講演番号：41

ブロックチェーンにおける永続性を確保したブロック群分散手法

Block Group Distribution Methods that Ensure Persistence in Blockchain

脇中 郁弥† 小川 猛志†
Fumiya WAKINAKA† Satoshi OGAWA†
† 東京電機大学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

近年，処理が必要なトランザクション数が増加しており， 今後ブロックチェーン参加ノードが保持するデータ量が大幅に増大していくと見込まれる[1]．各フルノードが均等にデータを分割して保持する提案[2]があるが任意のデータ量の保持やノード離脱への対応，ライトノードのデータ量削減などが考慮されていない．本稿では，それらを解決し，同時に長期間の永続性を保証する手法について検討状況を報告する．

2. ブロックチェーン

ブロックチェーンとは，取引履歴(トランザクション，以下 Tx)をブロックという単位でまとめ，そのブロック内の Tx を要約したブロックヘッダのハッシュ値をチェーン状に繋ぎ合わせたデータ構造である．ブロックの生成と全ブロックの保持を行うフルノードと，ブロックを要約したブロックヘッダのみ保持するライトノードの 2 種類がある．ライトノードは Tx を保持しないが，フルノードに問い合わせることで任意の Tx の検索・参照が可能である．

3. 先行研究

筆者らはブロックを一定個数(N 個)集めたブロック群と，その内部のブロックを要約したブロック群ヘッダという新しいデータ構造を定義することで，フルノードは空き容量に応じた個数のブロック群のみを保持していても従来どおり Tx の検索を可能とする手法を提案している[3]．ライトノードはブロックヘッダの代わりにブロック群ヘッダを保持すれば Tx の検索が可能になるためライトノードのデータ量もおおよそ 1/N に削減可能である．ただし，各フルノードが保持するブロック群を決定する仕組みや保持に対する報酬の割り当て方などの具体化（分散化手法)は今後の課題としていた．

4. ブロック群分散手法の要件

以下の要件を想定している．

① 各ノードが保持するブロック群最大数はユーザが設定するが，どのブロック群を保持するかはプロトコルと報酬で決定する．

② 公衆ブロックチェーンは，ノード毎の都合で自由に参加・離脱できる必要がある．よって，ブロック群毎に網内に存在するコピー数が変動する可能性がある．十分な永続性があることを保証できる最小コピー数が存在するとして，ブロック群毎に網内に存在するコピー数をおおよそ推定できる必要がある．

③ コピー数が不足する場合，当該ブロック群を保持するノード数を自動で増やせる仕組みが必要である．

④ ブロック群を保持する動機として，不正困難な報酬を支払う仕組みが必要である．

⑤ 同じブロック群を持つ複数のビザンチンノードが結託しても当該ブロック群の消失を防ぐため，どの非結託者が当該ブロック群を保持しているのか結託者から隠蔽できる必要がある．

5. ブロック群分散手法の案

以下に現在想定しているフルノードの動作概要を示す．

A. ブロック単位からブロック群単位の管理に移行時

(1)各フルノードは，N 個のブロックが蓄積するとそれらをまとめたブロック群を構成し，各々のストレージ容量に応じて，当該ブロック群を保持するか廃棄するか決定する．

(2)廃棄したかどうかの情報は他ノードに公開しない．

B. ブロック生成時

(3)ブロック群の保持証明・報酬

各ノードは生成したブロックが次ブロックで承認されると，ブロック群保持の証明として提出すべき Tx の通番を得る．(通番は PoS 等で導出された疑似乱数を用いて過去 20 年分からランダムに決定)

(4)当該ノードは，指定された Tx の保持証明(当該 Tx データと当該 Tx がブロック群内に存在するマークル木証明[2])を Tx として提出しデータ保持に対する報酬を得る(図 1 参照)．

(5)プロトコルによりブロック群毎の保持証明提出率を計算し台帳に記録．閾値未満の場合当該ブロック群保持の報酬を上げる．

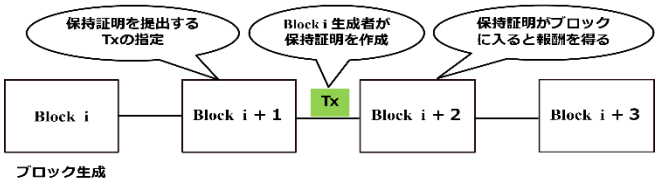

図 1 ブロック群の保持証明

C. ネットワーク参加時

(6)新たにネットワークに参加するノードは台帳を参照し，保持証明提出率の低いブロック群を優先して他フルノードからダウンロードする．

6. 今後の課題

今後は，保持証明提出率からブロック群保持数を推定する際の必要な精度や推定アルゴリズムの明確化，コピー数の補充不足を防ぐための具体的な条件の明確化する予定である．また，結託者がブロック群の消失攻撃を計画したとしても，結託者以外のノードの中で当該ノードの存在が予想されば攻撃を抑止可能だが，当該ノード数の期待値は，ノードの総数，参加・離脱率，保持証明提出時の Tx 指定数などに依存するため，攻撃抑止に十分な範囲に設計可能か，詳細検討していく予定である．

参考文献

[1] Ethereum, "Ethereum Full Node Sync (Default) Chart", (https://etherscan.io/chartsync/chaindefault), 2024.1.4
[2] YIBIN XU, YANGYU HUAN, "Segment Blockchain: A Size Reduced Storage Mechanism for Blockchain", IEEE, 13.1.2020.
[3] Masaki Obayashi, Takeshi Ogawa, "Reduction methods of the amount of data in blockchain node", ICETC2022, 29.11.2022.