Ethereum による貸出し承認システムの開発と評価

高松 毅瑠 †

明治大学総合数理学部 先端メディアサイエンス学科 菊池研究室 †

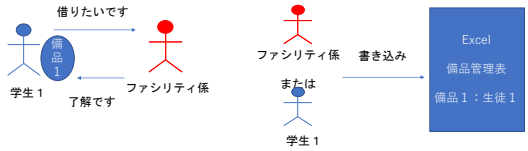

図 1　従来の貸し出し処理

1　はじめに

2020 年コロナウイルス感染対策のために出勤をできるだけ減らす試みが進んでおり，在宅でのリモートワークが推奨されている．しかしオンラインで承認することができない手続きが多くあり，承認のためだけに出勤する必要があることもある．

例えば Excel を使った備品を管理する応用を考える．共有されたファイルにはアクセス制御がなく，後から借りた備品の情報を書き換える不正が生じる可能性がある．第三者の承認なく不正に備品を持ち出す事も懸念される．

そこで，本研究では，ブロックチェインシステムを用いてこれらの認証の偽装や文章の不正更新を防止し，オンラインで承認と第三者による検証可能なシステムの開発を試みる．安全性と利便性を実現したシステムを実装し，その性能評価を報告する．

2　貸し出し承認システム

本研究室ではクラウドのファイル共有システムと Excel を使って，備品の貸し出しの依頼と管理者の承認をすることで備品を管理している．この管理法では管理者に連絡し，承認を受け，自分で Excel 上に記録することで備品を借りる事が出来る．処理の流れを図 1 に示す．

この手法の問題点として，

- 管理者になりすましが出来る点
- 別の生徒になりすましが出来る点
- 一旦書き込んだデータを後から改竄できてしまう点
- 管理者の不正を防ぐ事ができない点．

の 4 点が挙げられる

†Department of Frontier Media Science, School of Interdisciplinary Mathematical Sciences, Meiji University, Kikuchi Laboratory

3　要素技術

3.1　ブロックチェイン

ブロックチェインはネットワークに分散されたデータベースである．非中央集権的なシステムである事．記録されているデータを誰でも確認できる事，改竄が困難である事，が特徴である．

ブロックチェインでは取引（トランザクション）をブロックにまとめ記録している．また，ブロックはタイムスタンプ，前のブロックのハッシュ値，ナンス，トランザクションから成る．この構造により，あるブロックを改竄しようとするとそのブロック以降の全てのブロックを改竄する事が必要になり，改竄を困難にしている．

3.2　Ethereum

イーサリアム (Ethereum) はブロックチェイン技術を暗号資産以外の領域で使うために作られた暗号資産である．また，ここで使う仮想通貨をイーサ (Eth) と呼ぶ．

3.3　スマートコントラクト

スマートコントラクトは取引などの契約をブロックチェインに書き込み，自動で実行する機能である．あらかじめ決められた条件に当て嵌まった時のみプログラムが実行される仕組みになっている事で，不正な第三者の介入も，相手を信頼する必要もなく取引を行う事が出来る．

3.4　Solidity

イーサリアムではスマートコントラクトを実装するためのプログラミング言語として Solidity がある．Solidity で書かれたプログラムをブロックチェイン上に配置し，そのプログラムを Gas と呼ばれる手数料を支払って実行する事でスマートコントラクトを動作させる．

3.5　MetaMask

MetaMask は google crome のプラグインとして利用できるウェブウォレットであり，これを利用する事で Eth の支払いを伴うプログラムをウェブ上で実行する事ができる．

4　提案手法

4.1　概要

本研究では，研究室内での備品の貸し出しをブロックチェイン技術を用いてシステム化し，運用にかかるコス

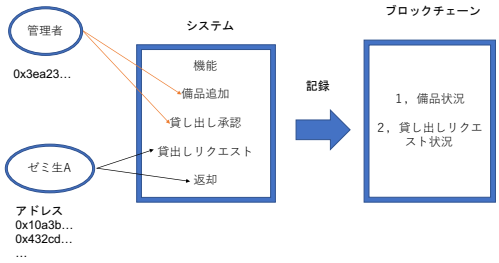

図 2　システム構成図

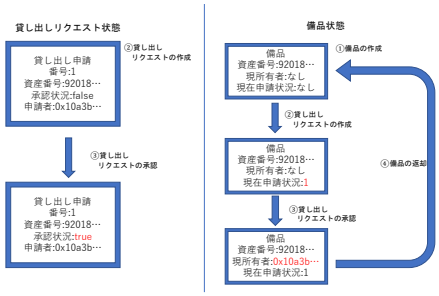

図 3　処理フロー

トと有用性を評価する．

4.2　システム構成

システム構成図を図 2 に示す．ブロックチェインには貸し出し状態を 2 つの情報に分けて記録している．1 つは貸し出しリクエストの状態，2 つ目は備品の状態である．また，この 2 つはシステム利用者の入力によって変化する．処理の流れを図 3 に示す．処理の流れは以下 4 つのステップで行われる．

(1) 管理者が資産番号をブロックチェイン上に記録する．
(2) 生徒が管理者に貸し出しリクエストを送信する．
(3) 管理者が貸し出しリクエストを承認する．
(4) 生徒が利用が終わった備品を返却する際にブロックチェイン上に記録する．

備品の登録，貸し出しの承認は管理者のアドレスでのみ行うことができる．

4.3　実証実験

12 月 5 日から 15 日までの 10 日間に渡り，菊池研究室内 18 名にシステムの導入から備品の貸し出し，返却まで行った．その際にかかった時間，手数料などを計測した．12 月 22 日システムの全機能を利用し，その手数料を調査した．

4.4　実験結果

被験者のシステム導入は 18 名全員が成功した．システム導入のためにかかった時間の平均は約 15 分であり，最大は 30 分，最短で 3 分 42 秒であった．また，30 分かかった際にはシステムにバグが起こっておりバグの対応に時間がかかってしまった．

表 1　プログラム実行によるコスト

機能名	動作	手数料
デプロイ	プログラムをブロックチェインに配置する．	0.03590924
makeFacility	備品の情報を記録する	0.000049033
CreateContract	貸し出しの申請を行う	0.000116253
viewContractname	申請の情報を見る（書き込みなし）	0.0
agreeContract	申請に許可を出す	0.00005085
returnFacility	備品の返却をする	0.000025

表 2　従来手法との比較

	(1) 管理者へのなりすまし	(2) 持ち主へのなりすまし	(3) 書き込み後の改竄	(4) 管理者の不正書込み，改竄
本手法	○	○	○	○
従来手法 (Excel)	×	×	×	×

プログラムを実行した結果を表 2 に示す．実験の際は 1Eth ＝ 61,695.57 円であった (2020/12/22 17:01:03)．実験の結果システムの導入には約 2,214 円，その後貸し出し機能を使う毎に手数料 (2 から 6 円) がかかる．

4.5　従来手法との比較

従来手法の問題点であった (1) 管理者へのなりすまし，(2) 持ち主へのなりすまし，(3) 書き込み後の改竄，(4) 管理者の不正書込み改竄，を比較する．

(1)(2) 本手法で作ったシステムに対してなりすましを行うには管理者の秘密鍵，所有者の秘密鍵を各々持っていなければならないため，Metamask での各々管理する過程の下では，不正は不能である．(3)(4) 不正な取引をブロック上に記録するには攻撃者がネットワーク全体のマイニングの 51 %以上を支配する必要があり，不正は困難なものになっている．書き込み後の修正はブロックチェインの性質上，書き換えが行われるとブロック上にその記録が残り，検出されずに不正な書き換えを行うことはできない．従来手法は以上の不正の全てに脆弱である．以上の比較を表 2 に整理する．

5　おわりに

本研究では Ethereum を用いた貸し出し承認システムを開発した．ブロックチェインの性質である改竄を防止した安全なシステムを開発した．システムの開発，利用にはデプロイが (2020/12/22 時点) 約 2000 円，1 つの貸出しリクエストを承認するまでに約 10 円かかる事を示した．本手法では 1 つの貸し出しに時間がかかり，すぐに持ち帰る事ができないと言ったデメリットがある．安全性の面とともに検討していくことを今後の課題とする．

参考文献

[1] 廣澤 龍典，上原 哲太郎，“ブロックチェインを用いた検証可能な抽選システムの提案”，*Computer Security Symposium (2019),pp,776-783,2018.*
[2] フォン ヤオカイ，松本 晋一，穴田 啓晃，川本 純平，櫻井 幸一，“次世代暗号通貨プラットフォーム Ethereum の実験的評価”，*Computer Security Symposium (2015),pp,1151-1158,2014.*