AWS-28

AWS で NFT の開発を始めるための３つのポイント

石尾 千晶
技術統括本部 ソリューションアーキテクト
アマゾン ウェブ サービス ジャパン合同会社

深津 颯騎
技術統括本部 ブロックチェーン プロトタイプ エンジニア
アマゾン ウェブ サービス ジャパン合同会社

スピーカー紹介

石尾 千晶

技術統括本部
ソリューション アーキテクト

好きなAWSサービス:
AWS Lambda

深津 颯騎

技術統括本部
ブロックチェーン プロトタイプ エンジニア

好きなAWSサービス:
AWS CloudFormation

目次

- NFT とは？
- NFT の開発におけるポイントとは？
- AWS を活用して開発を進めるには？
- 関連事例・リソースご紹介

このセッションでは、
- ブロックチェーン技術の基礎
- NFT のビジネス活用方法

については扱いません。
あらかじめ、ご了承ください。

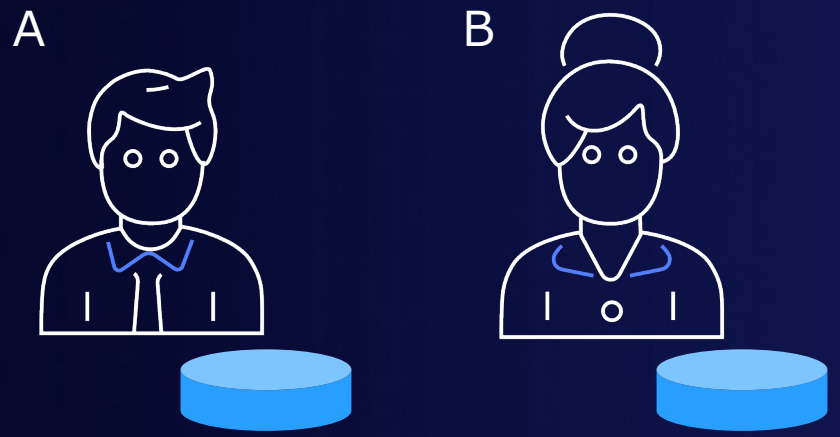
NFT とは？

- NFT = Non-Fungible Token（非代替性トークン）
- トークン：既存のブロックチェーン技術を使って発行された権利証
- NFT の例：デジタルアート、コレクション、サービス会員権
- 取引の改竄防止・なりすまし防止のために、公開鍵暗号などの暗号技術を活用

NFT とは？

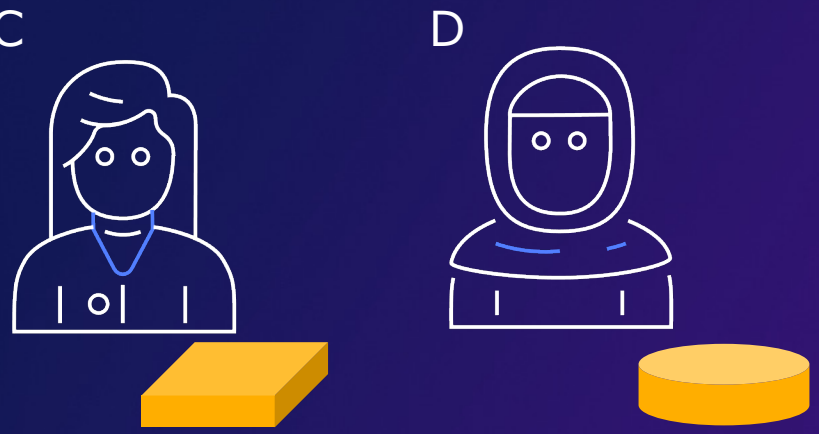
Fungible Token

代替できる
（同じトークンが存在する）



Non-Fungible Token

代替できない
（同じトークンは存在しない）

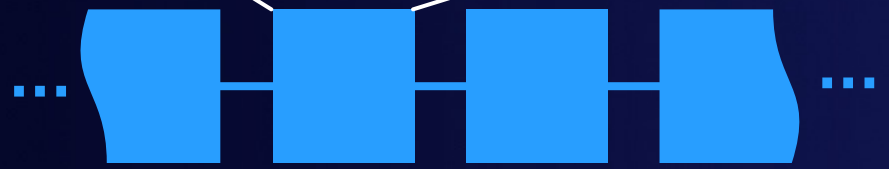


NFT とは？

Fungible Token

取引された数量を記録
ERC 20 などの規格がある

送信元	送信先	数量
A	B	1
B	C	3



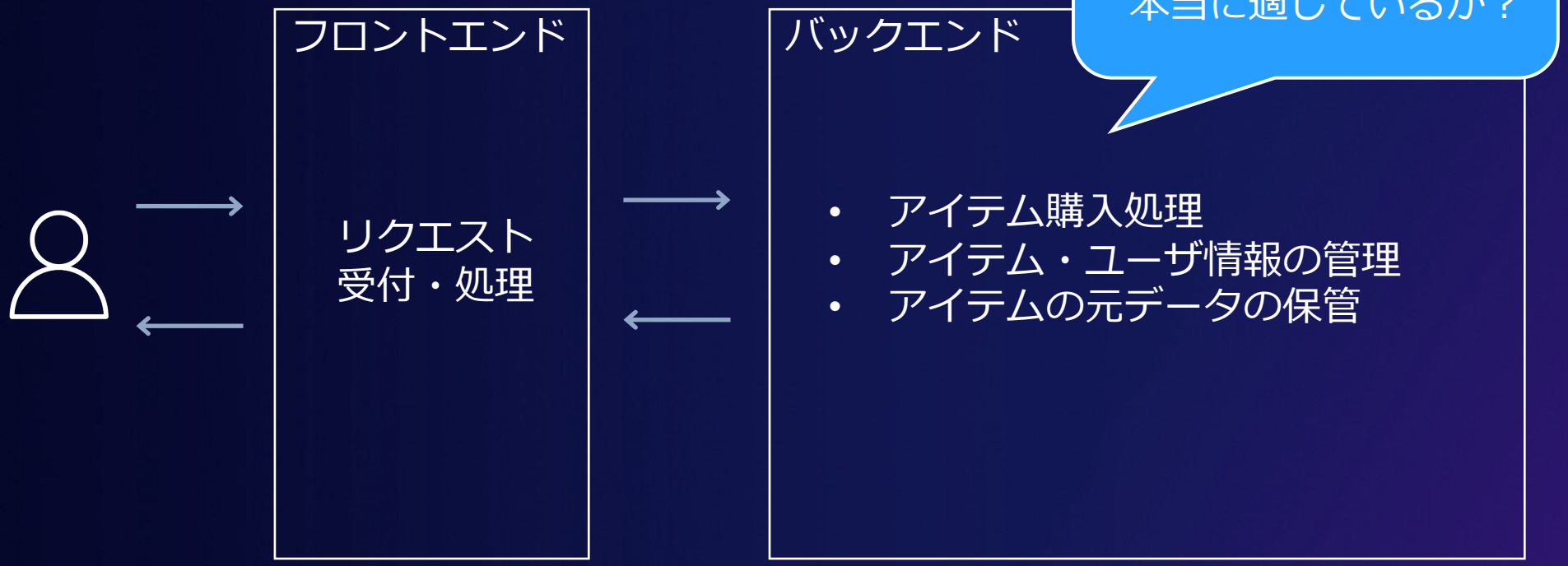
Non-Fungible Token

トークンの識別子・メタデータも記録
ERC 721, 1155 などの規格がある

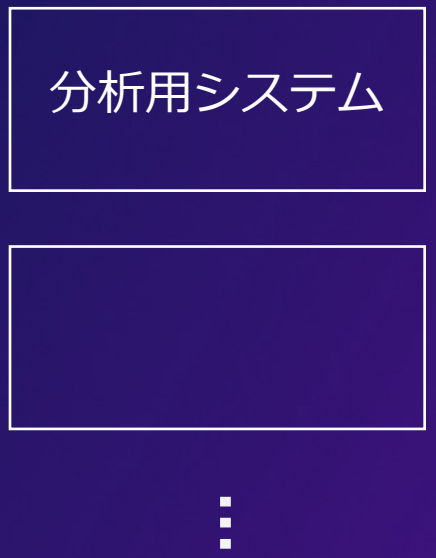
送信元	送信先	識別子	メタデータ
C	D	0001	{“name”: “item A”, “desc”: …, …}

NFT を活用したシステムの構成例

ゲームのアイテム購入機能
デジタルコンテンツ販売システム

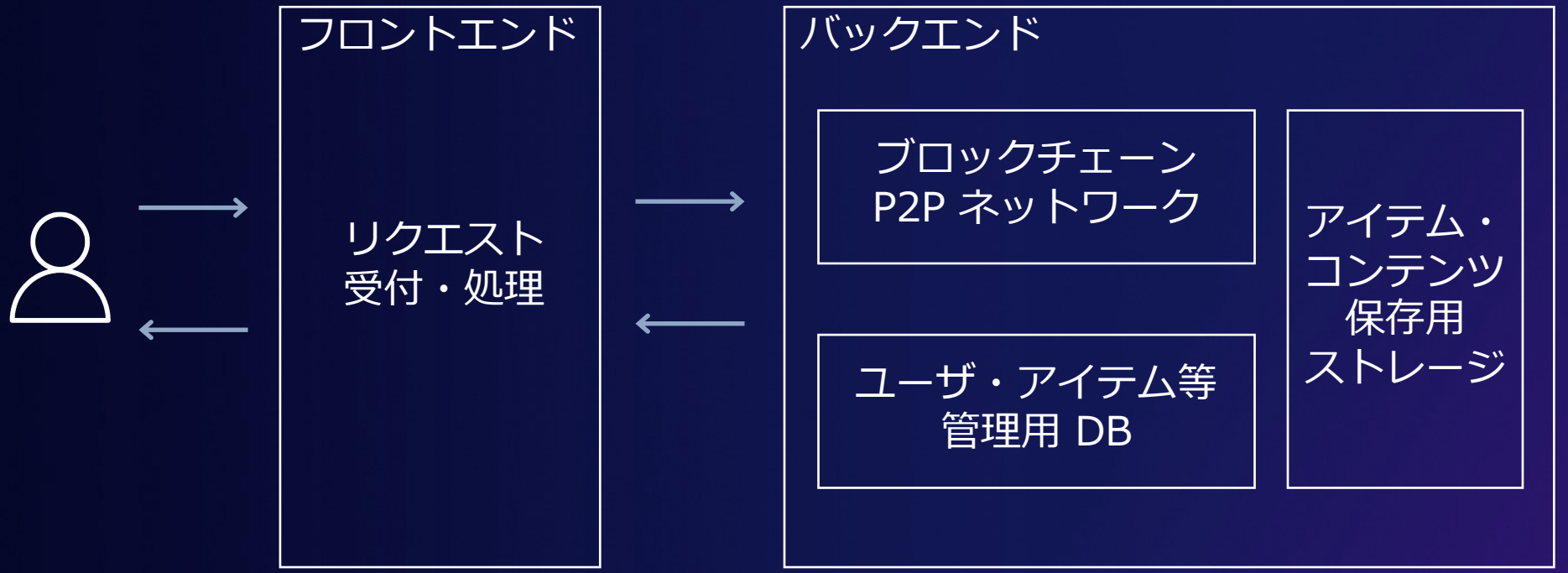


外部システム



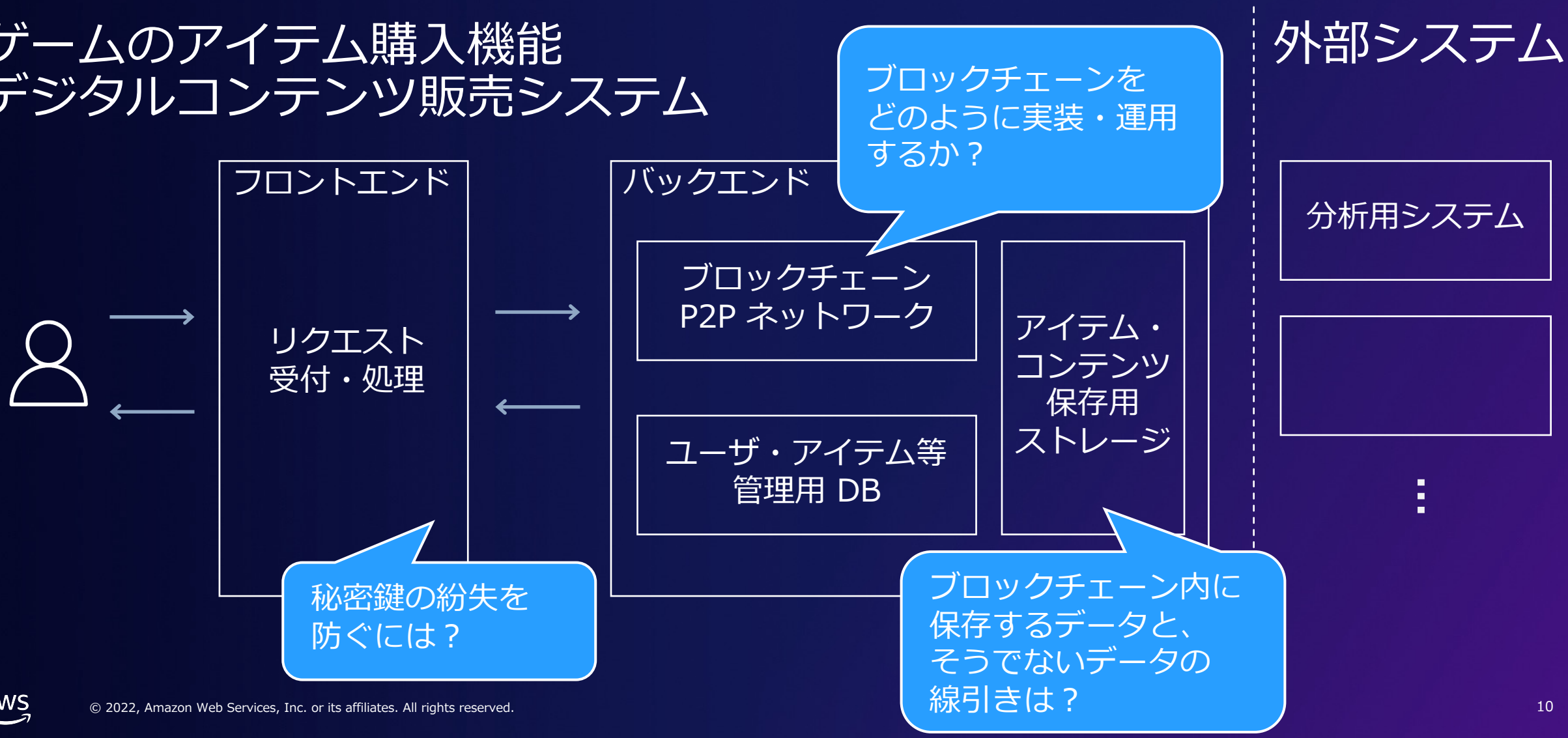
NFT を活用したシステムの構成例

ゲームのアイテム購入機能
デジタルコンテンツ販売システム



外部システム

NFT を活用したシステムの構成例



NFT の開発を始めるための 3 つのポイント

どのようにブロックチェーンを
実装・運用するか？

ブロックチェーンに
何のデータを保存する？

秘密鍵の紛失を
防ぐには？

課題① ブロックチェーンの実装と運用

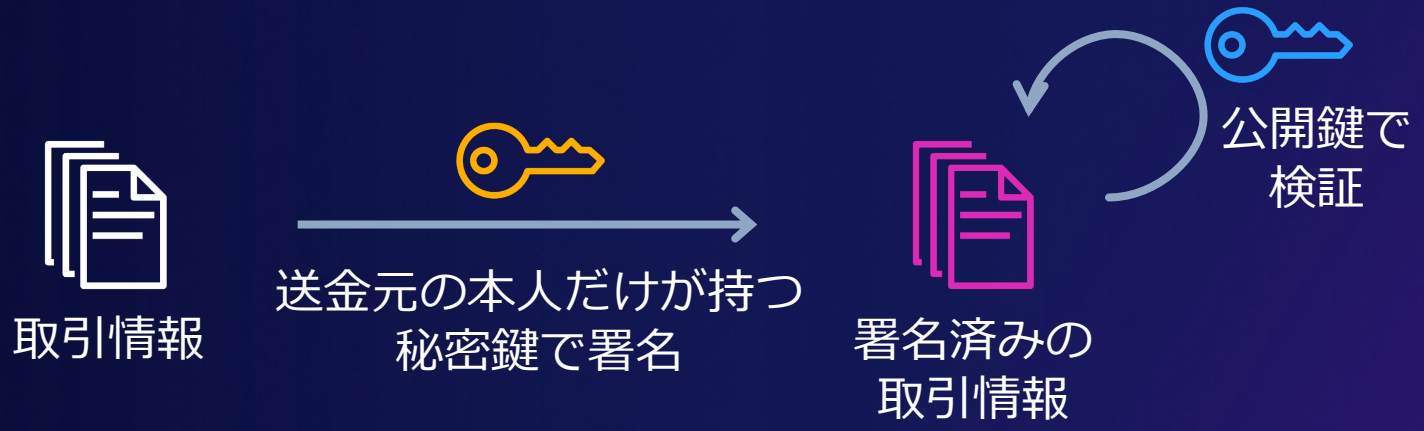
- ネットワーク構築に必要なリソースの購入の判断
- ブロックチェーンを構成するサーバ・ストレージの拡張性確保
- 各ノードの管理やメンテナンス

課題② データの保管方法

	オンチェーン	オフチェーン
データの保管場所	P2P ネットワーク上に 記録されるデータ	P2P ネットワークから 切り離されたストレージ上に記録 されるデータ
データサイズ	大きなデータは取り扱いにくい	大きなデータも取り扱える
データ検索	データの検索がしにくい	データの検索がしやすい
データの永続性	管理者がいなくなっても データは残る	管理者がいなくなったらデータに アクセスできなくなる可能性あり

課題③ 秘密鍵の管理

- NFT などの暗号資産の管理をすることは、秘密鍵の管理に相当
- 取引の送金元の本人であることを示すために、秘密鍵で署名する



- 秘密鍵を紛失すると、暗号資産に一切アクセスできなくなる上に、再発行ができない

課題①

マネージドサービスによる運用負荷の軽減

Amazon Managed Blockchain

ノード管理不要

ストレージの自動拡張

P2P ネットワーク管理が不要

複雑なセットアップが不要

課題②

オンチェーンとオフチェーンの使い分け

オンチェーン

ブロックチェーンを使った処理

- 他者と共有する必要のあるデータ、手続き
- 耐改竄性が求められるデータ
- リアルタイム性が必要な参照系処理

オフチェーン

ブロックチェーンを使わない処理

- フロントエンド、アプリケーション
- 他者と共有しないデータ
- 拡張性の高いストレージ
- 分析、検索
- イベントドリブンな他システム連携

課題②

オフチェーンでストレージ活用

- 大容量データの保存
- NFT保有者のみアクセス可能
- コンテンツの維持はサービス提供者

Amazon Simple Storage Service

課題②

オフチェーンでストレージ活用

大容量データの保存

コンテンツ自体の改竄耐性を
求める場合

コンテンツの維持はNFT所有者

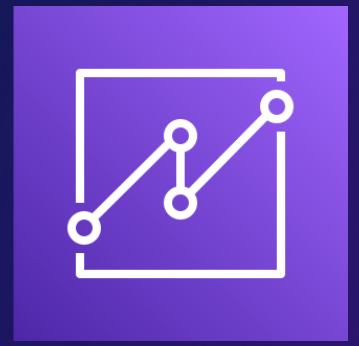
IPFS
(InterPlanetary
File System)

課題②

オフチェーンでデータ分析、検索

Amazon OpenSearch Service

Amazon Relational Database Service



Amazon QuickSight

ブロックチェーン内のデータの検索、分析は難しい
一度RDBMSやNoSQLにコピーしてから行う

課題②

ブロックチェーンと外部システム連携

ブロックチェーンのデータを
外部に送信

外部のデータを
ブロックチェーンに送信

ユースケース:
- ブロックチェーンのデータをDBに記録
- NFTの売買結果を経理システムへ反映
- ゲームの進捗に応じてブロックチェーンに記録

Amazon Elastic Container Service

AWS Lambda

課題③

AWS の鍵管理サービス

AWS Key Management Service (AWS KMS)

AWS CloudHSM

課題③

AWS Key Management Service

AWS Key Management Service (AWS KMS)

- 鍵の用意: KMS でキーペア（公開鍵と秘密鍵）を生成
- 署名には Sign API, 検証には Verify API を用いる
- 権限: 署名するアプリの実行基盤（EC2 インスタンス）にアタッチする IAM Role には上記 2 つが実行できる権限のみを付与

- メリット
  - 秘密鍵は KMS 上でのみ利用される
  - 鍵が AWS 上で一元管理される
  - 鍵管理インフラストラクチャの運用が不要
  - secp256k1の鍵形式に対応

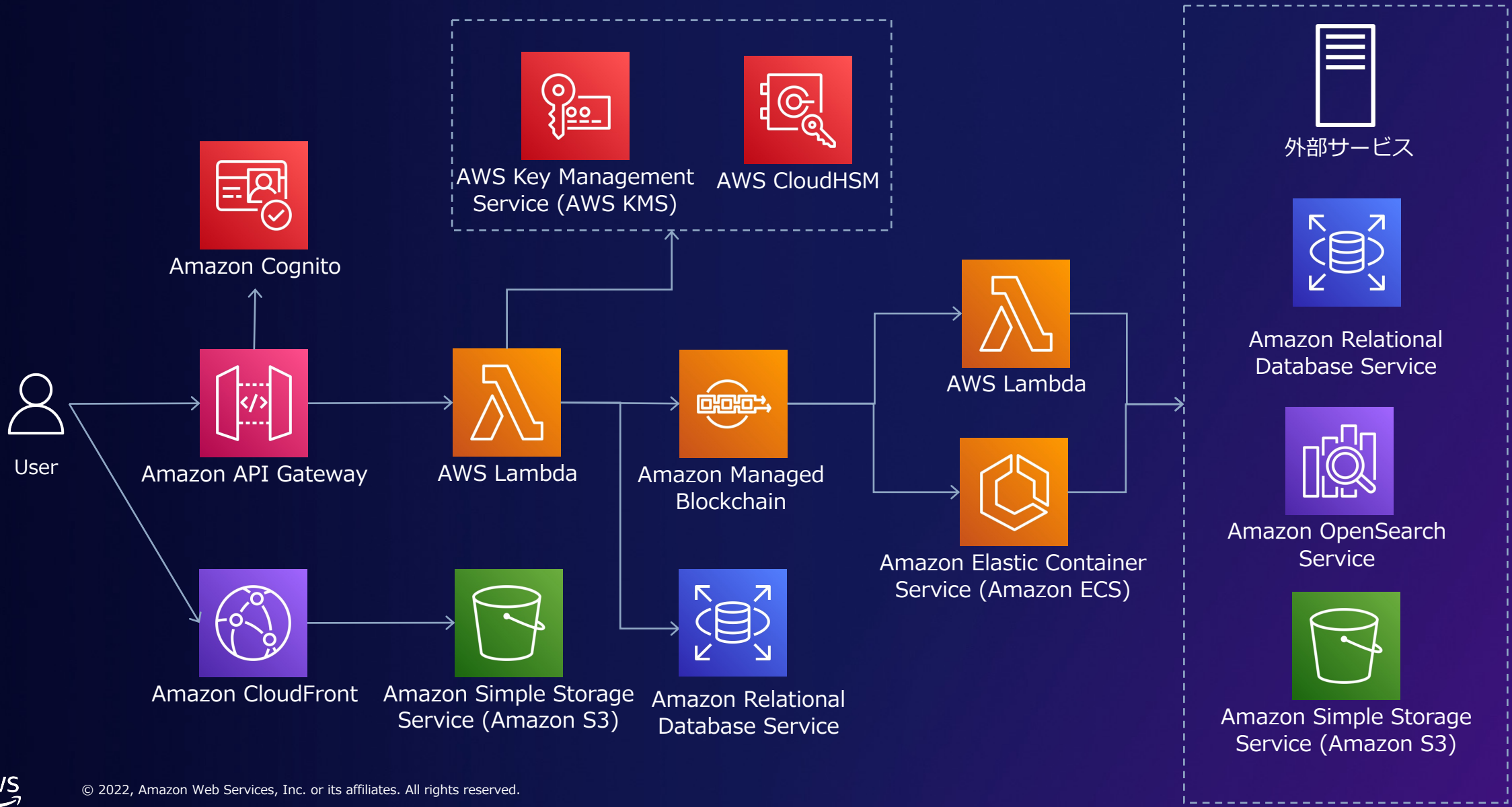
課題③

AWS CloudHSM

AWS CloudHSM

- AWS CloudHSM クライアントで以下を操作
  - 既に所有しているキーペア（公開鍵と秘密鍵）を AWS CloudHSM にインポート
  - 署名には Sign, 検証には Verify を用いる
- 権限: IAM ではなくCloudHSM ユーザーに対してアクセス許可を設定
- 暗号化アルゴリズム: インポートした鍵の暗号化方式
- メリット
  - 秘密鍵は CloudHSM 上でのみ利用できるように設定可能
  - 鍵が AWS 上で一元管理される
  - Bring Your Own Key (BYOK)が可能
  - secp256k1の鍵形式に対応

3つのポイントを抑えたアーキテクチャ



シンプレクス株式会社様
スケーラブルでセキュアなNFTサービスを迅速に構築

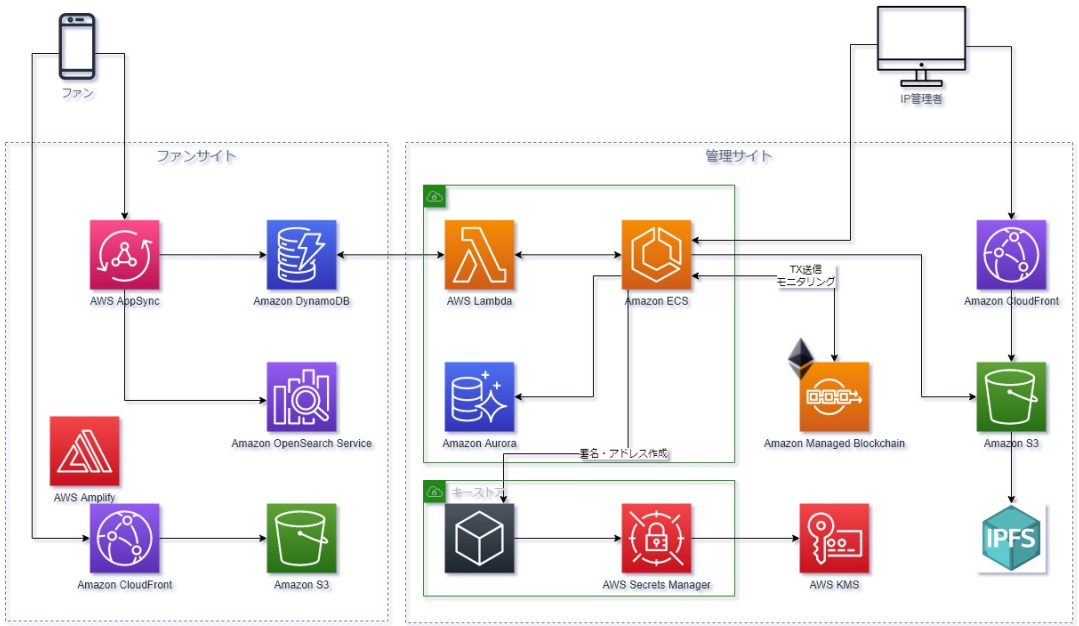
Simplex Inc.

ブランドの世界観を体現したデザインを効率的に
実現するNFTプラットフォーム

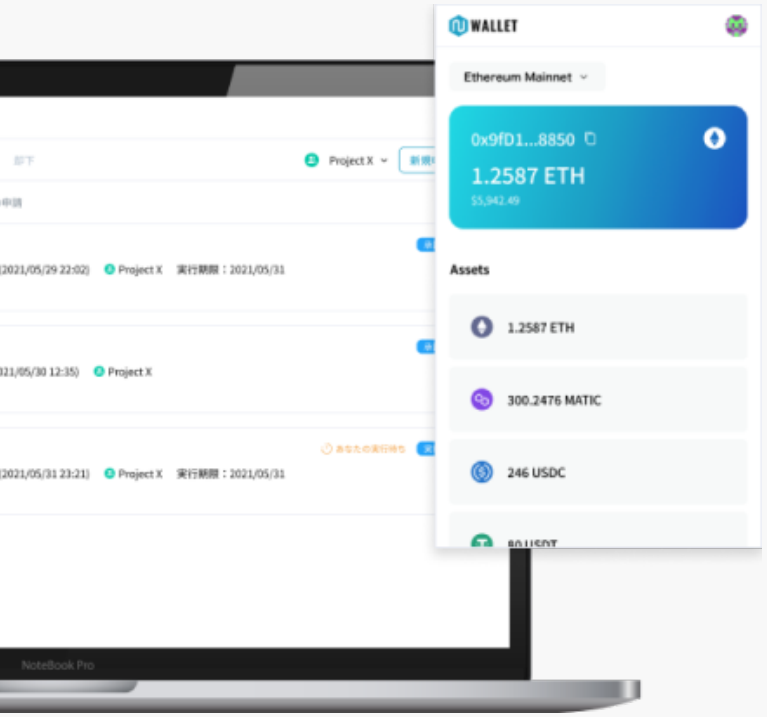
コンサルティング・UXデザイン・システム提供・運用改善
までワンストップで導入可能

ファンサイトは突発的な高負荷時でもユーザビリティを
損なわない高可用性を実現し、インフラコストを最適化

Amazon Managed Blockchainの活用によりノードの構築
や運用にかかるリソースを40%削減。
秘密鍵の漏洩や紛失への対策、構築からサービス提供まで
オンプレミス環境と比較して80%期間を短縮



double jump.tokyo様
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



ワークフロー機能で
秘密鍵の使用を管理

秘密鍵の共有管理機能で
作業の属人化を解消

秘密鍵での署名が必要な
様々な操作に対応

double jump .tokyo

SUITE

https://www.nsuite.io/ja

本日のまとめ

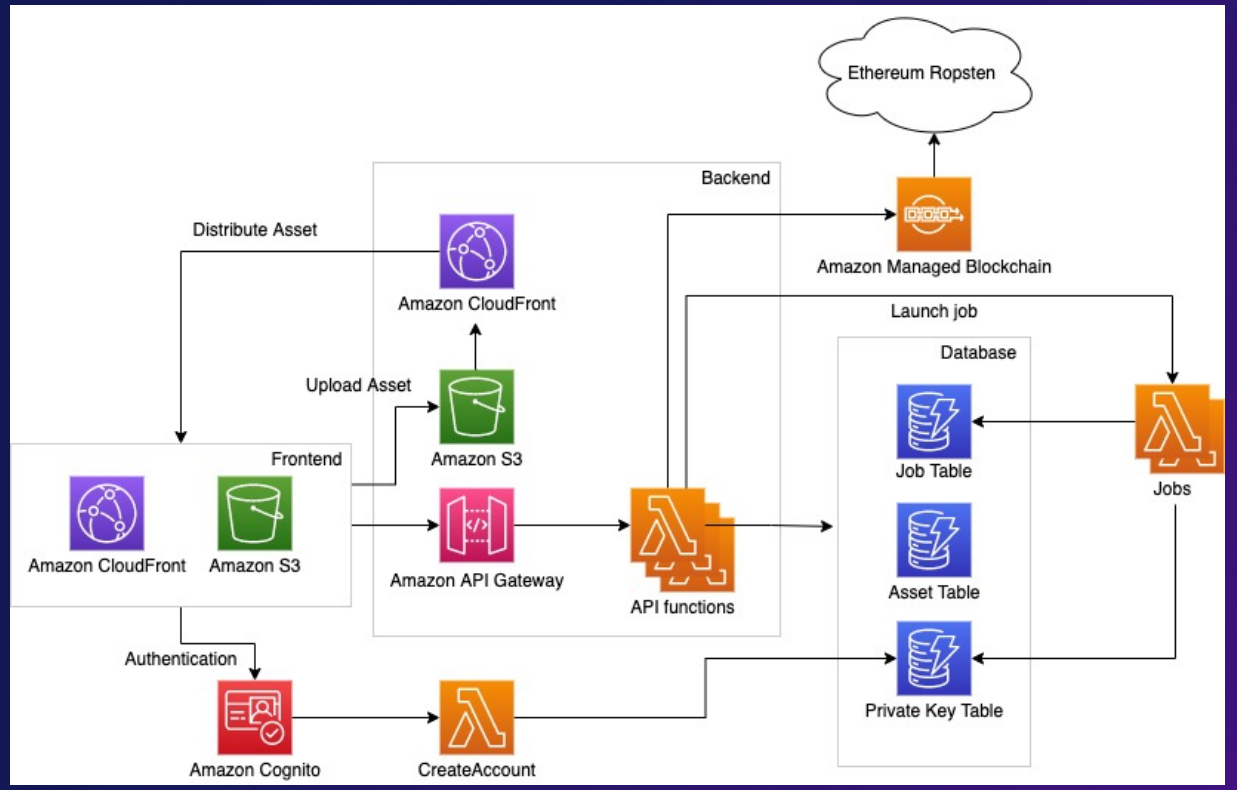
NFTを活用したサービスに必要なブロックチェーンノードをどのように運用するか
→ マネージドサービスを活用して運用負荷を減らす

ブロックチェーンに保存するデータは？
→ ブロックチェーンだけではサービスは作れない。オフチェーンも活用する。
→ オンチェーンは 「他者との共有」「改竄耐性」が必要なデータが適している
　オフチェーンは、検索や分析など参照系の処理、大容量データの保存が適している

秘密鍵の紛失を防ぐには？
→ ユーザーだけでなく、サービス提供者側の秘密鍵も守る
→ 鍵管理サービスを活用
　管理者であっても秘密鍵が見られないようにする

サンプルコード

- **Simple NFT Marketplace**
- 「NFTの発行」「マーケットで販売」「2次流通の際に知財保有者へロイヤリティの支払い」を実装したサンプルコード



https://github.com/aws-samples/simple-nft-marketplace

Thank you!

石尾 千晶 (Chiaki Ishio)

深津 颯騎 (Satsuki Fukazu)

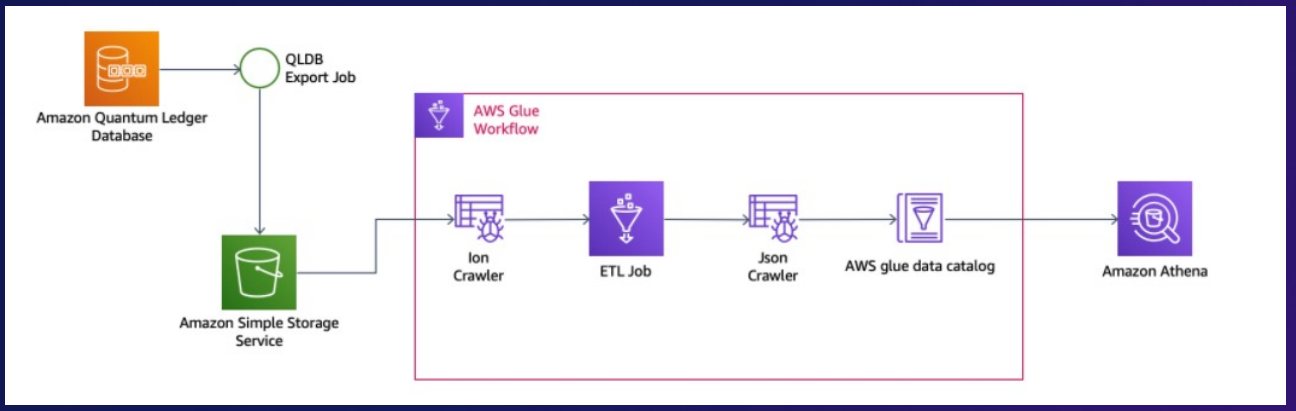
Twitter: @hkiridera

Appendix

ワークショップ

QLDBワークショップ

https://qldb-immersionday.workshop.aws/



Track-and-Trace Blockchain Workshop

https://track-and-trace-blockchain.workshop.aws/

お役立ち情報集

本日紹介した各サービスへのリンク
Amazon Managed Blockchain
AWS Key Management Service(KMS)
AWS CloudHSM

ブログ
How to sign Ethereum EIP-1559 transactions using AWS KMS

サンプルコード
aws-samples/aws-kms-ethereum-accounts
aws-samples/simple-nft-marketplace