

ブロックチェーンを用いた出席管理システムの提案

塚田研究室 218K6078 檜山 祐太

1 はじめに

各種学校や塾などでは、^{（出欠確認や集計処理など）}出席管理に関する作業は多くの労力を必要とし、その負担は小さくはない。しかし、学生の出席状況を把握することは必要不可欠であるため、近年では、ICT 技術を用いてより効率よく出欠を確認することができる出席管理システムの導入が数多く進められている[1]。

そこで本研究ではブロックチェーンを用いた出席管理システムのアーキテクチャを設計し、そのプロトタイプを実装する。

2 ブロックチェーン

ブロックチェーンとはデジタルな資産の移転や取引などの履歴データを複数の利用者と管理者によって共有される仕組みのことである。ブロックチェーンはいくつかの取引情報をブロックとしてまとめることで、矛盾した取引情報がないようにしている。また、取引情報をブロックとしてまとめる際に、矛盾した取引情報が同じブロックに含まれないように検証が行われる。ブロックは生成される際、1つ前のブロックのハッシュ値を含むことで連鎖する形態をとる。このブロックの連鎖のことをブロックチェーンという。ブロックチェーンのモデル図を図1に示す。

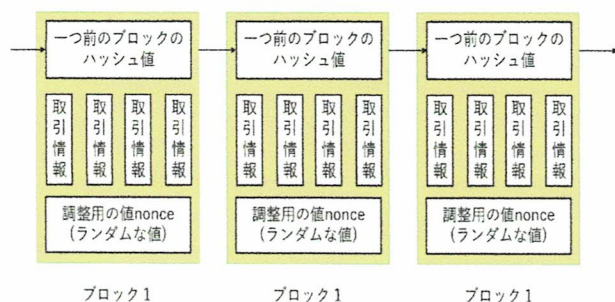


図1 ブロックチェーンのモデル図

2-1 ブロック構造

ブロックチェーンの各ブロックは1つ前のブロックのハッシュ値と複数の取引情報、調整用のランダムな値である nonce によって構成される。

2-4² ブロックチェーンの改ざん

ブロックチェーンの改ざんは容易ではない。なぜなら、攻撃対象のブロックを書き換えた場合、その書き換えたブロックのハッシュ値が変化するため、それ以降全てのブロックを作り直す必要がある。それに加え、次々に行われるブロック生成を追い越さなければいけないため、ブロックチェーンの改ざんは容易ではない。

3 出席管理システム

出席管理システムとは、学校や塾などにおいて、生徒の出欠状況を管理するシステムのことをいう。出席管理システムには様々な種類があり、中でも IC カードを読み取るカードリーダーを用いた出欠システムの導入が広く進んでいる。また、各種デバイスを管理端末とする出席管理システムも増加していて、こうしたシステムでは学生が所持しているスマートフォンやパソコンを使用し、クラウドで提供されるものもあるため、専用機器を準備する必要がなく、手軽かつ低コストで出席管理が可能である [1]。

4 アーキテクチャ設計

本研究で提案するシステムでは、生徒の出席情報はサーバに送信された際にサーバを介してブロックチェーンに登録される。学校はブロックチェーンに出席情報の確認申請を行うことで、部屋ごとの出席情報と生徒ごとの出席情報の確認を行うことができる。

4-1 要件定義

本研究で提案するアーキテクチャには次の3つの要件を定義することにした。

(1) 改ざん不可能：ブロックチェーンを用いて、出席者の情報を改ざん不可能にする。

(2) 出席情報の登録：生徒の出席情報がサーバに送られた際、その時点での時刻とともに生徒の出席情報をブロックチェーンに登録する。

(3) 出席情報の公開：学校はブロックチェーンに出席情報の確認申請を行うことで、部屋ごとの出席

A 情報と生徒ごとの出席情報の確認を行うことができる。

4-2 システム概要

本研究で提案する出席管理システムのアーキテクチャを図2に示す。

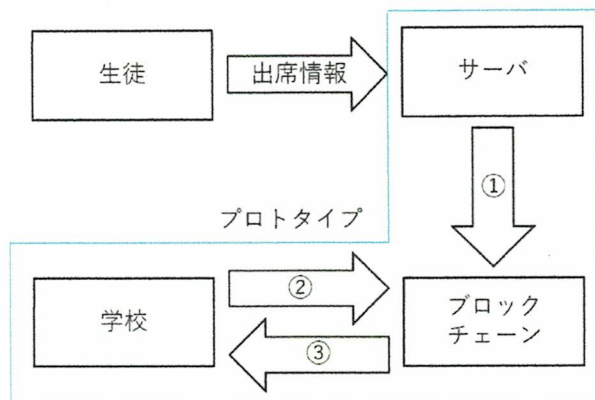


図2 アーキテクチャ図

①サーバに送られてきた生徒の出席情報をブロックチェーンに登録する。

②学校はブロックチェーンに出席情報の確認申請を行うことができる。

③ブロックチェーンシステムに学校から出席情報の確認申請が行われた場合、ブロックチェーンシステムから出席情報を学校に送信する。

今回の出席管理システムでは、生徒の出席情報をサーバに送信する部分以外の基本部分をプロトタイプとして実装する。

5 システム詳細設計

5-1 開発環境

本プロトタイプの作成においては、ブロックチェーンを利用した非中央集権アプリケーションであるEthereumを使用した。また、ソースコードはSolidity言語を利用して記述し、Solidityコンパイラのバージョンは0.4.15を使用した。開発環境はRemix[3]を用いた。

5-2 プロトタイプ概要

今回の出席確認システムは図2で示したプロトタイプ部分である。本プロトタイプは生徒の出席情報がサーバに送られてきた際に、その出席情報をブロックチェーンに登録し、学校による部屋ごとの出席情報と生徒ごとの出席情報の確認までの動作を目的

としたシステムである。また、部屋名と生徒名はあらかじめプログラム上に3つずつ登録しておくものとする。

6 実行結果

本プロトタイプを実際に動作させた結果、出席情報の登録や出席情報の確認が正しく動作することが確認できた。また、登録していない部屋名や生徒名が入力された際は、正しく動作し、ブロックチェーンへの登録は行われなかった。

今回のプロトタイプでは誰でも関数を実行できるようになっているため、関数を実行できる者に制限を設けたほうがよいと考える。また、今回のプロトタイプでは出席情報を削除する関数を導入していないため、古くなり必要がなくなった出席情報の削除ができないので、出席情報を削除する関数を実装したほうがよいと考える。

7 まとめ

ブロックチェーンを用いた出席管理システムを提案し、そのアーキテクチャを示すとともに、プロトタイプを実装した。その結果、出席情報の登録や出席情報の確認が正しく動作することが確認できた。

今回のシステムでは、管理者が存在せず誰もが全ての関数を実行できるようになっているため、関数を実行できる人に制限を設け、限られた人しか実行できないようにすることが今後の課題だ。また、出席情報を削除する関数を導入していないため、古くなり必要がなくなった出席情報の削除ができないので、出席情報を削除する関数を実装することも今後の課題だと考える。

参考文献

- [1] 出席管理システムの概要とおすすめのシステム
11 選、ミツカル
<https://mitsu-karu.com/article/attendance-management/>
- [2] 佐藤雅史、長谷川佳祐、佐古和恵、並木悠太、梶ヶ谷圭佑、松尾真一郎：ブロックチェーン技術の教科書、C&R 研究所(2018)
- [3] Remix - Solidity IDE
<https://remix.ethereum.org>

参考文献

重複して記述が多く冗長である。たとえばAとBとCや、XとYは同じとくりがんでいるだけである。1回だけ書けば十分である。そして、もっと他の重要なことを書くべきである。再提議は要求ないが、修正するならば再度読んでコメントしよう。