講演番号：3

分散型台帳技術を活用した金庫の相互情報管理方法の検討

B－6　Examination of information management method of safes using distributed ledger technology.

安部武尊† 末田 欣子†
Takeru ABE† Yoshiko SUEDA†
† 明星大学 情報学部
† School of Information Science, Meisei University

1. はじめに

近年、スマートフォン、ウェアラブル端末、センサーの向上により IoT が注目されている。本研究では、宝石や貴重品を保管する金庫の開閉時刻や物品情報などを取得可能にし、分散型台帳技術（ブロックチェーン）の特徴である改ざん防止を利用した、金庫内情報の相互情報管理システムについて提案し、実装、評価を行うことを目的とする。

2. 課題

金庫の IoT 化により取得した金庫内情報の消去や攻撃者が情報を改ざんする等の問題の可能性がある。

3. 提案手法

本研究では、分散型台帳技術を活用することで、金庫内情報の消去・改ざんの防止と検出を実現する。図 1 に示すとおり、一定時間で取得した金庫内情報を 1 日ごとにまとめ、ハッシュ化する。そのデータを分散台帳に記録し、利用者間で共有・保管する。

手順は以下の通りになる。

1. センサデータの取得
2. センサデータの暗号化
3. マークルルートの生成
4. ハッシュチェーンの生成
5. 鍵生成
6. トランザクションの生成
7. 台帳にセンサデータを入れる
8. マイニング

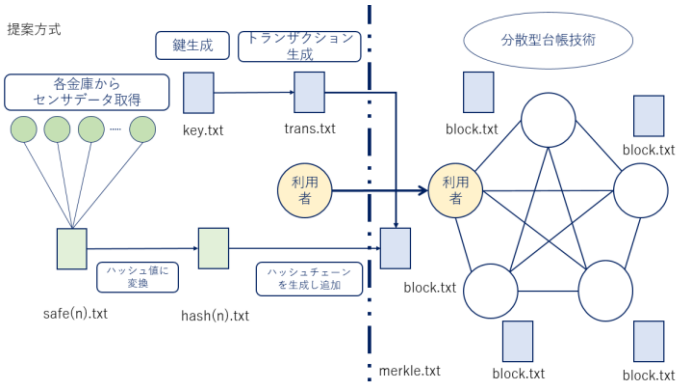

図 1　提案手法

4. 評価

評価項目は以下の通りである。

(1)マークルツリーを利用した平文の改ざん検知
(2)センサデータのハッシュチェーン生成確認
(3)マイニングの難易度の最適化
(4)分散型台帳技術を利用した各ノードの分散台帳が同様の情報かどうか確認

5. 評価結果

実装したプログラムにおいて、4. (2)センサデータのハッシュチェーンの生成を行い（図 2)、改ざんを行った場合(図 3)の網掛け部分が変化することを確認した。


```
[
  "hash_chain": "",
  "merkleroot": "820b7fd05fe1ca3af4ab744bd4f769f85791d6378d05b6c6138600ff36134899",
  "hash": [
    "069e44e87a8c3675f6b96501de91e9814e9faa148868c1f386050569b4fbf6bf",
    "100230af28078c471b8648c36d09b1511a45ea17dc8b2c69043e538d7bbba72b",
    "77da14140acd9dc556657b43b2735024dd12d7753e9f5629e8e63fe8498fda67",
    "b74105043fbf9d7e05048971b187750f78633b7ec2187cf324345bfa99f5acb8"
  ]
},
{
  "hash_chain": "c7e98a288107e7aefcb71c2206bbc2b9dc9fdb943db5408c24ff8508e9755f20",
  "merkleroot": "8b9a6e186d1bf9367177f825f013400c47cc86fdf44621e875494f831698ab64",
  "hash": [
    "cad30df0fcfb7c8da410ec1df30e607b4847f650340a3559478c5d32650c8f75",
    "5ddb6c3b6c46250b63862dadaf64e0f524320831c911aaf472a00bef49d3e9a9",
    "f0c122992fba1e37dcd632b8802de61b635f1b1ecbb8d84c6dac3f15b4bd10a7",
    "4ada2be5a435a806a1701b10af5a255464edaf33682853726f7bcc0fa3e02674"
  ]
},
```


図 2　ハッシュチェーン（1～8 日）


```
{
  "hash_chain": "",
  "merkleroot":
"820b7fd05fe1ca3af4ab744bd4f769f85791d6378d05b6c6138600ff36134899",
  "hash": [
    "069e44e87a8c3675f6b96501de91e9814e9faa148868c1f386050569b4fbf6bf",
    "100230af28078c471b8648c36d09b1511a45ea17dc8b2c69043e538d7bbba72b",
    "77da14140acd9dc556657b43b2735024dd12d7753e9f5629e8e63fe8498fda67",
    "b74105043fbf9d7e05048971b187750f78633b7ec2187cf324345bfa99f5acb8"
  ]
},
{
  "hash_chain": "b3da9c0fb31b0f05f4dfb71b40029f336f0c0014d9f378fbfbe925ee510f32b8",
  "merkleroot":
"c5e48c76787446d8f4e989641abb6e50f73866599c8cf3e118527591f200fbf6",
  "hash": [
    "cad30df0fcfb7c8da410ec1df30e607b4847f650340a3559478c5d32650c8f75",
    "5ddb6c3b6c46250b63862dadaf64e0f524320831c911aaf472a00bef49d3e9a9",
    "4e94864d3a5724076be1dc155d9d2f2122474563adbbc0a36e918cd49d33a18f",
    "4ada2be5a435a806a1701b10af5a255464edaf33682853726f7bcc0fa3e02674"
  ]
},
```


図 3　改ざんされたハッシュチェーン（1～8 日）

6. まとめ

本研究は、金庫の IoT 化を目指し、分散型台帳技術を用いることで金庫内情報を共有し、安全性を高めることができた。将来的には金庫から取り出すときに個人 ID カード等を使うことにより更なる安全性を追求していく。

参考文献

[1] 松浦健一郎, 司ゆき, ”入門仮想通貨の作り方　プログラミングで学ぶブロックチェーン技術・ハッシュ・P2P の仕組み”（2018）