ISS-P-047

ブロックチェーン秘密鍵のバックアップエコシステムについて —データ作成および検証プロトコルの実装—

白濱　敬也†　　森山　真光†
† 近畿大学大学院 総合理工学研究科

1. はじめに

ブロックチェーンは，非中央集権な仕組みとして近年注目されている．ブロックチェーンを利用するうえで，秘密鍵のバックアップが重要ではあるが，メジャーな BIP39[1]は可用性が低い．そこで，利便性の向上を目的と，ブロックチェーン秘密鍵のバックアップエコシステムにおける，バックアップデータの作成および検証プロトコルを実装する．

2. 先行研究

類似の先行研究[1]では，秘密鍵を暗号化し，暗号化データを秘密分散法[2]によって分割することでバックアップデータを作成している．また，バックアップデータはそれぞれ複数ノードに送信することでデータを保管している．ここで，ノードが保管するデータが紛失されていないかの確認が行えないという問題がある．本研究においては，データの保管証明(Proof of Custody 以下，*PoC*)を用いたエスクロー[2]によって，ノードによるデータ紛失問題を解決する．

3. エコシステムの概要

図 1 に秘密鍵バックアップデータの作成プロセスを示す．まず，パスワードとランダムソルトから鍵導出関数[3]による鍵派生処理を経て，暗号化鍵を導出する．次に，この暗号化鍵を用いて秘密鍵を暗号化する．そして，ランダムソルトは秘密分散法によって分割する．

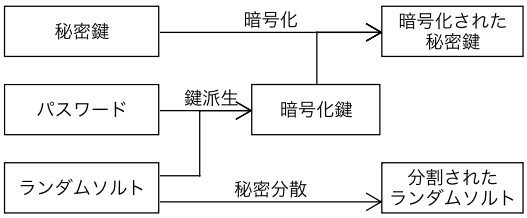

図 1 秘密鍵バックアップデータの作成プロセス

*PoC*は分割されたランダムソルトによるデジタル署名によって行う．データ保管者があらかじめ予測できないランダムなデータに対してデジタル署名を行い，署名を検証することで，その時点でのデータ保管は証明される．

エコシステムは，分割されたランダムソルトの保管サービスを提供するプロバイダと，そのサービスを利用するクライアントによって構築される．クライアントは分割されたランダムソルトにメタデータ加えた 32byte のデータを複数のプロバイダへ送信する．クライアントはエスクローを介してデータ保管サービス手数料を支払う．プロバイダはこれを受け取るために *PoC* を行う．

3. 実装

秘密分散関数は，Shamir[3]により提案された（ k, n ）しきい値法を用いた．この手法では，秘密情報を n 個に分割した際に任意の（ $k-1$ ）個からでは秘密情報に関して全く情報を得られない．鍵導出関数は，PHC（Password Hashing Competition）によって推奨されている Argon2[4]を用いた．Argon2 ではソルトを用いてハッシュ化している．

4. 結果

図 2 に実装したシステムを実行した様子を示す．分割数を 5，しきい値を 3 でデータの作成および検証を行った．

```
Password: P@$$W0RD
SSSS Params: {"shares":5,"threshold":3}
Argon2 Params: {"time":18,"memory":262144,"parallelism":1}
Seed: 5VXh7bALAYwS29oNTGQE8BK6fMYP9KQpRA9ayLwyYoCk
Encrypted Seed: 6EDpQ2aKpQhA3nXCFXdLAztXfFFSNxY8BUJPrrGk79yNAfLK2kCr8aaJy
pQpL4zkk2
Meta + Share [0]: 4yqjv9cLXVynECZta7HNrAgncJgYXhNSXeBoW66xQEg
Meta + Share [1]: 8tFPQshEMzgLqF3cptSuNodh9NTReUSE26ftfGqEq2C
Meta + Share [2]: Cnf2ubn8CVXaKBYYV1Knnqjxxz GMHtgtAQqib1CqtqT
Meta + Share [3]: Gh4gQKs22zAEZ1qX9iQSziKZEEZ9RS3eC8wETpUWC4Q
Meta + Share [4]: LbUKu3wusUoVHk6hYh1dcNh1a8V1UYcjd3DGFJbWBr9
Random Data: SAebbLWMDpsVc4oTMFh8iw
Signature [0]: iCkooMyhkczfURXdp74UvphXHgQYVwgR6ME7YFHD6UYji9641at8sobeYM
EvKuKcK87Mxvx9uc6BDMZdsXANooE
Signature [1]: 4Tny13V5oxMc6ZTt6mgpa8M7RY5iL1htDdq1zdxRctcpFHEsi73Rk3fc3o
K771RUCric7kdPtkp1aV1Zw8jjRctk
Signature [2]: 2shXpS8ySGymxr3FVt63iBAdYo7KnYyKmDvyGr9qSYAKoxKdiJoi7XuLZJ
R1cNhfZktkCTRy73auBUDAsCASH4UK
Signature [3]: 3Fo89YYqfWV1WKbiEvCT1iKvvhhe13tmNHMZpmXk9T7CpvYXWRNu2wYrwG
Wz33pgqPbQ8su2mxn82yYwKeoDKwJ6
Signature [4]: 4RJhMMBJ2GhdnrMvZjGZc8h67mRgo2DehF1TPSBArprq5UKENAqgsS2Gf9
s67L2jXwX6cKGWMdednou5mGHVNStq
```

図 2 暗号化とデータ分割

5. 今後の課題

今後はプロバイダがクライアントを認証する方法について考察し実装する予定である．

参考文献

[1] Feng Xiong, Ruiyang Xiao, Wei Ren, Rongyue Zheng, and Jianlin Jiang, “A Key Protection Scheme Based on Secret Sharing for Blockchain-Based Construction Supply Chain System”, IEEE Access Volume 7, pp.126773-126786, Sept-2019.

[2] 山本博資，“秘密分散法とそのバリエーション(符号と暗号の代数的数理)”，数理解析研究所講究録, 1361: 19-31, Apr-2004.

[3] A. Shamir, “How to share a secret”, Communications of the ACM, 22, pp.612-613, Nov-1979.

[4] Alex Biryukov, Daniel Dinu, and Dmitry Khovratovich, “Argon2: the memory-hard function for password hashing and other applications”, PHC, March-2017.

[1] Bitcoin Improvement Proposals

[2] 商取引の際に取引を仲介し安全を担保する第三者．

[3]与えられたパスワードから暗号用の鍵を生成する． ソルトやキーストレッチングによって攻撃耐性が高まる．