札幌AIラボ　AI普及啓発セミナー
「次世代デジタル社会を支えるWeb3.0」

講師：北海道大学大学院情報科学研究院　情報理工学部門 複合情報工学分野
調和系工学研究室 准教授
Sapporo AI Labテクニカルメンバー
山下　倫央　氏

開催日時：2023年1月26日（木）16:00～17:15
開催場所：札幌市産業振興センター産業振興棟2階 セミナールームD
YouTubeライブによるオンライン同時配信
共催：Sapporo AI Lab、一般財団法人さっぽろ産業振興財団
参加人数：（会場7名　配信聴講60名）

プログラムと内容の概略

Web3.0とは

ブロックチェーンを用いた分散型インターネットで、非中央集権型のプラットフォーム。

特定の管理者がおらず、プラットフォーマーを介せずに個人同士が直接やり取りを行う。

2021年頃から注目を集めた、新しいより良いインターネットのビジョンのための包括的な用語。ブロックチェーン、暗号通貨、NFT を使って所有権という形でユーザーに力を戻す。

バズワードに振り回されずに、基礎となる思想や技術で可能になることを明確に把握することが大切。

Web3.0もあれば、Web1.0やWeb2.0もある

Web1.0

企業による一方向の情報発信

限定的な情報発信の主体

主に企業による静的ウェブサイト

Web2.0

双方向の情報発信

プラットフォーム上で誰でも情報発信が可能。（Wikipedia・Mixi・YouTube・Facebook・Twitter）スマートフォン普及による飛躍的な発展を遂げた。

一握りの大企業がウェブ上で生み出されるトラフィックと価値を不均衡にコントロールできる。ユーザーはコンテンツを作成しても、コンテンツを所有したり、収益化の恩恵を受けることはない。

Web3.0の狙い

Web 2.0問題の例として挙げられるのは下記の2点。

・大企業の社内データをクラウドで管理していた。機密情報も GAFA のインフラで管理していたことで、データの消失で凄まじい損失が発生。

・Twitter や Instagram、YouTube のアカウントが停止されると、今まで投稿したデータは使用できなくなり、フォロワーやチャンネル登録者などの「資産」も消失する。

ところがWeb3.0は、非中央集権的・分散的なインターネットを実現する流れを目指すことで、GAFAなどのプラットフォーマーが中央集権的に支配していたデータの主導権をユーザに戻すことが可能となる。

ビットコインとは

金融機関のような信頼できる第三者を必要としない、当事者間で直接送金が可能な電子通貨システム。2008年 Satoshi Nakamoto により技術が公表。（Satoshi Nakamotoは国籍・個人かどうか含め不明）2009年より運用開始し、暗号資産の代表的存在。

ビットコインの取引量

取引量・価値は乱高下しているが、長期的に見ると価値は上昇している。

ビットコインが実現できる送金

銀行は取引履歴を保持し、改ざんしないことが前提にトランザクション（取引記録）は各銀行が管理して、信頼できる第三者として取引を仲介することに対して、ビットコインは、信頼できる第三者を必要とせずに、取引の記録は電子通貨システムに参加するユーザが分散して保持し、電子通貨で当事者間の直接送金ができる。

本人確認のための技術

電子通貨の課題として、本人確認が挙げられる。電子通貨はデータであり、現金と異なり実物が存在しないため、第三者が使用記録を取らなければ何回でも使用可能となる。

それを解決する技術として、本人確認のために他人に自分のコインを使わせない、デジタル署名がある。

デジタル署名の特徴は下記のとおり。

・秘密鍵を持っている本人にしか作れない

・他人に不正使用されない

・公開鍵が口座番号に相当

・秘密鍵が暗証番号に相当

・デジタル署名によって暗証番号にあたる秘密鍵を公開せずに本人確認できる

ビットコイン（仮想通貨関連）のリスク

秘密鍵を紛失すると、ビットコインにはアクセス不可になる。流出してしまうと他人に使われてしまうため、秘密鍵を適切に管理する必要がある。

400億円分のビットコインを保存したHDDをゴミとして捨てた人物は12年たってもなおHDDを探し続けている。

仮想通貨取引所 FTX が経営破綻

2019年 サム・バンクマン・フリード氏が香港で創設。日本にも「FTX Japan株式会社」があった。同社破綻のきっかけは「取り付け騒ぎ」。

2022年11月にFTXの財務の健全性を疑問視するニュースがあった。

業界最大手「Binance」のCEOは「FTX発行の資産を清算する」とツイッターに投稿。

「Binance」はFTXの買収を検討・翌日に撤回したが、投資家が FTX から資金を引き出した。

結果、顧客からの引き出し分の最大で80億ドル（約1兆1,000億円）が資金不足となり、FTX破産申請によりビットコインは急落した。

イーサリアムとは

電子通貨の送金の実現に特化していたビットコインを拡張して、2015年運用開始した。

特徴1　スマートコントラクトって？

Ethereum上で動作するプログラム。実体としてはContract Accountとして存在。

ブロックチェーン上に存在するので、誰でも確認可能である。

ユーザからのトランザクションにより起動して、記述されたプログラムを自動実行する。

特徴2　Dappsって？

Decentralized Applicationの略。ブロックチェーン上のスマートコントラクトによって実現されるサービス。

イーサリアムの公式ページで紹介されているDapps ↓

Uniswap

ERC-20トークン同士を交換するためのプロトコル。イーサリアム上の Ether などのスマートコントラクトとして実装。暗号資産の取引所を通さず他の暗号資産を購入可能。

分散型取引所（DEX：Decentralized Exchanges）

いわゆる分散型金融（DeFi：Decentralized finance）を実装

Axie Infinity

ベトナムのベンチャー企業によるゲーム。Play2Earn（遊んで稼げる）の代表格。

ゲーム内アイテムがNFTとして提供される。

ゲームのプログラム自体はブロックチェーン上に存在しない。

NFTとは？

Non-Fungible Token：非代替性トークン

token は辞書的には「代用貨幣」。偽造不可な鑑定書・所有証明書付きのデジタルデータ。

ERC-721

NFTのためのスマートコントラクトの標準

ERC (Ethereum Request for Comments)

ビットコインやEtherには固有のIDがついておらず、価値は均一である。ERC-721で固有のIDをもったトークンの作り方が定められたため、相互運用し易い。

代表的なNFTアーティスト

ピクセル画で有名となったCryptoPunksや、NFTブームの火付け役のアーティストのBeepleが挙げられる。

最大級のNFTマーケットプレイス　OpenSea

OpenSea　https://opensea.io/

NFT販売コントラクトを提供。

OpenSeaが管理するコントラクト上でのNFT作成機能を提供している。

出品した商品が購入されるとOpenSeaは手数料を得る

OpenSeaでは購入したNFTが売られる際に作者に一定の額が入るように設定可能

類似のマーケットプレイスとして Rarible などが存在

DAO

DAO：Decentralized Autonomous Organization

日本語では分散型自立組織と呼ばれる。

スマートコントラクトで組織を運営。中央の管理者が存在しない組織。

従来の株式会社は経営陣が給与や資産の使途を決定する。経営陣の不正を完全には防げない。

しかしDAOは、上記の役割をスマートコントラクトに置き換えて組織運営はスマートコントラクトの記述通りに自動的に実行する。透明性が高く、管理することはできない。

日本における Web3 関係の動向

日本政府の姿勢

2022年3月

自民党の NFT 政策検討プロジェクトチームのNFTホワイトペーパーが承認

2022年7月15日

経済産業省では、大臣官房に「Web3.0（ウェブ・スリー）政策推進室」を設置

日本では税制面から企業が集まりづらく、それに伴い人材も集まらない。よって日本国内の人材の海外への流出が問題となっている。

地方自治体におけるNFTの活用例

旧山古志村

新潟県長岡市にある人口約800人の村は、ジェネラティブNFTであるColored Carpを発行した。NFT発行益の一部の執行権限をNFT保持者に移譲し、「デジタル住民票」と呼称。

山古志村デジタル総選挙で使途を決定した。

スマートコントラクトのみで組織運営はしておらず、メンバーシップ判定にNFTを利用しているだけのため、厳密な意味での DAO ではない。

余市町

ふるさと納税の返礼品としてNFTを採用した。（事業者：株式会社あるやうむ）

現状では販売しただけで、NFT保持者だけが参加できるイベント等は開催されていない。

OpenSea でも確認できる。