スワームロボットシステムのための ブロックチェーン技術を応用したセキュアな情報共有手法の提案

西田裕輝[†1]　金子晃介[†2]　城島翔太[†1]
中山和也[†3]　堤優亮[†4]　櫻井幸一[†5]

概要：スワームロボットシステムとは,自律分散型ロボットが集団として一つの目標を達成するシステムであり,情報伝達の手段としては,Peer-to-Peer による無線ネットワークが主に利用される.Peer-to-Peer ネットワークの課題として,故障したノードや,悪意あるノードの存在により合意形成が困難となる問題があり,このような状況では協調システムは維持できない可能性がある.
本稿では,仮想通貨を支えるブロックチェーン技術を用い,スワームロボットシステムにおいてセキュアに画像共有を行う手法について提案し,Ethereum と呼ばれるブロックチェーンプラットフォームを用いて,実際にブロックチェーン上で画像データを共有する実験を行った結果を示す.

キーワード：ブロックチェーン, セキュリティ, 群知能ロボット

Proposal of Secure Information Sharing for Swarm Robot System using Blockchain Technology

YUKI NISHIDA[†1]　KOSUKE KANEKO[†2]　SYOTA JOHJIMA[†1]
KAZUYA NAKAYAMA[†3]　YUSUKE TSUTSUMI[†4]　KOUICHI SAKURAI[†5]

Abstract: The Swarm Robot System is one of robot control systems in which each autonomous distributed robot behaves to achieve their target by cooperating with others. As a method of their communication, Peer-to-peer wireless network is usually used for data transmission. One of Peer-to-Peer network problems is that they can't bring a correct result of consensus if there are several broken or malicious nodes in the network. In such a situation, the cooperative system of swarm robots becomes difficult to maintain. In this paper, we propose a method to securely share data in Swarm Robot System using Blockchain which is the core technology of Bitcoin, and also show the experiment result of the secure data sharing to transmit images captured by a web camera on Ethereum network.

Keywords: Blockchain, Security, Swarm Robotics

1. はじめに

近年,ブロックチェーンと呼ばれる技術の応用に関する研究が行われている.これは,仮想通貨ビットコインの根幹技術として,2008 年に Satoshi Nakamoto[1]によって提案された技術で,Peer-to-Peer(以下,P2P)型のネットワークにおいて全体での合意を達成することにより,改ざん困難な形で仮想通貨のやり取りを記録するシステムを提供している.ブロックチェーン技術を用いた,ビットコイン以外の仮想通貨が数多く提案されているが,この技術を仮想通貨の取引以外の分野で応用しようとする研究が行われている.そこで,我々はブロックチェーン技術のロボット分野への応用について提案を行った.

ロボットの性能の向上に伴って,様々な場面での運用が期待されており,近い将来,ロボットが作業を補助する,あるいは代わりに作業自体を行うことで,人の生活を支える社会の実現が予想される.ロボットの開発にあたっては,ロボットを高性能にすることで,より難易度の高い作業を行うことが可能になる.しかし,単一のロボットでは,障害が発生した場合目標の達成に支障が生じる可能性や,異なる環境での運用が難しいといった課題がある.これに対して,複数のロボットによって目標を達成しようとする設計が研究されている.このようなシステムの設計では,個々の自律的に行動するロボット同士が互いにコミュニケーションを取りあうことで,より効果的に目的を達成することができる.複数のロボットが協調しあい,群のように行動することで一つの目標を達成するようなロボットに関する研究分野を,スワームロボティクス(以下,SR)と呼ぶ.

SR とは自律分散型協調ロボット,つまり,個々の判断で行動する複数のマシンが,集団で一つの目標を達成するようなロボット群についての研究分野であり,集団の中に障害

†1 九州大学　大学院システム情報科学府
Graduate School of Information Science and Electrical Engineering, Kyushu University
†2 九州大学　サイバーセキュリティセンター
Cybersecurity Center, Kyushu University
†3 九州大学　工学部
School of Engineering, Kyushu University
†4 九州大学　理学部
School of Science, Kyushu University
†5 九州大学　大学院システム情報科学研究院
Faculty of Information Science and Electrical Engineering, Kyushu University

が発生したノードがあってもシステムとしては機能し続ける障害への耐性や,異なる環境においても柔軟に運用可能な性質が期待される.このようなシステムでは,ロボット同士が情報交換を行う必要があり,その情報伝達の手段としてはP2Pネットワークをベースとした無線通信がよく利用される[2].

本研究の目的は，仮想通貨を支えるブロックチェーンという技術を用いて,自律分散型のロボット群がセキュアに情報交換を行うことができる仕組みを提案することである.そのために,Ethereum と呼ばれるブロックチェーンプラットフォームを用いて,実際にプライベートなネットワークを構成し,スワームロボットを想定したデバイス間での画像データを共有する実験を行った.

本稿では,ブロックチェーン,スワームロボットシステムについて説明した後,ブロックチェーン技術を用いてロボット間でセキュアに画像データを共有する手法について提案し,実験結果の報告を行う.

2. ブロックチェーン

P2P ネットワークにおいて情報伝達を行う上での課題の一つとして,ビザンチン将軍問題[3]というものがある.これは,ある集団の中に一定数の悪意ある参加者が存在すると,全体での共通の合意が達成できないという問題である.この問題をスワームロボットに当てはめると,意図的に情報を改ざんするようなロボット,あるいは故障などにより正常な情報が伝達できないようなロボットが存在したとき,集団での知識の共有が困難になる可能性がある.この課題を解決する手段の一つとして,ブロックチェーン技術を応用できるのではないかと考えた.

ブロックチェーンとは,仮想通貨ビットコインを支える技術として提案された.ビットコインは非中央集権型のネットワーク構造で,P2Pによる仮想通貨のやり取りを実現している.ビットコインは P2P ネットワークにおけるビザンチン将軍問題を,ブロックチェーン技術を用いて解決した.

まず,ブロックチェーンの構造について説明する.ブロックの構造を図 1 に示す.ブロックチェーンは,複数の取引記録（トランザクション）を集めた,ブロックと呼ばれるデータがつながった構造となっている.ブロックには主にトランザクションと,直前のブロックのハッシュ値,Nonce と呼ばれる値が含まれている.ハッシュ値とは,ハッシュ関数によって出力された値である.ハッシュ関数は,あるデータに対して特定の処理を行うことで,一定の長さのデータを出力し,これをハッシュ値と呼ぶ.同じデータからは同じハッシュ値が,異なるデータからは異なるハッシュ値が出力され,また,ハッシュ値からは元のデータを復元することができないことがハッシュ値の特徴である.ブロックチェーンはこのハッシュ値を利用して,ブロック同士がチェーン上につながった仕組みを形成している.ブロック内のデータ

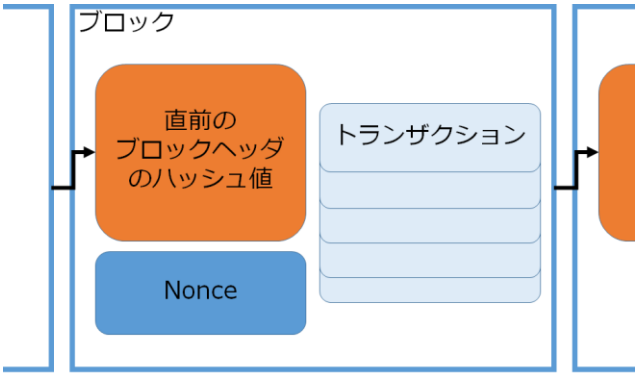

図 1　ブロックの構造

が書き換えられると次のブロックに含まれた,書き換えがあったブロックのハッシュ計算の入力が変わり,出力であるハッシュ値も変わる.そのブロックハッシュ値は次のブロックに含まれ,ハッシュ計算のための入力となっているため,書き換えがあったブロック以降のブロックに含まれるハッシュ値が次々に変更されていくことになる.ゆえに,ブロックチェーンは,データの書き換えが,続くブロックに次々に影響を与えていくようなチェーン上の構造となっている.したがって,過去の取引記録を改ざんするには,その時にブロックチェーンに含まれたトランザクションを改ざんするのに加えて,それ以降のブロックに含まれるハッシュ値をすべて計算しなおさなければならないような仕組みとなっている.

しかし,ネットワーク上でブロックが無作為に作られると,どのブロックチェーンが正しいものなのか判断ができなくなる.ビットコインの P2P ネットワーク上では,中央組織が存在しないため,ネットワーク上で分散して共有される正しい元帳であるブロックチェーンを一つに決定する仕組みが必要となる.これを解決するのが,コンセンサスアルゴリズムという仕組みである.コンセンサスアルゴリズムにはいくつかの種類が考案されているが,ビットコインや今回の実験で使用した Ethereum では「Proof-of-Work」(以下,PoW)と呼ばれるアルゴリズムを採用している.PoW は,最初に「ブロックのハッシュ値が一定の値以下となる」という条件を満たしたブロックを,新しいブロックとしてブロックチェーンにつなげるというルールを定めている.ブロックを生成するためには,ブロックに含まれる Nonce の値を総当り的に変更してブロックハッシュ値を次々と計算し,この条件を満たす Nonce を見つける必要がある.この,トランザクションをブロックに含め,膨大な量のハッシュ計算を行い,ブロックの生成権を得るための行為を「マイニング」と呼び,マイニングを行うノードを「マイナー」と呼ぶ.ブロックを生成するにあたって,マイナーは自身のアドレスへ報酬を与えるトランザクションをブロックに加えることができる.また,各トランザクションには手数料が含めら

れており,この手数料はブロックの生成者に支払われることになっている.ブロックチェーンネットワークでは,このブロック生成の報酬とトランザクション手数料を得るために,多くのノードがマイニングを行っている.不正なトランザクションが承認されると,仮想通貨の信頼性が低下し,マイニングによって得た通貨の価値が下がってしまうため,マイナーが正しいブロックを作り続ける動機となる.

ブロックチェーンネットワークでは,最もブロックのつなげられたチェーンこそが,最もマイナーによって支持されてきたチェーンということになり,そのようなチェーンに含まれたトランザクションのみが有効なトランザクションであると認識される.したがって,ネットワーク上では,つながったブロック数が最大のブロックチェーンが,共通の台帳ということになる.ゆえに,過去の取引記録を改ざんするには,ブロック中のトランザクションの改ざんをした後,他の通常のマイナーがチェーンを拡張し続けるよりも早く,続くブロックのハッシュ値を計算しなおし続け,現在正規のものとして認識されているチェーンより,自身が拡張したチェーンに多くブロックをつなげる必要がある.

ブロックチェーンは,このチェーン状の構造と,コンセンサスアルゴリズムにより,トランザクションを改ざんすることが困難な仕組みを提供している.

3. スワームロボットシステム(SRS)

SR は自然界において,群れを形成する社会生成物に発想を得ている.例えば,アリはフェロモンを媒介とすることで巣から餌への経路を環境上に残すことによって,餌を探し,巣へ運び込むというタスクを集団で実行することができる.また,個々では運搬できないような大きさの対象物であっても,複数の個体が協調して作業に当たることで運搬することを可能にしている.このような生物の協調作業をロボット群によって実現したものが,スワームロボットシステム(SRS)である.

SRS とは自律的に行動する複数のロボットが,互いに通信を行い協調することで,集団として一つの目標を達成することを目的としたシステムである.このようなシステムでは,実際の社会性生物の群れの特徴から,以下のような性質を持つことが期待されている[4].1)頑健性 : 群の行動はそれぞれのロボットの単純な作業から形成されるものであるため,個々のロボットに故障などの障害が発生したとしても,別のメンバーロボットによって補填することが可能であり,システムとしては正常に機能し続けることが可能である.2)柔軟性 : 環境の変化に対して群としての作業を調整することにより,柔軟に対応することが可能である.3)拡張性 : システムを構成するロボット台数に対して,ロボットの協調作業を崩さずにある程度の拡張が可能である.

SRS はその分散した性質から,個々の行動制御は局所的な通信にのみ依存し,群全体でのグローバルな知識については利用されないことが一般的である.しかし,システム全体で情報を共有することは,個々のロボットの行動を効率化する可能性がある.例えば,あるロボットが特定の状況について学習,あるいは収集した結果を群全体に共有することが可能であれば,システムに属する他のロボットはそのデータを用いることで,学習・収集のステップを経ずに効率的に行動を選択できる可能性がある.群でのグローバルな知識の共有を実現するには,ネットワークでの正しい知識について合意ができること,また,共有された知識が改ざんされないことが必要である.そこで,本研究では前述のブロックチェーン技術を SRS へ適用することを試みた.

4. 実験

SRS へのブロックチェーンの応用に関しては,Ferrer[5]によりそのフレームワークが提案されており,その応用によって,SRS におけるセキュリティ・分散意思決定・異なる行動制御の切り替え・ビジネスモデルについての課題の解決の可能性が述べられている.そこで私は,SRS 環境へブロックチェーン技術を応用することで,改ざん困難な形で情報を共有することができるという仮説を立て,その検証のためにスワームロボットを想定したデバイスを用いて,具体的なネットワーク構成を提案し,デバイス間で画像データを共有する実験を行った.

4.1 Ethereum

今回の実験では,Ethereum と呼ばれるブロックチェーンプラットフォームを使用した.Ethereum を使用した最大の理由は,「スマートコントラクト」と呼ばれる仕組みである.スマートコントラクトとは,あらかじめ定められたルールに従って契約が自動的に執行される仕組みのことで,Ethereum では,コントラクトコードと呼ばれるチューリング完全なコードをブロックチェーン上に記述することが可能であり,コントラクトコードをもつアカウント（以下,Contract）が存在する.Contracct は,一般のアカウントと同様アドレスを持ち,そのアドレス宛に実行に必要な手数料を含めたトランザクションを送信することで,コードを実行することが可能である.Ethereum はこのスマートコントラクトの仕組みから,ブロックチェーン上で実行可能なアプリケーションのためのプラットフォームとして利用される.SRS 環境でのブロックチェーンの応用では,ロボット同士の通信をブロックチェーン上に記録するだけでも,改ざん困難な形でデータを共有することができると考えられるが,スマートコントラクトによって,ロボット群によって収集されたデータを利用したアプリケーションの実装が期待できる.このため,スマートコントラクトの仕組みを持つ Ethereum が SRS に適していると考え,実験に使用するプラットフォームとして選択した.

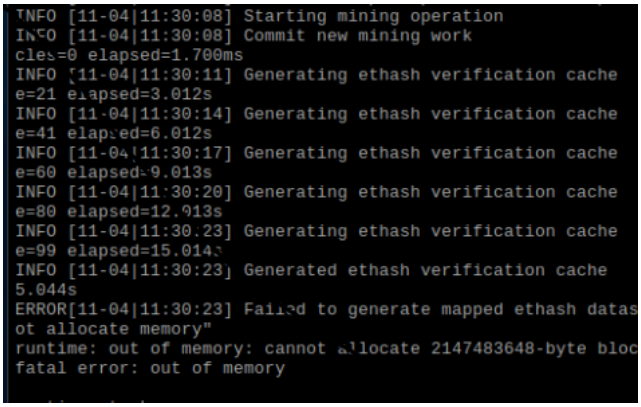

図 2　Raspberry Pi でマイニング実行時のログ画面

4.2 実験概要

スワームロボットを想定したデバイスとして,2 台の Raspberry Pi3 Model B (メモリ : 1GB, CPU : ARM Cortex-A53)を用い,一方を送信デバイス,もう一方を受信デバイスとして使用した.

実験は,ブロックチェーン上の Contract を介したデバイス間での画像データの共有を行った.Contract には文字列を引数として受け取る関数と,受け取った文字列を返す関数のみを実装した.送信デバイスは接続された web カメラで画像の撮影を行い,トランザクションに Contract の関数の引数として画像データを埋め込んで,Contract のアドレスへと送信することで,Contract の変数として画像データを登録した.受信デバイスは Contract の変数の値を返す関数を実行し続け,画像データを取得した.画像データはトランザクションに埋め込むために,160×120 サイズの画像を Base64 に変換して送信した.

4.3 実験結果

最初に,Raspberry Pi のみを用いてネットワークを構成し実験を行ったところ,送信デバイスから Contract へデータを送ることができなかった.Ethereum の PoW に用いられているアルゴリズムには,メモリを大量に使用するという特徴があり,Raspberry Pi ではそのためのメモリを確保できなかったために,送信デバイスから送られたトランザクションを含んだブロックが作成できず,ブロックチェーンにつなげられなかったことが原因であった(図 2).

そこで,マイニング用のスーパーノードを配置したネットワーク構成を考えた(図 3).スーパーノードとして Windows PC(メモリ:8GB, CPU: intel core i5)を接続し,マイニングはスーパーノードに任せて,Raspberry Pi は画像データのやり取りだけを行うような構成に変更した.

実験の結果,送信デバイスから Contract へ送られた画像データを,送信先の Raspberry Pi でブロックチェーン上から参照することに成功し,トランザクションを参照すると画像データが記録されていることが確認できたため,改ざん困難な形で画像データ送信記録をブロックチェーン上に記録することに成功した(図 4).

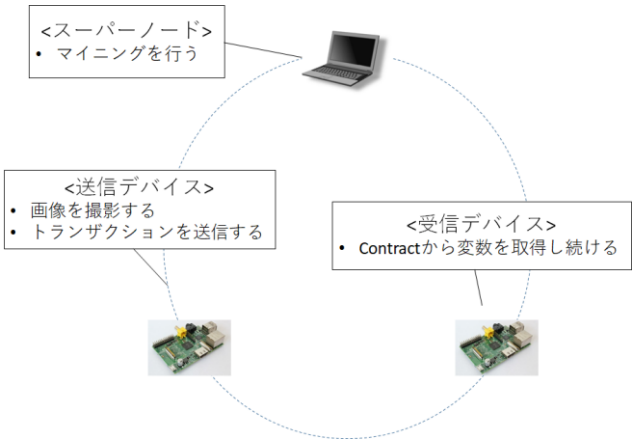

図 3　マイニング可能なネットワーク構成

図 4　実験結果

5. まとめ

本研究では,仮想通貨ビットコインの根幹技術であるブロックチェーン技術を SRS 環境に適用することで,改ざん困難な形でデータを共有することができるという仮説の検証のため,ブロックチェーンプラットフォームの一つである Ethreum を用いた実験を行った.

実験の結果,スワームロボットを想定した,Raspberry Pi のみのネットワークではマイニングが行えないという問題のために,マイニングを担当するスーパーノードを配置したネットワーク構成を提案し,ブロックチェーンを介した改ざん困難な形での画像共有に成功した.しかし,スーパーノードを必要とする現在のネットワーク構成では,完全な自律分散とは言えない.今回プラットフォームとして使用した Ethereum の PoW に用いられるアルゴリズムではメモリを大量に使用するという特徴のために,メモリの限られたデバイスではマイニングが行えなかった.今後は PBFT のようなマイニングを必要としないコンセンサスアルゴリズムについての調査を行う.

謝辞　本研究は, 国立研究開発法人科学技術振興機構(JST)戦略的国際共同研究プログラム(SICORP)の支援, JSPS 科研費 JP15H02711 の助成を受けたものです.

参考文献

[1] Nakamoto, S., “Bitcoin: A Peer-to-Peer Electronic Cash System”, http://bitcoin.org/bitcoin.pdf, 2008.
[2] Brambilla, M., Ferrante, E., Birattari, M., et al. “Swarm robotics: a review from the swarm engineering perspective”, Springer, Swarm Intelligence, Vol.7, Issue 1, pp.1-41, 2013.
[3] Lamport, L., Shostak, R. and Pease, M., “The Byzantine Generals Problem”, ACM Trans. Program. Lang. Syst., Vol. 4, No.3, pp.382-401, 1982.
[4] Sahin, E., “Swarm Robotics: From Sources of Inspiration to Domains of Application”, Lecture Notes in Computer Science, Vol. 3342, Springer, pp.10-20, 2005.
[5] Ferrer, E.C., "The blockchain: a new framework for robotic swarm systems", arXiv preprint arXiv:1608.00695, 2016.

【 この位置に改ページを入れ, 以降のページを印刷対象外とする 】

1 Nakamoto, S., “Bitcoin: A Peer-to-Peer Electronic Cash System”, http://bitcoin.org/bitcoin.pdf, 2008.
2 Brambilla, M., Ferrante, E., Birattari, M., et al. “Swarm robotics: a review from the swarm engineering perspective”, Springer, Swarm Intelligence, Vol.7, Issue 1, pp.1-41, 2013.
3 Lamport, L., Shostak, R. and Pease, M., “The Byzantine Generals Problem”, ACM Trans. Program. Lang. Syst., Vol. 4, No.3, pp.382-401, 1982.
4 Sahin, E., “Swarm Robotics: From Sources of Inspiration to Domains of Application”, Lecture Notes in Computer Science, Vol. 3342, Springer, pp.10-20, 2005.
5 Ferrer, E.C., "The blockchain: a new framework for robotic swarm systems", arXiv preprint arXiv:1608.00695, 2016.