ブロックチェーン応用講座

Vol.4: トークン

小林 聖弥 / Seiya Kobayashi

目次

1. トークンとはなにか

2. さまざまなトークン規格

3. ステーブルコインの仕組み

💻 ワークショップ #1: インターフェースを理解しよう

💻 ワークショップ #2: ERC-20ベースのステーブルコインに触れてみよう

目次

1. トークンとはなにか

2. さまざまなトークン規格

3. ステーブルコインの仕組み

 ワークショップ #1: インターフェースを理解しよう

 ワークショップ #2: ERC-20ベースのステーブルコインに触れてみよう

1. トークンとはなにか

トークン := **なにかしらの価値**を表すもの

現実社会におけるトークン

- 通貨（e.g., 日本円）
  → 国家が発行・価値担保
- 権利（e.g., 航空券）
  → 発行体が権利の行使を保証
- 証明（e.g., 卒業証明書）
  → 発行体が有効性を保証

ブロックチェーンにおけるトークン

ネイティブトークン = ETH

- 発行体: **Ethereum**
  → 🤔 誰にどのように発行？
- 用途: **PoS・ガス代**
  → 投機用途はあくまで副作用

非ネイティブトークン

- 発行体: **誰でも**
  → 実体は**スマートコントラクト**
- 用途: **通貨・権利・証明・資源**
  → 投機用途はあくまで副作用
  → 🤔 誰が価値を担保する？

1. トークンとはなにか

非ネイティブトークン := スマートコントラクト

- **スマートコントラクト := ブロックチェーン上のプログラム**
  → EOA（i.e., ECDSAの鍵ペア）であれば、誰でもデプロイ（公開）できる
  → デプロイされたスマートコントラクト内のデータは、誰でもアクセスできる

- **オブジェクト指向**: スマートコントラクトとしてトークンをどのように表現するか
  1. **性質・データ**: スマートコントラクトにおける状態（ステート）
     - 単位（e.g., 1JPYC = 1円、1KWT = 1kWh）
     - 所有者（e.g., Aさんが10,000トークン、Bさんが50,000トークン）
  2. **効用・挙動**: スマートコントラクトにおける関数
     - 送付（e.g., BさんからAさんに10,000トークン送付）

1. トークンとはなにか

🗣️ トークンの仕組みから各種概念を再考する

Q1: 各種トークンデータはウォレットに格納されている？

→ 🤔 格納されていない場合、どこに格納されている？ウォレットは何を保有している？

Q2: アカウントの秘密鍵を紛失すると、保有トークンのデータは削除される？

→ 🤔 秘密鍵を復旧する方法はある？削除されない場合、何かしらのリスクはある？

Q3: 存在しないアカウントアドレスにトークンを送付することはできる？

→ 🤔 そもそもアカウントが存在するとは？送付されたトークンは誰がどのように動かせる？

目次

1. トークンとはなにか

2. さまざまなトークン規格

3. ステーブルコインの仕組み

💻 ワークショップ #1: インターフェースを理解しよう

💻 ワークショップ #2: ERC-20ベースのステーブルコインに触れてみよう

2. さまざまなトークン規格

ERC（Ethereum Request for Comments）:= スマートコントラクト実装に関する標準規格

- EVMチェーンでは、さまざまな標準実装規格（実装インターフェース）が定められている
  - **相互運用性（interoperability）**の担保

    → 相互運用性がないと、複数コントラクトを跨る実装（e.g., 為替）が煩雑になってしまう
  - **開発コスト**の削減

    → 各々が同じような実装を繰り返すことのマクロ経済的合理性がない
- トークン規格は大きく分けて2つに分類される
  1. **代替可能性トークン（Fungible Token・FT）**

     → 1つのトークンは他の1つのトークンと、その価値において代替できる（e.g., 通貨）
  2. **非代替可能性トークン（Non-Fungible Token・NFT）**

     → 各トークンはそれぞれ唯一の価値を保有する（e.g., デジタルアート）

2. さまざまなトークン規格

ERC-20（FT）

- 特徴
  - **トークン毎の残高**
    → 関数 balanceOf の実装
  - **トークン送付ロジック**
    → 関数 transfer・transferFrom の実装
  - **分割可能性**
    → 関数 decimals の実装
- ユースケース: ステーブルコイン、RWA

ERC-721（NFT）

- 特徴
  - **ユニークなトークンID**
    → 同じメタデータでも異なるIDを持つ
  - **トークンと所有者（アドレス）の紐付け**
    → 関数 ownerOf の実装
  - **分割不可能性**
    → 所有するかしないかの2択のみ
- ユースケース: 不動産、カーボンクレジット

目次

1. トークンとはなにか

2. さまざまなトークン規格

3. ステーブルコインの仕組み

💻 ワークショップ #1: インターフェースを理解しよう

💻 ワークショップ #2: ERC-20ベースのステーブルコインに触れてみよう

3. ステーブルコインの仕組み

ステーブルコインには複数の実装手法（i.e., 価値担保手法）がある

裏付け資産担保型

- 特徴
  - 価値担保: **100%以上の裏付け資産**
    → e.g.）現金、国債、暗号資産（BTC）
  - トークン規格: ERC-20ベース
  - 最も幅広く使われている手法
    → e.g.）USDC、USDT、EURC、JPYC
- 🤔 リスク？

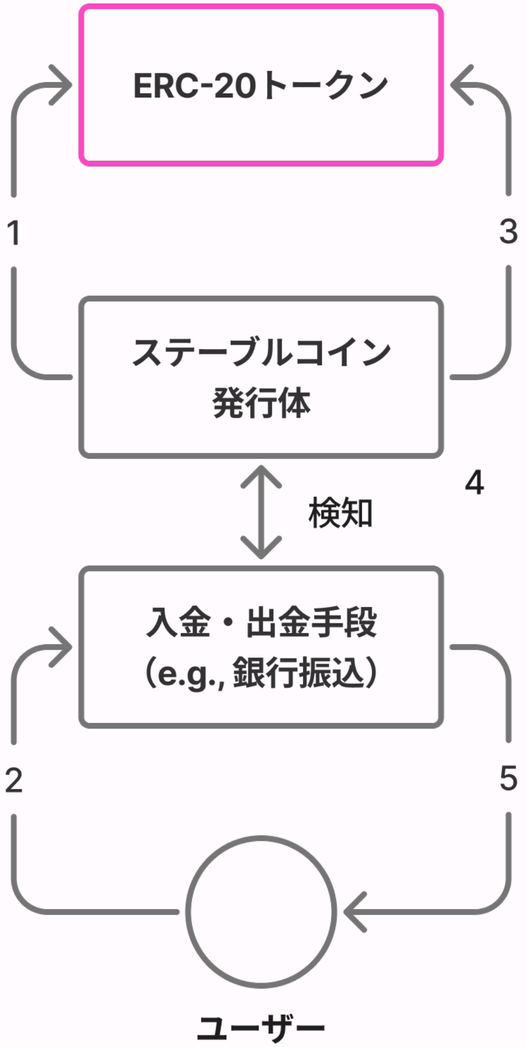
アルゴリズム型

- 特徴
  - 価値担保: **スマートコントラクト**
    - 独自トークンの価値で裏付け
      → e.g.）1UST = $1 of LUNA
    - 裁定取引によるインセンティブ
      → UST↘: UST購入 & LUNAへ交換
- 🤔 リスク？
  → LUNAショック（2022年）

3. ステーブルコインの仕組み

裏付け資産担保型ステーブルコイン := ERC-20トークン

1. ERC-20ベースのスマートコントラクトのデプロイ
   → デプロイ時点で一定額を発行（mint）する場合もある
2. **ユーザーから法定通貨（e.g., 日本円）を預かる**
   → ここで預かる通貨が裏付け資産となる
3. **ユーザーのアドレスに対してステーブルコインを送付**
   → 預かった金額に応じた額を送付
4. 2の預かり資産を運用（100%以上担保）
   → 運用益がステーブル発行体の主な収益源となる
5. **ユーザーがステーブルコインを償却すると、法定通貨が返却される**
   → ステーブルコインは焼却（burn）される



目次

1. トークンとはなにか

2. さまざまなトークン規格

3. ステーブルコインの仕組み

💻 ワークショップ #1: インターフェースを理解しよう

💻 ワークショップ #2: ERC-20ベースのステーブルコインに触れてみよう

💻 ワークショップ #1: インターフェースを理解しよう

$ git pull origin main を実行 → ./lectures/4/README.md へ

目次

1. トークンとはなにか

2. さまざまなトークン規格

3. ステーブルコインの仕組み

💻 ワークショップ #1: インターフェースを理解しよう

💻 ワークショップ #2: ERC-20ベースのステーブルコインに触れてみよう