7ZG-05

小規模向けのブロックチェーンを用いた情報セキュリティシステム*

梅原拓也† 徳永順平† 園田皓平† 榎原博之‡

関西大学大学院理工学研究科システム理工学専攻† 関西大学システム理工学部電気電子情報工学科‡

1 はじめに

近年、IT の発展に伴い, 様々な業界で IT 技術が取り入れられている. 情報のリスク意識は急激に高まりつつあり, セキュリティ上のリスク対策をすることは非常に重要となっている.

また一方で, 仮想通貨であるビットコインの基盤技術として登場したブロックチェーンが, データを不変的に永続的に維持でき, 第三者からの干渉を免れるという特徴を持つことから, 大きな注目を集めている. ビットコインに代表されるように, ブロックチェーンは金銭の取引に利用されることが多く, 様々な金融分野で採用されている. また, ブロックチェーンは金融分野に限らず他の分野のサービスにも採用されている. 例えば, 不動産分野では, 偽造不可能な財産記録, 透明性, 検証可能性, および手数料の削減のためにブロックチェーンが採用されている. また, 食品分野では, 食品の動きを追跡し, 食品の安全性や, 食品の作成者および食品の流通を管理するためにブロックチェーンが採用されている.

そこで, 本論文では, 現実の空間での合議によって参加者を限定する新たなブロックチェーンを用いた情報セキュリティシステムを提案する. 提案システムを利用することで, データの安全性や信頼性が保ちやすく, 処理速度の速いシステムの構築が可能となる.

2 ブロックチェーン

ブロックチェーンは, P2P ネットワークであり, インターネットを通じて分散されているノードに, これまでの取引履歴や記録などが蓄積され, 取引単位（ブロック）ごとに 1 つのチェーン上に時系列に繋げて管理する技術である. 1 つのブロックをチェーン上に繋げる際には, 合意形成アルゴリズムが利用される. あらゆるノードにデータが分散して蓄積されるので, どこか 1 つを改ざんしようとしても難しく, データの安全性や信頼性が保ちやすいメリットがある. また, ブロックチェーンはノードを限定するかどうかでパブリックブロックチェーンとプライベートブロックチェーンの 2 種類に分類される. パブリックブロックチェーンとプライベートブロックチェーンの比較表を表 1 に示す.

パブリックブロックチェーンは, 管理者がいない非中央集権的な仕組みである. 運営管理や監視をする特定の人物や団体がいない代わりに, 不特定多数の参加者による相互監視や取引の承認, 取引履歴の蓄積をしていく仕組みになっている. パブリックブロックチェーンにおけるデメリットは, 合意形成に厳密なプロセスを行う必要があるため, 処理に時間がかかってしまうことやコストが高くなってしまうことが挙げられる.

プライベートブロックチェーンは, 1 人の人物や 1 つの組織が管理者となり, 参加者も不特定多数の誰もが参加できる形ではなく, 特定のメンバーに限り, 一定の組織やコミュニティ内のみで利用できるものである. これにより, 非中央集権的なパブリックブロックチェーンよりも, 合意形成の迅速化や低コスト化が図れる. プライベートブロックチェーンにおけるデメリットは, 管理者による不正や改ざんが行われてしまうというリスクがあることが挙げられる.

表 1 パブリックブロックチェーンとプライベートブロックチェーンの比較表

	パブリック	プライベート
管理者	不在	単独の組織
透明度	高い	低い
参加者	誰でも参加可能	管理者による許可制
合意形成	厳格 (PoW[1],PoS[2]等)	厳格でない (PBFT[3]等)
処理速度	遅い	速い

3 提案システム

本論文では, 現実の空間での合議によって参加者を限定する新たなブロックチェーンを用いた情報セキュリティシステムを提案する.

提案システムでは, 大学の研究室のように小規模（20〜30 人程度の人が所属する組織）での利用を想定し, 参加者の追加は, 現実の空間での合議によって行う. これにより, 管理者がいない非中央集権的な仕組みとなり, 参加者は特定のメンバーに限られるため合意形成の迅速化や低コスト化が図れる. 提案システムを利用することで, データの安全性や信頼性が保ちやすく, 処理速度の速いシステムの構築が可能となる.

提案システムの概要図を図 1 に示す. また, 提案システムの手順を以下に示す.

*Information security system using Blockchain in small organization

†Umehara Takuya, Tokunaga Junpei, Sonoda Koukei·Faculty of Engineering Science, Kansai University

‡Ebara Hiroyuki·Graduate School of Science and Engineering, Kansai University

[1]Proof of Work

[2]Proof of Stake

[3]Practical Byzantine Fault Tolerance

3.1 現実の空間での合意

新たにシステムへ参加したいユーザ（以下, 新規ユーザ）が現れた場合, システムの参加者全員が, 現実の空間で集合し, 新規ユーザが悪意のあるユーザでないか, 信頼できるユーザかを合議し, システムへの参加を許可するかどうかを決定する.

3.2 参加の決定

現実の空間での合議によって, システムの参加者全員が新規ユーザを信頼できる状態でのみシステムへの参加が許可される.

3.3 システムへの反映

新規ユーザがシステムへの参加を許可された場合, 現実の空間で合議によって「合言葉」を決める. そして, システムの参加者全員が決められた「合言葉」をシステムに入力することで新規ユーザがシステムに追加される.

3.4 参加者の削除

システムの参加者の削除は, 参加者の追加と同様に, 現実の空間での合議によって行われる.

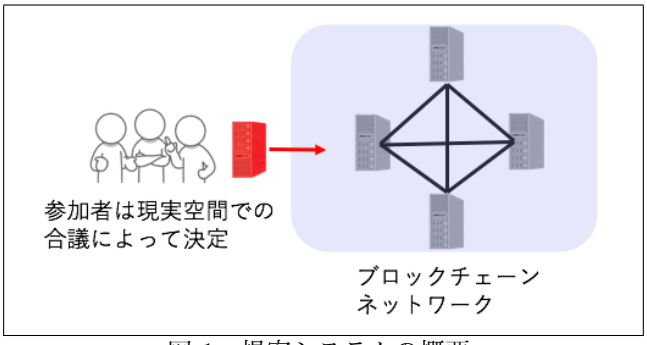

図 1 提案システムの概要

4 考察

4.1 合意形成アルゴリズム

提案システムは, 現実の空間での合議によってシステムの参加者を限定しているため, ブロックを追加するための合意に達するために高い計算量が必要な PoW アルゴリズムではなく, PBFT アルゴリズムを使用することができる. PBFT アルゴリズムはコアノードにブロックの追加権限を集中させて, コアノードによる合議制において合意を形成する. 提案システムでは, コアノードは, ランダムで決定する.

4.2 非中央集権

提案システムは, システムの参加者を現実の空間での合議によって管理しているため, 不正を働くような悪意のある参加者は存在しないと考えられる. また, 提案システムの参加者は全員が対等な立場であり, 絶対的な管理者がおらず, 非中央集権的な仕組みとなる. そのため, 管理者による不正や改ざんが行われてしまうというリスクはないと考えられる.

4.3 小規模な組織

提案システムは, 20〜30 人程度の人が所属するような組織のシステムに利用されることを想定している. 例えば, 大学の研究室内のシステムや, 小規模な会社のシステムでの利用を想定している. これらの組織では, システムを利用するメンバーが変更されるのは年に 1 度程度で同じタイミングのみと考えられる. そのため, システムの参加者を追加するために, 現実の空間での合議を行うのは年に 1 度程度で良いと考えられる. また, パスワードの変更などのシステム上の変更を行う場合も現実の空間での合議が必要である. しかし, システム上の変更を行うことは滅多にないと考えられる.

4.4 提案システムの利用例

提案システムは, システム構築の際, 情報セキュリティの基盤システムとして利用することができる. 例えば, 提案システムを利用して, 一度の認証で複数のシステムを利用することができるシステムを構築することを考える. 公開鍵認証基盤を利用するのであれば, 提案システムのブロックチェーン上にユーザ（提案システムの参加者）の公開鍵と署名を格納し, それらを利用することで一度の認証で複数のシステムを利用することが可能となる.

5 まとめ

現実の空間での合議によって参加者を限定する新たなブロックチェーンを用いた情報セキュリティシステムを提案した. 提案システムは, 管理者がいない非中央集権的な仕組みであり, 参加者は特定のメンバーに限られるため合意形成の迅速化や低コスト化が図れる. また, 提案システムを利用することで, データの安全性や信頼性が保ちやすく, 処理速度の速いシステムの構築が可能となる. 今後の課題としては, 提案システムの実装することや, 実装した後, 提案システムを利用して, 一度の認証で複数のシステムを利用することができるシステムを構築することである.

謝辞

本研究の一部は, JSPS 科研費 18K11484 と, JSPS 科研費 17K01309, 関西大学大学院理工学研究科高度化推進研究費, 関西大学先端科学技術推進機構「緊急救命避難支援のための情報通信技術に関する研究開発」研究グループの助成を受けている.

参考文献

[1] Jong-Hyouk Lee, “BIDaaS:Blockchain Based ID As a Service” IEEE Access, vol.6, pp.2274-2278 (2017).

[2] Lei Xu, Lin Chen, Nolan Shah, Zhimin Gao, Yang Lu, Weidong Shi, “DL-BAC: Distributed Ledger Based Access Control for Web Applications” WWW ’17 Companion Proceedings of the 26th International Conference on World Wide Web Companion pp.1445-1450 (2017).

[3] Zhimin Gao, Lei Xu, Glenn Turner, Brijesh Patel, Nour Diallo, Lin Chen, Weidong Shi, “Blockchain-based Identity Management with Mobile Device” CryBlock’18 Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems pp.66-70 (2018).