

Ethereumによる貸し出し承認システムの開発と評価

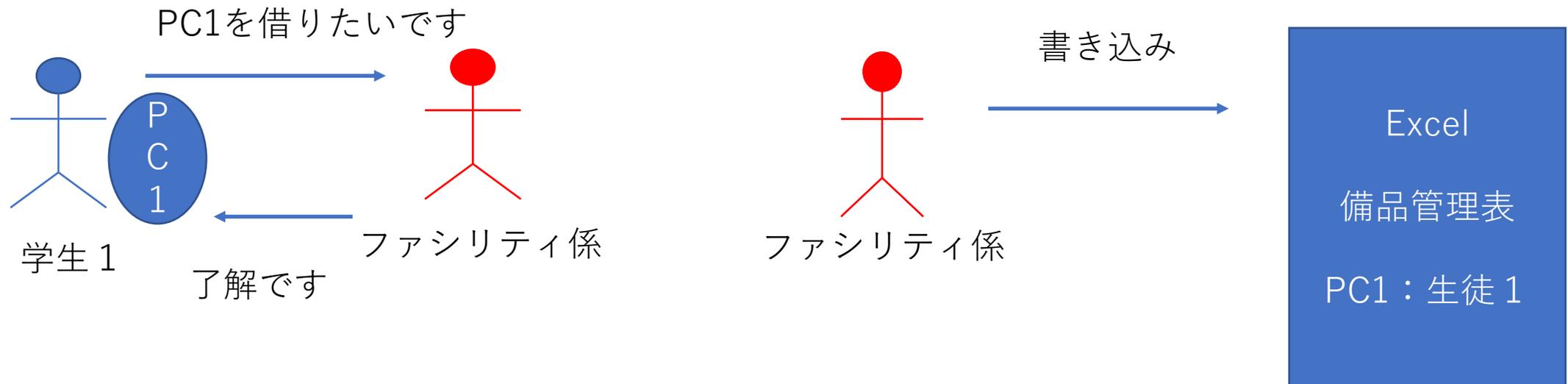
菊池研4年

高松毅瑠

研究背景

- 菊池研究室では備品の管理をExcelで行っていたが、管理方法が曖昧で不正が起こる可能性があった

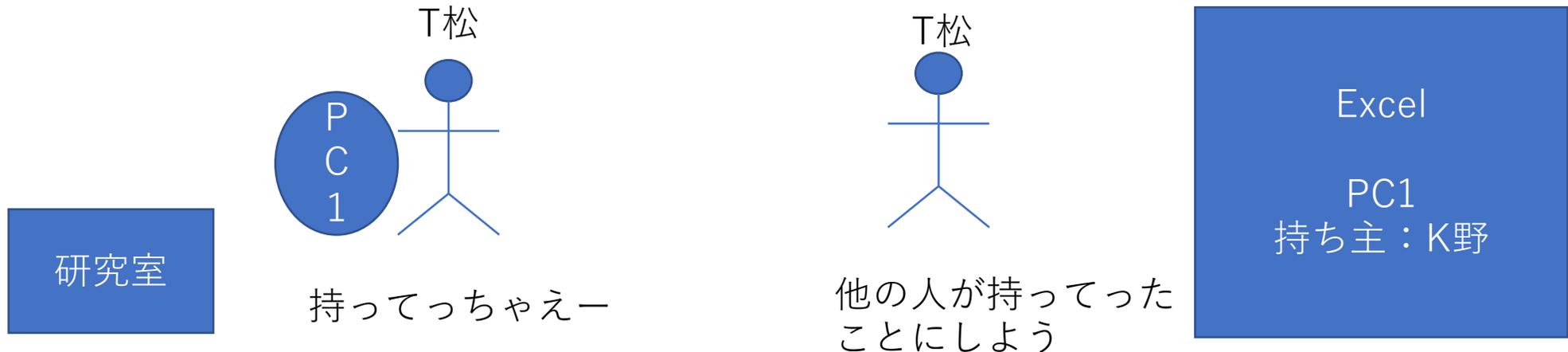
例



貸し出し承認システム

- 管理者，ユーザーのなりすましができる
- 後からデータの改竄ができる
- 管理者のみの書き込みにした場合，管理者の不正が防げない

例

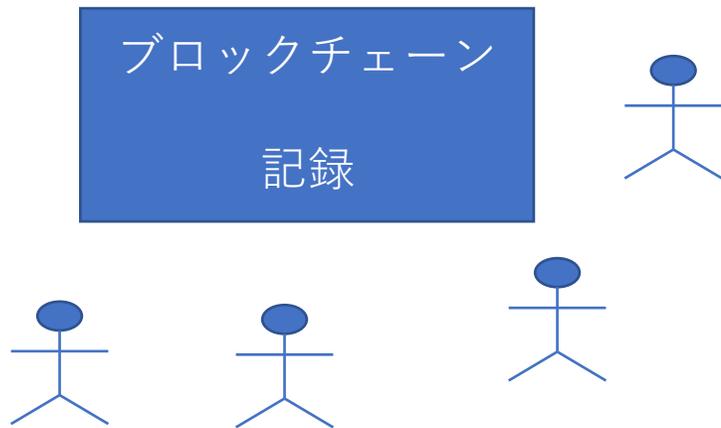


研究目的

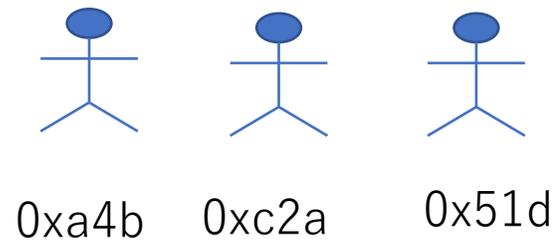
- 安全な貸し出しシステムの開発
- システムの導入にかかる時間, コストの評価

提案手法

- Ethereumを用いて取引データをブロックチェーン上に記録する.
- Metamaskを用いて全ユーザーをブロックチェーン上のアドレスと紐付ける.



誰でも見れる



全員に一つずつアドレス

Ethereum(イーサリアム)

- ブロックチェーン技術を暗号資産以外の領域で使うために作られたプラットフォームの名称. 暗号通貨としても流通している.

- 記録を誰でも確認できる

→後から不正を確認可能

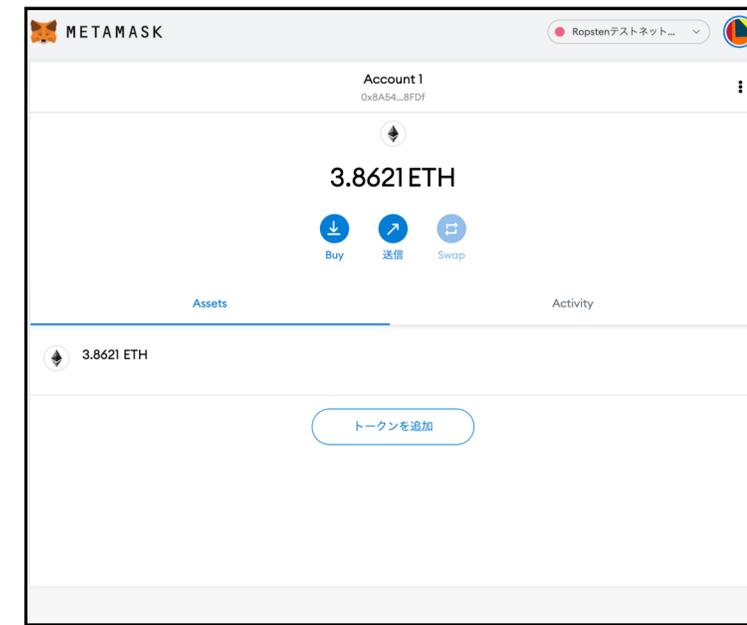
- 改竄が困難である

→不正な記録ができない

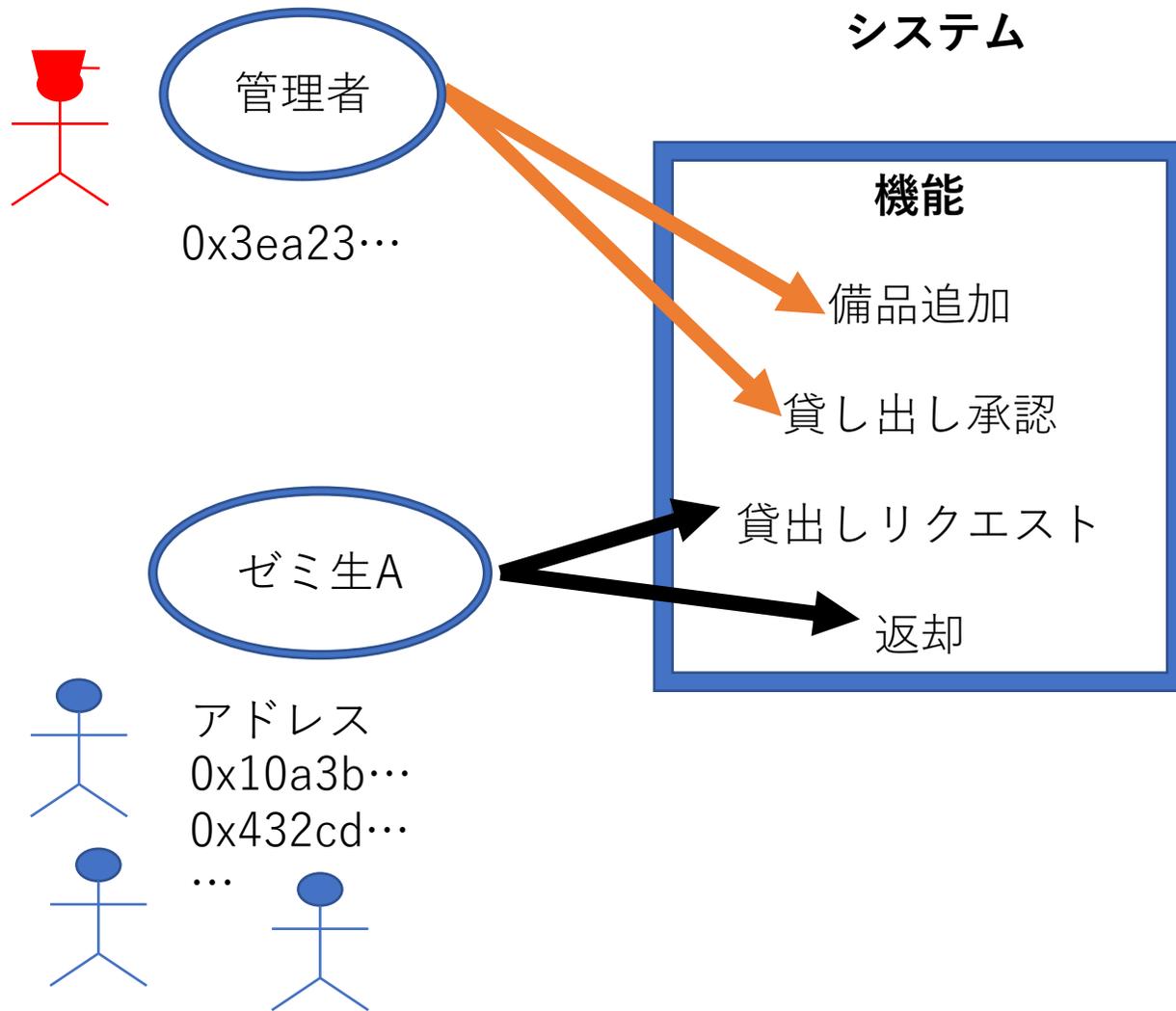
	ビットコイン	イーサリアム
知名度	○	△
暗号通貨	○	○
契約の自動処理	×	○

Metamask

- google chrome のプラグインとして利用できるウェブウォレット。Googleアカウントと紐付けて一人一つずつアドレスを取得できる。
- アドレスの秘密鍵は個人が所有する。
- 暗号通貨Ethを手数料として支払う事でシステムを利用することができる。



システム構成



ブロックチェーン



ブロックn-2
ブロックn-1
ブロックn

デモ

アプリ YouTube Amazon.co.jp: Pri... Lifebear [ライフベ... ホーム | Ethereum... ログイン|フューチャ... 菊池研究室— 明治大... Ethereum: イーサ... スマートコントラク... windy.mind.meiji.a... »

貸し出し管理

管理者アドレス

備品の資産番号を入力し”リクエスト送信”ボタンを押すことでその備品の貸し出しをリクエストできます。

リクエスト送信

リクエストの番号を入力することで、リクエストの承認状況を調べることができます。管理者のみ貸し出しを許可することができます。

確認 貸し出し許可

備品の資産番号を入力し登録、確認することができます。

登録 確認 返却

システム導入実験

システムの可用性の調査

- Metamask導入
- ウェブサイト接続
- 貸し出しリクエスト送信

期間	人数
12/5~12/22	18

システム導入実験

最短	最長	平均
3分42	30分	15分

システムバグ有り

被験者のコメント

- システムの導入に時間がかかる。
- ボタンの応答が遅い。
- 貸し出しまでの処理に時間がかかる。

システム利用コスト

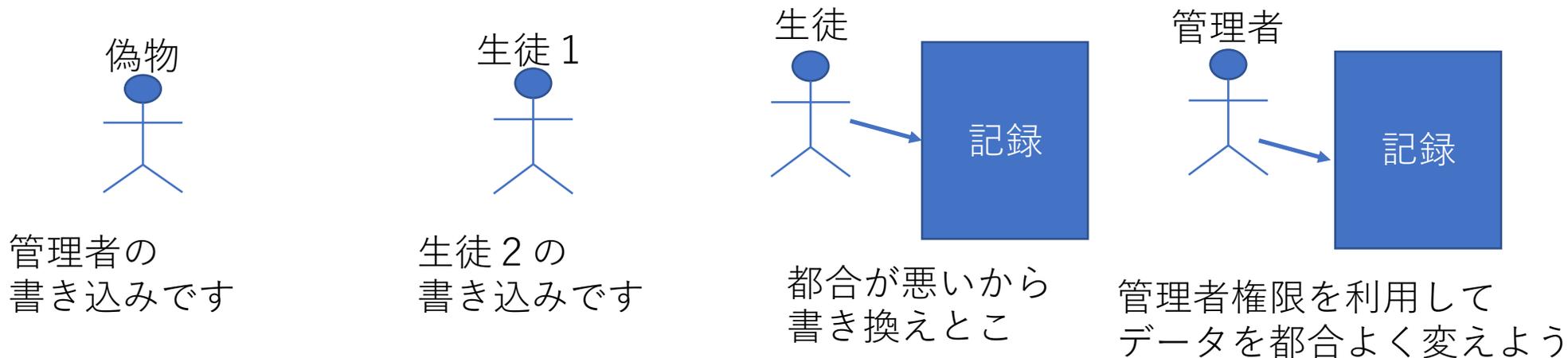
- システムを使用するコスト（手数料）が実現可能かどうか調べる.
- 2020/12/22, 1Eth=61,695.57
- システムのプログラムをブロックチェーンに配置, 全機能を使用し, その手数料を調査する.

システム利用コスト

機能名	動作	手数料
デプロイ (プログラムの配置)	プログラムをブロックチェーンに配置する	0.03590924 Eth 2215円
makeFacility	備品の情報を記録する	0.000049033 Eth 3円
CreateContract	貸し出しの申請を行う	0.000116253 Eth 7円
viewContractname	申請の情報を見る (書込みなし)	0.0
agreeContract	申請に許可を出す	0.00005085 Eth 3円
returnFacility	備品の返却	0.000025 Eth 1円

従来手法との比較

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



まとめ

- システムのデプロイに約2000円，一連の貸し出し処理に約10円かかる。
- 本システムの導入難易度は高く，システムとしてより使いやすくする必要がある。