

NFT 紹介

IPFS とは

- HTTPはロケーション指向型プロトコル
- `https://www.utmc.or.jp/newcomer.html` は `www.utmc.or.jp` サーバーにある `newcomer.html` にアクセスしてウェブページを取得する。
- サーバー管理者には
 - サーバーを安定稼働させる責務が生じると同時に
 - アクセスに関する権力が集中する（ファイルを改竄できる、アクセスを制限できる等）

IPFS とは

- IPFSはコンテンツ指向プロトコル
- コンテンツのハッシュ値を求めコンテンツのIDとして採用する。
- 同じコンテンツを保管している場所ならどこからでも取得できる
→ 近い地域のサーバーが参照され負荷が分散される。
- ハッシュ値を指定するのでコンテンツの改竄が難しい（コンテンツの正当性を検証できる）
- ストレージ提供者には仮想通貨が支払われコンテンツ保持の動機になる。

参考：[IPFSとは何か？](#)

ブロックチェーンの仕組み (PoW)

- 取引データごとにブロックが生成される。
- ブロックの中身は
 1. 前のブロックのハッシュ値
 2. タイムスタンプ (いつ取引が行われたか)
 3. トランザクション (取引データ)
 4. nonce

ブロックチェーンの仕組み (PoW)

- ブロックのデータからハッシュ値が導かれる。
 - 決まった条件を満たすハッシュ値となるようなnonceを求めたい。
 - 適切なnonceを（おそらく総当たりで）計算し（マイニング）、最初に求めた人にブロック生成の権利が与えられ、手数料が支払われる。
- 過去のデータを改竄するとハッシュ値が変わる。つじつまを合わせるにはそれ以降のブロックのnonce値をすべて求め直す必要がある（非現実的）
- 取引記録に手数料がかかる（ガス代）

ブロックチェーンの仕組み

- 他にもコンセンサスアルゴリズムは存在する
- **PoS**：ブロック生成権はランダムだが、通貨の保有量が多いほど与えられる確率が高まる。
 - 高度な計算資源は必要ない。環境にやさしい。
 - 取引の承認スピードが速い。
 - 通貨の流動性が落ちる。
- その他：コンセンサスアルゴリズムの基礎と初心者が抑えておきたい5種類のアルゴリズム

NFT とは

- ブロックチェーンによって唯一性が担保されたトークン。
- 画像データなどをそのままブロックチェーンに載せるのは扱いにくいのでIPFSへのリンクなどのメタデータを記録する。
- **スマートコントラクト**：ブロックチェーン上での契約。自動販売機のようなもの。これにしたがってNFTをやり取りする。
- **mint**：NFTを発行すること。これにもガス代がかかる（ので今回は実例は断念）。
- Ethereum上でのOpen seaなどのマーケットプレイスが有名。