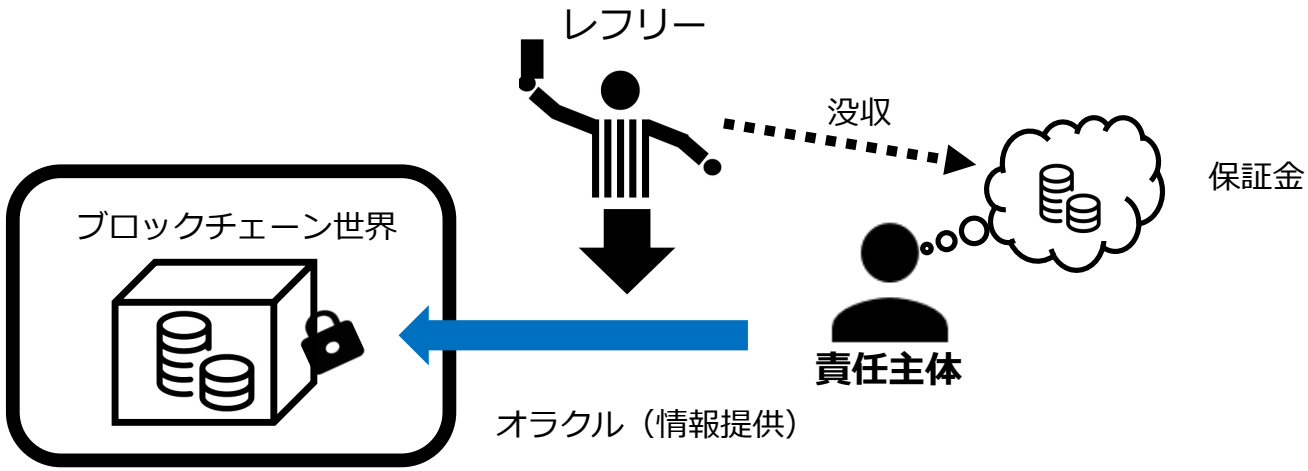


HTLC は責任ある主体を創る

- **保証金をHTLCにデポジットした主体**



- **もし不正を行えば保証金が没収される可能性がある（責任主体になる）**

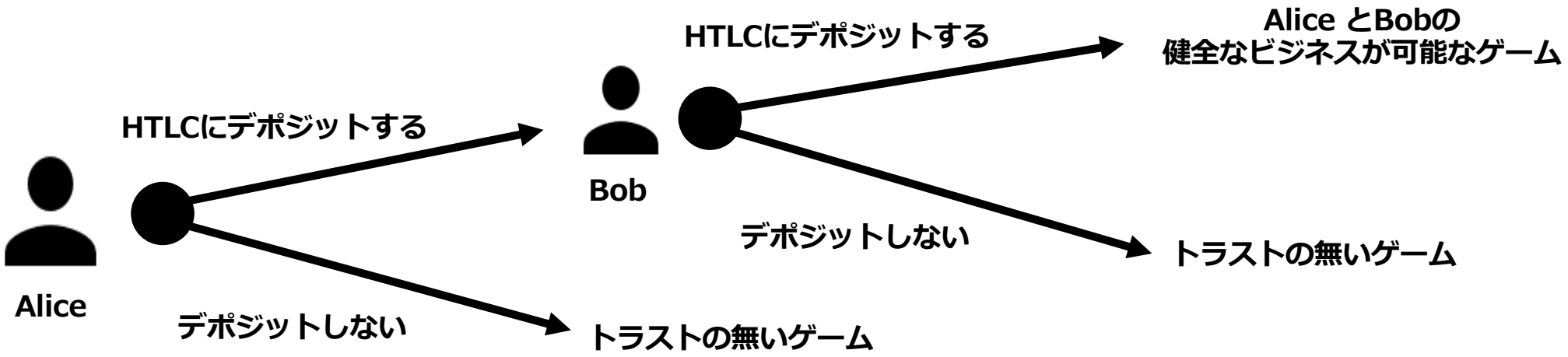


信頼できる主体たちによる「新たなゲーム」の創生

●ゲームを選ぶゲームという視点

- 当事者たちが，HTLCによって「信頼できる主体」になることで健全なビジネスが可能になる

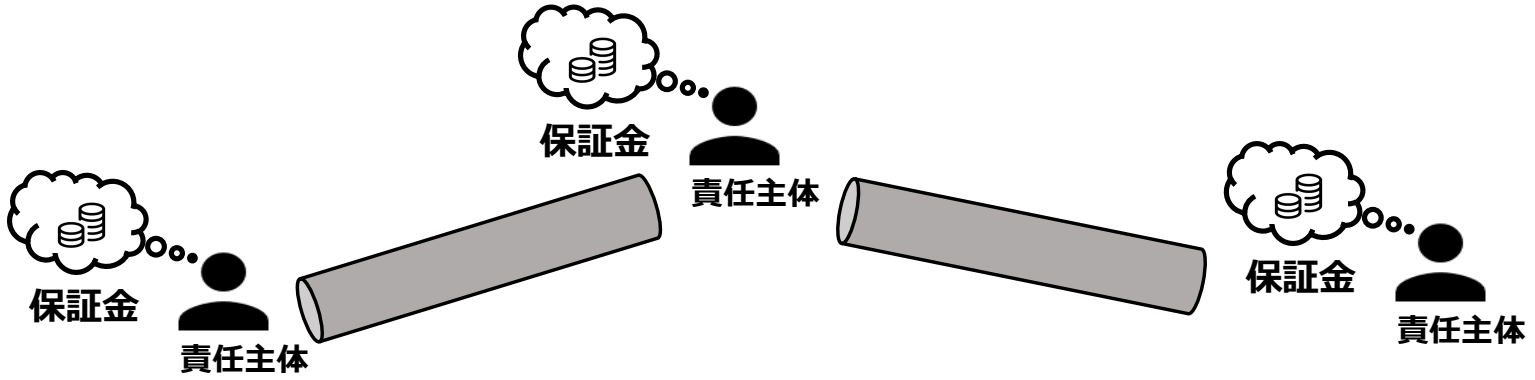
●ゲームを選ぶゲームのゲーム木



HTLC の利用例

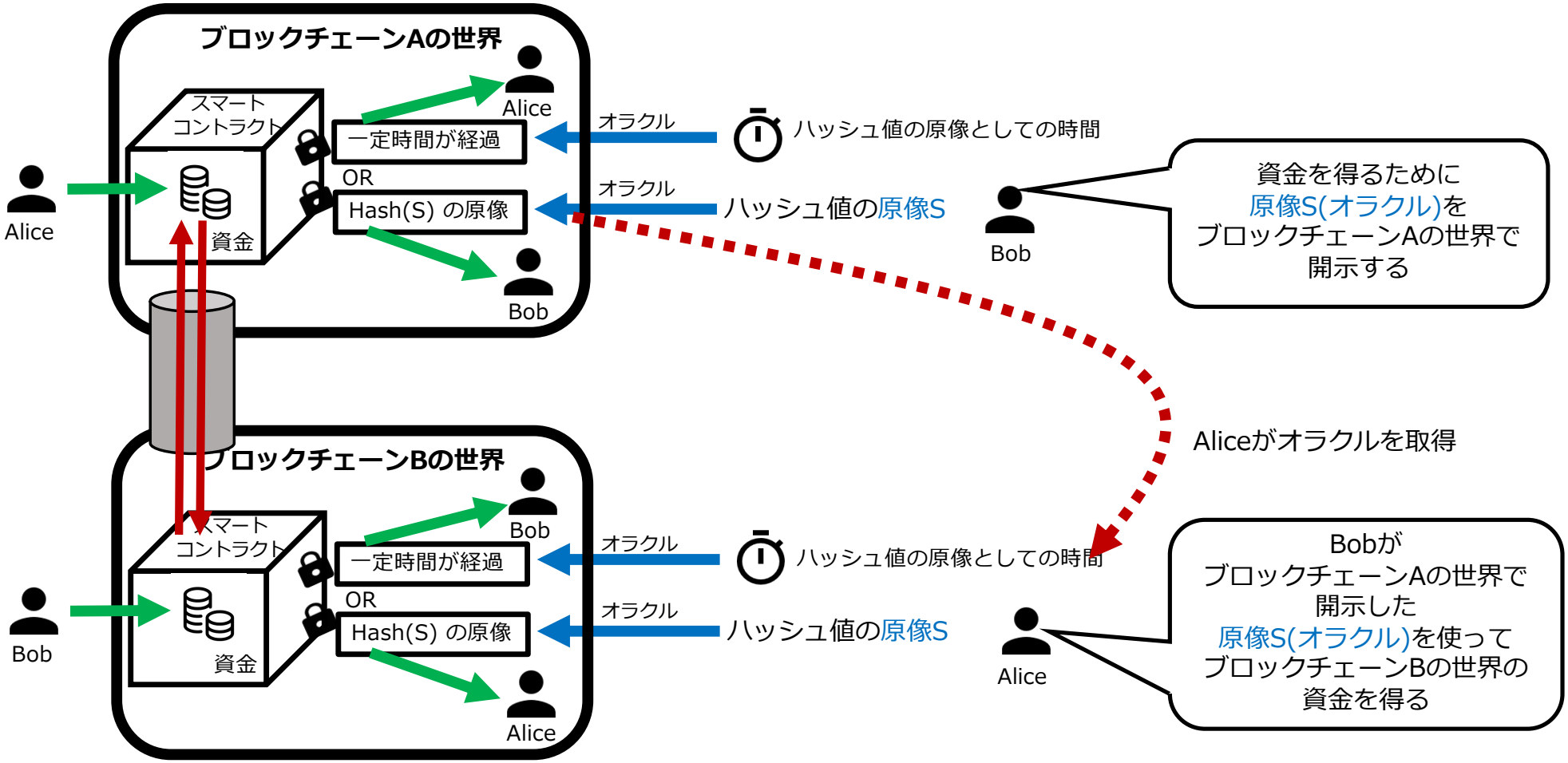
- **ペイメントチャンネル**
  - 送金する両者が自分の資金をHTLCにデポジットする　＝　ペイメントチャンネルが形成される

- **ライトニングネットワーク**
  - 参加者が自分の資金をHTLCにデポジットする　＝　送金ネットワークのノードになる



アトミックスワップ

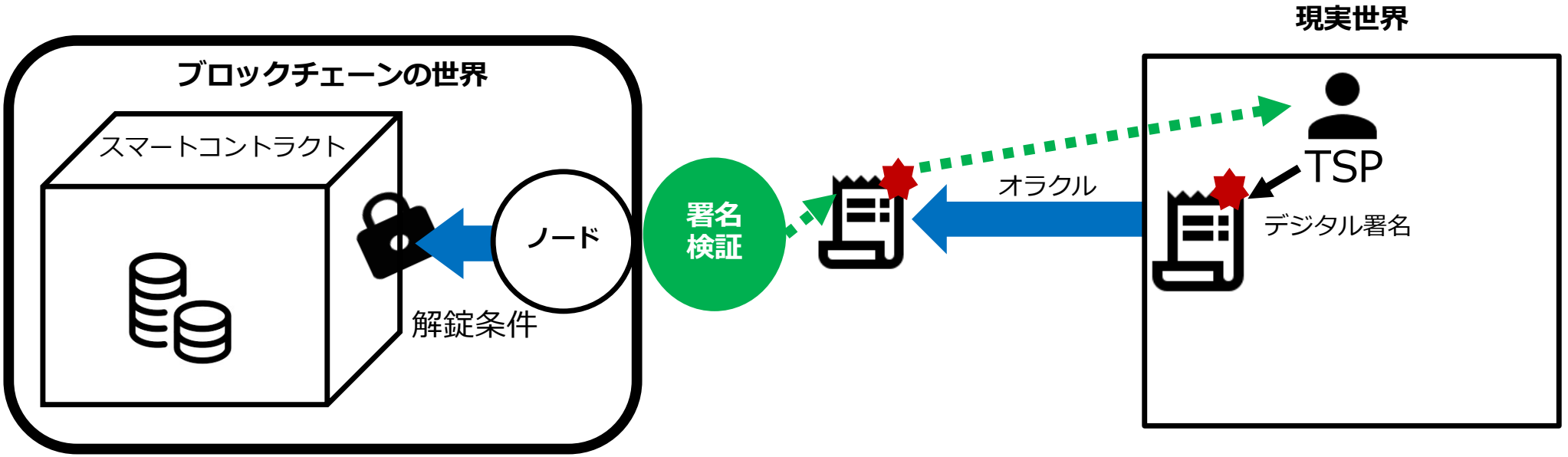
- **HTLCによって，ブロックチェーン間で価値の交換を行うチャンネルをつくる**



集中管理型オラクル

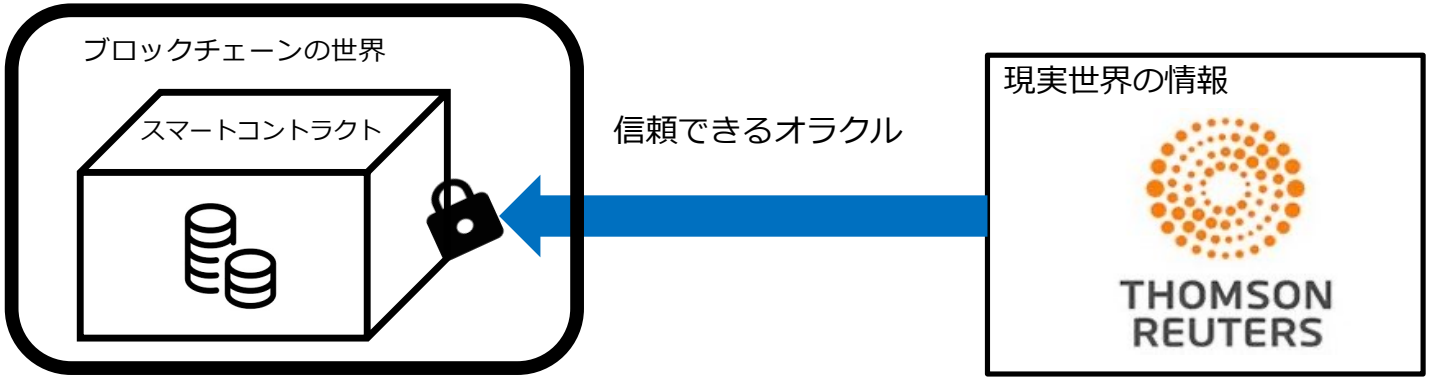
- **信頼できる第三者（TSP）によるオラクル**
  - ブロックチェーンの内側と外側をつなぐ「特定の」主体（群）が存在する
- **デジタル署名が基本**
  - ブロックチェーンのオラクル処理機構で署名検証

    サブスクリプション型，リクエスト応答型，プッシュ型など



マスメディア／ジャーナリズムの再定義

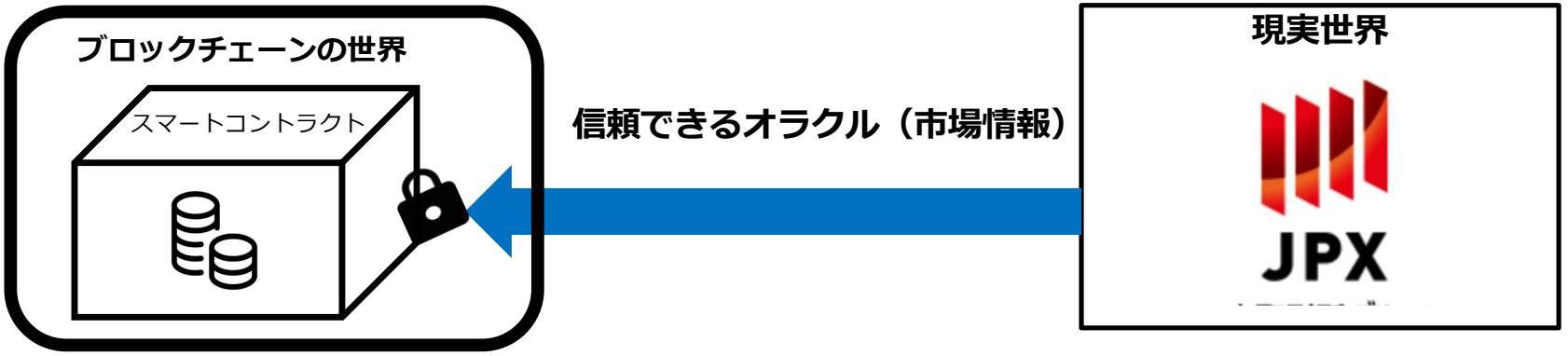
- **スマートコントラクトのための信頼できるオラクル（現実世界の情報）の提供者**
  - トムソン・ロイター社は，自社の情報を Ethereumのオラクルとして提供している
- **リカルディアン・コントラクトのオラクル版が必要**
  - リカルディアン・コントラクト（人間可読で機械可読なコントラクト）
- **信頼できる「機械可読なオラクル」の提供者が必要**



WSJ　NIKKEI　BBC　CNN　ALJAZEERA　人民日報　NHK

FinTechに必要な基盤は「信頼できるオラクル」

- **FinTechはスマートコントラクト用の信頼できる金融市場の情報サービスを必要としている**
  - 機械可読な（人間可読ではなく）FinTechのための信頼できる情報へのサブスク・サービス



  - メガバンクや監査法人などもトラストの社会的起点としての役割を持つべき

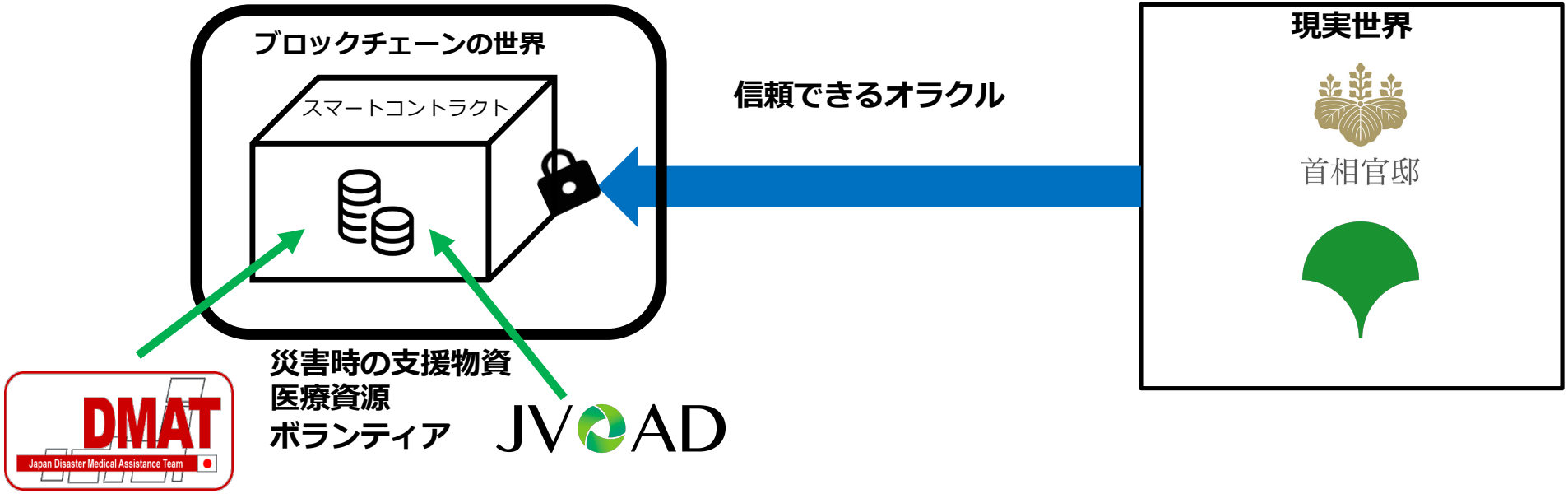
    三色のブロックチェーンの運用ではなく

MIZUHO みずほ銀行　SMBC 三井住友銀行　MUFG 三菱東京UFJ銀行

Deloitte. デロイト トーマツ　EY Building a better working world　pwc　KPMG

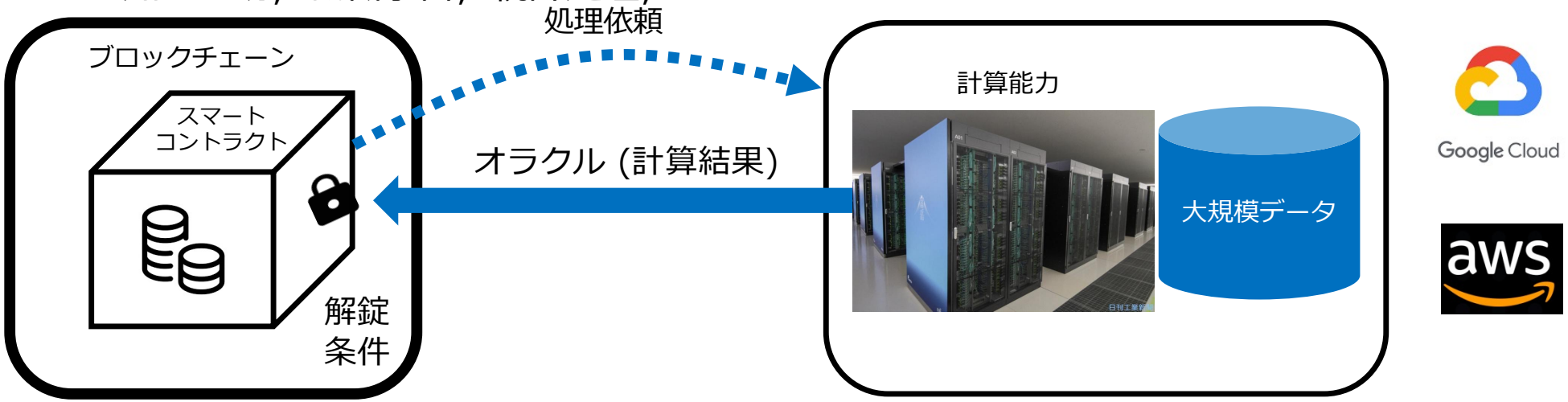
災害時対応の基盤にも「信頼できるオラクル」が必要

- **ブロックチェーンのロバストネス，レジリエンスもトラスト無しでは機能しない**
  - 地震，洪水，パンデミックなど
- **機械可読な（人間可読ではなく）政府／自治体の情報共有サービス（信頼できる情報）**
  - 自治体職員も被災する／パンデミックによる行動制限の可能性がある



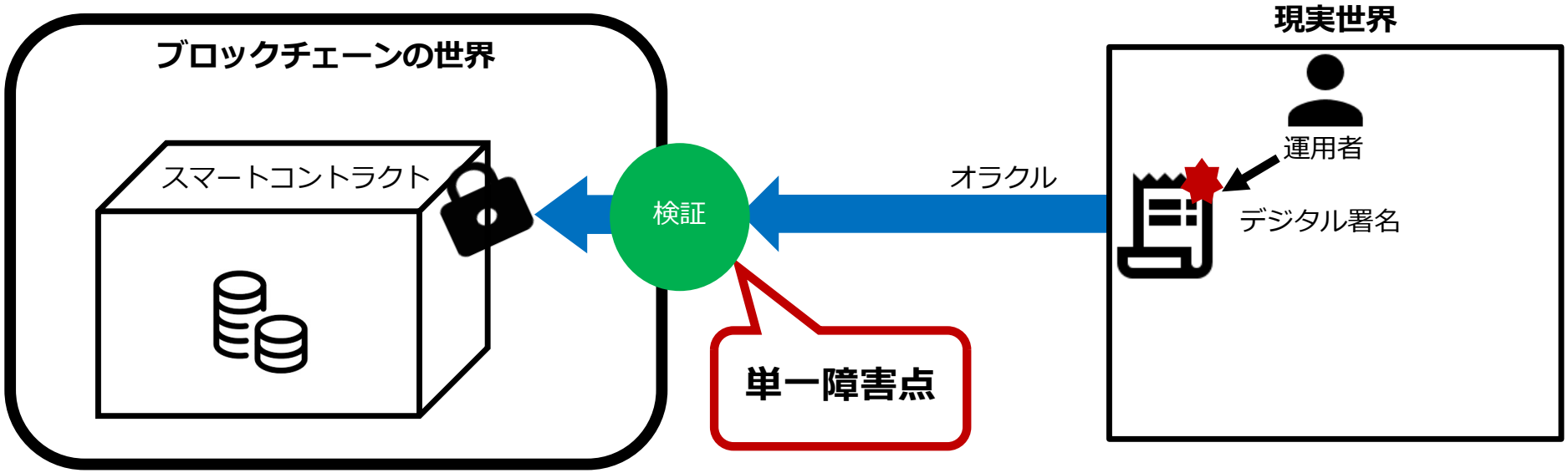
computational oracle (計算処理オラクル)

- **ブロックチェーンは計算処理やストレージのコストが大きい**
  - オンチェーンで複雑な計算や大量のデータを扱うのには限界がある
- **複雑な計算や大規模ストレージが必要な処理は外部で実行し，結果をオラクルとしてもらう**
  - ゼロ知識証明，機械学習，統計処理，…



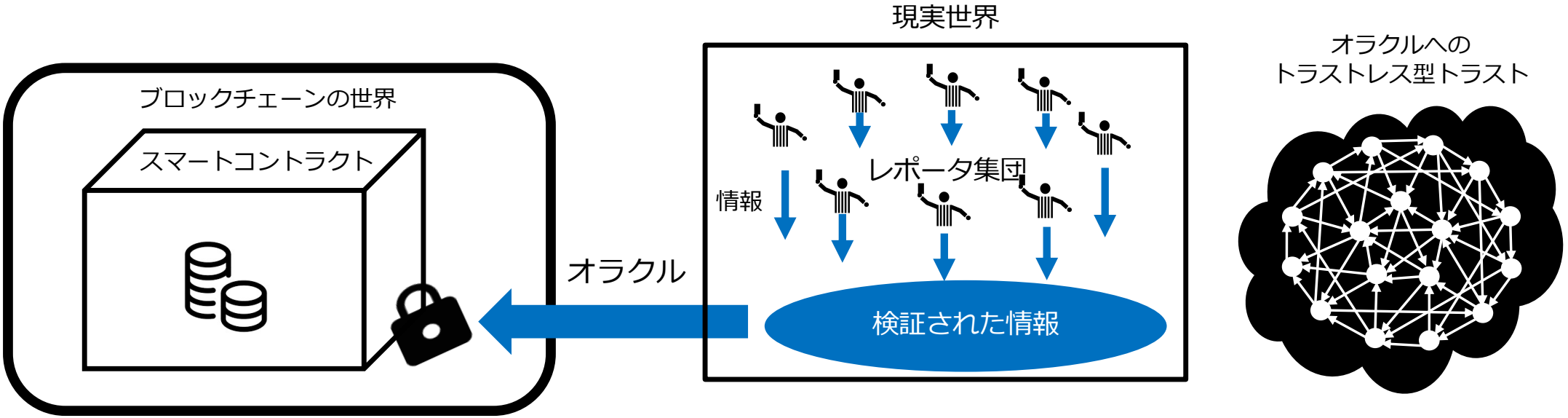
集中管理型オラクルの問題点

- **オラクルのトラスト　＝　運営者のトラスト**
- **単一障害点になる**
  - DDoS攻撃などの対象になる



分権型オラクル

- **「レポータ」による情報提供 (Augurの例)**
  - レポータは予め保証金(REP)をデポジットしている
  - 誤情報を流したレポータは，保証金を没収される



ニック・サボの「スマートコントラクト」

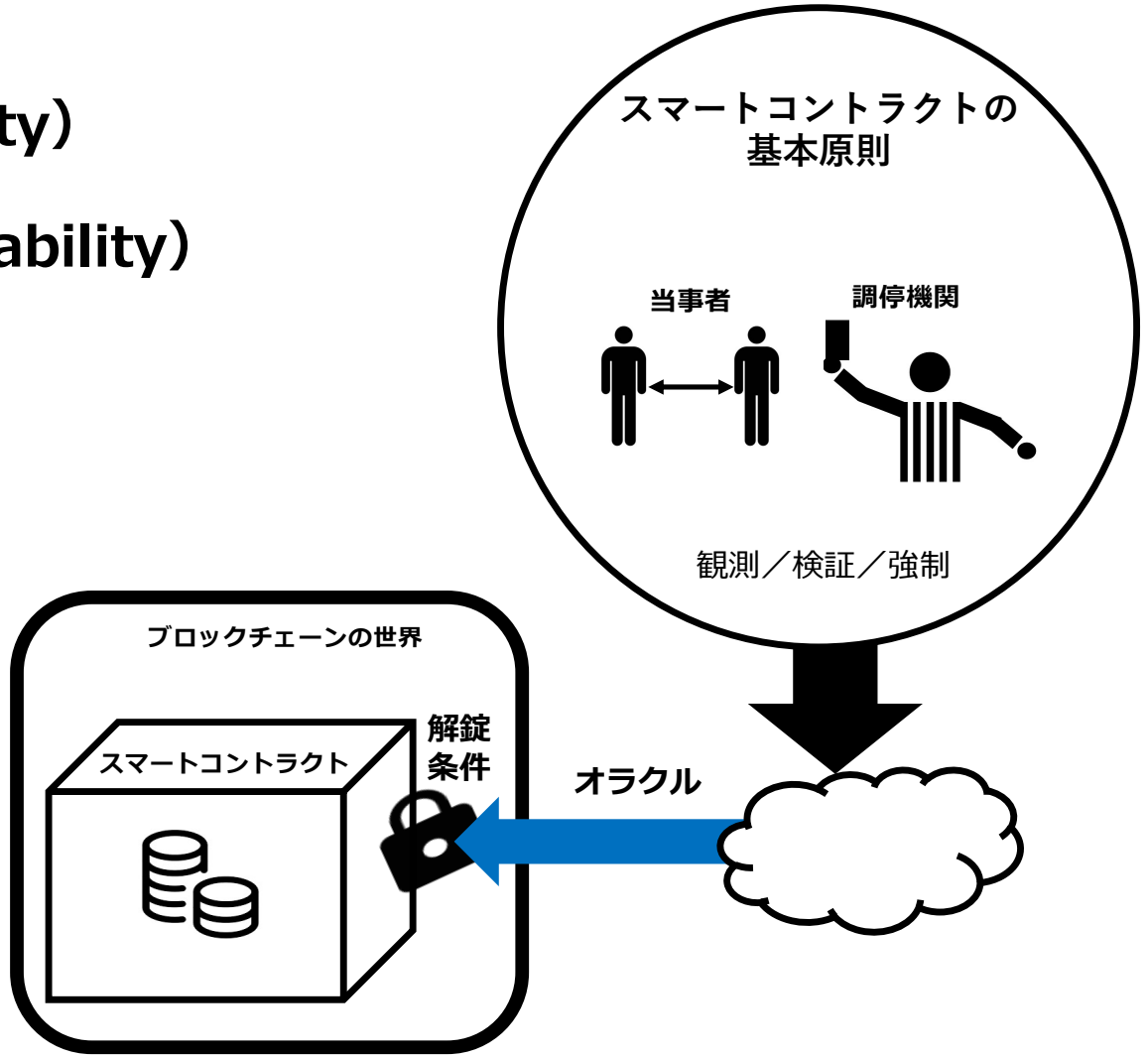
Nick Szabo

- **Bitgold (bitcoin の前身) を開発した暗号学者**
  - 2000年にジョージ・ワシントン大学で法学の学位を取得
- **コモン・ローによる調停と法執行のアルゴリズム化**
  - 英米法では，伝統や慣習の視点から帰納法的に調停が行われる
  - 判例主義，陪審員による判断

    大陸法（ドイツ法，フランス法→日本法）は原理原則から演繹的に判断される

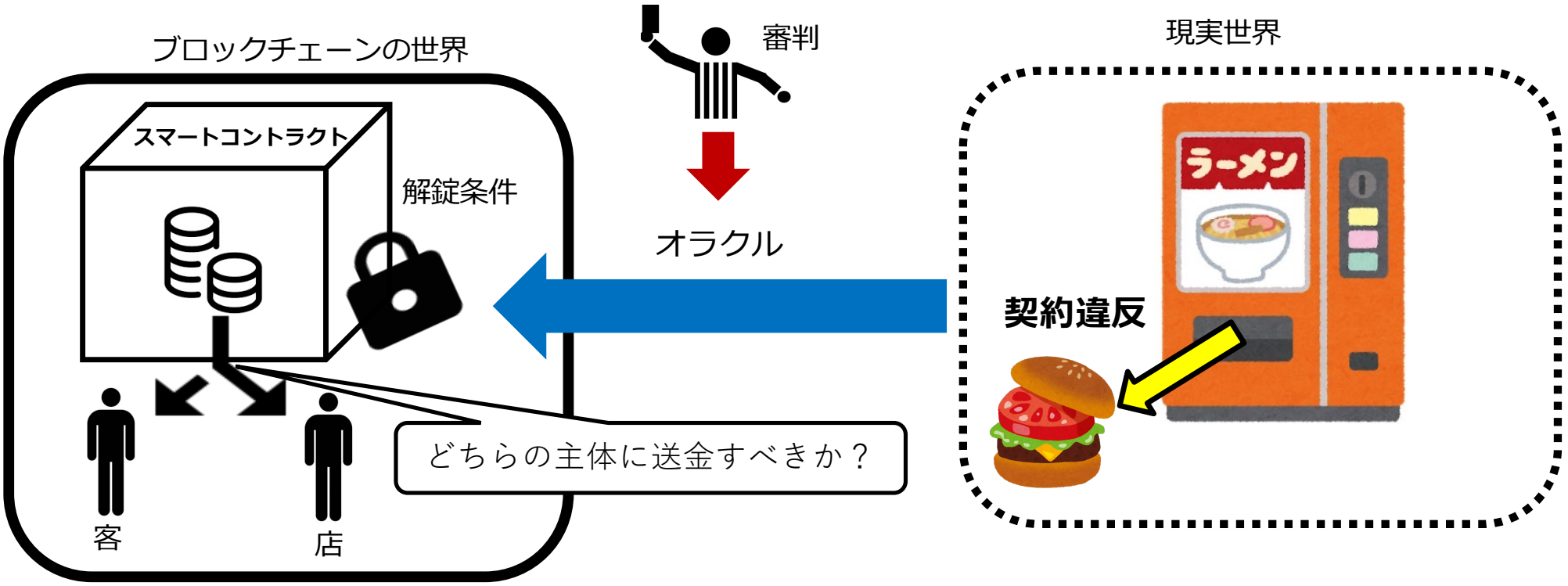
ニック・サボのスマートコントラクトの基本原則

- 観測可能性（observability）
- 客観的検証可能性（verifiability）
- 契約当事者関係（privity）
- 強制力（enforceability）



スマートコントラクトは自動販売機ではない

- **契約違反，不履行発生時の調停解決方法がより重要**

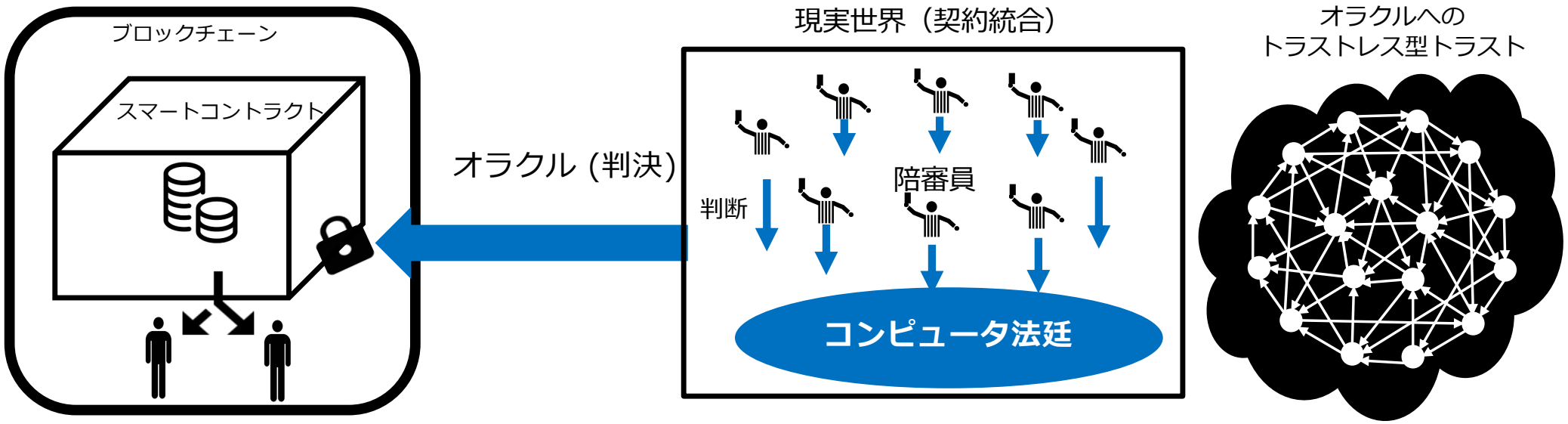


contractual integration (契約統合)

●分権型調停機能

- 陪審員（＝レポータ）
- コンピュータ法廷

  中央政府無しに陪審員たちの集合知を利用して紛争を解決する



サプライチェーンのトレーサビリティへの適用例

●サプライチェーンのためのオラクルのトラスト要件

- 外部情報（オラクル）がすべての工程で正確で欠損が無いこと

●食肉のサプライチェーンの例

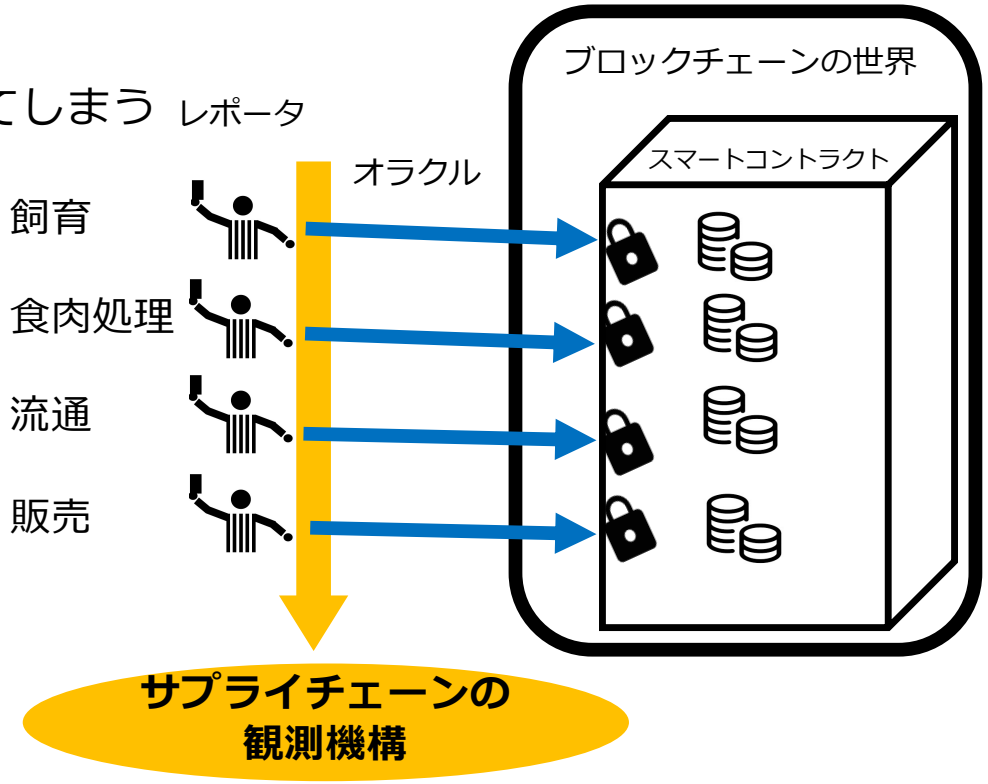
- どこか１箇所でも問題があれば食肉が汚染されてしまう
- 全供給行程に責任あるレポータが存在

  レポータは責任に応じた保証金をデポジット

  情報の不正が判明すると保証金が没収される

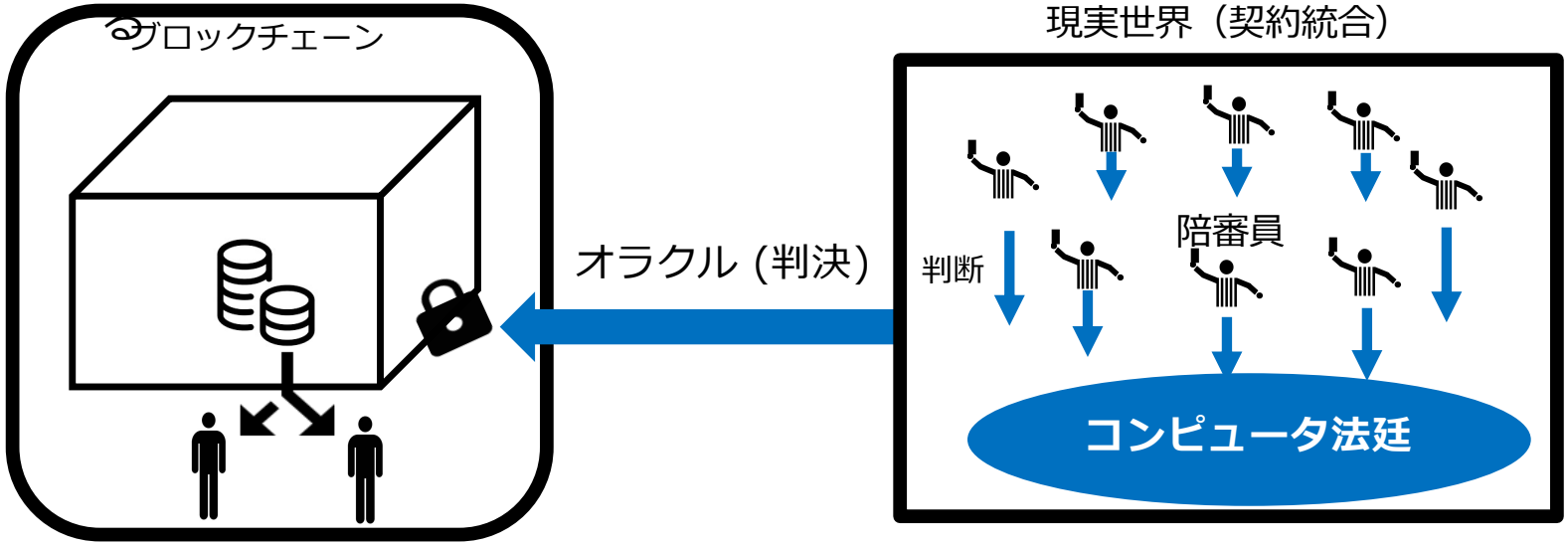
●契約統合による調停が本当に機能するか？

- ヴィリのパラドクスが重要な課題になる



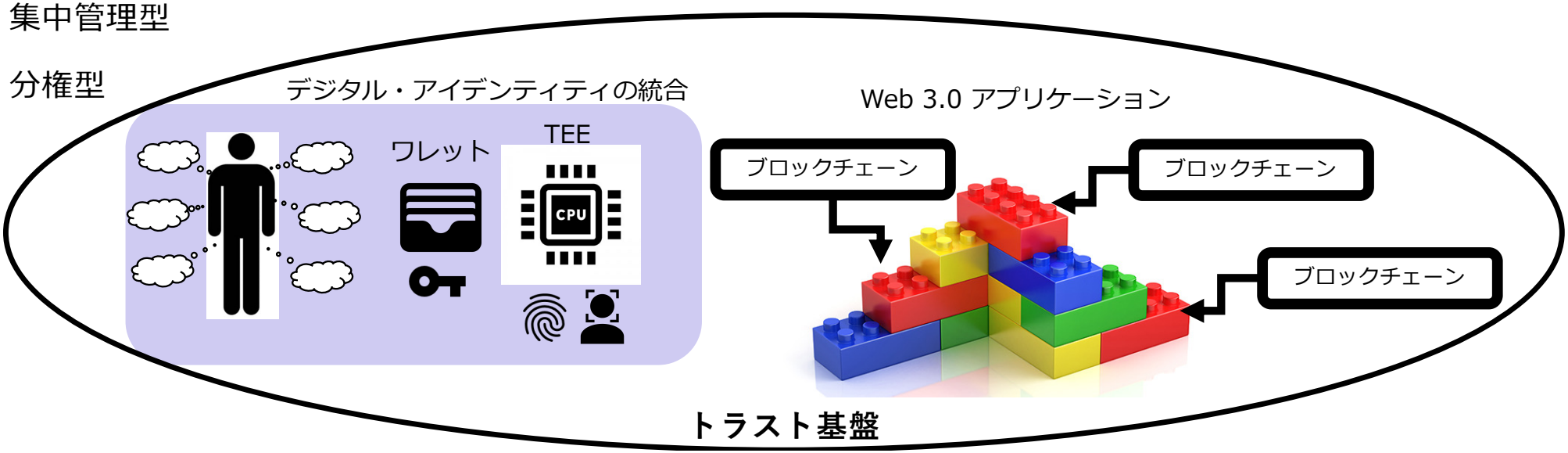
オラクルのプライバシ

- **英米法の契約 = 当事者間のプライベートな約束**
  - 第三者の介入の拒絶　→「それはあなたのビジネスではない」
- **スマートコントラクトは基本オフチェーンで実施すべき**
  - ゼロ知識証明やマルチパーティ計算などで，検証結果のみをブロックチェーンで受け取



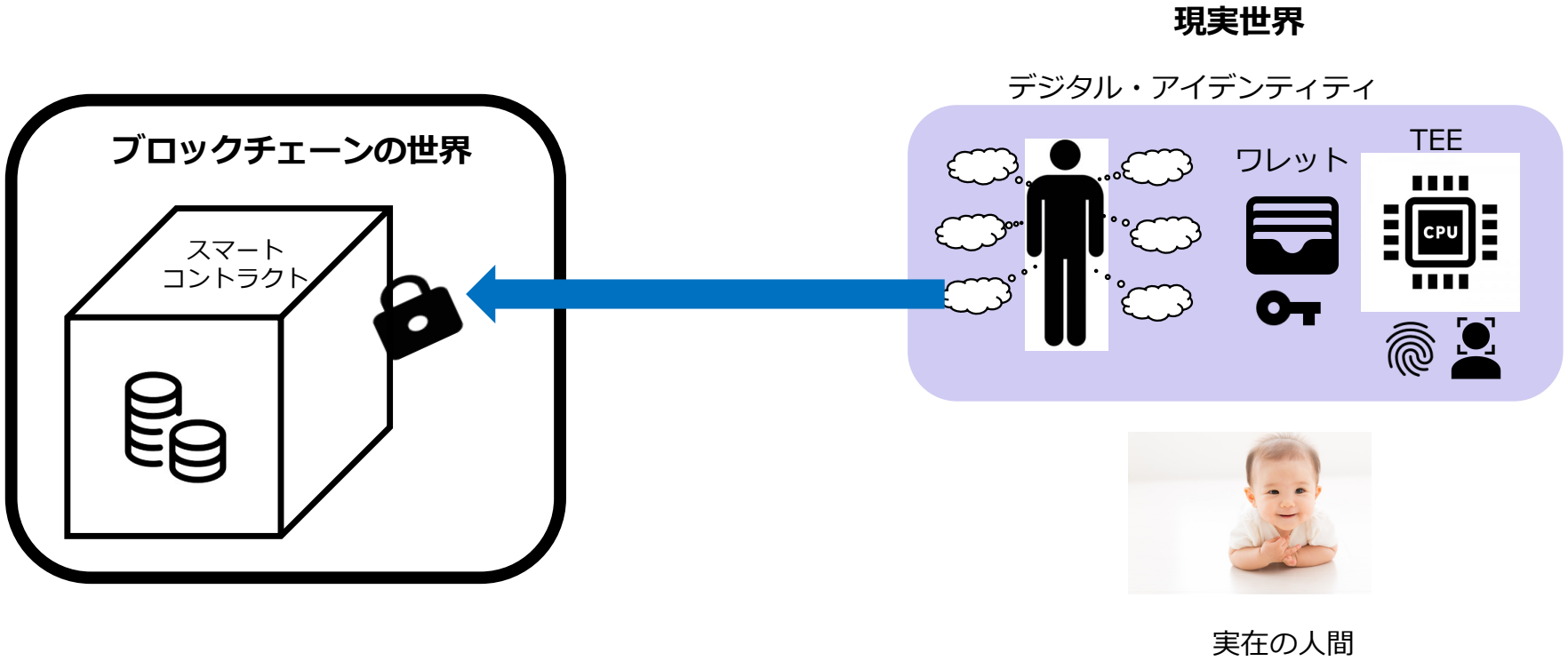
ブロックチェーン連携とWeb 3.0のトラスト基盤

- **Web 3.0 とブロックチェーン**
  - web APIを介したマイクロサービスの集合体＋デジタルアイデンティティの統合
  - ブロックチェーンはマイクロサービスの一つ
- **ブロックチェーンを含むweb 3.0 のトラスト基盤**
  - ランダムオラクルモデル（HTLC）
  - 集中管理型
  - 分権型



デジタル・アイデンティティの重要性

- オラクルは，ブロックチェーンと現実世界を接続するもの
- 最も重要なオラクル　＝　実在する人間



ブロックチェーン視点でのオラクルのトラスト

- **ブロックチェーンの健全な発展に不可欠な基盤**