Web3のアプリケーションと用語解説

2022.11.30

Internet Week 2022

C71 Web3の羅針盤

慶應義塾大学大学院 政策・メディア研究科

阿部涼介

自己紹介

SFC KEIO UNIVERSITY

阿部涼介 (あべ りょうすけ, chike)

- 修士（政策・メディア）
- 慶應義塾大学大学院 政策・メディア研究科 特任助教 (2022.4 ~)
- WIDE Project Board Member (2022.3 ~)

- 2016年よりブロックチェーン関連技術の研究に従事
  - （金融以外も含めた）ブロックチェーン応用のために求められる周辺技術を含めたアーキテクチャ

- **Fabchain: Managing Audit-able 3D Print Job over Blockchain** (2022)
  - Ryosuke Abe, Shigeya Suzuki, Kenji Saito, Hiroya Tanaka, Osamu Nakamura, Jun Murai
  - IEEE International Conference on Blockchain and Cryptocurrency 2022
- **Ethereum に基づいたアプリケーションの実行時間定式化の検討と計測** (2020)
  - 阿部涼介, 鈴木茂哉
  - 研究報告 マルチメディア通信と分散処理 (DPS) 2020
- **Mitigating Bitcoin Node Storage Size by DHT** (2018)
  - Ryosuke Abe, Shigeya Suzuki, Jun Murai
  - The Asian Internet Engineering Conference 2018
- **Attack Incentive and Security of Exchanging Tokens on Proof-of-Work Blockchain** (2018)
  - Ryosuke Abe, Keita Nakamura, Kentaro Teramoto, Misato Takahashi
  - The Asian Internet Engineering Conference 2018
- **Storage Protocol for Securing Blockchain Transparency** (2018)
  - Ryosuke Abe, Hiroki Watanabe, Shigeru Fujimura, Atsushi Nakadaira
  - The 1st IEEE International Workshop on Secure Digital Identity Management Workshop in COMPSAC 2018
- **パーソナルファブリケーション時代における Blockchain を用いた製造情報保存システム** (2017)
  - 阿部涼介, 斉藤賢爾, 村井純
  - マルチメディア, 分散協調とモバイルシンポジウム 2017

混迷を極めるWeb3関係の用語

- 本来技術用語は標準化団体等で慎重に議論して進められる
  - やったもん/提案したもん勝ちの現状
  - オレオレ専門用語が飛び交い理解が難しい面がある

- 本講演では、取り沙汰されるアプリケーションの説明をしながら必要な用語を適宜補う
  - ただしこれらの用語も完全に定まったものではない

そもそも「Web3」も…

- Web1.0/Web2.0に関して元々の定義を歪めてWeb3と対比させてる議論も散見される
  - Tim Berners-Leeはブロックチェーンベースのアプリケーション等を「Web3」と呼ぶことに批判的[1]

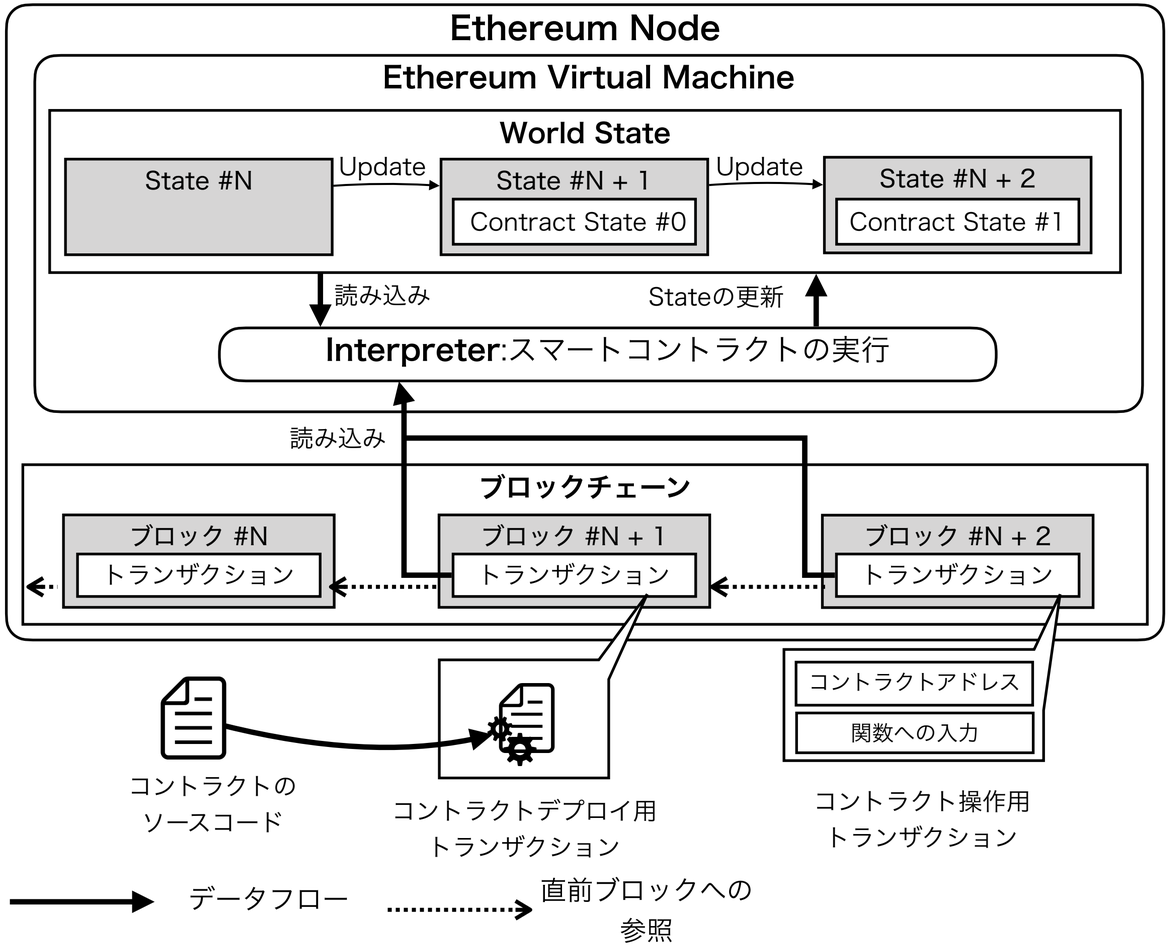
- Web3.0(Semantic Web)とWeb3
  - 「Web3は最近のWeb3.0はSemantic Web」という主張
  - ただの表記揺れであって、そんな綺麗に分かれてない
  - 初期の提唱者Gavin Woodは「Web3.0」と表記 [2]

- これらの明確な定義を追い求めるよりも個々のアプリケーションそれぞれの有用性および課題を議論するべき
  - 「ブロックチェーンをどのように活用できるか？」という問い

[1] Ryan Browne, Web inventor Tim Berners-Lee wants us to ‘ignore’ Web3: ‘Web3 is not the web at all’, 2022, https://www.cnbc.com/2022/11/04/web-inventor-tim-berners-lee-wants-us-to-ignore-web3.html
[2] Gavin Wood, ĐApps: What Web 3.0 Looks Like, 2014, https://gavwood.com/dappsweb3.html

ブロックチェーンでできること

- あるブロックが存在した時点での特定データの存在証明
  - 改竄困難
  - 全ノードへのレプリケーションによる永続化
- コード/その実行命令を存在証明
  - 事前に記述された特定プロセスの自動実行
  - 実行結果の存在証明
- c.f., 阿部のブログ記事「ブロックチェーンでそんなことはできない」[2]
  - ブロックチェーンの定義とその特性、取り沙汰される応用の正当性に関する議論



Ethereumにおけるプログラム(コントラクト)とプログラムの実行

[2] 阿部涼介, ブロックチェーンでそんなことはできない, 2022, https://chike0905.hatenablog.com/entry/2022/05/27/103801

取り沙汰されるアプリケーション

- トークン
  - 仮想通貨
  - NFT (Non-Fungible Token)
  - その他トークンの機能/用途による分類
    - ガバナンストークン
    - ユーティリティトークン
- トークンの交換プロトコル
  - DeFi (Decentralized Finance)
- 組織運営の自動化
  - DAO (Decentralized Autonomous Organization)

仮想通貨

- Bitcoinから始まる「The ブロックチェーンのアプリケーション」
  - コインの支払い処理をブロックチェーン上に記録する

- 次第に「ブロックチェーンに組み込まれている通貨」以外の通貨（=トークン）が登場
  - トークン: 価値(など)を代替する何か

> • Token
>
> 1. a round piece of metal that you use instead of money in some machines
> 2. formal something that represents a feeling, fact, event etc
>
> ロングマン英英辞典より

- 様々な機能をトークンのコードに仕込むことで、多様なアプリケーションが期待された
  - Token Economics: トークンを用いた経済圏を作り出し、ゲーミフィケーション等で目的の達成を促すようなスキーム
    - トークンに価値(価格)があること前提となるケースが散見される
  - トークンを実現するためのブロックチェーン上のプログラムの標準としてEIP-20などがある

EIPとERC

- **EIP** (Ethereum Improvement Proposals): Ethereumの仕様決定のための企画文書群 [1]
  - **ERC** (Ethereum Request for Comments): EIPの中でもアプリケーションレベルのプロトコルを規定するための文書
    - ERCに分類される文書の中で定義されるコントラクトを「ERC-(EIP番号)」と呼ぶ

- さまざまなタイプのトークンの仕様などが定義されている
  - ERC-20: トークンのためのコントラクト [4]
  - ERC-721: 代替不可能なトークンのためのコントラクト [5]
  - ERC-1155: 代替不可能/可能なトークン両方を扱うコントラクト [6]

- Ethereum以外でも、EVM互換のコントラクトランタイムを持つブロックチェーンでは同一の仕様を用いてコントラクトが実装できる

[3] Martin Becze, Hudson Jameson, et al., EIP-1: EIP Purpose and Guidelines, 2015, https://eips.ethereum.org/EIPS/eip-1
[4] Fabian Vogelsteller, Vitalik Buterin, EIP-20: Token Standard, 2015, https://eips.ethereum.org/EIPS/eip-20
[5] William Entriken, Dieter Shirley, Jacob Evans, Nastassia Sachs, EIP-721: Non-Fungible Token Standard, 2018, https://eips.ethereum.org/EIPS/eip-721
[6] Witek Radomski, Andrew Cooke, Philippe Castonguay, James Therien, Eric Binet, Ronan Sandford, EIP-1155: Multi Token Standard, 2018, https://eips.ethereum.org/EIPS/eip-1155

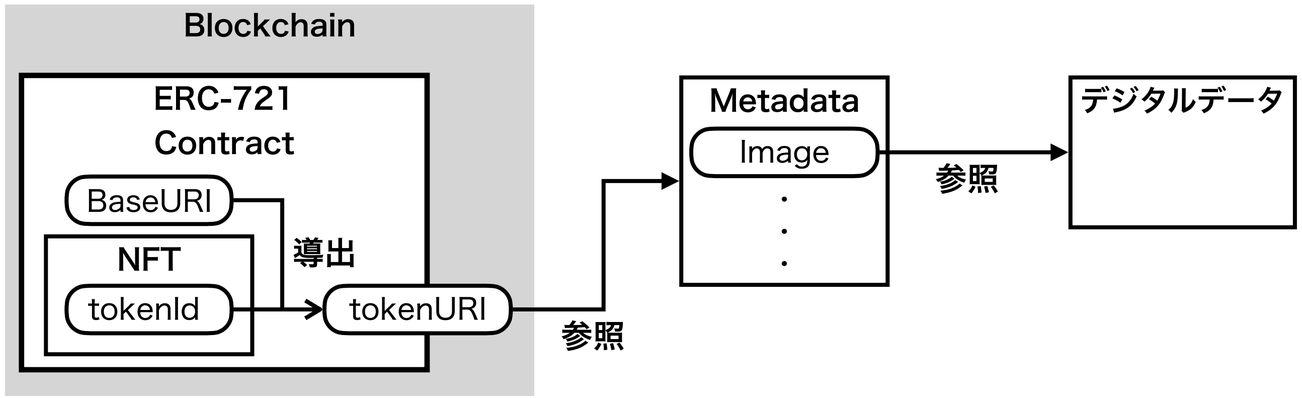
Non-Fungible Token (NFT)

- それぞれのトークンを識別可能にしたトークン
  - Bitcoinは1BTCであればどのトークンであっても同一の1BTCとして扱う
  - 一般的にNFTでは個々のトークンを「TokenId」と呼ばれる識別子で識別する
    - EIP-721で定義されるNFTでは、それぞれのトークンの識別子は1つのスマートコントラクトの中では一意

- デジタルアートやゲームのアイテムといったデジタルデータ、現実世界の様々な権利などを表現できると期待されている
  - トークンの所有権転移は代替可能なトークン同様、ブロックチェーンに記録されたプログラムに応じて実行される
  - 転移時に元々の発行者へ一定のロイヤリティを払い出す、などの仕組みを組み込むことが可能

NFTとデジタルデータの結びつき

- NFTは「特定コントラクト内において」tokenIdで識別される
  - 広く参照される実装では、コントラクト内に定義されたBaseURIとtokenIdを結合した値でブロックチェーン外のMetadataを参照する [7]
  - Metadataからデジタルデータを参照



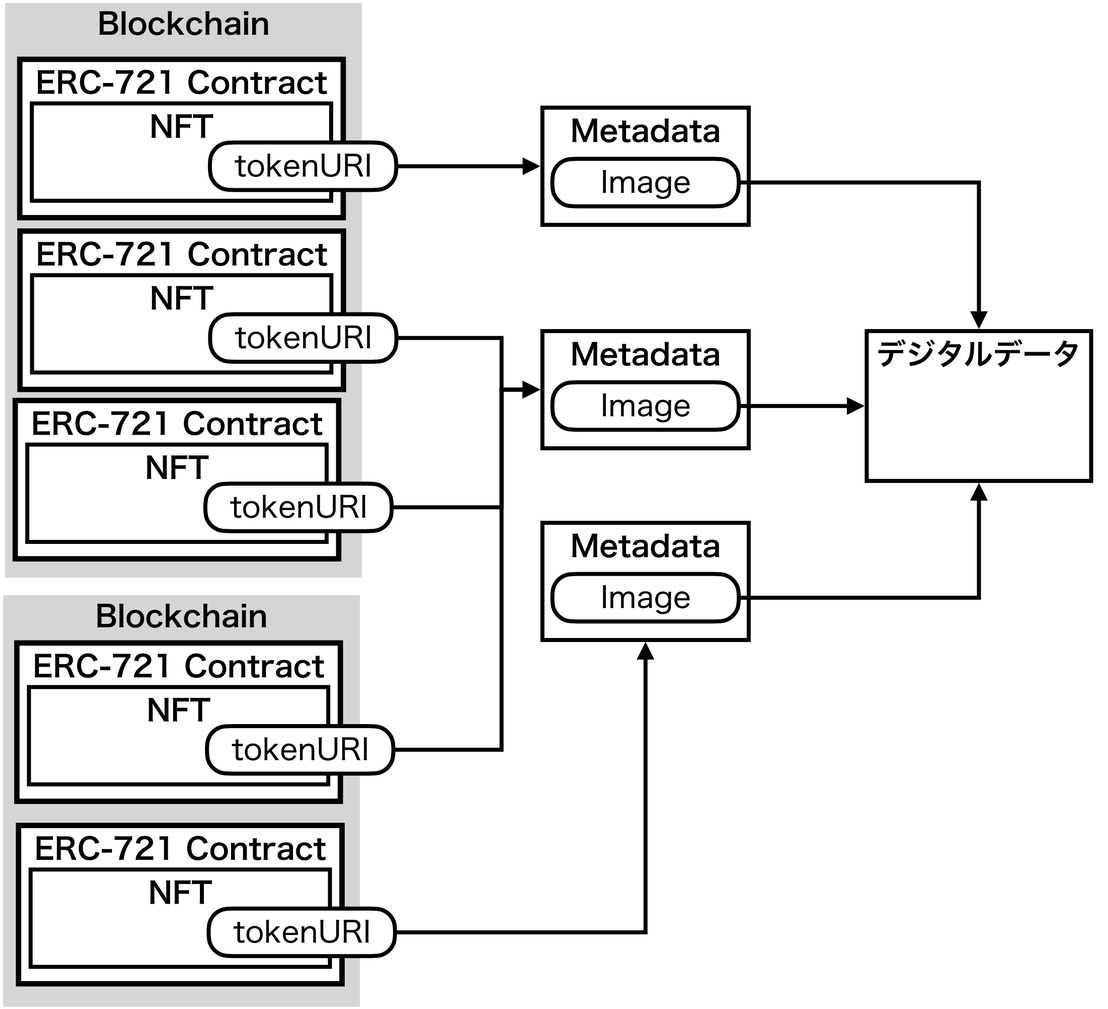
[7] OpenZeppelin/openzeppelin-contracts ERC721.sol, https://github.com/OpenZeppelin/openzeppelin-contracts/blob/96163c87e38ab2e3b047deab06c7be402296324d/contracts/token/ERC721/ERC721.sol

NFTとオフ/オンチェーン

- NFTのtokenIdの一意性は「特定のコントラクト」の中でしか保証されない
  - ➡ コントラクト外部のMetadataおよびデジタルデータは複数のNFTから参照されうる
  - NFTがNon-Fungibleであるのは<u>NFT自身のみ</u>

- デジタルデータを含めて全てブロックチェーン上に記録する手法も検討されている
  - <u>オンチェーン/オフチェーン</u>: ブロックチェーン上に記録されるものがオン、それ以外がオフ

➡ 手数料の問題



複数のNFTから参照されるデジタルデータ

トランザクション手数料

- コントラクトをデプロイ/実行する際にはトランザクション手数料を仮想通貨立てで支払う必要がある
  - 手数料は各トランザクションをブロックチェーンに記録する作業を行う報酬となる
  - EthereumではGasと呼ばれ、Gas量は操作するコントラクトの計算量および記録するデータ量によって決定
    - GasはEtherにその時々のレートで変換
    - Etherが高騰すると手数料が高くなる + 仮想通貨のボラティリティの高さ

- 全てをオンチェーンでアプリケーションを作るには手数料のコストとのバランスを勘案する必要がある

手数料とスケーリング問題

- 手数料がかかることに加え、そもそもブロックチェーン自体のトランザクション処理性能が低いことによってアプリケーションに必要な性能が満たせず、スケールしない

- On-Chain Scaling: ブロックチェーン自体の性能を上げる手法
  - Sharding: 複数のチェーンを並列実行し、トランザクション処理性能を上げる [8]

- Off-Chain Scaling: オフチェーンで行われるやりとりの一部等をブロックチェーンに書き込む手法
  - ブロックチェーンへの書き込みが最小限に抑えられるため、手数料の削減が期待できる
  - ブロックチェーンとは独立してオフチェーンでのやり取りは処理できるため、高速に処理できる
  - Bitcoin: Payment Channel/Lightning Network [9]
  - Etheruem: Rollup[10, 11] など

[8] Sharding, https://ethereum.org/en/upgrades/sharding/
[9] Joseph Poon, Thaddeus Dryja, The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments, 2016, https://lightning.network/lightning-network-paper.pdf
[10] OPTIMISTIC ROLLUPS, https://ethereum.org/ja/developers/docs/scaling/optimistic-rollups/
[11] ZERO-KNOWLEDGE ROLLUPS, https://ethereum.org/ja/developers/docs/scaling/zk-rollups

ユーティリティートークン

- **ユーティリティートークン**: トークンに何らかの実用性/意味を持たせ効用（ユーティリティ）を持つもの
  - ある組織（など）への所属の証明
  - ガバナンストークン: 投票権の保持を示すトークン
    - 保有量に応じた重みつき投票などが実現できる

DAO

- 定義は非常に不明瞭だが、語だけでみると
  - 分散(Decentralized): 中央管理者なしに
  - 自律(Autonomus): それぞれが独立して動く
  - 組織(Organization): 組織
  - ➡ さまざまなプロセスにスマートコントラクトを適用することで管理主体への依存度を下げる

- 例えば特定の管理主体が存在しない組織
  - ユーティリティトークンによって組織への所属を証明
  - 何らかの意思決定（ガバナンス）はガバナンストークンを用いた投票
  - ブロックチェーン上に刻まれたコードによって自動実行される組織運営
    - 組織内のタスクを実行したことの報酬支払い等

DAO実現の課題

- 現状の技術はまだ追いついていない
  - 「タスクの実行」はどう検知する？
  - ガバナンスは本当に投票の仕組みだけで分散的に実現できるか？
    - トークン保有量に基づく重みづけ投票だと、寡占したらどうなるか？
    - 投票できるからと言って必ずしもみんな投票をするか？
  - 自動実行するコードをどこまで信頼できるか？
    - コードにバグはないか？
  - など

DeFi (Decentralized Finance)

- ブロックチェーン上のコードによって特定の管理者なしに金融サービスに類することを実現する
  - 仮想通貨同士の交換/レンディングなど
  - 交換レートの計算等が公開された台帳上で実行される
  - 透明性高く、コードに基づいて確かに実行されることが期待される

- プログラムのバグにどう対応するか？
  - DAO的な枠組みで解決を図る
    - 特定のガバナンストークンを持つもので決議を行うが、投票の定足数が非常に低い [12]
    - DAOの大きな課題の一つが現れている事例の一つ

[12] 金融庁 令和３年度：分散型金融システムのトラストチェーンにおける技術リスクに関する研究, https://www.fsa.go.jp/policy/bgin/ResearchPaper_qunie_ja.pdf

まとめに代えて

- アプリケーション自体は様々出てきているが、個々に課題が多く残る
  - ブロックチェーン自体: スケーリング/手数料問題 等
  - アプリケーションのあり方: NFTにおける識別子/DAOにおける技術的未成熟さ/DeFiにおける運用上のリスク等
  - それらの課題にどれだけ真摯に取り組めるか、が今後の鍵ではなかろうか

- そのためには「実現したいこと」という目的ベースの議論することが重要
  - 特定技術の利用が目的だと、個々の技術の弱み等を見落としかねない
  - 技術に基づいた議論をする以上は、それぞれの用語の示す意味や、技術そのものの特性を冷静に見つめることが重要ではなかろうか