CUS-34

NFT を取り巻く技術要素と AWS 利活用

満足 亮
double jump.tokyo 株式会社
CTO

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

本セッション資料や記載内容については一切の転用を禁止しております

はじめに

- 資料及び口頭で話す内容は弊社で培ったノウハウを含むものでありますが、背景など全て伝え切れるものではありません。実際のビジネス等に活かす場合は法的な確認が必要な場合があります。
- 本発表で事例にあげる暗号資産、NFT等の購入を推奨するものではありません。
- 特に言及のなくブロックチェーンと言った場合、Ethereumを前提とします。
- 本発表は、2022年3月時点収録されたものであり、公開時の市場状況と乖離している可能性があります。

© 2022 double jump.tokyo inc. All Rights Reserved

double jump

.tokyo

© 2022 double jump.tokyo inc. All Rights Reserved

double jump.tokyo株式会社

- 2018年4月創業
- ブロックチェーンゲームの開発、運営

  NFTの設計、発行、販売
- **Re-building the future of gaming**

  with blockchain technology!

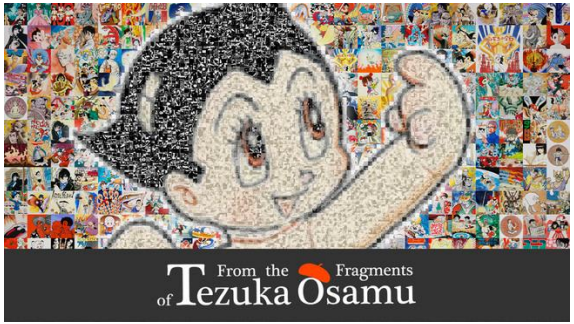
© 2022 double jump.tokyo inc. All Rights Reserved

Re-building the future of gaming with blockchain technology!

© 2022 double jump.tokyo inc. All Rights Reserved

NFT事業支援 「NFTPLUS」

- ゲーム、エンターテイメントコンテンツを中心に
  NFTのプロデュース、制作、コンサルティング
  共同事業開発



©2021 SQUARE ENIX CO., LTD. All Rights Reserved.
Powered by double jump.tokyo Inc.

©2021 Tezuka Productions, All Rights Reserved.
Produced by double jump.tokyo Inc.

Copyright Souun Office
Produced by double jump.tokyo

© 2022 double jump.tokyo inc. All Rights Reserved

ブロックチェーンゲーム開発、運営

- 自社開発タイトル運営を含むブロックチェーンゲーム事業
- ブロックチェーンゲーム開発支援国内外含め、7タイトルを支援中

BRAVE FRONTIER HEROES

MyCryptoHeroesエンジン x ブレイブフロンティアIP
Alim社と共同開発
2020年1月リリース

MyCryptoSaga

リアルタイム対戦を楽しむポーカーライクなマインドカードゲーム
2021年5月リリース

MyCryptoHeroes

日本発、世界No1を記録したブロックチェーンゲーム
現在、MCH社へ運営を移管。分散コミュニティの形成を目指す
2018年11月リリース

© 2022 double jump.tokyo inc. All Rights Reserved

ビジネス向けNFT管理サービス「N Suite」

NFT発行や暗号資産の送金、スマートコントラクトのデプロイなど、NFT/Web3領域の事業をスムーズかつ効果的に行うための製品を揃えたビジネスツールセット

© 2022 double jump.tokyo inc. All Rights Reserved

NFT、知ってますか？

© 2022 double jump.tokyo inc. All Rights Reserved

NFTの特徴

デジタルアセットの新たな価値を与える

1. **所有の証明**
2. **譲渡およびトレース**
3. **作成者（本物）の証明**
4. **コンテンツの参照先を記録**

© 2022 double jump.tokyo inc. All Rights Reserved

NFTとは？

- **Non-Fungible Token**はブロックチェーン上で構築できる代替不可能なトークンのこと

  暗号資産 = 通貨を表すトークン

  NFT = モノや権利の**所有を表す**トークン
- 2017年から概念が提唱され、2018年、2019年に**ゲームとしてのユースケースを確立**。2020年後半より、**アートやエンタメ分野での注目が集まる**。
- 日本法律上の暗号資産ではないため**比較的ビジネスがしやすい領域**
- イーサリアム上の代表的なNFT規格として**ERC721**がある
  - ERC721を中心に解説

© 2022 double jump.tokyo inc. All Rights Reserved

比較的ビジネスがしやすいとは？

- **NFTにビジネス上、法律上の定義はなく、その特性を持って判断される**
- よくある例
  - 決済手段等の経済的機能がある ⇨ 暗号資産として扱うべき
  - 暗号資産交換業 / 税務会計処理の困難さ
  - 収益配分があるNFTを販売する ⇨ 金商法のルールで扱うべき
  - 集団投資スキーム持分
  - ガチャでNFTを販売だ！ ⇨ 刑法賭博罪のリスク
- 実際のビジネス、企画に応じて法的な確認が必要な場合があります。

© 2022 double jump.tokyo inc. All Rights Reserved

スマートコントラクト

- 暗号資産/仮想通貨で有名なビットコインではなく、
  スマートコントラクトのあるイーサリアムがNFTにおいての主役
- スマートコントラクトとは、**ブロックチェーン上に作成した任意のプログラム**を言い、NFTもスマートコントラクトとして実装される
- スマートコントラクトでは、
  ブロックチェーン上に**状態**と**ログ**を残すことができる

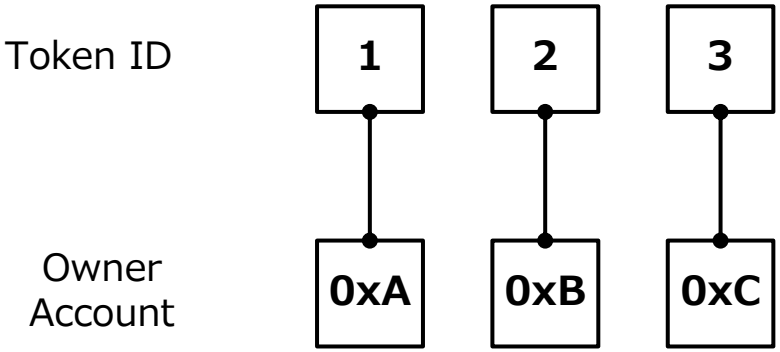
© 2022 double jump.tokyo inc. All Rights Reserved

ブロックチェーン上で所有を表す

ブロックチェーン上に、

Token IDと所有者であるアカウントアドレスが保存されている

＝ブロックチェーンによる所有の証明



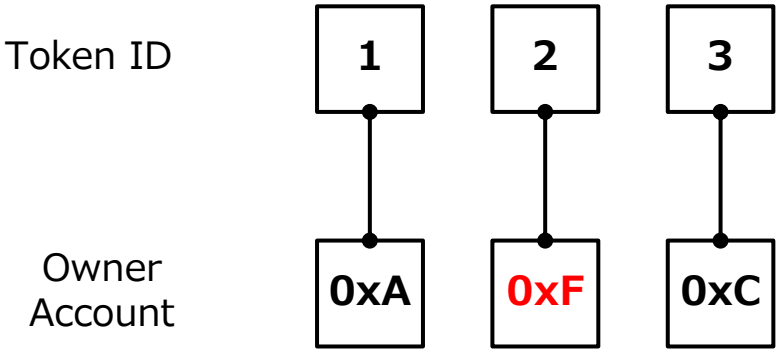
© 2022 double jump.tokyo inc. All Rights Reserved

所有を書き換えることで譲渡を表現

Token IDに対する所有者を書き換えることで「譲渡」を表現する。

またブロックチェーン上に書き換えの履歴を残す

＝デジタルアセットの**「譲渡」とそのトレース**



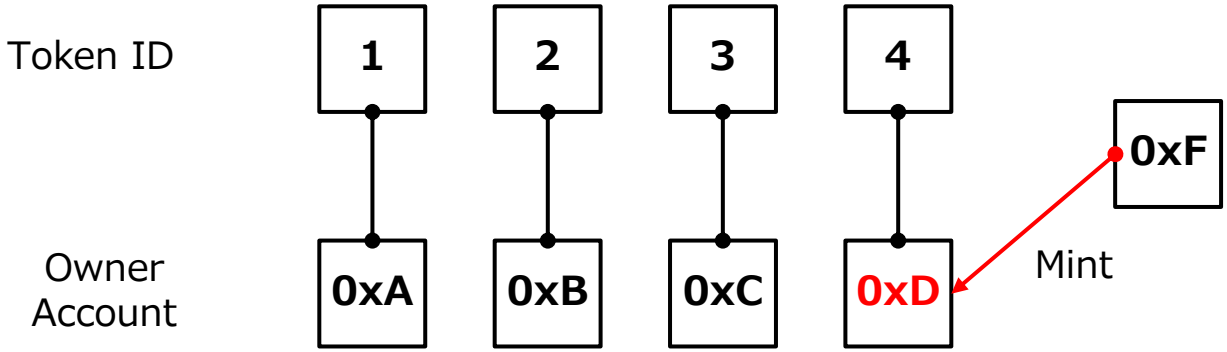
© 2022 double jump.tokyo inc. All Rights Reserved

発行者の制限および履歴

新たなToken IDに対して、所有者を割り当てることを発行とする。

そのトランザクションの実行者は改竄困難である。

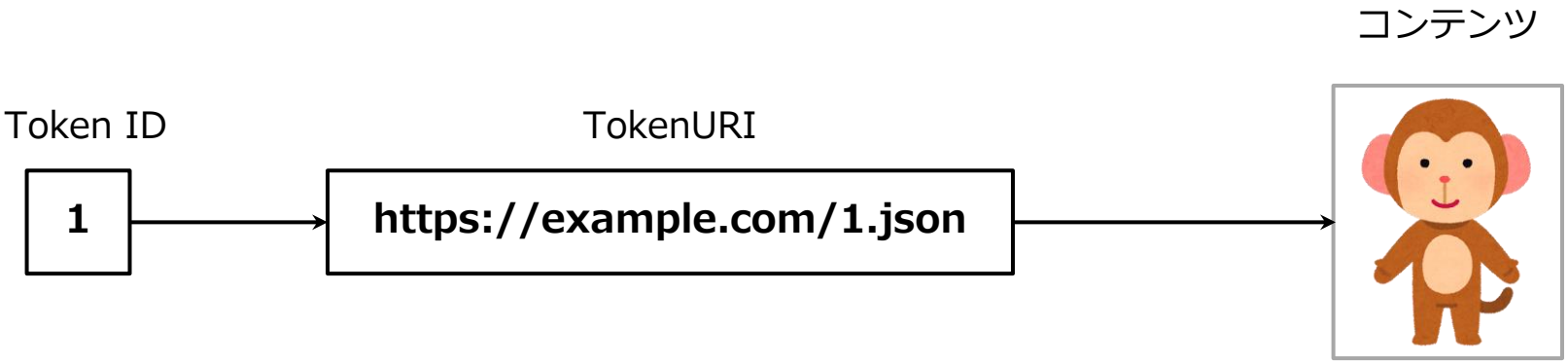
＝発行者が自明であることで**本物の証明**が可能



© 2022 double jump.tokyo inc. All Rights Reserved

コンテンツの参照先を保存

Token IDに紐づくデータ（メタデータ）の格納先をブロックチェーン上から取得できる。メタデータからコンテンツ（画像/音声/動画など）が参照可能。
＝ブロックチェーンから**コンテンツを参照可能**



© 2022 double jump.tokyo inc. All Rights Reserved

技術的には単純なNFTがなぜ注目されるのか
NFTが何を変えているのか

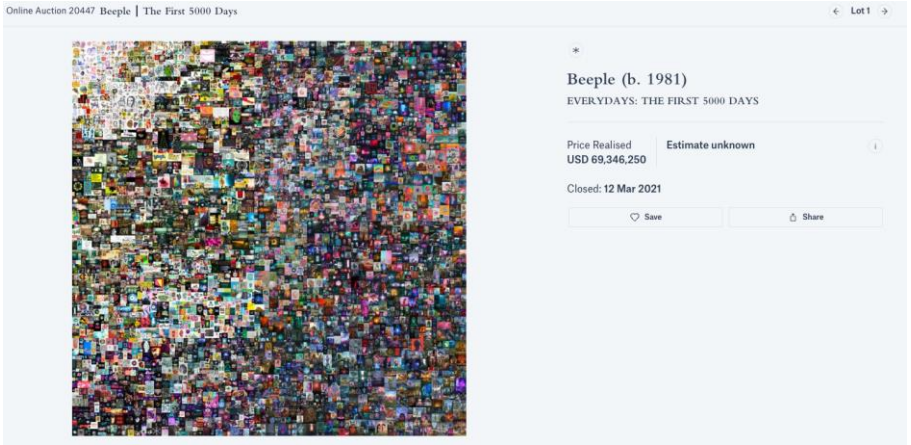
© 2022 double jump.tokyo inc. All Rights Reserved

NFTが変えるもの（コンテンツ視点）

- コピー可能で価値を付けづらかったデジタルアセットが唯一性、トレーサビリティを得たことで

  現実世界と同じような価値を認めることができるようになった

  - コピー可能であっても**「本物」をブロックチェーンが保証**してくれる
- Beeple The First 5000 Daysは
  クリスティーズでオークション
  6900万ドルもの値がついた



https://onlineonly.christies.com/s/beeple-first-5000-days/beeple-b-1981-1/112924

© 2022 double jump.tokyo inc. All Rights Reserved

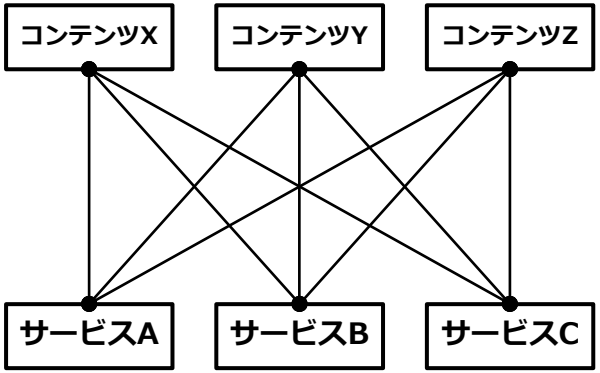
NFTが変えるもの（ビジネス視点）

- コンテンツ、アートをインターネットを通して**グローバルに展開可能**
- 個人アーティストが暗号資産を通してマネタイズ可能になった
  - Zombie Zooのような例も
- デジタルアセットの唯一性があることで**二次流通が可能**に
  - **二次流通手数料を発行者へ分配**も可能
  - マネタイズの手法の一つとして二次流通も視野に
    - 安価に販売して保有者コミュニティを盛り上げることで二次流通収益が期待できる
- **購入者へリーチする手段があるため、データの活用、リテンション、広告の手法が変わる**

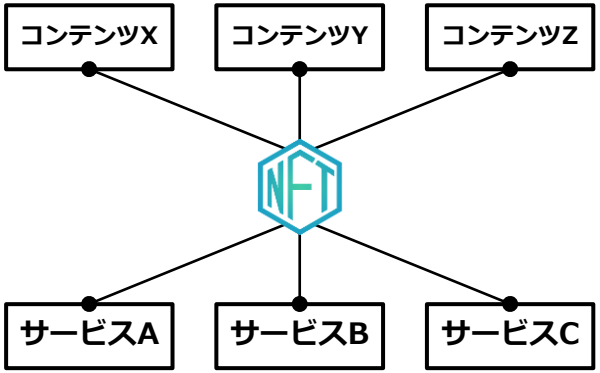
© 2022 double jump.tokyo inc. All Rights Reserved

NFTが変えるもの（サービス視点）

- NFTを介することでコンテンツへのアクセス方法が標準化、統一化
  - NFTは媒介としてのメディア、コンテンツの**Hub**
- 2022年に入ってメタバース分野で注目、言及される要因の一つ



従来はコンテンツをサービス
ごとに把握 or 保存



NFTによってコンテンツへの
アクセスが標準化、統一化

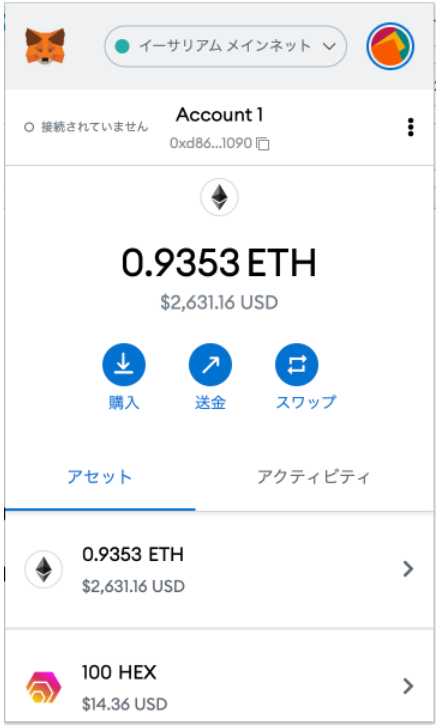
© 2022 double jump.tokyo inc. All Rights Reserved

NFTをビジネスで扱うには

© 2022 double jump.tokyo inc. All Rights Reserved

ウォレット

- 暗号資産の送金、ブロックチェーン上へのトランザクションの実行を担うコンポーネント
- PCブラウザの拡張機能やモバイルアプリとして提供される
- MetaMaskが有名
- いくつかの役割に分類できる
  - 秘密鍵の管理
  - Webサイトからのトランザクションデータを署名
  - ブロックチェーン（RPC エンドポイント）との接続

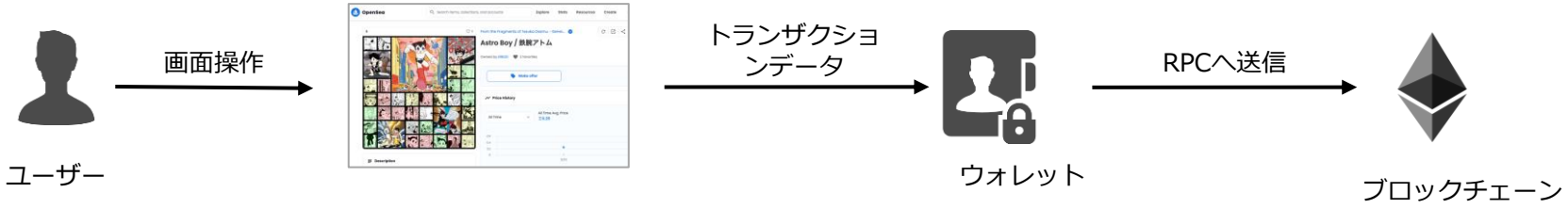


© 2022 double jump.tokyo inc. All Rights Reserved

ブロックチェーンへのトランザクション

汎用的なトランザクション

複雑なトランザクション



© 2022 double jump.tokyo inc. All Rights Reserved

ウォレットの要素を分解

1. **秘密鍵の管理**
    a. チーム内での共有の難しさ
2. **トランザクションへの署名処理**
    a. トランザクションデータの準備とそのデータを仕様に基づき署名する
3. **ブロックチェーンノードの管理**
    a. ノードRPCの接続管理
    b. 複数のブロックチェーンを利用するマルチチェーンは当たり前の時代に

© 2022 double jump.tokyo inc. All Rights Reserved

ブロックチェーン文脈での秘密鍵とは

- 電子署名(DSA)を行うための秘匿すべき鍵
- **署名メッセージ**と**署名**から秘密鍵の対となる**公開鍵**を得られる
- ブロックチェーン上のアカウント、アドレスは公開鍵のハッシュ値であることが多い
- **楕円曲線DSA(ECDSA)の曲線secp256k1**が比較的利用される
- 実態としては**巨大な数字**
- **一度共有した場合、永遠に共有を取り消すことはできない**
    - ビジネスにおいて退職などを考慮できない

© 2022 double jump.tokyo inc. All Rights Reserved

秘密鍵/暗号資産管理のビジネス上の課題

- **秘密鍵管理の属人化**
  - 複数人での共有が困難
- **処理実行者の証跡、記録が困難**
  - 複数人で鍵を共有した場合、誰が実行したのか？
- **NFT等、誤配布等の防止**
  - 専用のUIでも作らない限り、実行するトランザクションが正しいかの確認が難しい
- **セキュリティ要件と内部統制**
  - 暗号資産の送金、利用が承認なく実行可能
- **ハードウェアウォレットの管理**
  - 秘密鍵のエクスポートが可能な場合、業務遂行に物理的な制約

© 2022 double jump.tokyo inc. All Rights Reserved

ブロックチェーンノード

- ブロックチェーンネットワークに接続し、トランザクションを受け付けてくれる/処理してくれるサーバ
- 自前で構築することも可能
- INFURA, Alchemyなど事業者も少なくない
- アマゾン ウェブ サービス（AWS）でも提供されている（後述）

© 2022 double jump.tokyo inc. All Rights Reserved

NFTをビジネスで扱うための課題

- 秘密鍵の共有が困難であり属人化
- 承認フローが存在しない
  - 実行者の証跡がない
  - 暗号資産の送金、利用が承認なく実行可能
  - 実行トランザクションの意図が記録されない
- ブロックチェーンノードを選択、管理
  - サービス要件やコストを加味してブロックチェーンノードを選択する必要がある

© 2022 double jump.tokyo inc. All Rights Reserved

AWSの活用

© 2022 double jump.tokyo inc. All Rights Reserved

AWS Key Management Service (AWS KMS)

- イーサリアムで使われる**ECDSA secp256k1曲線の秘密鍵に対応**
- 作成した秘密鍵自体は**AWSアカウント管理者であっても取り出し不可能**
- 暗号処理である「署名」だけをAPIとして提供
  - トランザクションに必要なのは「署名」
- 署名リクエストは**AWSの機能で管理**可能
  - AWS Identity and Access Management (IAM) でアクセス制御
  - AWS CloudTrailでのロギング
- トランザクションデータへの署名は自身で実装する必要あり
  - AWS KMSとの接続を行うOSSライブラリを検討

© 2022 double jump.tokyo inc. All Rights Reserved

Amazon Managed Blockchain (AMB)

- ブロックチェーンノードの**マネージドサーバ**を提供
  - 自前で構築する手間が不要
- **パブリックネットワーク**への接続をサポート
  - 現在はイーサリアムに対応
- 他ノードサービスと比べ、**リクエストの制限が少ない**ことがメリット
- RPCへのリクエストには、AWS Credentialを使った署名処理が必要

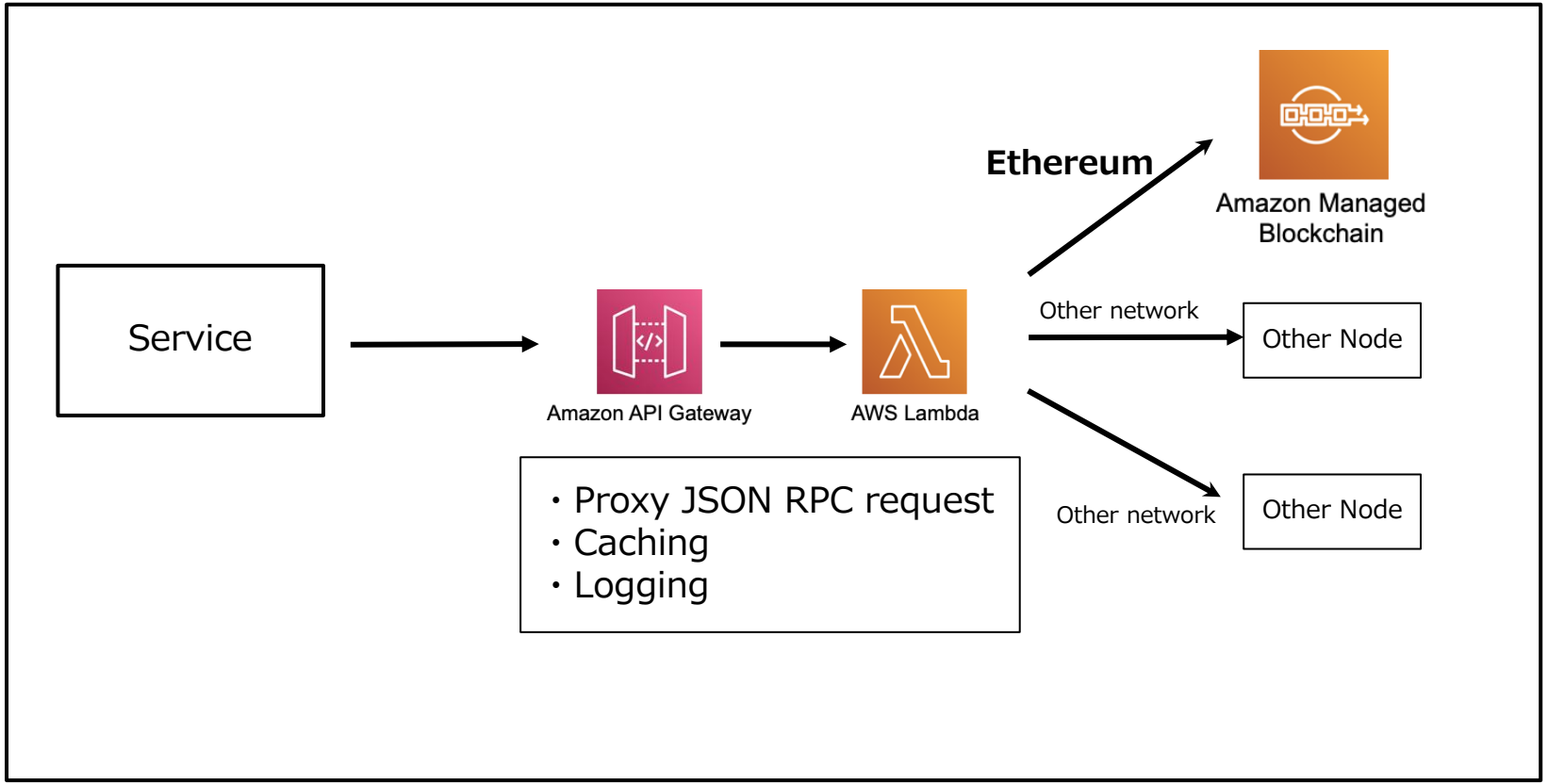
© 2022 double jump.tokyo inc. All Rights Reserved

ブロックチェーンノードゲートウェイ

- **Amazon API Gateway+AWS Lambda**を使ったブロックチェーンノードゲートウェイを構築
  - CredentialのSign処理をAWS Lambdaで実行
  - ロギング、キャッシュ等
  - バックエンドに複数のノードサーバを準備しフェイルオーバー
- イーサリアムノードへの接続**Amazon Managed Blockchain (AMB)**を利用
  - AWS Lambdaで署名処理を実装
- 実際にサービスを行う場合はAMB非対応のネットワークなども利用する
- 複数プロジェクトで共通利用できる

© 2022 double jump.tokyo inc. All Rights Reserved

Blockchain Node Gateway

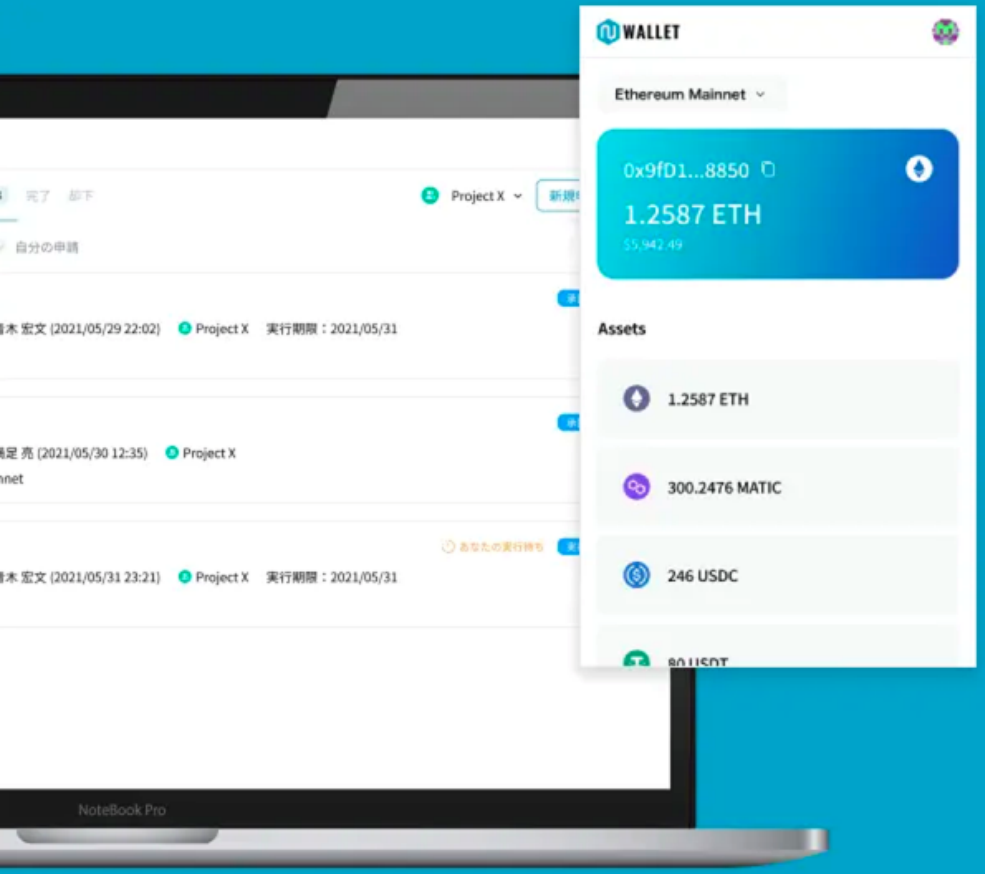


© 2022 double jump.tokyo inc. All Rights Reserved

NFTをビジネスで扱うための課題

- 秘密鍵の共有が困難であり属人化 ⇨ **AWS KMSで解決**
- 承認フローが存在しない ⇨ **?**
  - 実行者の証跡がない
  - 暗号資産の送金、利用が承認なく実行可能
  - 実行トランザクションの意図が記録されない
- ブロックチェーンノードを選択、管理 ⇨ **Amazon Managed Blockchain で解決**

© 2022 double jump.tokyo inc. All Rights Reserved



SUITE

複数人で秘密鍵管理できる
ビジネス向けNFT管理サービス

© 2022 double jump.tokyo inc. All Rights Reserved

N Suiteにビジネス向けNFT管理サービス

- AWS KMSで作成された鍵を使うブラウザ拡張 N Wallet
  - 秘密鍵を使ったオペレーションをクラウド化
- トランザクションの承認ワークフロー
- スマートコントラクトのデプロイ
- トランザクションの記録

AWS KMSを使ったチームでの鍵管理に加え

ビジネス上必要となる承認ワークフローをご提供

© 2022 double jump.tokyo inc. All Rights Reserved

まとめ

- NFTの特徴、技術的な要素
- NFTがビジネスに与えるインパクト
- NFTをビジネスで扱うためのウォレットとその課題
- AWSを利用した課題への対応
- N Suiteご紹介

NFT事業やブロックチェーンゲームの開発支援も行なっており、

関連するビジネスのお手伝いをしています。

© 2022 double jump.tokyo inc. All Rights Reserved

Thank you!

満足 亮

double jump.tokyo 株式会社
CTO

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

本セッション資料や記載内容については一切の転用を禁止しております