5ZC-01

# ブロックチェーンを用いた分散ネットワークの外部からの評価と登録

森 優大 †　　佐藤 周行 ‡
東京大学 †　　東京大学 ‡

## 1 はじめに

近年，ブロックチェーンはさまざまな分野への応用が期待されている．その応用はIoTやワイヤレスセンサネットワーク，マルチエージェントシステム（MAS）のような分散システムにまで広がっている．

このような分散システムは小規模で計算能力に限りがある．また，システムを複数に分割し，異なるシステム間で情報を相互に通信することもある．ブロックチェーンは参加するノードの計算量をもとに安全性を保証するものであるから，小規模なかつ計算能力が制限されたシステムでは安全性を保証することが困難となる．また，異なるシステム間で情報を相互に通信する際には，何らかの方法を用いて通信先のシステムが安全であるかを評価しなければならない．

本研究ではブロックチェーンと分散システムを安全に運用するための従来技術を組み合わせることでこれら問題の解決を試みる．分散システムの安全性に関する情報をブロックチェーンに記録するシステムを提案する．各分散システムは自システム内で検出されたビザンチンノードの情報を上位層に置かれたブロックチェーンに送信する．他の分散システムは通信しようとしている分散システムが信頼できるかを，このブロックチェーンの情報を使用して評価できる．

## 2 分散システムの合意問題

分散システムは従来からその安全な運用について研究されている．本研究では分散システムの合意問題について検討する．

分散システムの合意問題では，ビザンチン将軍問題 [1] と呼ばれる問題がある．これは，不特定のノードが一時的に故障して不正な情報を送信したり，悪意のあるノード（ビザンチンノード）が故意に不正な情報を送信したりすることがあるという前提での合意問題を解くことである．ビザンチン将軍問題では，全ノード数 $n$ に対してビザンチンノードの数を $f$ とすると，$3f \geq n$ のときその問題を解くいかなるアルゴリズムも存在しないことが示されている．そのため，分散システムの安全な運用のためにはビザンチンノードの数を全体のノード数に対して低い割合を維持することが重要となる．

ブロックチェーンのアーキテクチャでは，このような問題に対して，計算量というコストを課しビザンチンノードの参加を防ぐことによって安全に運用を実現している．しかし，この方法は計算量の制限される分散システムに適用することが難しい．一方で，ビザンチンノードの検出については，特に制御工学の分野でさまざまな研究がなされている．制御工学の手法では比較的小さな計算量でビザンチンノードの検出が可能である [2]．このような手法によってビザンチンノードを検出し，その割合を安全性の指標とすることで，分散システムを安全に運用できると考える．

## 3 提案手法

提案手法の概要を図 1 に示す．システムは 2 つの階層からなる．下位層はマルチエージェントシステムやワイヤレスセンサネットワークのような分散システムである．この分散システムはビザンチンノードを検出する能力をもつとする．上位層は分散システムのビザンチンノードの記録を行うブロックチェーンである．下位層の分散システムに関する情報を記録する機能はスマートコントラクトとして実装する．

下位層の分散システム内でビザンチンノードが検知されたとき，その情報を上位層のブロックチェーンに記録する．他の分散システムはその情報をもとに通信を行いたい分散システムが安全であるかを評価する．

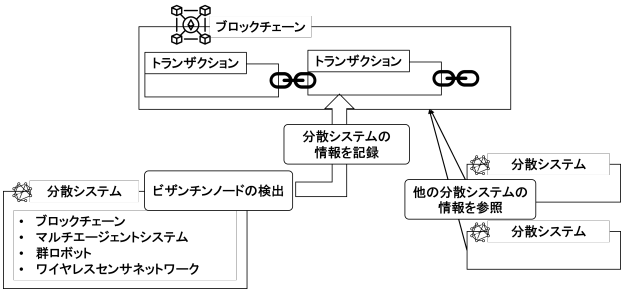


図 1: 提案手法の概要

External evaluation and registration of distributed system using blockchain
† Yudai Mori, University of Tokyo
‡ Hiroyuki Sato, University of Tokyo

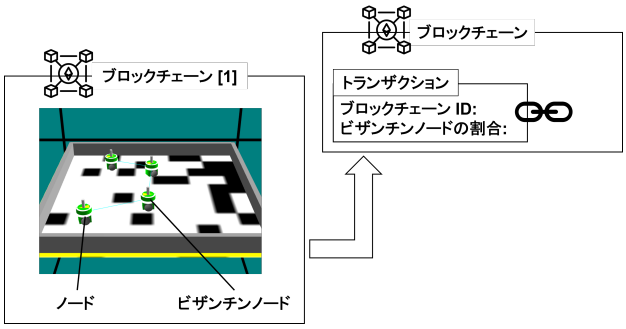


図 2: 検証のためのシステムの概要

## 4 検証

### 4.1 検証のためのシステムの概要

提案手法の有効性を検証するために，Strobel らの群ロボットをブロックチェーンで制御する手法 [3] をもとに提案手法を実装した．検証のために実装したシステムの概要を図 2 に示す．

下位層には Strobel らによる群ロボットのシミュレーションを用いた．この手法では床のタイルの割合について合意問題を解いている．黒と白のタイルがランダムに配置された床について，全体に占める白のタイルの割合を決定することをこの群ロボットシステムのタスクとして，シミュレーションを行う．各ロボットはブロックチェーンノードとして機能する．各ロボットはブロックチェーン上に実装されたスマートコントラクトを使用して，白のタイルの割合に関する投票を行う．これにより，群ロボットシステム全体として白のタイルの割合を決定する．このシミュレーションにおいて群ロボットシステム内にビザンチンロボットを発生させ，それを検知する．ここで，ビザンチンロボットは，タイルの割合を常に 0 と送信するものと定める．ビザンチンロボンとの手法にも Strobel らの手法を適用する．ブロックチェーン上に実装されたスマートコントラクトはビザンチンロボットを検知すると，その投票を無視し，上位層のブロックチェーンに記録する．

我々はこの手法に, 群ロボットシステム内でビザンチンロボットを検出したときに上位層のブロックチェーンにその情報を送信するコントラクトを追加した．これにより，上位層のブロックチェーンは群ロボットシステム内のビザンチンロボットの割合を記録できる．

### 4.2 実装

上位層のブロックチェーンのスマートコントラクトはローカルに立ち上げた Ethereum プライベートチェーン上に実装した．Ethereum ブロックチェーンはブートノード，JSON-RPC 用エンドポイント，マイナーの 3 ノードで構成され，それぞれを 1 つの Docker コンテナとして立ち上げた．下位層のスマートコントラクトが JSON-RPC 用のエンドポイントとして機能するノードに JSON 形式でリクエストを発行することで，上位層のスマートコントラクトが呼び出され，ブロックチェーンに情報を記録する．下位層の群ロボットシステムには Strobel らの手法に対して上位層のブロックチェーンに情報を送信するコントラクトを追加した．

### 4.3 結果

以上のような実装を行った結果，群ロボットシステムのビザンチンノードの割合をブロックチェーン上に記録することができた．また，外部からその情報にアクセスでき，評価が可能であることが示された．

## 5 議論

提案手法とその検証では, 分散システム内でビザンチンノードの検知したときにその情報を上位層のブロックチェーンに記録し，他の分散システムはその情報を参照することによって，通信しようとしている分散システムが安全であるかを評価できることを確かめた．

本研究では，合意問題におけるビザンチンノードの定義を単純化することで検出を簡単にしている．実用のためには，運用する分散システムごとにビザンチンノードの検出手法の適用を考える必要がある．これは今後の研究課題とする．

## 6 まとめ

本研究では，分散システムのビザンチンノードの割合をブロックチェーンに記録することにより，他の分散システムが通信対象としたい分散システムを評価するための仕組みを提案した．先行研究をもとに提案手法の有効性について検証した．分散システムに対するビザンチンノードの検出手法の適用については今後の課題とする．

## 参考文献

[1] Lamport, L., Shostak, R. and Pease, M.: The Byzantine Generals Problem, *ACM Trans. Program. Lang. Syst.*, Vol. 4, No. 3, p. 382 – 401 (online), 10.1145/357172.357176 (1982).

[2] Pasqualetti, F., Bicchi, A. and Bullo, F.: Consensus Computation in Unreliable Networks: A System Theoretic Approach, *IEEE Transactions on Automatic Control*, Vol. 57, No. 1, pp. 90–104 (online), 10.1109/TAC.2011.2158130 (2012).

[3] Strobel, V., Castelló Ferrer, E. and Dorigo, M.: Blockchain technology secures robot swarms: A comparison of consensus protocols and their resilience to Byzantine robots, *Frontiers in Robotics and AI*, Vol. 7, p. 54 (2020).