卒業研究発表
ブロックチェーン技術の進展による Web3セキュリティの課題分析

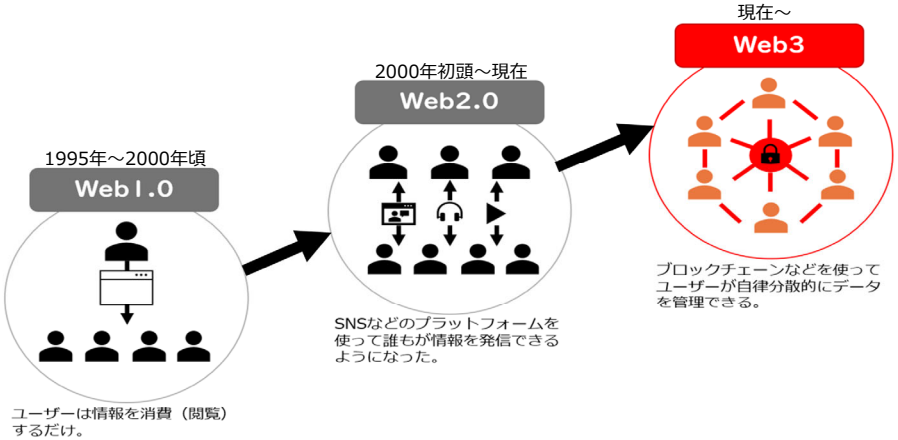
2025/2/25

千葉工業大学　社会システム科学部　経営情報科学科
2141108　宮前陸

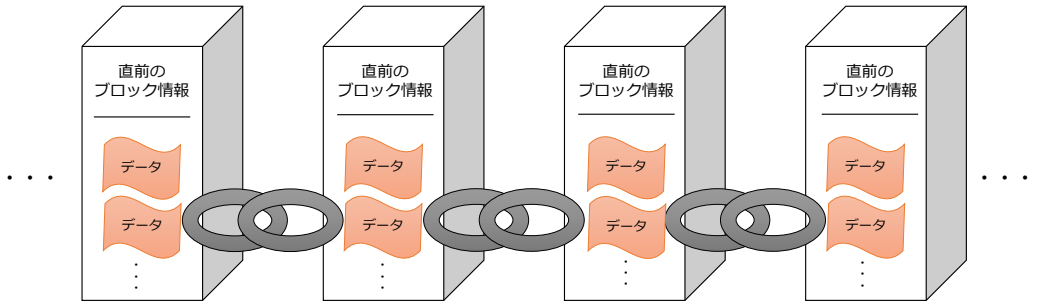
指導教員：新谷幸弘

目次

はじめに
インターネットの遍歴



はじめに
ブロックチェーンとは



ブロック単位でデータを管理し、ブロックを鎖（チェーン）のように連結して保管する技術

先行研究

セキュリティに焦点を当てたブロックチェーン技術の最新の研究動向
面和成

アブストラクト　ブロックチェーンは，金融や医療など様々な分野において研究が盛んであり，注目を集めている技術である．一方で，ブロックチェーン・暗号資産へのサイバー攻撃によって，莫大な暗号資産が盗まれる実被害も報告されている．本稿では，ブロックチェーンにおけるセキュリティ面を中心に，ブロックチェーンのセキュリティリスク，及びブロックチェーンを応用したセキュアシステムに関する最新の話題を取り上げ，それらの研究動向について概観する．

ブロックチェーンのセキュリティリスク・セキュアシステムに関する最新の研究動向の概観

研究目的

安全で信頼性の高いWeb3環境を実現するために、Web3環境におけるセキュリティリスクの課題を分析

研究方法

ブロックチェーンの実装

・分散型ネットワークにおけるブロックチェーンの動作を検証するため、ブロックチェーンを実装

DAppsの開発

・ブロックチェーンの実装応用として、DApps (Decentralized Applications) を開発

ハニーポットによる攻撃の観測

・Ethereumネットワークにハニーポットを実装し、攻撃の観測

・観測されたメソッドから、攻撃の種類や頻度を分析

・Web3環境における具体的なセキュリティ対策の提案

研究方法

ブロックチェーンの実装

・分散型ネットワークにおけるブロックチェーンの動作を検証するため、ブロックチェーンを実装

DAppsの開発

・ブロックチェーンの実装応用として、DApps (Decentralized Applications) を開発

~~**ハニーポットによる攻撃の観測**~~

~~・Ethereumネットワークにハニーポットを実装し、攻撃の観測~~

~~・Web3環境における具体的なセキュリティ対策の提案~~

ハニーポットによる攻撃の観測は中断

・観測結果を評価するための基準が必要である
・実装の条件が整っていない
・結果が出るまで長時間かかる

Web3におけるセキュリティリスクの分析

・ハニーポットを用いて観測した先行研究から想定されるWeb3のサイバー攻撃のリスクを抽出

・Web3環境における具体的なセキュリティ対策の提案

研究結果・考察
ブロックチェーンの実装

```
(base) C:\blockchain>python mining.py
43.207.156.47 is selected. Block length = 2
57.180.18.245 : {"message":"Chain is posted."}
43.207.156.47 : {"message":"Chain is posted."}
52.196.166.234 : {"message":"Chain is posted."}
```

マイニングに成功することで、ブロックチェーンに
新たなブロックが追加された

研究結果・考察
ブロックチェーンの実装


```
{
    “time”: "2024-05-08T05:26:25.476393+00:00",
    "transactions": [
      {
            “time”: “2024-05-08T05:25:53.917390+00:00”,
            “sender”:”36b8874ea74ce2bca5a1bd61ef8854024af6b2d141456f9a47525316db11ddb6d7dd4eb1254f212
                  2940374ca99f1786e093718732286baf4bc27a72a5d265e90”,
            "receiver":"d8a812edb79ea6f9a311b32b5dbed6199ec7f56c600a69f90c83c780fd9abfd583d8e0b770ec95c
                  7644ba27d4484f6d9f93907b345077f5c7b4c6fd901cb6faa",
            "amount": 5,
            "signature":"f8236bb5c2f59437d948fdaa9bf5572aa004a809f5d6fd95dc605dce94a107c121a72a00fbba4f5
                  485506978bec7cb7f4d19f48edcalefeacfebfa165bcc4988",
      },
      {
            "time": "2024-05-08T05:26:25.475392+00:00",
            "sender": "Blockchain",
            "receiver":"36b8874ea74ce2bca5a1bd61ef8854024af6b2d141456f9a47525316db11ddb6d7dd4eb1254f212
                  2940374ca99f1786e093718732286baf4bc27a72a5d265e90",
            "amount": 256,
            "signature": "none"
      }
    ],
    "hash": "d84a0c11eea2f303c2faa8c808b3d3cc3c40c0a2904b7bd6939f21bf768f91eb",
    "nonce": 124
}
```


送信者、受取主のウォレットアドレス

送金額

電子証明

一つ前のブロックの情報から出力された文字列

研究結果・考察
DAppsの開発

主な使用ツール

Next.js
Webフレームワーク

TypeScript
Webページ開発言語

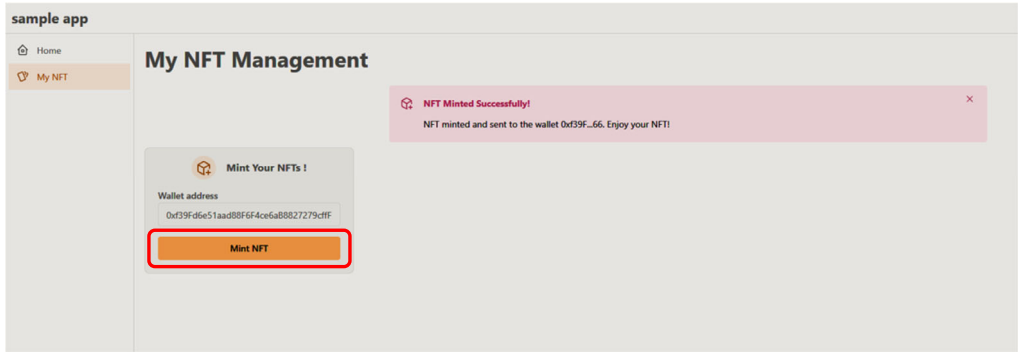
HardHat
スマートコントラクト用
フレームワーク

Solidity
スマートコントラクト
開発言語

MetaMask
ウォレット、仮想通貨の購入に使用

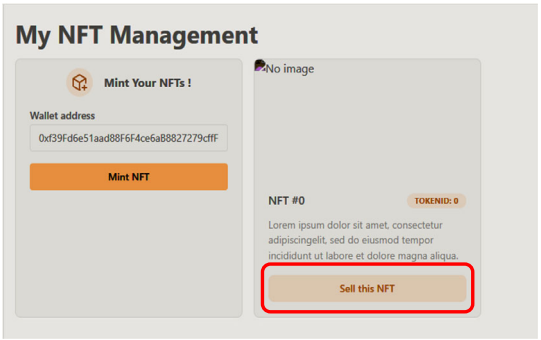
研究結果・考察
DAppsの開発

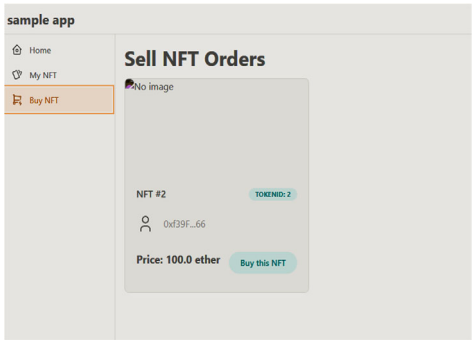
NFTの生成機能



研究結果・考察
DAppsの開発

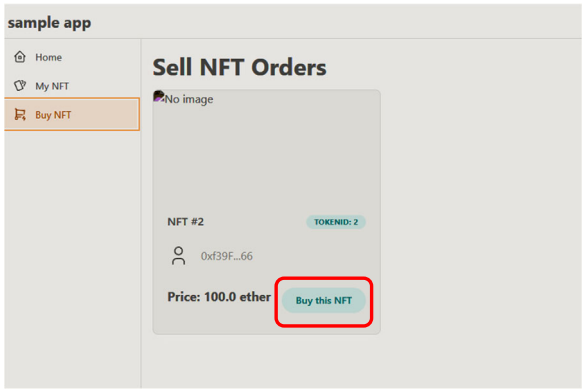
NFTの出品機能





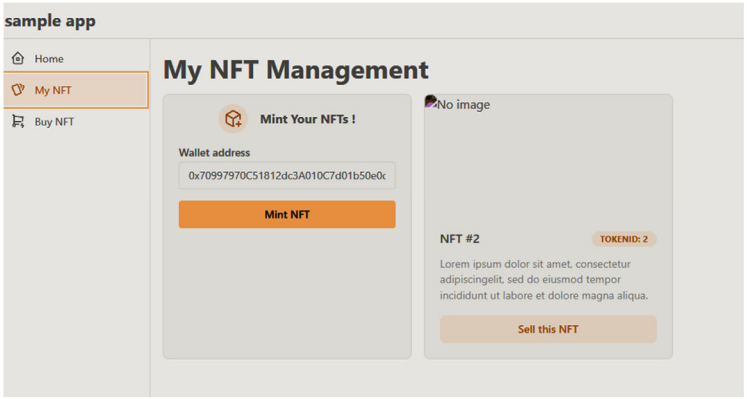
研究結果・考察
DAppsの開発

NFTの購入機能

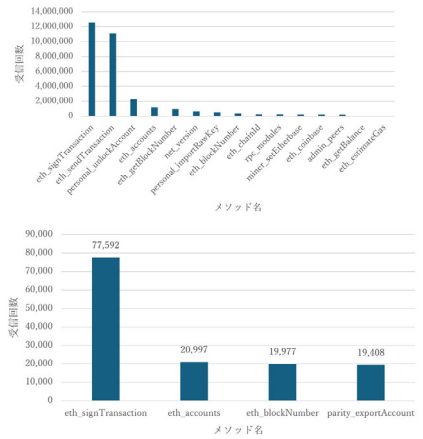


研究結果・考察
DAppsの開発

NFTの購入機能



研究結果・考察
Web3におけるセキュリティリスクの分析

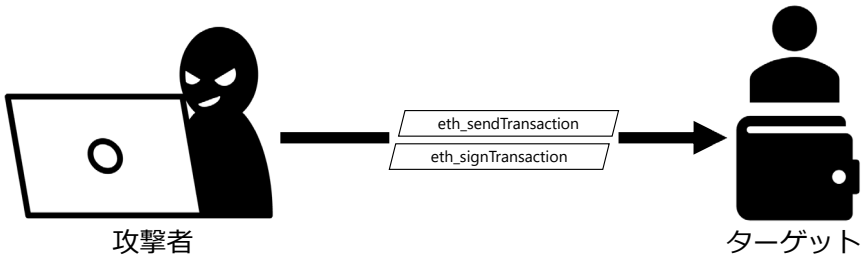


考えられるリスク

- ポーリングアタック
- 辞書攻撃
- マイニング報酬の横取り
- スマートコントラクトへの攻撃
- エクリプス攻撃

研究結果・考察
Web3におけるセキュリティリスクの分析

ポーリングアタック

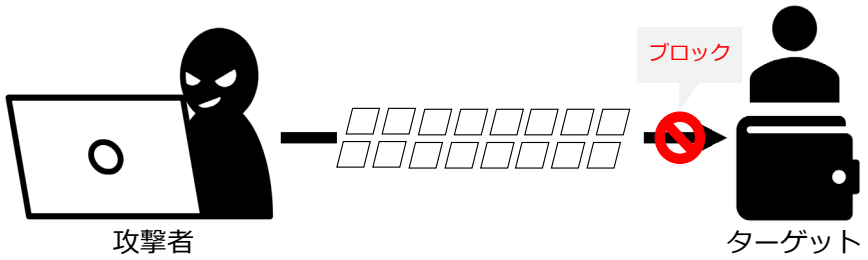


攻撃者が送金メソッドを絶え間なく送信する攻撃

ターゲットが攻撃に気づかずにアカウントのロックを解除すると、送金が実行される

研究結果・考察
Web3におけるセキュリティリスクの分析

リクエストのレート制限



同一IPアドレスや特定のウォレットに対して短時間で大量の攻撃に使用されるメソッドが送信された場合、一定時間そのリクエストをブロックする

まとめ　参考文献

まとめ

・Web3特有の攻撃手法が確認できた
・ポーリングアタックに対して有効な対策として、リクエストのレート制限が有用であることを示した

今後の課題

・Ethereumネットワークにハニーポットを実装し、攻撃頻度や新たな攻撃が確認できるか分析する

謝辞

本研究の実施にあたり、五郎丸秀樹先生、高木徹先生に御協力を頂きました。

御礼申し上げます。

Dimas Subhan Charles Lim「Unveiling Attack Patterns: A Study of Adversary Behavior from Honeypot Data」、2023 IEEE International Conference on Cryptography, Informatics, and Cybersecurity、IEEE、2023、178~183 頁

Dimas Subhan Charles Lim「 Analyzing Adversary's Attack on Ethereum Collected from Honeypots」、2023 11th International Conference on Information and Communication Technology 、IEEE、2023、313~318 頁

面和成「セキュリティに焦点を当てたブロックチェーン技術の最新の研究動向」、電子情報通信学会 基礎・境界ソサイエティ Fundamentals Review 、 18 巻 1 号 p. 88-100 、2024

陳 浩太・面 和成、「Ethereum ネットワークにおけるハニーポット設置に向けた攻撃活動の分析」、『信学技報』120 巻 411 号、電子情報通信学会、2021年、265~272 頁

王 佳・佐々木貴之・面 和成・吉岡克成・松本 勉、「Etherpot:イーサリアムのクライアントへのサイバー攻撃を観測するためのハニーポット」、『信学技報』121 巻 69 号、電子情報通信学会、2021 年、56~61 頁