魔法を信じるな。

メタバースと Web3, NFT (非代替性トークン), DAO (分散型自律組織) のリアリティ

早稲田大学 大学院経営管理研究科

斉藤 賢爾

このお話では

- 現在、一部の意見として, 暗号資産や NFT に代表されるようなブロックチェーンの応用 (いわゆる「web3」) とメタバースに必然的な関連性があるかのような主張が見られます
- そうした主張の難点のひとつは、暗号資産や NFT が関わることで仮想空間への参加が資産形成のためのゲームに変わってしまい、メタバースが持つ本来の可能性が損なわれうることです
- その一方で、なぜブロックチェーンとメタバースを結びつける見解が存在するかは興味深くもあります

- このお話では、web3 の概念が登場するまでの歴史的経緯を検討し、web3 に特徴的な概念かつメタバースと結びつけられがちなものとして、特に NFT と DAO がそれぞれ何であるかを改めて整理しつつ、それらのリアルな状況を明らかにします

メタバースとは？

- 仮に次のように定義します
  - 「あえて仮想的な空間にマッピングされた情報空間（インフォスフィア）」
  - そのマッピングをユーザが自発的に組み換えることが可能

- ユーザがアイテムや空間そのものを創造できる
  - アイテムや区画をトークン化し、トークンを所有することを通してそれらのデジタル資産をプレイヤーが所有、つまり排他的に支配できるようにするという考え方があるようです
  - 技術の特性に照らして、そうした考え方は正しい方向でしょうか？

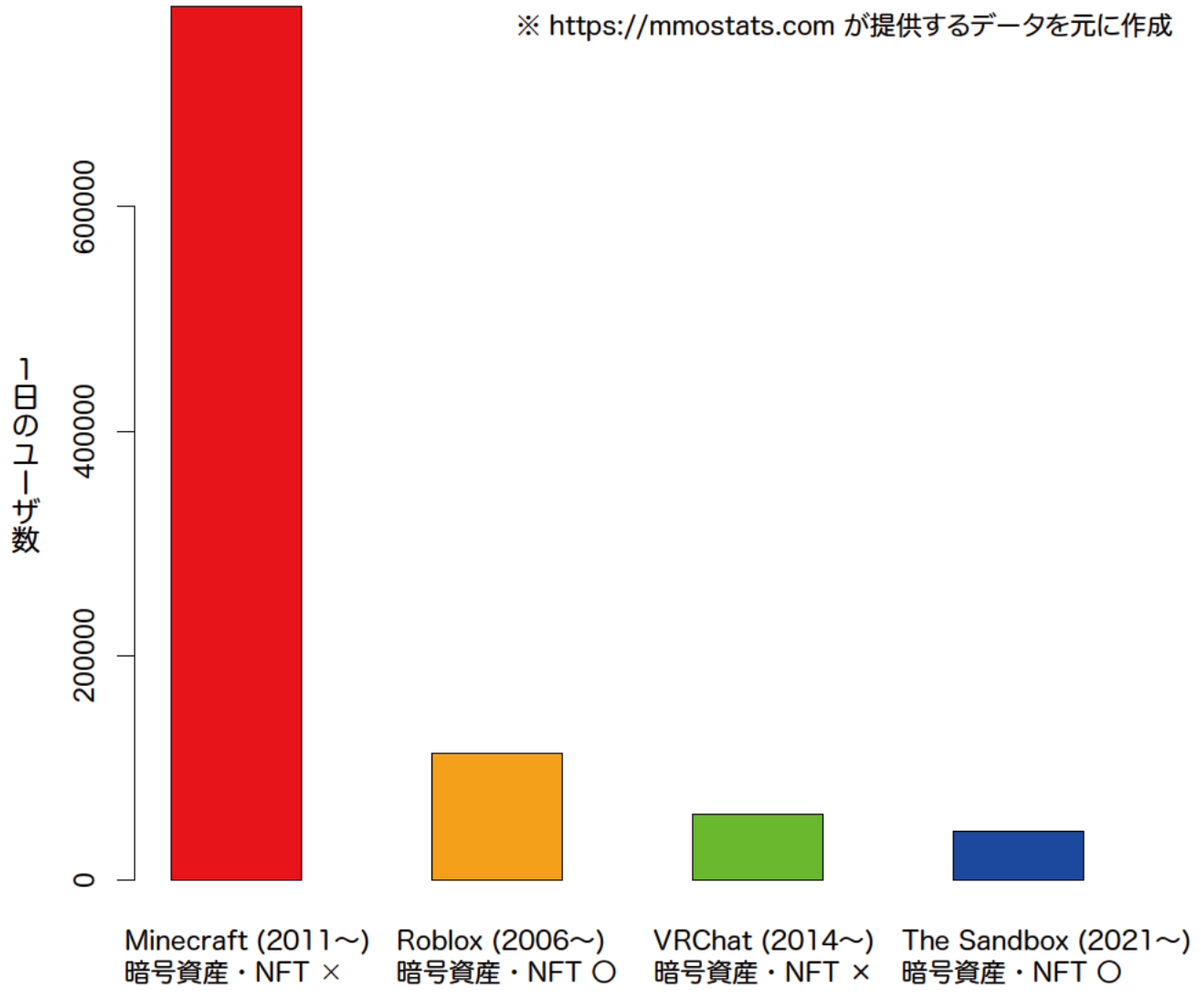
NFT を禁止するメタバース系ゲーム

- Minecraft
  - プレイヤーが立方体のブロックを自由に配置・破壊し、創造的な建築物やアート作品を作ることができるサンドボックス型のビデオゲーム
- VRChat
  - プレイヤー自身が制作できる仮想空間をオンラインで訪れ、アバターを通して他のプレイヤーとの交流を楽しむことができる、仮想現実 (VR) 対応のソーシャルプラットフォーム

- 理由
  - プレイヤーにゲーム体験にフォーカスしてもらうため
    - ゲーム内のアイテムが NFT に紐づけられると、その市場価格の上下にプレイヤーの関心が逸らされてしまう
  - なによりも、NFT が暗示する「希少性と排除」の考え方が、Minecraft が大切にしている「包摂」の考え方と馴染まない

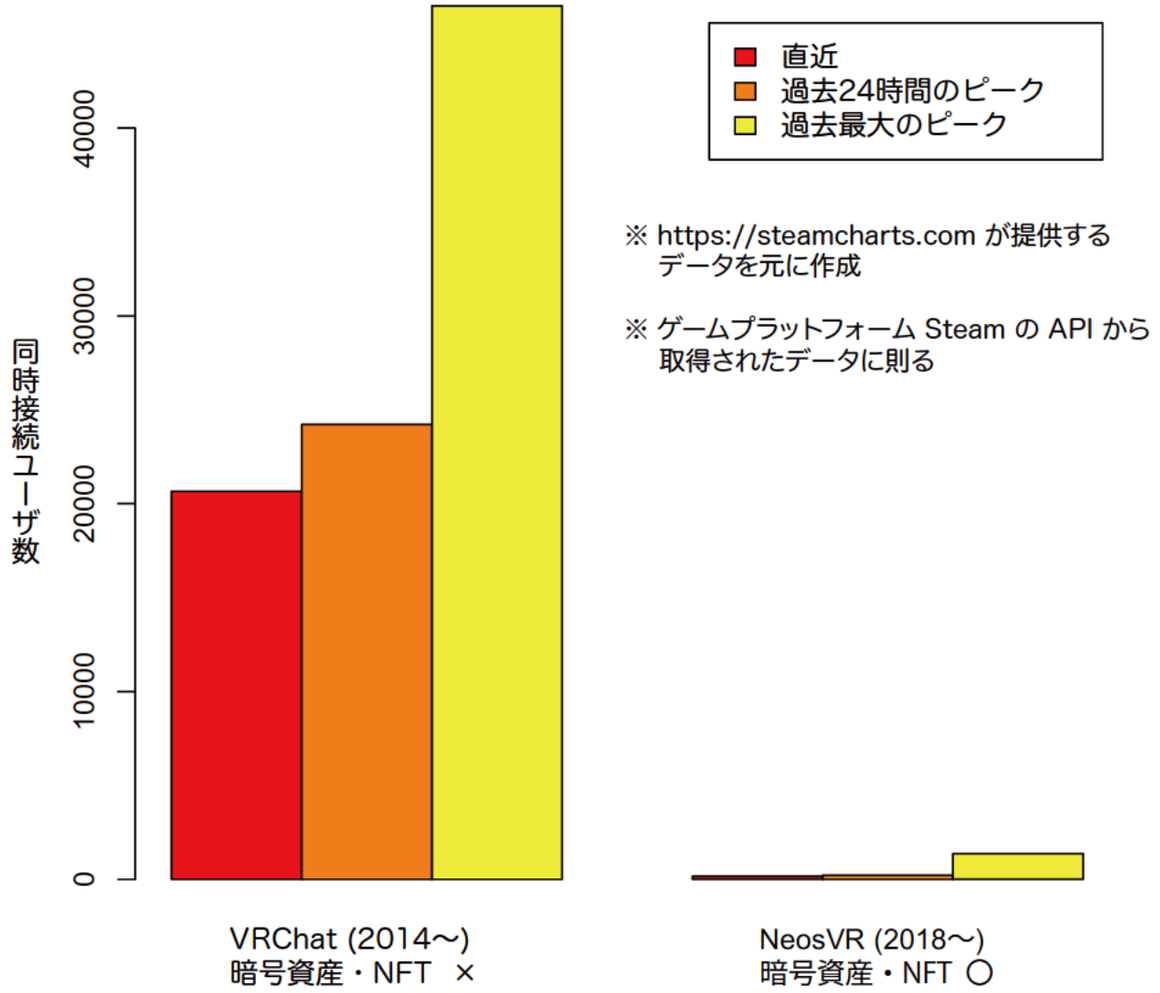
メタバース系ゲームのユーザ数の比較

※ https://mmostats.com が提供するデータを元に作成



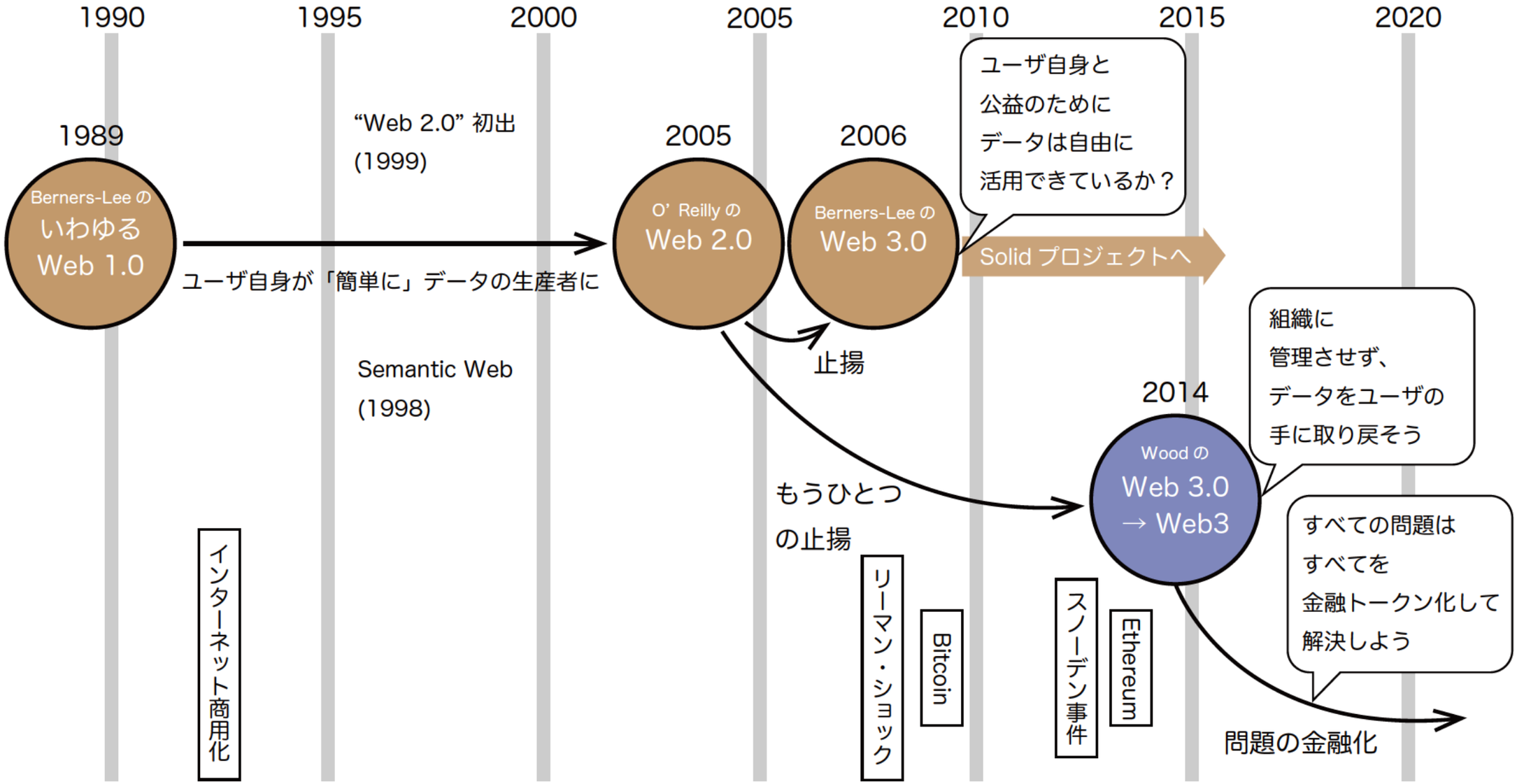
- 算出アルゴリズムが非公開のため参考程度
- 以下は月間実働ユーザ数での比較
  - ZEPETO (2018～)
    (暗号資産・NFT ◯)
    - The Sandbox の 100 倍程度
    - Roblox/Minecraft の $\frac{1}{10}$
  - Axie Infinity (2018～)
    [育成ゲーム]
    (暗号資産・NFT ◯)
    - The Sandbox の 2 倍
  - Decentraland (2020～)
    (暗号資産・NFT ◯)
    - The Sandbox の $\frac{1}{10}$

VRChat vs. NeosVR (ユーザ数の比較)



- 全ユーザ数を表していないため参考程度
- NeosVR は NFT を禁止していた
  - 理由はマイニングの電力消費の環境への影響 (現在は当たらない)
- VRChat に希少性は馴染まない
  - その世界にひとつしかないアイテムで遊びたければ、各々の仲間内でその世界のインスタンスを作って遊ぶ
  - 遊びたい全員が遊べる

Web 1-2-3


1990
1995
2000
2005
2010
2015
2020
1989
Berners-Lee の
いわゆる
Web 1.0
ユーザ自身が「簡単に」データの生産者に
“Web 2.0” 初出
(1999)
Semantic Web
(1998)
2005
O’ Reilly の
Web 2.0
2006
Berners-Lee の
Web 3.0
ユーザ自身と
公益のために
データは自由に
活用できているか？
Solid プロジェクトへ
止揚
もうひとつ
の止揚
2014
Wood の
Web 3.0
→ Web3
組織に
管理させず、
データをユーザの
手に取り戻そう
すべての問題は
すべてを
金融トークン化して
解決しよう
問題の金融化
インターネット商用化
リーマン・ショック
Bitcoin
スノーデン事件
Ethereum

Web 3.0 や *Web3* は何を解きたいか

- いわゆる Web 1.0 (Berners-Lee) : ~~Read~~
  - 研究者のための出版メディア → 基本的に全員が論文を書き、読むのだから最初から双方向
  - 「ユーザがデータを管理するが、出版は容易でない」
- Web 2.0 (O'Reilly) : Read × Write ← 前から
  - 「ユーザはデータを管理できないが、出版が容易」
- Web 3.0 (Berners-Lee)
  - 「ユーザがデータを管理し、かつ出版が容易」を目指す → Solid (Social linked data)
- Web 3.0 → Web3 (Wood)
  - Ethereum をウェブから使えるようにする ← web3.js, web3.py
- Web3 (Dixon) : Read × Write × ~~Own~~
  - 「私たちがオンラインで行うほぼすべてのことの内部に、トークンという形で金融資産を組み込む」(Bloomberg)
  - 他者へのトラストに依らずにトークンは所有できても、トークンが指したり包含するものは所有できない

ブロックチェーン：満たすべき性質

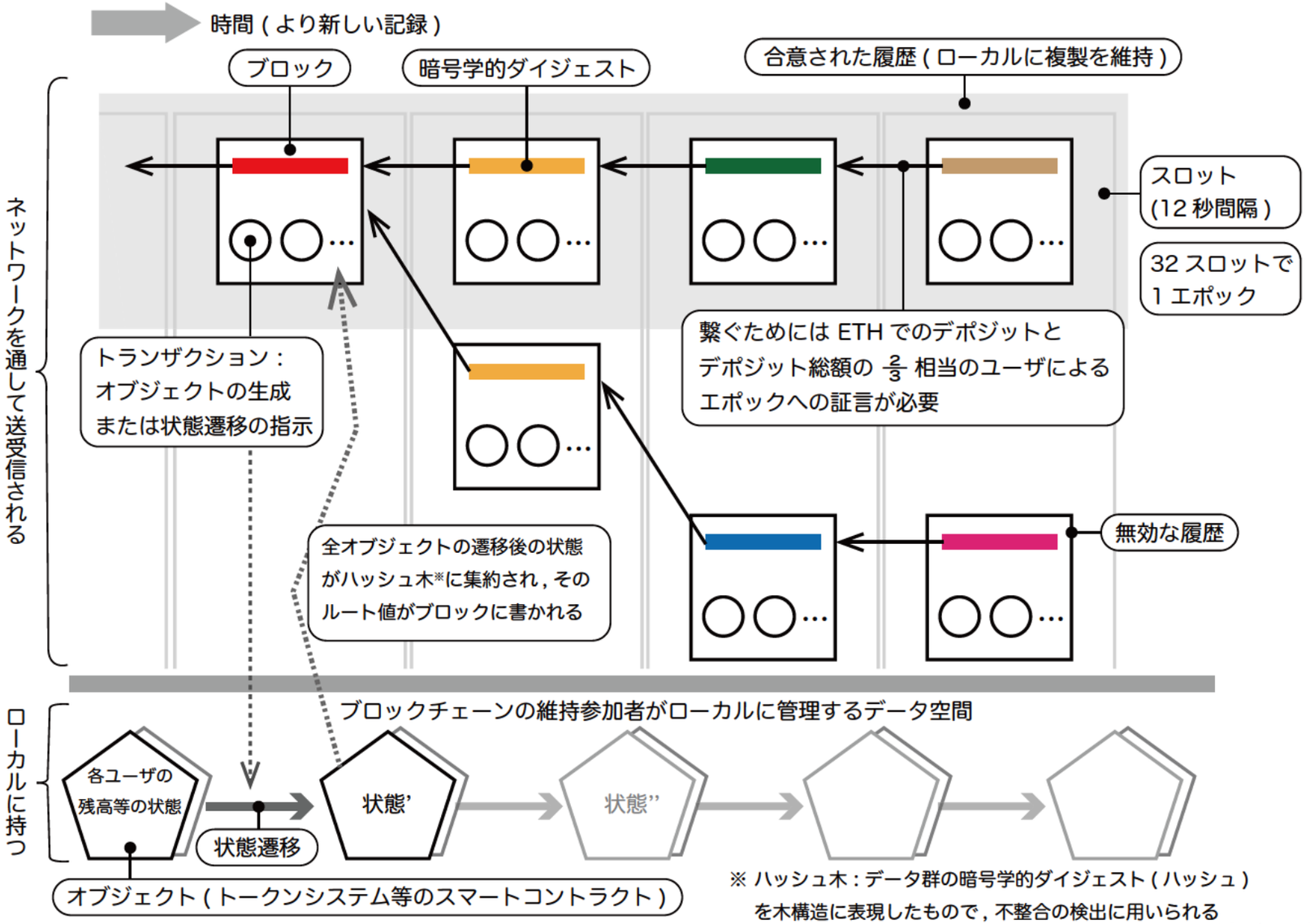
- 元々 Bitcoin を可能にするために発明され、
  「自分が持つコインを自分だけが自由に誰かに送るのを誰にも止めさせない」
  必要があるのだから . . .

- 自己主権性：ユーザ自身が意思決定して実行できる (例：アカウントを勝手に作れる)
- 耐検閲性 (狭義)：他者の意思で記録やその確認を妨げられない
- 耐障害性：故障によっても記録やその確認を妨げられない
- 耐改ざん性：過去の記録を抹消・改変・捏造できない

⇒ といった広義の「耐検閲性」が満たされる必要がある

- いかなる方法によっても記録の否定ができない
- 技術なので動作条件がある
  - ブロックチェーン特有の動作条件は「ネイティブ暗号資産の市場価格が十分に高い」

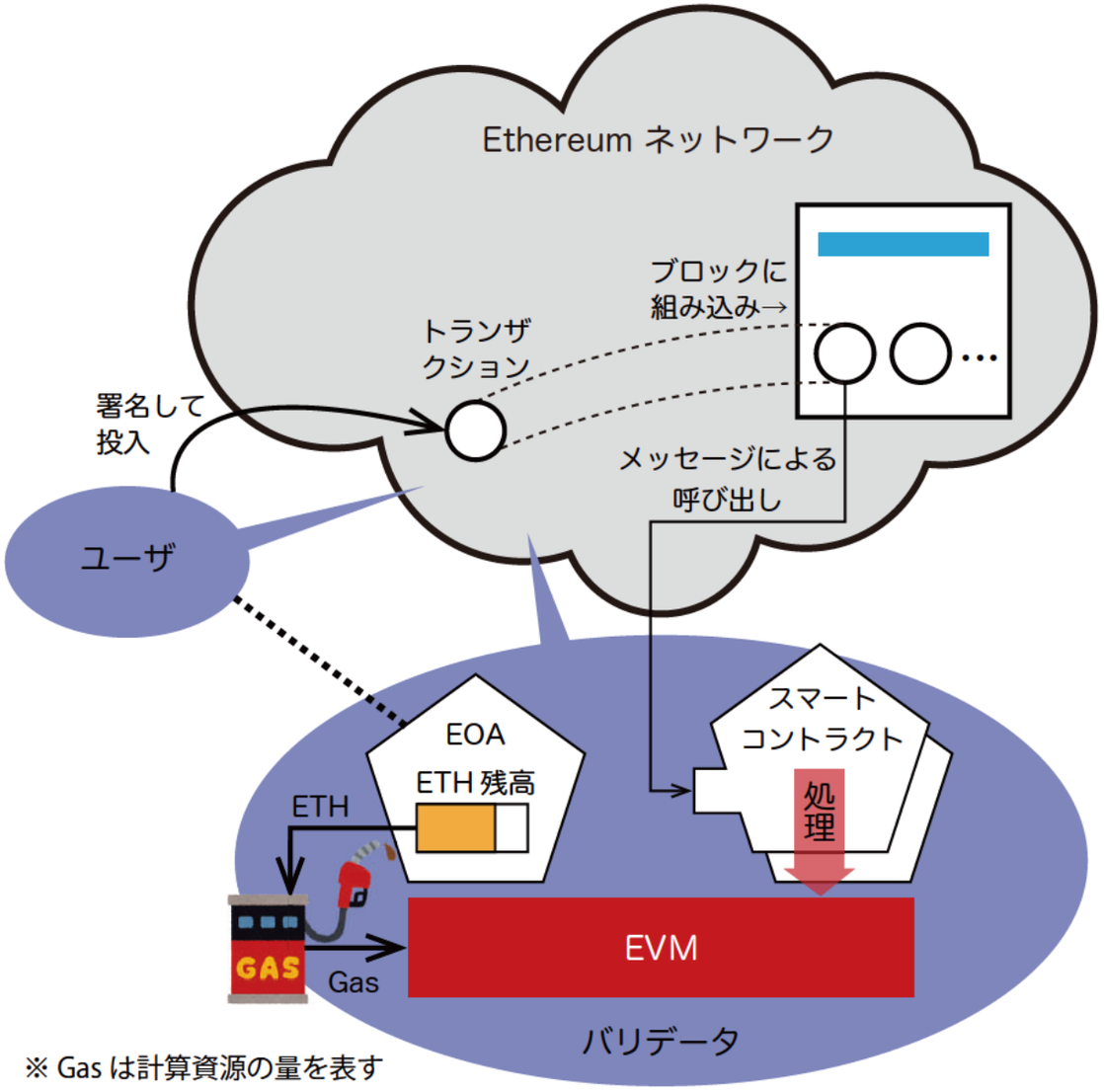
Ethereum ブロックチェーンの構造



※ ハッシュ木 : データ群の暗号学的ダイジェスト (ハッシュ)
を木構造に表現したもので , 不整合の検出に用いられる

- 大事なことは . . .
- ETH で報酬を得る
  バリデータたちが
  自発的に参加する
  - だから ETH の市場
    価格が十分に高い
    必要がある
- 各自がもつ状態マシンの
  状態を確実に一致させる
  - 等しい初期ブロック
    から始まる
  - ブロックを全員に
    コピー
  - ブロックの並びが
    等しい
  - 非決定でない処理

スマートコントラクトの実行機構



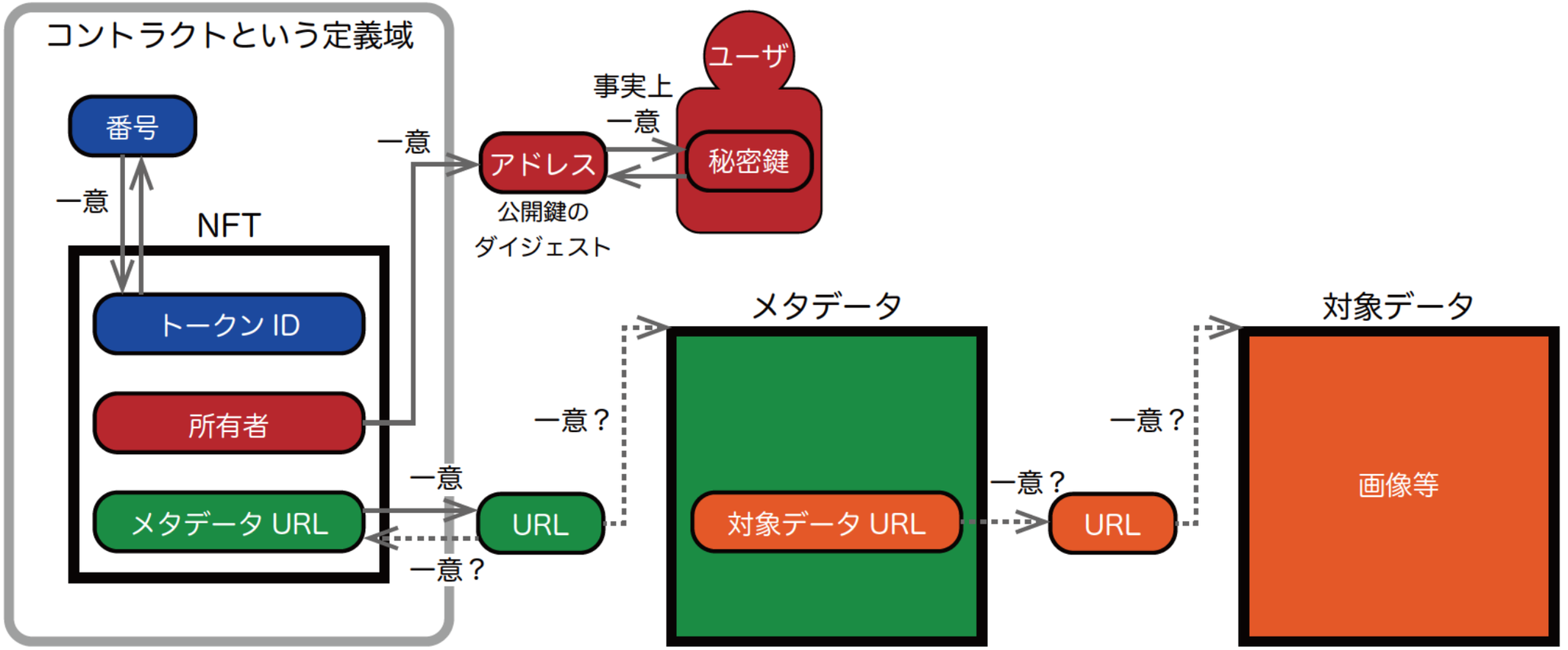
※ Gas は計算資源の量を表す

※ Gas 使用料を ETH で支払うユーザがトランザクションを投入しない限り
スマートコントラクトは動作しない

- 広義の耐検閲性を満たす台帳に
プログラムコードとデータを
書き込んで実行できるからこそ
スマートコントラクトは有用

- 大事なことは . . .
- Ethereum 仮想マシン (EVM) が
スマートコントラクトを実行する
- それを指示するユーザは ETH で
計算資源量を買わなければ
ならない
- 誰かが計算資源量を買わないと
スマートコントラクトは動かない
↑ DAO 実現への落とし穴

ERC-721 仕様にもとづく NFT

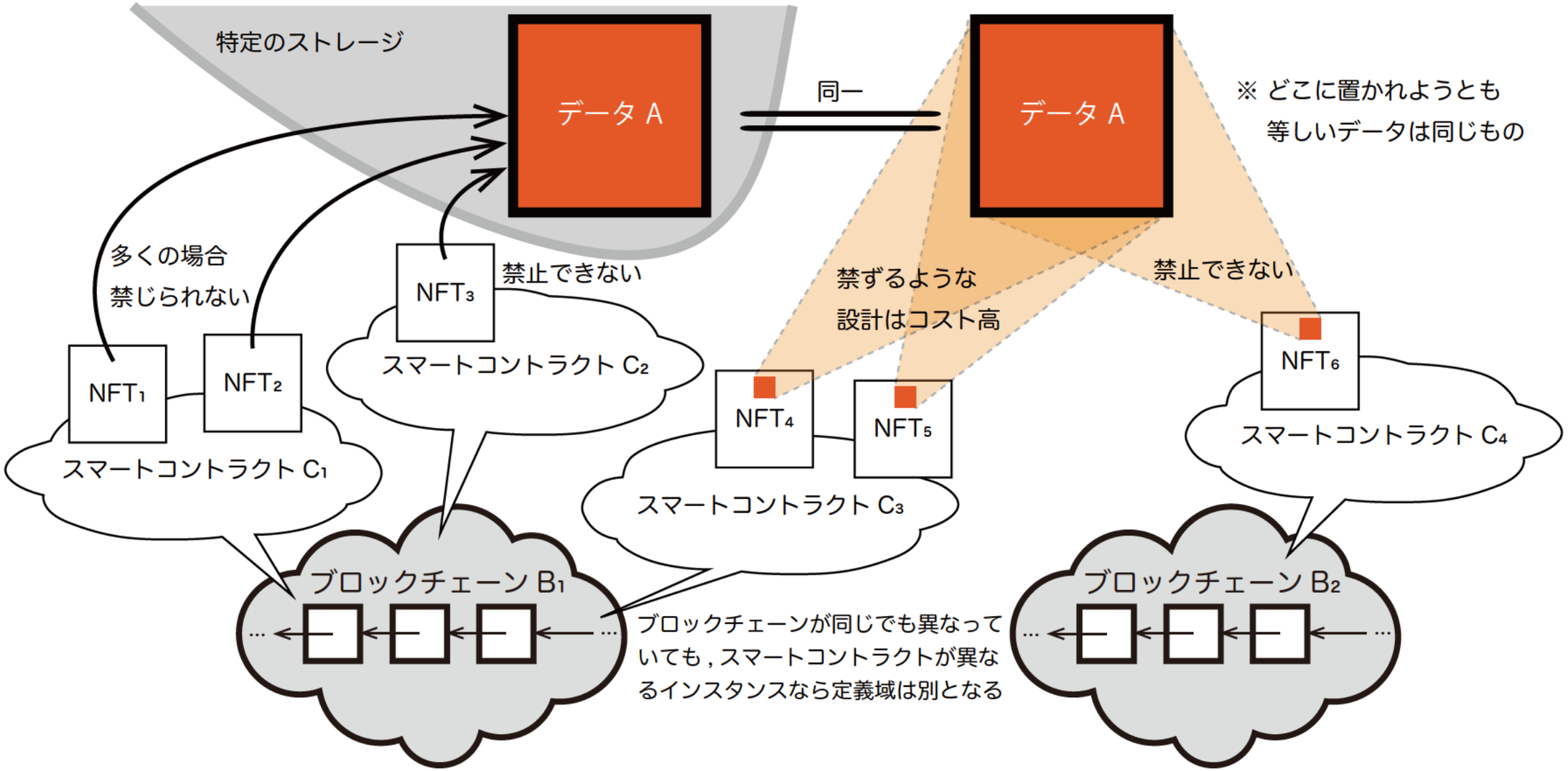


※ そのコントラクトという定義域の中で , 実線矢印で示した一意性を保証するに過ぎない

※ 破線矢印で示した一意性は , 実装・運用の工夫次第で保証できる

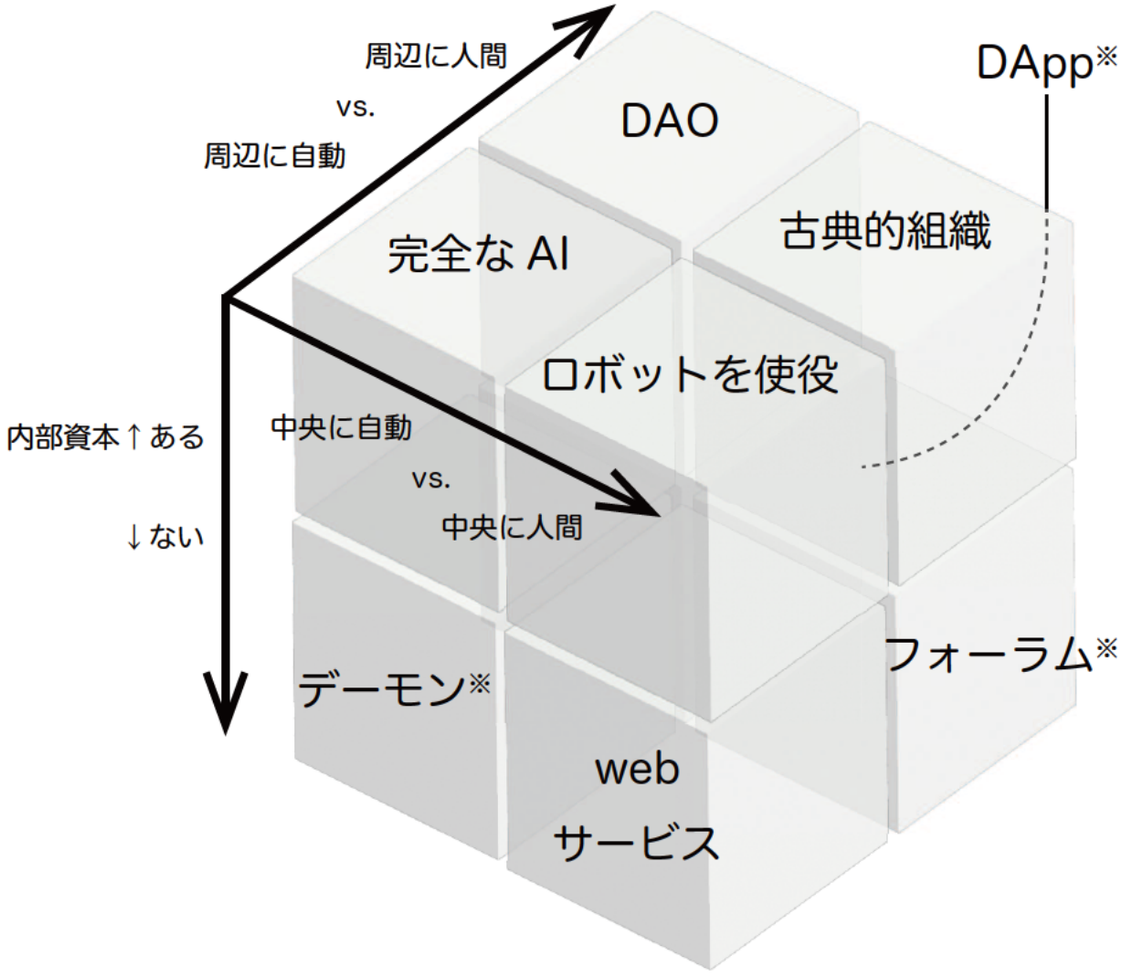
例えば , URL にそれが指すリソースの暗号学的ダイジェストを含めること (例 : IPFS の利用) により「URL → データ」の一意性を保てる (その場合でも「データ → URL」の一意性は無い)

NFT の唯一性にまつわる幻想を捨てよう



※ NFT がデータを指す方式とデータを格納する方式は，データの可用性は異なるとしても一意性に関わる性質は変わらない

DAO と各種組織のキューブ



※ DApp：スマートコントラクトによるアプリケーション (Decentralized App)
※ フォーラム：人々が特定の話題について議論したり情報を交換したりする場
※ デーモン：バックグラウンドで稼働し，イベントに自動的に対応するプログラム

- 左のキューブには矛盾がありますが、それはさておき . . .
- Buterin による DAO の定義 (2014)
  - インターネット上に自律的に存在するが、自動システム自身にはできない特定のタスクを担うために、人間を雇うことに大きく依存している
  - そのため、内部に資本（報酬として使われ人間を駆動する）をもつ
  - 意思決定を自律的に行う

DAO なのか、そうではないのか

- Bitcoin は DAO？
  → DAO
- Ethereum は DAO？
  → うん、まあ . . . DAO？ (人間がさっさと意思決定するけど)

- スマートコントラクトで作ったものは DAO？
  → え？. . . あれれ？
  - 自律的には動いていない (呼び出されないと動かない)
  - トークンの持ち分による投票に意思決定を依存している
    - 提案はスマートコントラクトのコードとして書かれる
    - それを全員が読めることが前提となる
  - 可決した提案を実行する (計算資源量を買う) のは誰？
    - 決まった誰かがやるなら、その人に拒否権があり実質的な支配者では？
    - 誰でもできるなら、真意を難読化した提案を用いて容易に攻撃できる

まとめ

- 「所有」の概念が深く考えられていないというリアリティ
  - なんでもトークン化すれば解決するのか？(しませんよね . . . します？)
  - 他者へのトラストに依らずにトークンは所有できても、トークンが指したり包含するものは所有できません
  - トークンの所持は証明でき、ブロックチェーンは広義に検閲できないので、誰にも邪魔されずに各自の意思表示はできます
    - したがって、トークンの所持量に応じた投票は実現できます
    - しかし投票は意思決定における最後の手段では？
      - 投票をする前にやるべきことがあると分かっている DAO もあるようですが、その部分、普通に Web 2.0 的に動いていたりしませんか？

- そもそも . . .
  「同じ志をもって物事を行う集団」は誰かが所有できるべきものなのでしょうか