

モジュール5 - Suiの高度な機能

Suiの高度な機能

このモジュールでは以下のような高度な機能について学びます

SuiでのAI構築とスマートコントラクト連携

zkLoginとスポンサー付きトランザクションによる円滑なオンボーディング



目次

1. zkLoginの仕組み
2. スポンサー付きトランザクション — ガス代の支払い代行
3. Suiのオラクル — オフチェーンデータのオンチェーン利用
4. Suiのクロスチェーンブリッジ
5. Suiでの自律型AIエージェント構築
6. 演習

zkLoginの仕組み

ユーザーログイン

- ✓ GoogleやFacebookなどの既存認証情報でウォレット生成
- ✓ 認証情報とウォレットが直接紐づかない

プライバシー保護

- ✓ JWTとソルトからZKProofを生成し、アカウントの秘匿性を確保します。

なぜ重要か

- ✓ 使い慣れたWeb認証情報でdAppにログインしつつ、ゼロ知識証明によってプライバシーを保護します。

ドキュメント

<https://docs.sui.io/concepts/cryptography/zklogin>

zkLoginを支える主な技術

1. ゼロ知識証明
2. OpenID Connect
3. @mysten/zklogin

ガスレストランザクション

ガススポンサーの役割

- ✓ユーザー、ガスステーション、スポンサー間で手数料をシームレスに管理します。

サービス例

- ✓ShinamiのGas Stationを利用することで、ガス代のスポンサーが容易になります。

<https://blog.sui.io/shinami-gas-station-tutorial/>

ユースケース

- ✓ゲームdAppが初期トランザクションのガス代を負担し、ユーザー獲得を促進します。

演習

- ✓スポンサーを設定します。
- ✓ガスレストランザクションを送信します。
- ✓レシートとガス支払者をオンチェーンで確認します。

Suiでのオラクル利用

利用可能なオラクル

- ✓ Chainlink
- ✓ Band Protocol
- ✓ Mysten Labs製のsimple oracleとmeta oracle

開発者向けガイド

- ✓ 天気オラクルの実装例
<https://docs.sui.io/guides/developer/app-examples/weather-oracle#initialize-the-project>
- ✓ Moveオラクルのサンプルコード
<https://github.com/pentagonxyz/move-oracles>

演習 — オンチェーン価格フィードの実装

要件:

POST API

`http://localhost:8080/price?symbol=ETH/USD` を作成し、NodeスクリプトでJSONをパースして、Moveオラクルコントラクトの `submit_price` 関数を呼び出します。

Suiのクロスチェーンブリッジ — 相互運用性

Sui Bridge (ネイティブブリッジ)

✓ 対応資産: ETH, WETH, USDT, WBTC, LBTC

✓ 方式: ロック & ミント 方式

<https://bridge.sui.io/>

その他のブリッジ

✓ Wormholeのメッセージング機能でSuiと接続

<https://wormhole.com/docs/tutorials/messaging/sui-connect/>

CircleのCCTP (USDC用)

✓ USDCのクロスチェーン転送の概要

SuiでのAIエージェント構築

エージェントロジック

- ✓ オンチェーンでのアクションはMoveスマートコントラクトで定義します。

オラクルと自動化

- ✓ データフィードを接続し、スポンサー付きトランザクションでプロセスを自動化します。

外部AIモデル

- ✓ 意思決定にオフチェーンのAIモデルを統合します。

セキュリティ

- ✓ Moveのケイパビリティとアクセス制御を活用します。

Nimbus AI Agent Kit

1. このキットはSui上でAIエージェントを構築するためのサポートを提供します。
2. ウォレット残高の取得をサポートします。
3. 複数のSui DeFiプロトコルとの連携をサポートします。

<https://agent.getnimbus.io/>

演習

- ✓ **UNCHAINの学習コンテンツ**

<https://buidl.unchain.tech/Sui/Sui-zklogin/>

- ✓ **スターターキット**

<https://github.com/unchain-tech/sui-zklogin-app>

zkLoginのサンプルアプリを作ってみよう！

- ✓ Google認証でウォレットを作成できるようにします
- ✓ 秘密鍵の管理無しでSUIの送金とNFTのミントが試せるようなアプリを作ります

演習

- ✓ サンプルAIエージェントキット:

<https://docs.getnimbus.io/sui-ai-agent/introduction>

- ✓ SDK:

<https://www.npmjs.com/package/@flowx-finance/sdk>

シンプルなAIエージェントを作成する

- ✓ SDKでウォレット残高を監視します。

- ✓ Moveで定義したロジックに基づき、オンチェーンアクションを実行します。

Thank you!