ISS-A-039

ブロックチェーンを用いた高等教育単位プラットフォームにおける鍵漏洩対策手法

坂本　悠旗†　　藤野　貴之†
†近畿大学工学部電子情報工学科

1. はじめに

近年，仮想通貨技術を筆頭にブロックチェーンを用いた技術が普及してきている．ブロックチェーンは仮想通貨に限らず様々な分野での適用が研究されている[1]．本研究は，EduCTX と呼ばれるブロックチェーン技術を用いた高等教育単位プラットフォームの研究を起点に，EduCTX における鍵漏洩の対策手法を提案，およびプロトタイプを実装し，動作確認を行うことを目的とする．

2. ブロックチェーン技術の概要

ブロックチェーンとは，ノードと呼ばれる端末複数が協調動作することによって実現される分散台帳技術である．従来のデータベース技術に比べ，改ざん耐性が非常に高く，単一障害点が存在しないなどの技術的特徴を持つ．本研究では主要なブロックチェーンプラットフォームの 1 つである Hyperledger Fabric を使用した．

3. EduCTX の概要

EduCTX[2]とは，欧州単位互換制度(ECTS)の概念に基づいたブロックチェーンベースの高等教育単位プラットフォームである． EduCTX は，ECTX トークンと呼ばれるトークンを学業の単位として処理，管理，制御する．この ECTX トークンを，大学の鍵と学生の鍵の 2 of 2 で多重署名したウォレットアドレスに貯めていき，その移転記録をブロックチェーンに保存することで単位システムを構築する．このとき，学生の鍵は学生自身の成績照会や，潜在的な雇用主などの第三者に対して学生の成績の一部あるいはすべてを提供する際のアクセス制御に用いられる．一方，大学の鍵はその単位をたしかにその大学が発行したことを証明するために使用される．この単位システムはブロックチェーンの改ざん不可能性などから安全に単位を管理でき，完全な単位情報を学生あるいは学生が情報を開示することを認めた潜在的な雇用主に提供する．また，異なる大学間で単位移転をする際にもこの統一された EduCTX プラットフォームの特性によって従来の事務手続きを大幅に短縮できると考えられる．

4. EduCTX の問題点

EduCTX では学生の鍵と大学の鍵の二つの鍵によって署名を行う．学生の鍵が漏洩した場合については論文中に記述があるが，大学の鍵が漏洩する可能性にいては言及されていない．しかし，大学の鍵が漏洩し，改ざんされた成績が登録されるシナリオは十分に考えられる．ブロックチェーンの来歴から，最も古くに登録された成績が正しいものだと決定すれば，鍵漏洩による成績改ざんは容易に防ぐことができると考えられる．しかし，それでは大学が誤った成績をつけた際，訂正のため新たな成績を追加することに対応できない．本研究では，この大学の鍵が漏洩した場合の対策手法を提案する．

5. 提案する鍵漏洩対策手法の概要

成績に署名するのに使用される鍵(DSK ： Data Signing Key)と DSK を署名する鍵(KSK：Key Signing Key)およびそれらを管理する認証局(CA ： Certificate Authority)を用意する．DSK が漏洩したことが発覚した場合には CA が該当 DSK を失効し，新たな DSK を生成，それを KSK で署名する．新たに生成して KSK に署名された DSK により，失効された DSK で署名されている成績情報を対象に再署名を行う．大学が正当な成績修正を実施する場合にも再署名が行われる可能性があるため，それらは来歴表示によって確認される必要がある．以上の一連の動作によって漏洩した旧 DSK は効力を失い，署名されていた成績情報は新 DSK により再度署名され成績の正当性は保たれる．このようにして鍵漏洩の対策を行う．実際の運用では KSK の管理をさらに商用 CA に委任することによって KSK 漏洩の対策も行うべきである．

6. プロトタイプ実装と動作確認

Linux 上に Docker を用いて Hyperledger Fabric ブロックチェーンの環境を構築し，単位プラットフォームを作成，提案鍵漏洩対策手法が動作することを確認した．

7. 今後の課題

現在の構造では，実際に鍵が漏洩してから漏洩が発覚して失効が行われるまでの間，有効な鍵が悪用される可能性が存在する．そのため，通常ではない鍵の使用の検知，あるいは鍵漏洩自体を検知する仕組みが必要である．

参考文献

[1] K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," in IEEE Access, vol. 4, pp. 2292-2303, 2016.

[2] M. Turkanović, M. Hölbl, K. Košič, M. Heričko and A. Kamišalić, "EduCTX: A Blockchain-Based Higher Education Credit Platform," in IEEE Access, vol. 6, pp. 5112-5127, 2018.