ブロックチェーン応用講座

Vol.1: ブロックチェーン

小林 聖弥 / Seiya Kobayashi

目次

目次

💻 PCセットアップ

- 次回以降のセッションに向けて、PCのセットアップを行いましょう
  - Vol.1: ブロックチェーン（レクチャー + ディスカッション）
  - Vols.2-3: スマートコントラクト（レクチャー + **コーディングワークショップ**）
  - Vol.4: ステーブルコイン（レクチャー + **コーディングワークショップ**）
  - Vol.5: AMM（レクチャー + **コーディングワークショップ**）
  - Vols.6-7: RWA（レクチャー + **コーディングワークショップ**）

- ✅ TODOs
  - インストール確認: Chrome・VS Code（・AIツール）
  - アカウント作成: Gmail・GitHub・MetaMask
  - インターネット回線確認: Google Meet

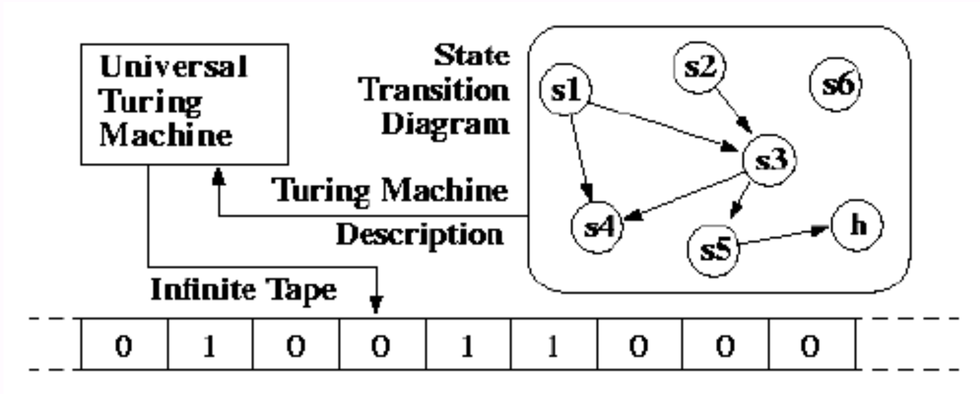
目次

1. ブロックチェーンとはなにか

ブロックチェーン = コンピューターネットワーク

- コンピューターとはなにか
  - **理論: チューリングマシン（1936）**
    - **計算 := 状態遷移** → 紙 + ペン（+ 理性的な頭脳）のみであらゆる計算は可能
    - アイデア:

      計算ルールと初期・途中状態を記録
      できる無限の長さのテープがあれば、
      あらゆる計算は模倣できる
      → 🤔 無限のテープをもってしても、
      計算できない問題は存在するのか？



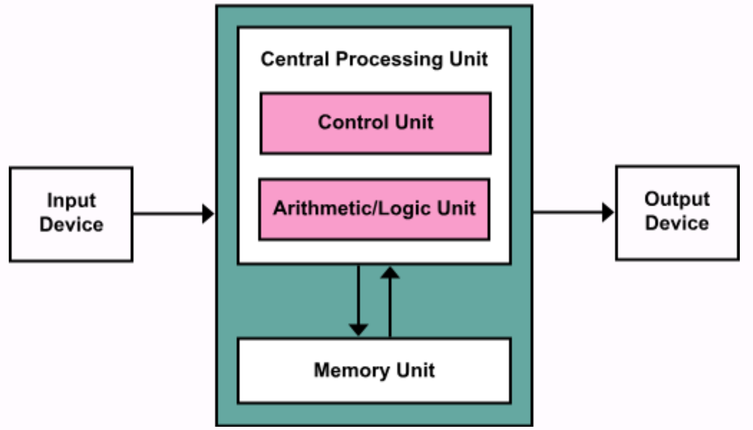
https://web.mit.edu/manoli/turing/www/turing.html

1. ブロックチェーンとはなにか

ブロックチェーン = コンピューターネットワーク

- コンピューターとはなにか
  - **実用: ノイマン型コンピューター（1945）**
    - **計算機械 := データ + プログラム**
    - アイデア: 汎用型コンピューターの構成要素は以下
      - CPU: e.g.）CU・ALU・レジスター
      - RAM（Random Access Memory）
      - I/O: e.g.）キーボード・ストレージ
      - Bus: データとプログラムで同一のバス

        → 🤔 問題点はあるか？



https://en.wikipedia.org/wiki/Von_Neumann_architecture

1. ブロックチェーンとはなにか

ブロックチェーン = 不特定多数により所有・実行されるコンピューターネットワーク

- 不特定多数のコンピューターが…
  - 所有するもの → **データ + プログラム**
  - 実行するもの → **プログラムによるデータの状態遷移（の計算）**

  → 🤔 どのようにデータが格納され、プログラムが実行されているのか？

- **分散性 ≠ 非中央集権性**
  - 分散的ネットワーク（e.g., AWSを用いた中央集権的なロードバランシング）

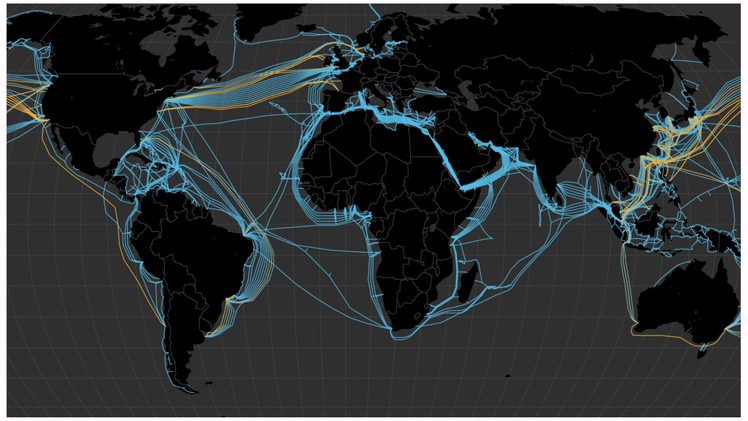
    → 分散処理アルゴリズム（e.g., MapReduce、Raft）によって成立
  - 非中央集権的ネットワーク（e.g., Bitcoin、Ethereum）

    → コンセンサスアルゴリズム（e.g., PoW、PoS）によって成立

1. ブロックチェーンとはなにか

余談: コンピューターによる通信の仕組み

1. 海底ケーブルモデル（大陸間通信の99%が利用）
    - コンピューター ↔ LAN ↔ WAN ↔ 海底ケーブル



The New York Times

2. 人工衛星モデル（e.g., Starlink）
    - コンピューター ↔ LAN ↔ アンテナ（Dish）↔ 人工衛星

3. Bluetoothモデル（e.g., BitChat）
    - コンピューター ↔ コンピューター
      → インターネット回線に依存しない
      → 🤔 問題点はあるか？

https://en.wikipedia.org/wiki/Starlink

目次

2. ブロックチェーンのユースケース

ワールドコンピューターであることが活きる条件 = トラストレスな連携（Trustless Coordination）

- 2種類の信用（トラスト）最小化対象
  - **仲介者**に対する信用の最小化
    → 単一障害点の排除、取引のスケーラビリティ向上・低コスト化
  - **取引者**に対する信用の最小化
    → 取引公平性の向上

→ 🤔 トラスト「レス」というが、本当に信用が不要なのか？
どこか別のものへ信頼を移しただけではないのか？

- 単純な計算・格納コストでは、**中央集権的サーバーの方が圧倒的にコストが低い**
  → ブロックチェーンを用いない方が理にかなったユースケースも数多くある

2. ブロックチェーンのユースケース

ブロックチェーンでない方が理想的なユースケース

- **一個人・一組織内で閉じた仕組み**（e.g., オンプレサービスの代替）
  → 仲介者・取引者ともに信用をおくことのリスクが低い

- **大量のデータを捌く・格納する必要がある仕組み**（e.g., AI推論、動画ストリーミング）
  → ブロックチェーンは大量のデータを格納するインフラとしては設計されていない
  → IPFS等のデータ格納に最適化された非中央集権プロトコルを用いる

- **秘匿性の高いデータを扱う仕組み**（e.g., KYC）
  → 現時点（2026年）では、ネイティブにプライバシーを保護する仕組みが存在しない
  → ゼロ知識証明等の現代暗号技術の応用が検討されている

2. ブロックチェーンのユースケース

金融領域（DeFi）

- ❌ **銀行ネットワークの非効率性**（ボトルネック = 取引の運用コスト）
  → 既存の決済プロバイダー（e.g., Stripe）が徴収する手数料の7割程度は銀行への手数料

- 関連する概念・技術
  - **ハイリスクDeFi**
    - 既存の金融取引（e.g., 為替、貸付、保険、デリバティブ）をオンチェーンで模倣
      → ブロックチェーンを用いた方が取引コスト・スケーラビリティともに改善
  - **ローリスクDeFi**
    - 法定通貨と価値を1:1で連動させた**ステーブルコイン**による送金・決済（🤔 どちらが難しい？）
      → 主に国際間決済・マイクロペイメント領域で既存の決済インフラに大きく勝る

2. ブロックチェーンのユースケース

サプライチェーン領域

- ❌ **利害相反の関係にあるステークホルダー**が多く存在

  → 仲介者に対する高い信用リスク、スケーラビリティの向上・低コスト化のインパクトの大きさ

- 関連する概念・技術
  - **RWA（Real-World Assets）**
    - 電気・カーボンクレジット等の現物資源をブロックチェーン上でトークン化し、DeFiの利点（e.g., スケーラビリティ・低コスト性・透明性）を活かす仕組み
  - **オラクル（Oracles）**
    - IoTで取得したセンシングデータ等の外部データをトレストレスな形でブロックチェーンへ提供する仕組み（e.g., Chainlink）

2. ブロックチェーンのユースケース

非中央集権的ID（Decentralized ID・DID）

- ❌ IDという概念は、あらゆるデジタルサービスを横断する**社会的デジタルインフラ**
  → 特定サービスへの依存は、大きなリスク（e.g., 単一障害点）となる
  → 24時間365日動き続けるブロックチェーン、個人レベルのデータ主権性は最適な手段

- 関連する概念・技術
  - **生体認証（e.g., World ID）**
    - 最も安全とされる認証方法で、指紋認証・顔認証・虹彩認証などが実用化されている
  - **ゼロ知識証明（Zero Knowledge Proofs）**
    - 特定の事実を秘匿しつつ、主張（計算）の正しさを証明できる暗号技術
      → e.g.）公的なIDデータを用いて、年齢を隠しつつ未成年でないことを対外的に証明する

2. ブロックチェーンのユースケース

ガバナンス

- ❌ 国や自治体、組織におけるガバナンスも**多様なステークホルダーの多い社会的インフラ**

  → ブロックチェーンの改竄不可能性・透明性・コスト的優位性が活きる

  → 🤔 オンライン選挙を実現するための技術インフラとして、

  パブリックブロックチェーンは最適か？実現にあたって何が難しそうか？

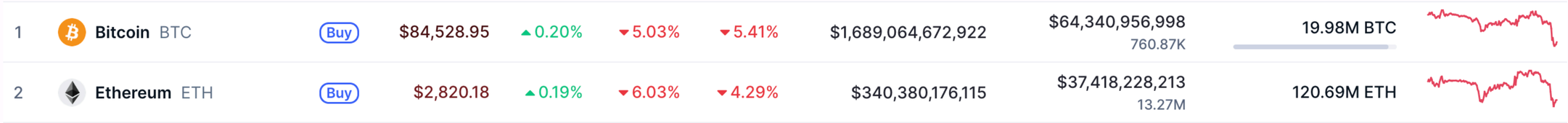
- 関連する概念・技術
  - **閾値署名（Threshold Signatures）**
    - 複数人の同意があってはじめて有効になる電子署名（e.g., 5-of-7）
  - **所属証明（e.g., マークルツリー）**
    - 特定の集団に所属していることを効率的に証明する暗号技術

目次

3. ブロックチェーンの仕組み

- パブリックブロックチェーンの二大巨頭（2026年）
  - **Bitcoin（2009〜）:= デジタルゴールド**
  - **Ethereum（2015〜）:= ワールドコンピューター**

- 両者の仕組みを以下の3つの側面から比較する
  1. **セキュリティ**
  2. **プログラマビリティ**
  3. **スケーラビリティ**



1	Bitcoin BTC	Buy	$84,528.95	▲0.20%	▼5.03%	▼5.41%	$1,689,064,672,922	$64,340,956,998 760.87K	19.98M BTC
2	Ethereum ETH	Buy	$2,820.18	▲0.19%	▼6.03%	▼4.29%	$340,380,176,115	$37,418,228,213 13.27M	120.69M ETH

3. ブロックチェーンの仕組み

1. セキュリティ

- **コンセンサスアルゴリズム（Consensus Algorithm）**
  - 管理者・仲介者なしに、**自律分散的に処理を実行する**ための仕組み（プロトコル）
    - **パーミッションレス**

      → 誰でも（プロトコル毎の条件を満たせば）ネットワークに参加できる
    - **経済的インセンティブ・ディスインセンティブ**

      → ネットワークに貢献（e.g., ブロックの生成・追加）すると報酬が貰える

      → 悪意のある行動（e.g., 51%攻撃）を仕掛けると、天文学的な経済的ダメージを負う
    - **アルゴリズム的に定義された挙動**

      → Mempool同期 → Tx選出 → ブロック生成 → ネットワークへの提案 → ブロック追加

      → 🤔 アルゴリズムは誰が決める？悪意のあるアルゴリズムに書き換えられたらどうなる？

3. ブロックチェーンの仕組み

1. セキュリティ

- コンセンサスアルゴリズムの比較の前に... **ハッシュ関数**とはなにか？
  - $h = f(x)$: 任意長の文字列xを入力値として取り、固定長の文字列hを返却する暗号学的関数
    1. **原像耐性（Pre-image Resistance）**
       - ハッシュ値hから、元の文字列xを計算することが暗号学的に難しいこと
    2. **第二原像耐性（Second Pre-image Resistance）**
       - 文字列xに対して、$h(x) = h(x')$となるようなx'を計算することが暗号学的に難しいこと
    3. **衝突耐性（Collision Resistance）**
       - $h(x) = h(x')$となるような文字列のペア$\{x, x'\}$を計算することが暗号学的に難しいこと

    → 🤔 攻撃者にとっては、1の計算が一番難しいが、2と3ではどちらが難しいか？

3. ブロックチェーンの仕組み

1. セキュリティ

- アナロジー: **誕生日のパラドックス**
  - 自分と同じ誕生日の人が50%以上の確率で1人以上存在するために必要な最低人数
    - $1 - (\frac{364}{365})^n \geq 0.5 \rightarrow n = 253$

      → 第二原像の計算量は2^n（nはハッシュ値のビット長）
  - 同じ誕生日の人が50%以上の確率で1ペア以上存在するために必要な最低人数
    - 23人いれば、253通りの組み合わせができる（$\frac{23 \cdot 22}{2}$）

      → 衝突を起こす組み合わせの計算量は$2^{n/2}$（nはハッシュ値のビット長）

→ 💡 攻撃者にとっては、**2の第二原像の計算の方が難しい**

3. ブロックチェーンの仕組み

1. セキュリティ

- コンセンサスアルゴリズムの比較
  - Bitcoin: **PoW（Proof of Work）**
    - ブロック追加の条件 = **ブロックマイニング**
      - 条件を満たすブロックヘッダーの組み合わせを**一番早く計算できた**1名（約10分毎）
        - ハッシュ関数を元にした条件: $SHA256(SHA256(block\_header)) < TARGET$
      - ブロック追加者には、ブロック毎に3.125 BTC（約4,000万円）の報酬
    - **発行上限額による価値の担保**
      - 発行可能総量: 2,100,000 BTC（既に200万BTC弱が発行済み）
      - 4年に1度の報酬半減期: 6.25 BTC (2020) → 3.125 BTC (2024) → 1.5625 (2028)
        - BTCは、マイニング以外の手段では新規発行されない

3. ブロックチェーンの仕組み

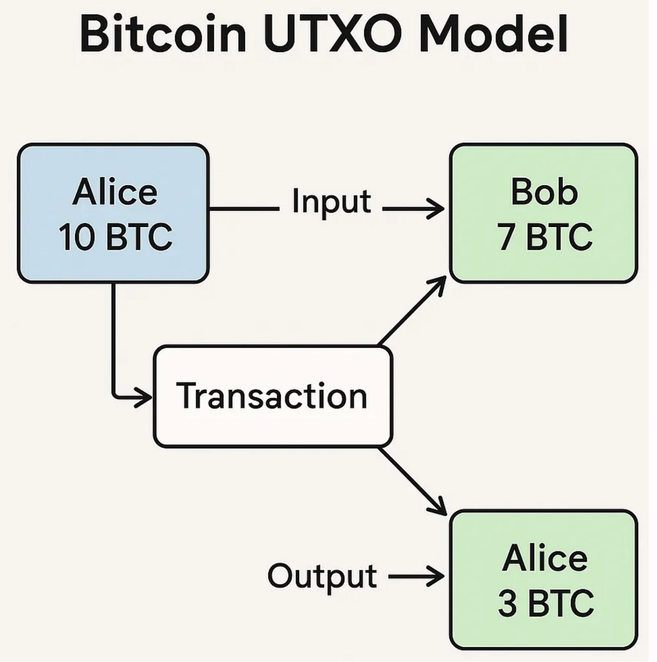
1. セキュリティ

- コンセンサスアルゴリズムの比較
  - Ethereum: PoW（〜2022）→ **PoS（Proof of Stake・2022〜）**
    - ブロック追加の条件 = **ETHのステーク & ランダム選出**
      - ランダム選出アルゴリズム（RANDAO）によってブロック提案者が選出（12秒毎）
        - ステークしたETH量（32ETH・1,400万円〜）に応じて重み付けが行われる
      - ブロック追加者には、ブロック毎に0.1 ETH（約5万円）程度の報酬
        - 実際には、MEV等の活用によってより多額の報酬が得られる
    - PoSへの移行によって**使用電力量を99.9%以上削減**
      - Bitcoin PoW: 年間約200TWh（オランダの年間電力消費量程度）
      - Ethereum PoS: 年間約0.01TWh

3. ブロックチェーンの仕組み

2. プログラマビリティ

- Bitcoin: 用途が限定された計算基盤
  - **基本的に送金BTC額の変動のみ**計算可能
    - **UTXO**（Unspent Transaction Output）と呼ばれる
      一度のみ使用可能なオブジェクトに基づく計算モデル
      → 🤔 お釣りはどう扱う？どのような利点・欠点がある？
  - BitVMと呼ばれる汎用計算基盤も導入できるが、
    複雑性の高さから大規模実用には至っていない

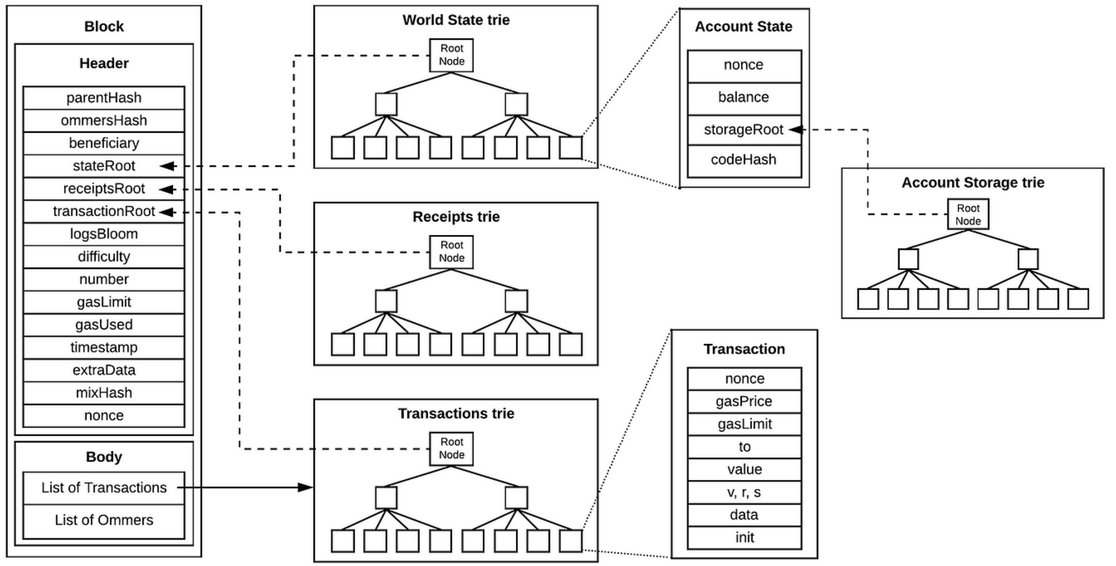


Medium

3. ブロックチェーンの仕組み

2. プログラマビリティ

- Ethereum: 汎用的な計算基盤
  - **Ethereum Virtual Machine**
    → 任意の計算を可能にする仮想マシン
    - 銀行口座残高に似たアカウントモデル
      → 🤔 どのような利点・欠点がある？
    - 任意のトークン（通貨）やアプリも
      柔軟に設計・発行・公開できる
      → e.g.）ステーブルコイン、NFT、SBT



Block, transaction, account state objects and Ethereum tries

Medium

3. ブロックチェーンの仕組み

3. スケーラビリティ

- Bitcoin
  - メインネット（Bitcoin L1）: 5~7 TPS（Transactions per Second）
  - ライトニングネットワーク（Bitcoin L2）:（理論的には）数百万 TPS

    → Bitcoin L1ネットワークの制約と、UXの低さからEthereum L2ほどは使われていない

- Ethereum
  - メインネット（Ethereum L1）: 12~20 TPS（Transactions per Second）
  - **Ethereum L2（e.g., Base, Arbitrum）: ~100,000 TPS**（🤔 これは十分？）

    → プログラマビリティ・インターオペラビリティの高さから世界中で利用されている

目次

4. ブロックチェーンの性質

1. セキュリティ

- **非中央集権性（Decentralization）**
  - パーミションレスなコンセンサスアルゴリズムによって担保
    → クライアント実装の多様性も重要なファクター（🤔 なぜ？）

- **変更不可能性（Immutability）**
  - ブロックチェーンに対する攻撃（e.g., 33%攻撃）の経済的コストによって担保

- **透明性（Transparency）**
  - 全ての取引は公開されるが、**誰がUTXO・アドレスの保有者であるかは分からない**

4. ブロックチェーンの性質

2. プログラマビリティ（Ethereumに限定）

- **スマートコントラクトによる処理の自動化（Automation）**
  - 全てのクライアントは、計算基盤であるEVMを用いてスマートコントラクトを実行する

- **トークン化（Tokenization）**
  - 各トークンの実体はスマートコントラクト
    → トークンに任意のロジックを持たせることができる
  - EIP（Ethereum Improvement Proposal）や、ERC（Ethereum Request for Comments）というグローバル規格に沿って実装されるため、**代替可能性**（Fungibility）が担保される
    → e.g.）ERC-20トークンは、他のERC-20トークンと技術的互換性がある

4. ブロックチェーンの性質

3. スケーラビリティ（Ethereumに限定）

- **コスト効率性（Cost Efficiency）**
  - 仲介者が存在しないため、管理・仲介コストがなく圧倒的に低い
    → 国際間送金であっても、実際の処理は単一のスマートコントラクト上の状態遷移のみ

- **取引スピード（Finality）**
  - 取引が確定するまでのスピードが極めて早い
    → 決済（認可→クリアリング→セトルメント）においては、即時セトルメントが可能
    → 🤔 即時セトルメントが実現できると何が良い？L1のFinalityはもっと遅いのでは？
  - 最先端の証明技術を用いると（理論的には）L2のTPSをさらに向上させることができる
    → マイクロ・ナノペイメント（0~1円の決済額）への応用

目次

5. ブロックチェーンの課題と解決策

🤔 **非中央集権性はどのように向上させられるか、どこまで向上させるべきか？**

- 具体的にどの部分が中央集権リスクが高いか？
- 理想的な非中央集権の程度・度合いは？
- 非中央集権化のトレードオフはあるか？

5. ブロックチェーンの課題と解決策

- 💡 解決策
  - 軽量クライアント・ステートレスクライアント
    - **DAS（Data Availability Sampling）**を応用して、クライアントの計算資源的制約を緩和
  - 最低ステーク額の低減
    - Vitalik: 32ETH（約1,400万円）→ **1ETH（約43万円）**程度が理想的
  - PBS（Proposer-Builder Separation）
    - 計算資源の多いバリデーターが、MEV経由でより多くのETHを手に入れられる状況を緩和
  - クライアント実装の多様化・形式検証
    - **形式検証された複数団体・言語による実装**がそれぞれ同割合で利用されている状態が理想的

- ❓ 潜在的課題
  - 閾値署名（i.e., BLS）はバリデーター数の増加にどこまで耐えられるか

5. ブロックチェーンの課題と解決策

- ⚠️ **量子耐性（Quantum Resistance）**
  - 汎用型量子コンピューターの実現によるセキュリティ崩壊危機
    → ❌ Ethereumが電子署名で利用しているECDSAには量子耐性がない（🤔 何が問題？）

- 💡 解決策
  - **耐量子電子署名（Post-Quantum Digital Signatures）**
    - ハッシュベース署名（XMSS）、格子ベース署名（Falcon）
  - **Lean Consensus（Ethereum）**
    - 耐量子電子署名とハッシュベースのzkVMを組み合わせた未来のEthereum設計図

- ❓ 潜在的課題
  - スケーラビリティは担保できるのか

5. ブロックチェーンの課題と解決策

- ⚠️ **ユーザープライバシー**
  - 誰がどのアドレスを保有しているかはわからない（🤔 何が問題？）
  - 秘匿性の高いデータは暗号化してオンチェーンに置けば良いのでは？（🤔 何が問題？）

- 💡 解決策
  - **ステルスアドレス（ERC-5564）**
  - **ゼロ知識証明（ZKP）**

- ❓ 潜在的課題
  - 各国の金融規制（e.g., KYC/AML）にどう対応するか
  - プライバシー技術の導入によるオーバーヘッド

5. ブロックチェーンの課題と解決策

- ⚠️ **低いUX**
  - クリプトウォレット（e.g., MetaMask）の管理の煩雑さ
  - オンランプ（法定通貨 → 暗号通貨）・オフランプ（暗号通貨 → 法定通貨）の障壁

- 💡 解決策
  - ERC-4337規格
    - アカウント抽象化: ウォレットレスなアカウント管理（e.g., 生体認証、Googleログイン）
    - ガス代抽象化: ガス代スポンサー・任意のERC-20トークンでのガス代支払い

- ❓ 潜在的課題
  - アカウント復旧方法はどうするか（e.g., デバイス紛失時）