講演番号： 33

公衆ブロックチェーンにおける合意形成方法の検討

Novel Consensus Building Method for Public Blockchain

矢澤 倫己† 小川 猛志†

Hitomi YAZAWA† Takeshi OGAWA†

† 東京電機大学大学院システムデザイン工学研究科情報システム工学専攻

† Graduate School of System Design and Technology, Tokyo Denki University

1. はじめに

トラストレスな環境で数千以上のノード間で安全な取引を可能とする公衆ブロックチェーン技術(分散台帳技術)が大きな注目を得ている. しかし取引承認性能と合意形成アルゴリズムに関する大きな問題がある. 本稿では, 著者らが提案しているトランザクショングラフ[1]を活用し, 後者を解決する新たな手法を提案する.

2. 既存の合意形成技術

公衆ブロックチェーンの合意形成アルゴリズムは, PoW に比べ消費電力が大幅に少ない PoS が主流になりつつある. 各ノード(台帳を管理するフルノードまたは台帳を持たないが取引に参加可能なライトノード)は台帳の更新を要求するトランザクション(以下, Tx)を任意の時刻に発行する. PoS では一定周期(以下, slot)毎に Tx を複数束ねた 1 つのブロックが選定され, ブロック単位で各フルノードが持つ台帳に反映することを繰り返すことで各台帳の同一性を保証する. PoS は, Ethereum[2]や Algorand, Tendermint, HotStuff, Polygon 等で採用されており手法の一部に差分があるが共通して以下の特徴がある.

(1) 出資(Stake)したノードの中から数 100 程度の代表ノードがくじもしくは輪番で選定され, 台帳に反映するブロックとその順番を投票により決定. 代表ノードの不正発覚時には出資を没収することで不正を抑止

(2) 投票と集計は代表ノード間でオフチェーンで行い, 他フルノードはその結果に従い各々内の台帳を更新する.

(3) 投票アルゴリズムは PBFT をベースとして採用.

PBFT(Practical Byzantine Fault Tolerance)[3]とは分散台帳技術の一つであり, 少数のノード間で安定した合意形成が可能であることが知られている. PBFT では代表ノード(1 つ)が台帳に反映する Tx とその順番を全ノードに提案し, 全ノードによる 2 回の投票(prepare/ commit)で各々2/3 よりも多いノードが承認した場合その提案が合意されたと判断し各々の台帳を更新する. 投票は電子署名が必要でかつノード数の自乗の個数が必要なため数 10 以上のノード間の合意形成には適さないとされている.

3. 既存の PoS の問題点

合意形成が少数のノードに依存するため, それらへの DoS 攻撃の危険がある. また出資金に応じて投票権を得るため, 特定の企業によるブロック生成報酬の占有や, 都合の悪い Tx の承認を後回しにするなどの不正が懸念される. 投票に参加するノード数を多くすることでそれらの問題が緩和されるが既存手法では限界がある.

4. Tx グラフ

著者らは, フルノードが生成またはライトノードから受信した Tx に他の Tx のハッシュ値を付与することで有向非巡回グラフを形成し, ブロックには Tx 自体ではなくこのグラフの先端 Tx のみを格納し, 先端 Tx から辿れる全ての Tx についても承認したとみなす手法(図 1)を提案している. 1 つのブロックで多数の Tx の承認が可能なため, 従来技術に比べて大幅な性能向上(例:Ethereum の 20Tx/s に対し約 200 倍)が可能と見込んでいる.

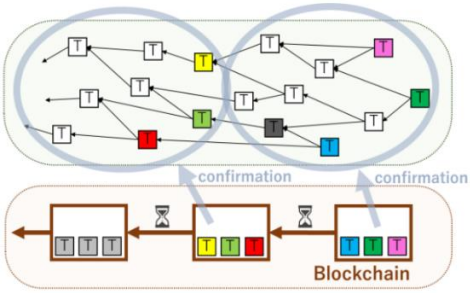

図 2 Tx グラフを用いた検証

5. 提案手法

代表ノードを選定せず全フルノードが, PBFT のアルゴリズムに従った投票を実施する. ただし投票専用のメッセージは作成せず, Tx グラフを利用するためメッセージ数は増えず署名の計算量も増加しない. 以下に手順を示す.

(1) 受信締切時間までに有効なブロックを受信したノードはそれを祖先に持つ先端 Tx(prepare 相当)を作る

(2) Tx を受信するとブロック毎に当該ブロックを有効としたノード数をカウントアップして, フルノード数の 2/3 を超過した場合当該ブロックの state を commit に遷移し, 以後送信する Tx に当該ブロックの ID(BID)を付与.

(3) 受信 Tx に BID があった場合, 当該ブロックを有効としたノード数をカウントアップし, フルノード数の 2/3 を超過した場合 2 回の投票で当該ブロックが有効であることについて全フルノード間の合意が形成されたと判断.

提案手法では, 各フルノードは 1 回の合意形成周期中に 2 回以上 Tx の送信が必要である. 現状の Ethereum を参考にフルノード数を 1 万, 周期を 384 秒とすると, 52Tx/s に該当するため, Tx グラフと組み合わせることで実現性は十分高いと考えている.

6. 今後の課題

投票に参加できるフルノード数を十分な精度で観測できる必要がある. Ethereum 等の代表ノード管理手法が適用可能か精査する必要がある. その後シミュレータを作成し, 提案手法の安全性の確認と性能評価を行う予定である.

参考文献

[1] 島津俊輝, 小川猛志, "ブロックチェーンにおけるトランザクション処理性能向上技術", 信学会論文誌 JB, Vol.J104-B No.7, pp.613-618.

[2] Vitalik Buterin, et al., "Combining GHOST and Casper", 2020.

[3] MiguelCastro,BarbaraLiskov,"Practical Byzantine Fault Tolerance" the Proceedings of the Third Symposium on Operating Systems Design and Implementation, 1999.