日本銀行 第5回 FinTech フォーラム


# Ethereum ブロックチェーンに関する技術動向

カレンシーポート株式会社
代表取締役・CEO　杉井　靖典

2018年2月7日

# 代表取締役・CEO 杉井 靖典 - プロフィール

## カレンシーポート株式会社 - CurrencyPort Limited


- ✓ 経済産業省　ブロックチェーン検討会　委員
  システム評価軸整備検討委員会　委員
- ✓ 日本銀行　決済システムフォーラム　プレゼンター
  FinTechフォーラム　プレゼンター
- ✓ 全国銀行協会　ブロックチェーン活用可能性検討会　委員
  ブロックチェーン研究会　メンバー
- ✓ ブロックチェーン推進協会（BCCC）副代表理事
- ✓ 日本ブロックチェーン協会　正会員
- ✓ FinTech協会　会員

【著書】

- ✓ いちばんやさしいブロックチェーンの教本
- ✓ 書籍「ブロックチェーンの衝撃」
- ✓ ムック「ブロックチェーン＆ビットコイン入門編」

# Ethereumの開発コミュニティ

## EIP (Ethereum Improvement Proposal)とERC (Ethereum Request for Comment)

「EIP」と「ERC」は、ともに、GitHubでチケット管理されている技術提案
https://github.com/ethereum/EIPs/issues

「EIP」は、Ethereumのシステム全体に関わる様々な改善提案全般
「ERC」は、Ethereum上で動作するスマートコントラクトにより実現される機能の実装に関する標準仕様の提案（プロジェクトの自由意思で採択可能な技術提案）

EIP ⊇ ERC（ERCはEIPの部分集合）

コアデベロッパー同士によるオンライン会議「Core Devs Meeting」が定期的に開催されており、議題とされた提案の承認を得る。この模様はYouTube上でライブ放送され、世界中のだれもが自由に視聴・参加できるオープンな場となっている
https://www.youtube.com/channel/UCNOfzGXD_C9YMYmnefmPH0g

# Ethereum上に発行するトークンの標準仕様提案

CurrencyPort

## ERC20

Ethereum Token Standard（現時点で最もシェアの高いトークンの表現仕様）
EOA（Externally Owned Account）と呼ばれる、利用者アカウント（≠コントラクト）宛にのみ送信可能

## ERC223

ERC20の改良提案。誤ってトークンを取扱えないスマートコントラクトのアドレス宛にトークンを送信してしまうと、トークン移動ができなくなってしまう不具合（ゾンビトークン）の問題を解決する提案
トークンを受取れないコントラクトアドレスに送ってしまった時、送り主にトークンを戻す機能を追加

## ERC777

ERC20として振舞いながら、トークンを送受信できるスマートコントラクト用のインターフェイスを定義

## ERC721

ERC20、ERC223、ERC777 がそれぞれFungible Token（代替可能なトークン）を定義した規格であるのに対し、ERC721は、Non-Fungible Token（代替不可能なトークン）を定義するために提案された規格

※トークン様式に関する標準提案は、これら以外にもいくつか存在します

# 代替可能なトークンと代替不可能なトークン

## 代替可能なトークン（Fungible Token） ERC20、ERC223、ERC777

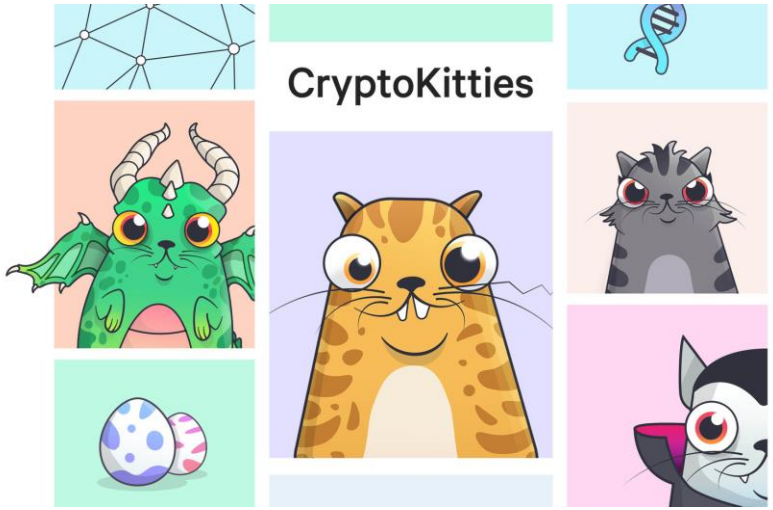
通貨、証券、ポイント、スタンプ、クーポン等
保有している数量のみで、価値の評価が可能なトークン

## 代替不可能なトークン（Non-Fungible Token） ERC721

不動産の権利、座席の予約券、ゲームのアイテム、くじ引き抽選券等
他のリソースと代替不可能で、個別に価値の評価をすべきトークン

IPSF等、外部のP2P分散ストレージに配置したドキュメントと連携して
個別の価値を表現可能

事例）CryptoKitties
⇒　人気でEthereumのトラフィックを占有してしまったため
　　現在では、専用のブロックチェーンに移行



# 識別可能な資産の登記（Distinguishable Asset Registries）EIP821

CurrencyPort

## ブロックチェーン上の物理的またはデジタルの識別可能なアイテムの所有権を追跡する仕組み

代替不可能なトークン（NFT: Non-Fungible Token） ERC721 に対する所有者とその資産を参照するスマートコントラクト

例）不動産の権利登記、美術品のオーナー確認、ゲームアイテムの所有者確認

- ✓ NFT（ブロックチェーン上の資産の表現）… 265bits ハッシュ値
- ✓ DAR（その資産を登録するコントラクト）… 160bits アドレス

**URIの表現様式**

```
nft://<chain's common name>/<DAR's address>/<NFT's ID>
```

**URIの表現例**

```
nft://ethereum/0xF87E31492Faf9A91B02Ee0dEAAd50d51d56D5d4d/0xfaa5be24e996feadf4c96b905af2c77c456e2debd075bab4d8fd5f70f209de44
```

参照：**ERC721** … Identify （人間、グループ、オブジェクト、およびマシンに対する一意のID付け）

# 仲裁標準（Arbitration Standard）ERC792

## 仲裁可能契約 (Arbitrable contract)と、仲裁人契約 (Arbitrator contract)に関する標準提案

- ✓ 仲裁の判決と執行の役割を分離する目的で制定された標準
- ✓ 仲裁可能なコントラクトには標準の仲裁機構を配置せず、利用者が仲裁人サービスを提供するコントラクトを選択可能とする
- ✓ 仲裁可能なコントラクトには、紛争を起こすために必要な仲裁費用や、異議申し立てに必要な控訴費用が設定される。利用者はこれを基に、紛争を新規に起こしたり、異議申し立てにより控訴したりすることができる
- ✓ 仲裁可能なコントラクトは、仲裁人サービスを提供するコントラクトによって与えられた裁定が強制的に適用される
- ✓ 証拠の取扱いについては、別のERCの対象となるべき（未着手）

↓

**ADR手続きの自動化**

# Ethereum のハードフォーク

## ブロックチェーンの永続的な分岐による仕様変更

新規コインは生まれない

- ✓ **計画的なアップデートによる公式のハードフォーク**
  ⇒次ページ参照

- ✓ **ブロックチェーンの存続にかかわる思想分裂によるハードフォーク**
  例）The DAO Attack の流出事件巻き戻し
  ETH(Ethereum) … 巻き戻し許容派
  ETC(Ethereum Classic) … 巻き戻し拒絶派

新規コインが生まれる

- ✓ **アルトコインを新規生成するためのハードフォーク**
  例）Ether Zero
  取引承認時間の短縮、取引承認にマスターノードを置く、取引手数料なし
  ただし、存在目的を含めてその是非が問われている

# Ethereum の計画的なアップデートによる公式のハードフォーク

## プロトコルを改善するために参加者の賛同を得て実行される仕様変更

- ✓ **Frontier（フロンティア）** 2015-07-15～
  - 基本的な機能の実証実験の開始
- ✓ **Homestead（ホームステッド）** 2016-03-14～
  - より多くの人が利用できる環境へのアップデート
  - マイニングの難易度調整アルゴリズムの変更
- ✓ **Metropolis（メトロポリス）**
  - Proof of WorkからProof of Stake への移行準備
  - □ **Byzantium（ビザンチウム）** 2017-10-16～
    - 匿名性の強化
    - マイニングの難易度調整アルゴリズムの変更
  - □ **Constantinople（コンスタンチノープル）** 未定
- ✓ **Serenity（セレニティ）** 未定
  - Proof of WorkからProof of Stakeへの移行完了

ハードフォークしても
新たなコインを生まない工夫

**ディフィカルティ・ボム**
**難易度調整爆弾**

古いプロトコルのマイニング難易度を
ブロック生成毎に指数級数的に上げる

⇒ **アイスエイジ（氷河期）**

# Ethereumのスケーラビリティ向上対策（「Raiden」プロジェクト）

CurrencyPort

## オフチェーン処理技術によりペイメント機能の能力を大幅に拡張する

✓ **μRaiden**
- Raiden Networkを利用しトラストレスな当事者間支払い機能の拡張（1:n）
- 1秒以内の取引完了と手数料の圧縮（1/100以下）

✓ **Raiden Network**
- Ethereum版のセカンドレイヤー技術
- μRaidenを相互接続してネットワーク化、複数の第三者を経由してルーティング
- ペイメントチャンネルを開く際に利用者の資金をデポジット（ロック）する

✓ **raidEX**
- Raiden Networkを利用した分散型取引所
- 複数トークン間アトミックスワップの実現(DVP)

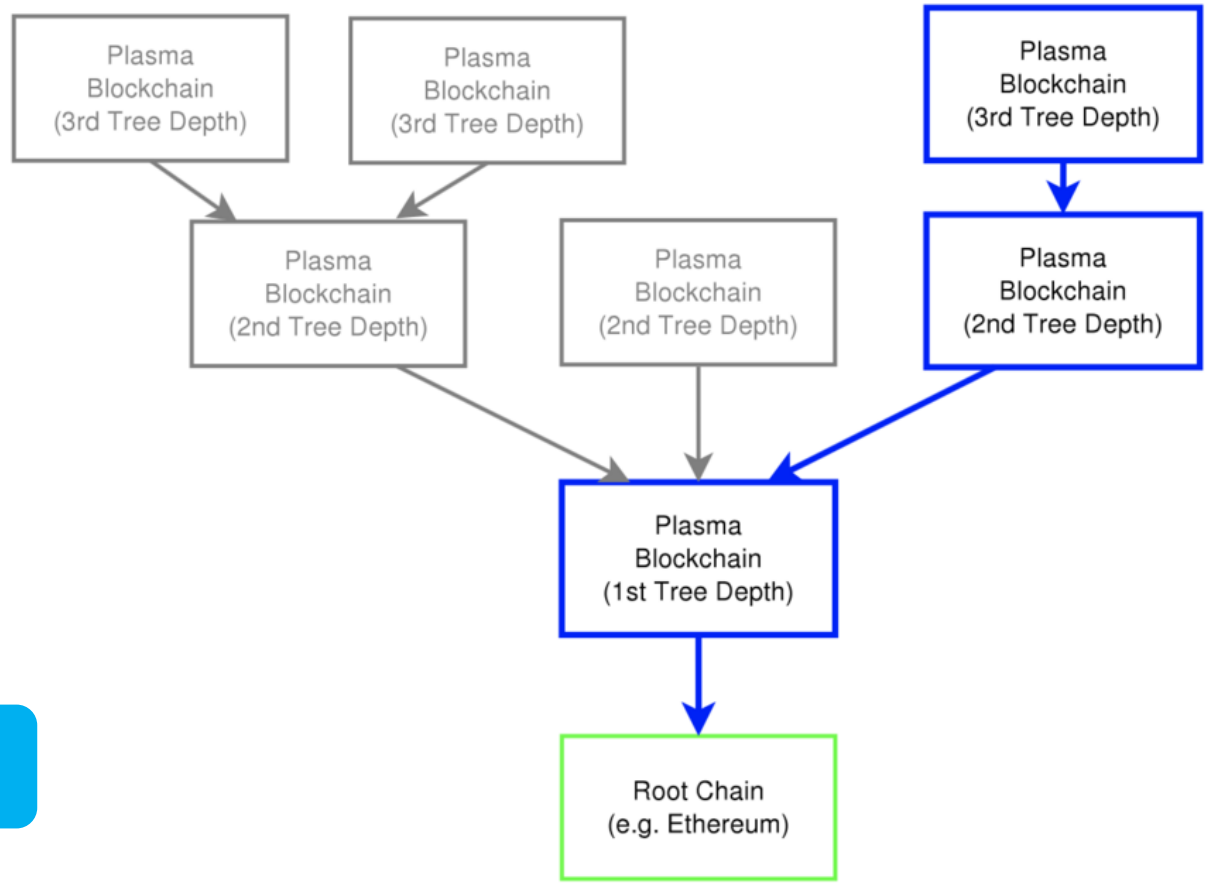
※課題：最新のステートを保持している参加者の誰かがオンラインである必要がある
インフラ維持のためのインセンティブモデル設計が難しい

# Ethereumのスケーラビリティ向上対策（「Plasma」プロジェクト）

## ブロックチェーンネットワークの階層化によりトランザクション処理能力を大幅に拡張する

- ✓ オフチェーン処理ではなくブロックチェーンを階層化して並列処理を行うアプローチ
- ✓ Ethereumのルート・ブロックチェーンに保存されるデータサイズは減少する
- ✓ トランザクション手数料が減少
- ✓ トランザクションの実行速度が向上
- ✓ スマートコントラクト実行速度の向上

**1秒間に数十億のトランザクション実行を目指す**

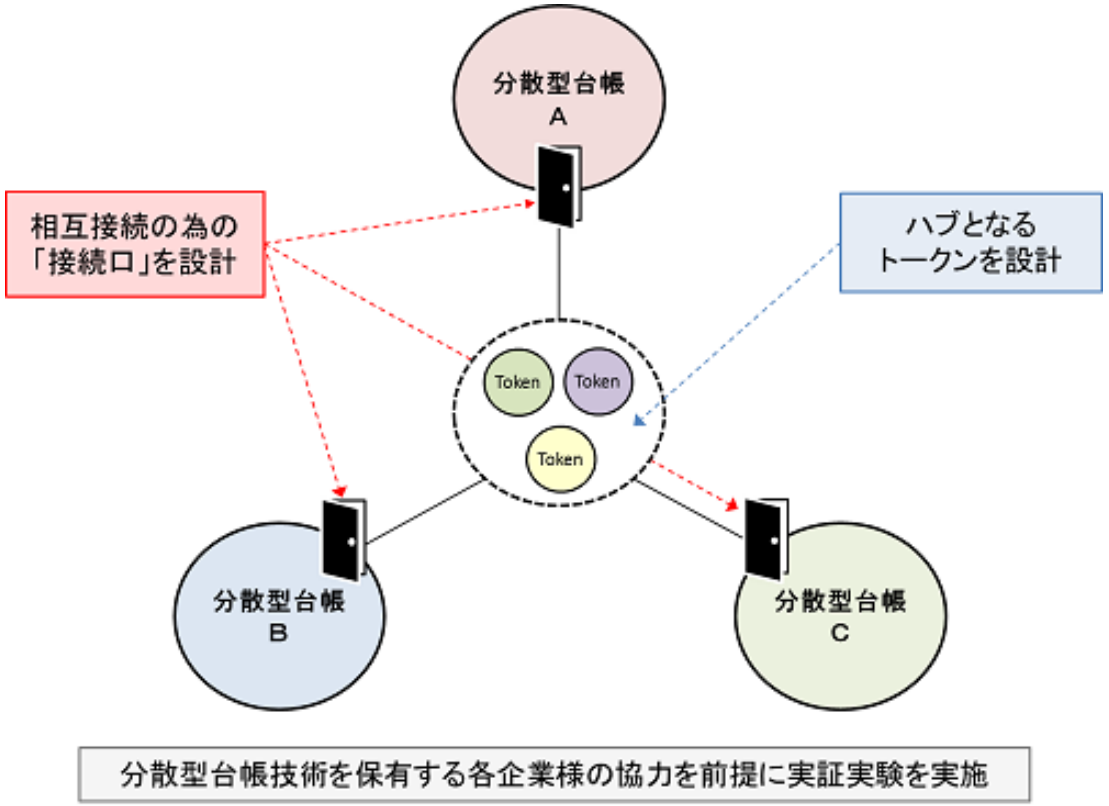


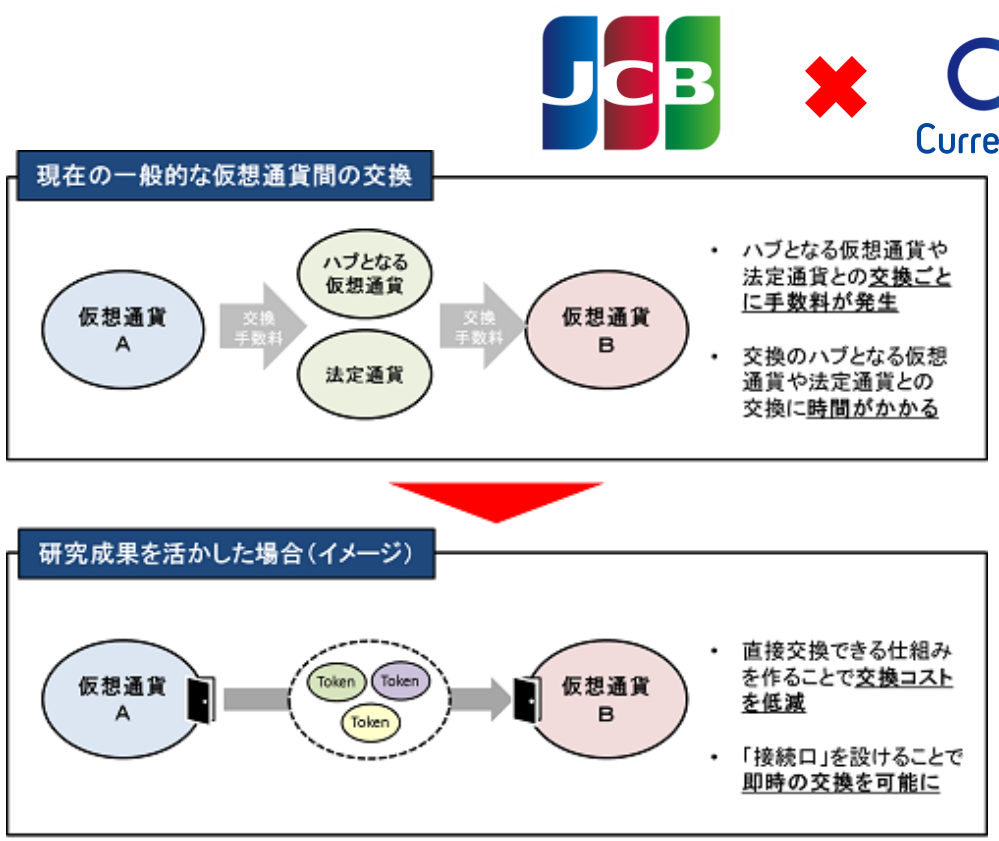

課題：withholding attack（Plazmaのブロックをわざと承認しない攻撃）

出典：https://plasma.io/plasma.pdf

# 異種ブロックチェーン間のインターオペラビリティとスケーラビリティ

## ブロックチェーンネットワークの相互接続により運用柔軟性の高いネットワークを構築する




**国内のブロックチェーン・コア開発ベンダー10社程度による共同研究コンソーシアム化を想定**