SecHack365

PolyTorus

https://polytorus.com/

https://github.com/PolyTorus/polytorus

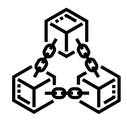
量子時代に向けたレイヤー1ブロックチェーン

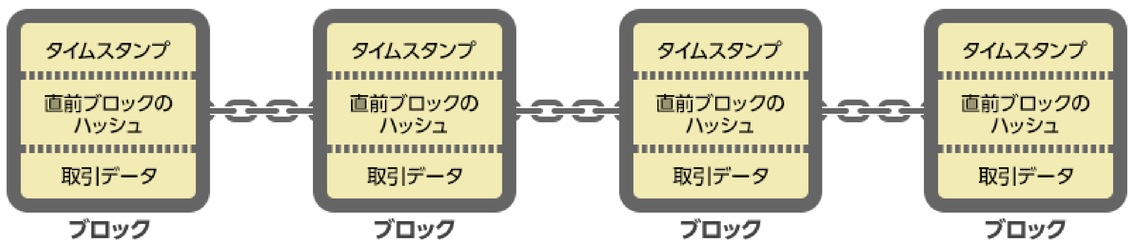
研究駆動コース 26R 中西陽路

ブロックチェーンとは

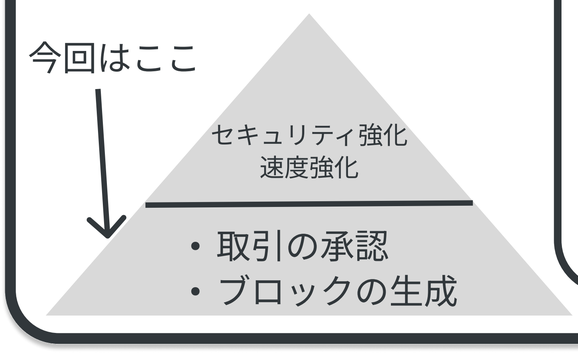
ひとつ前のHash値を参照することで、
ブロックが連鎖し改ざんが困難な仕組みになっている

- 個人の資格の証明
- 芸術品購入
- ゲーム
- 仮想通貨





レイヤー1とは



有名なレイヤー1ブロックチェーン

Bitcoin　Sui　Ethereum　Solana

必要性

量子コンピュータ攻撃の対策
長期的なデータ保管の安全性確保
市場の透明性確保

ユースケース

被災したらどうする?

現金も使えない、クレカも使えない、
誓約書書くの嫌...

オフライン決済対応ブロックチェーンしかない!!!

量子コンピュータの脅威

1. 量子コンピュータの発展
2. Shorのアルゴリズムが実用レベルに到達
3. RSAや楕円曲線暗号が危殆化
4. 量子コンピュータの攻撃飛んでくる
5. アカウント乗っ取り
6. 貯金0円になる

改善点

1. 既存システムの危殆化

2. 取引速度速い
3. ノード参加難しい

→

1. 量子耐性のある暗号への移行
高速な耐量子暗号の採用

2. 取引速度の維持　WebRTCの採用
3. ノード参加の簡略化

弱点

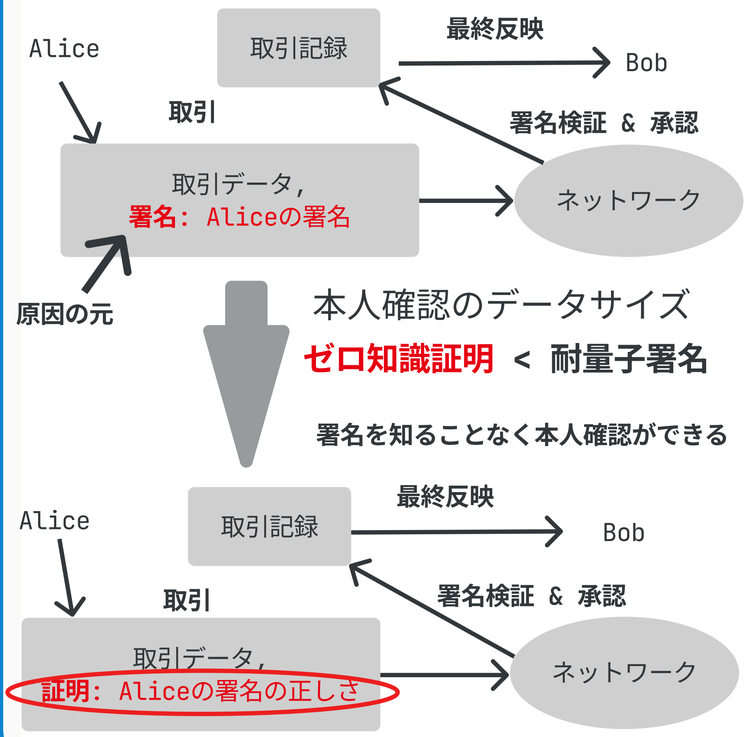
ECDSAの3倍

署名長が大きい
署名生成/検証速度は段違いで早い

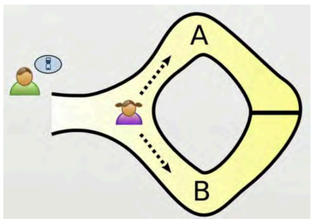
	公開鍵長 + 署名長 (Byte)	鍵生成 (ms)	署名 (ms)	検証 (ms)
Falcon	**897 + 666 = 1563**	**8.64**	**1/5.948**	**1/27.933**
CSI-Fish	512 + 956 = 1408	400	1480	1480
SQISign	64 + 204 = 268	218	1081	19

- **ストレージ容量の増大**
- **スケーラビリティの低下**
- **ノード間通信コストの増大**

取引サイズ削減方法



ゼロ知識証明



- 情報開示しない
- 情報の正確性担保
- プライバシー保護

- 医療業界
- 金融業界
- 認証システム

FALCON

- Compactness
- Speed
- Scalability
- RAM Economy

GPVフレームワーク + NRUE格子 = FALCON

FALCON
Fast-Fourier Lattice-based Compact Signatures over NTRU

解決結果

約22%減

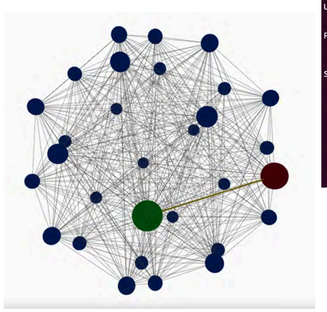
1536 bytes ⟶ 1217 bytes

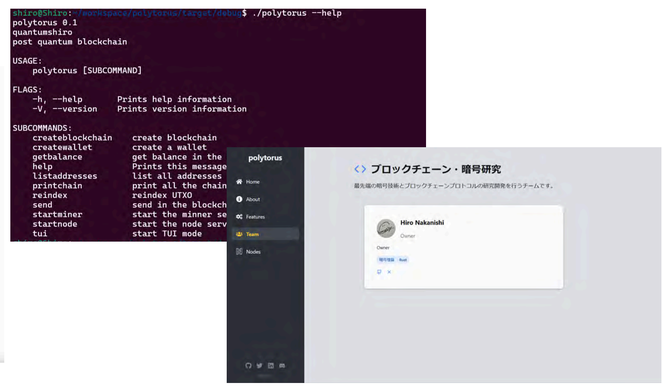
２万倍遅い

0.0075356 sec ⟶ 219.6475256 sec

SCIS2025
FALCONを用いた量子耐性ブロックチェーンの
トランザクションサイズ削減に関する検討

SCISという学会で
発表できた





基本的な送受信

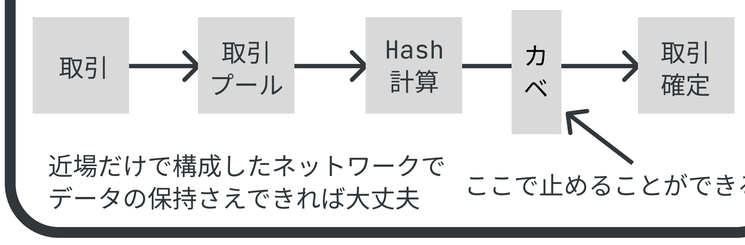
1. 財布の作成
2. AliceからBobへの送金
3. ブロック確定機能

Base58Encodeにより非常にコンパクト
コマンド一つで送金可能
CUIからもTUIからもGUIからも操作可能

オフライン決済

- 任意のタイミングでの取引確定が可能

即時取引確定も可能 ⟶ 取引時間短縮!!!



高速な通信

サーバを建てずにクライアント同士で通信可能

- WebRTCによる低遅延高クオリティな通信
- トランザクション削減技法によるデータサイズ削減

これによりできるだけ取引が可能に

WebRTC

今後の展望

- コミュニティの規模を大きくする
- ノードの運用維持方法を考える
- GUIによる送受信ページの作成
- OSSコミッターを増やす
- 高速なブロックチェーンを真似る
- コンパクト性を強調する

SecHack365での一年間

春-夏

- ブロックチェーンって何?
- どうやって自分らしさを出していこうか
- やっぱり最近流行のZigで書こう！！
- Zigって通信周りまだしょぼいなぁ
- おとなしくRustで書くかぁ
- 単純に耐量子暗号にすり替えると問題あるぞ??

秋-おわり

- 解決した問題学会に発表したいなぁ
- いやぁ論文執筆進まんなぁ
- ある週で大量に進捗を生み出す
- 地道な修正を行って無事に発表終了
- 謎のこだわりでHP破壊行為
- 無事修了へ

NICT

一人だけじゃここまで楽しく過ごすことはできませんでした。
皆さんありがとうございました。