L-013

自律分散型協調メッセージングシステムにおけるルーティング方式の検討
Consideration of Routing Method on Autonomous Distributed Collaborative Messaging System

市川博彬[1)]　小林亜樹[2)]
Hiroyoshi Ichikawa　Aki Kobayashi

1　はじめに

筆者らは、Bitcoin[1] で普及したブロックチェーン技術の特徴を利用して、2 者間のシンプルなメッセージングシステムにおいて、他者間通信を中継することが、自ノードを起源とする通信を行う権利を得る手段とすることで、通信自体をインセンティブとするプロトコルを提案し、通信システム内における利用者が引き起こす不正について検討した [2][3]。従来はルーティングを既知としてきたところ、本稿では、ルーティング方式についての検討を行う。提案システムでのある状況を想定しながら、既存の各ルーティング手法との比較を行い、提案システムにおける経路情報の取得方式についての方針を検討する。

2　提案メッセージングシステム

2.1　概要

本研究で対象とするメッセージングシステム [2][3] は、ネットワーク内の任意のノードから他のノードへの、1 対 1（ユニキャスト）のメッセージングサービスとする。提案メッセージングシステムのモデルを図 1 に示す。システムには近接のシステム参加ノード同士の広帯域な接続と、比較的狭帯域だが全参加ノードへのブロードキャストに適した通信チャネルの 2 種類の接続があると仮定する。ブロードキャスト用通信チャネルは、LTE のような広範囲な通信ないし近接接続を利用したフラッディングのような機構が備わっているものと想定している。

メッセージは送信者から送信され、中継者を経て、最終的に受信者まで転送される。システム内で新規のメッセージを送信することができる権利（送信権）を報酬とし、各システム参加ノードが中継に参加するよう動機付けを行う。メッセージを中継したこと、またメッセージが受信されたことなどの通信情報をブロックチェーンに記録することにより、自律分散的に送信権の消費や発生を担保することで、自律分散的な協調メッセージングシステムを実現する。ブロックチェーンにおけるチェーンの連結には、中継したメッセージ内にカプセル化された情報を必要とする仕組みとする。受信者に中継メッセージが届いた段階で、当該情報が中継者にもたらされるプロトコルとする。その結果、通信中継自体が、次の通信開始の権利を得ることになり、通信自体をインセンティブとする方式である。ネットワークは、多数のノードから構成され、ノードは、一部のノードとのみ直接通信できるものとする。直接通信が不可能なノードとの通信は、他のノードを介して、中継処理を行うことで、最終的なメッセージングを実現する。

2.2　ブロックチェーン

ブロックチェーンは、自律分散的な仮想通貨システムの Bitcoin 上で自律分散的に財となるデータを発行・管理するために考案されたものである。Bitcoin システムにおいて、仮想通貨の授受や発行のデータは、ブロックチェーンと呼ばれるデータ構造に記録される。ブロックチェーンは、各システム参加ノードによって自律分散的に記録され、不正に改竄されたデータの記録が困難な仕組みになっている。

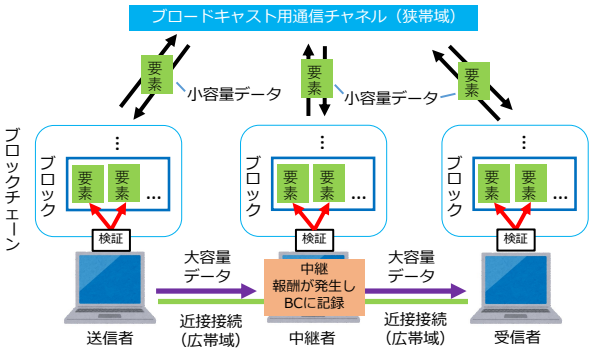

図 1　システムモデル

2.3　送信時処理

本稿で「ブロードキャスト」とは、ブロックチェーンのデータを共有するための、システム全体に対する通信とし、「送信」とは、隣接ノードに対する通信とする。

ネットワークは互いにブロックチェーンを共有するノード群で構成される。ノード参入時処理、ブロードキャストの具体的な方法などは、紙面の都合により省略する。送信時の処理を、メッセージを 1 つ送信する例（図 2）を用いて説明する。ここでは、図 2 に示す中継者（$I_1,\ldots,I_n$）が、送信者（S）が作成したメッセージの中継を行い、受信者（D）に届けることとする。以下に説明に用いる文字を示し、手順を説明する。

S：sender, I：intermediary, D：destinator (receiver),
$\mathcal{S}$：sender ID, $\mathcal{I}$：intermediary ID, $\mathcal{D}$：destinator ID,
M：message, h：cryptographic hash function,
$A||B$：concatenated data of A and B,
C：confirmation (random number), K：message key,
transaction：$T\{h(M), \mathcal{S}, \mathcal{D}, h(h(K)), h(M'),$
$h(h(M')||C), h(h(C))$, route information from S to $D\}$,
P：previous block hash, and R：reward information.

① S は、D 宛の M を作り、T を作る。
② T をネットワーク全体にブロードキャストする。
③ S は M と C' と K を I_1 に送信する。
④ I_1 は M と C' と K を I_2 に送信する。
⑤ I_2 は M と C' と K を I_3 に送信する。
⑥ I_{n-1} は M と C' と K を I_n に送信する。
⑦ I_n は M と C' と $h(k)$ を D に送信する。
⑧ D は C' から C を取り出す。
⑨ D は C をブロードキャストする。
⑩ I_n は K をブロードキャストする。

1）　工学院大学大学院工学研究科
2）　工学院大学情報学部情報通信工学科

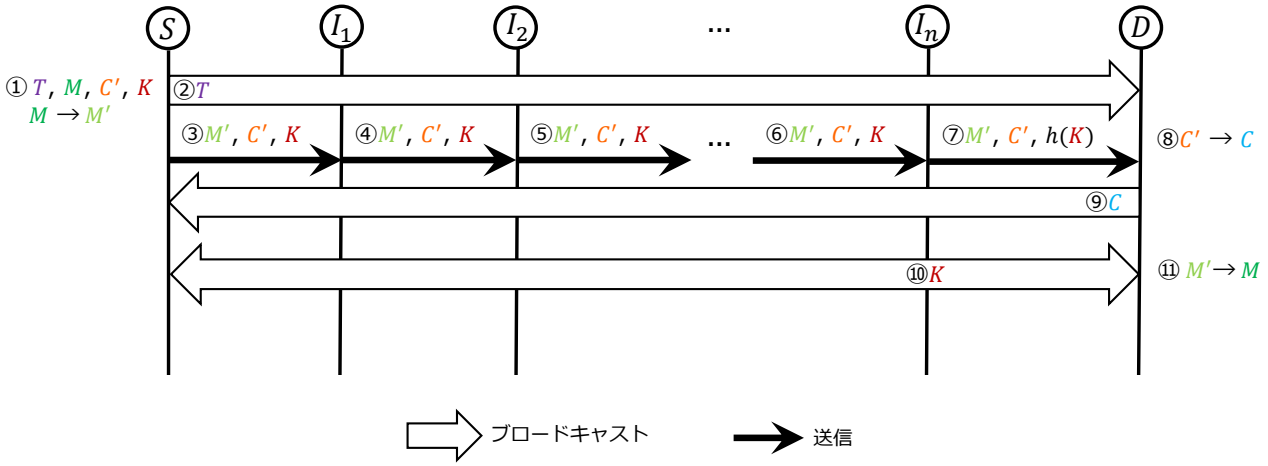

図 2　シーケンス図

⑪　D は M' から M を取り出す。

3　ルーティング

3.1　関連研究

陶山ら [4] は、DTN 環境におけるルーティング手法を提案した。通信中のノードの移動が考慮されており、メッセージが送信されてから受信者に到達するまでの間に最適な経路が変更した場合、動的に経路が変更されるように設計されている。岩井ら [5] も、DTN 環境におけるルーティング手法を提案した。送信者がメッセージを送信する際、送信者からみて接続可能な固定基地局を利用することが検討されている。また、ノードの移動計画を経路決定に利用することが検討されている。

これらの手法について、筆者らの提案メッセージングシステムへの適用を検討する。陶山らの手法については、あるメッセージについて、送信者と受信者の間で、どの中継者を経由したかを不正なくブロックチェーン上に記録する手法の追加の検討を行えば、適用可能であると考える。岩井らの手法については、送信者からみて常に接続可能な固定基地局があり、またノードの移動計画が決定可能な条件下では、適用可能であると考える。

3.2　求められる要件

ここでは、提案メッセージングシステムにおけるルーティング手法の検討方針について述べる。

本提案手法は、中継者に報酬を与えるため、メッセージを中継したノードの情報をブロックチェーンに記録する。そのため、メッセージ 1 つごとにそのメッセージが転送された経路の情報をブロックチェーンに記録する必要があると考える。そのための簡単な手段として、ソースルーティングによる経路決定を行うことを検討する。

本システムでは、モバイルアドホックネットワーク（MANET）での利用を想定するため、ノードの移動が発生する。このため、メッセージが送信者により送信されてから受信者により受信されるまでの間に、経由する予定の中継者ノードが通信不可能になる可能性があることを考慮する必要がある。

参加ノードが、隣接するノードの情報をブロードキャストにより発信し、各ノードがどのノード同士が隣接しているのかという情報をまとめ、各々が受信者までの経路を把握することが考えられる。また、ブロードキャストによる通信によらず、隣接するノード同士で経路情報を交換する方法も考えられる。この際の中継インセンティブは発生しないものとするが、経路情報はデータサイズが小さいものとし、動機付けは問題にならないと仮定する。

提案メッセージングシステムは、メッセージ通信の最終ステップ終わるとブロックが生成される仕組みになっているが、ブロックの生成間隔が長いと、ブロックチェーンを利用したシステムでの不正な行為が起きやすいことが指摘されている [6]。このこと考慮しつつ、1 つのメッセージ転送の開始から終了までの許容できる時間を想定する必要がある。少なくとも、DTN のような数時間程度以上は、不正な行為が行われるおそれのある観点から、望ましくないと考えられる。

4　おわりに

ブロックチェーンを用いた、他者通信の中継インセンティブが付与できる、自律分散型協調メッセージングシステムについて、そのルーティング方法の方針を検討した。今後はその検討を進めるほか、提案メッセージングシステムの未検討となっている諸問題について検討を進める。

参考文献

[1] Satoshi Nakamoto, “Bitcoin:A Peer-to-Peer Electronic Cash System,” https://bitcoin.org/bitcoin.pdf, May 2008.

[2] 市川博彬 , 小林亜樹, “自律分散型メッセージングシステムにおけるメッセージ送受信検証に関する検討,” 2018 年信学総大, 通信講演論文集 2, p. 96, March 2018.

[3] Hiroyoshi Ichikawa and Aki Kobayashi, “Collaborative Messaging Protocol with Multiple Intermediate Nodes,” Proceedings of 7th International Congress on Advanced Applied Informatics, July 2018. (accepted)

[4] 陶山優一，横田裕介，大久保英嗣，“移動端末を用いた災害情報システムにおける DTN ルーティング手法,” 信学技報 USN，Vol. 108, No. 399，pp. 117–121, January 2009.

[5] 岩井正敏，桧垣博章，“固定基地局を含む無線マルチホップネットワークにおける無線ノード移動計画を用いた DTN 配送手法,” 情処学論, 55(8), pp. 1876–1885, August 2014.

[6] 中西建登, 大坐畠智, 加藤聰彦，“Bitcoin における安全な決済確定高速化手法の検討,” 信学技報 NS, Vol. 117, No. 3, pp. 13–18, April 2017.