講演番号：45

公衆ブロックチェーンへの DoS 攻撃防止方法

A study to prevent DoS attacks on public blockchain

児玉　純良†　小川　猛志†
Kiyora KODAMA†　Takeshi OGAWA†
† 東京電機大学システムデザイン工学部情報システム工学科
† Department of Information System Engineering, Tokyo Denki University

1. まえがき

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．PoS では一般に一定周期(以下，slot)毎に 1 つのブロック(台帳の更新コマンド=トランザクションを複数束ねたもの)のみを有効として台帳に反映することで，各ノードが持つ台帳の同一性を保証する．ただし 1slot で複数のブロックが生成された場合にどのブロックを有効とするかノード間の合意を形成する仕組みが必要である．Ethereum や Algorand, Tendermint, HotStuff, Solana, Polygon 等では少数の代表ノードが 1slot 毎に有効な1つのブロックを投票で決定し他のノードはその決定に従う仕組みが採用されているが，代表ノードへの権力集中や DoS 攻撃の可能性等の課題が知られている．本稿では後者に注目し詳細と対策案を示す．

2. 既存の合意形成技術

Tendermint[1] 等ではブロック生成ノードは輪番だが，Ethereum[3]や Algorand[2]等では slot 毎に更新する乱数(以下 seed)を用いて各 slot のブロックの生成ノードや投票ノードもランダムに更新しており，それら代表ノードによる不正を困難としている．それらの処理の概要を以下に示す．

(1) Algorand：各ノードは slot 毎に seed の値に対する独自のデジタル署名を計算しその値が閾値以下であればブロックを作成し更新した seed を添付して同報する(VRF)．生成されるブロック数は平均値= τ のポアソン分布に従う(τ 推奨値は 27)．各ノードは複数のブロックを受信するとデジタル署名の値が最小のブロックのみ転送する(soft vote)．同様に seed 値に基づき決定した投票ノードは締切時刻までに受信したブロックの中で，デジタル署名の値が最小のブロックを次ブロック候補とし，そのブロック(1 つ)を有効と認めるかどうかについて投票を行い，2/3 以上が有効と認めた場合当該ブロックが次ブロックとして確定する(BA)[2]．

(2) Ethereum：32 個の slot をまとめて 1epoch とし，n 段目の epoch 内のブロックが確定するとそれらの署名の値を元に各ノードは n+2 段目の epoch の slot 毎の seed を更新し同一の結果を得る (Randao)．各ノードは合意形成に参加できるノードのリスト(Validator list)を共有しており，その中から seed の値に基づき slot 毎のブロック生成ノードや投票ノードの ID が指定される．当該 slot のブロック生成時刻になると当該代表ノードはブロックを作成して同報する．当該ノードがルール通りに動作すれば生成されるブロック数は 1 つであるがルールを破り複数のブロックを生成しチェーンを分岐させる可能性があるため，各投票ノードは epoch 毎にどのチェーンの先端ブロックを有効とするか投票を行い，2/3 以上が有効と認めた先端ブロックを含むチェーンを有効として確定する(Gasper)[3]．

3. .既存技術の課題

(1) 課題1：Gasper では，32～64slot 前(現状 6～13 分前)に当該 slot の代表ノードが公知になるため，ブロック生成ノードへの DoS 攻撃が可能[3]

(2) 課題2：Algorand では，デジタル署名値が 0 に近いブロックを締切時刻間際で同報することで，どのブロックも 2/3 以上の承認をされず，当該 slot の台帳更新を妨害する DoS 攻撃が可能(Gasper で検討中の対策も同様)[2]

(3) 課題3：両者ともに，多数のノードが結託し秘密鍵を共有した場合，当該グループの中で連続してブロックを生成するかどうか予見し特定の決済の成立を遅らせたり順序を入れ替えるなどの不正な取引制御が可能．

4. 解決手法の案

Algorand 同様各ノードは当該 slot の seed 値のデジタル署名を計算しその値が閾値以下の場合にブロックを生成して同報する．ただし soft vote は行わず全ブロックを全ノードに伝搬させ，各ブロックについて「締切時刻までに受信できたかどうか」について投票で決定する．投票で有効とされたブロックをデジタル署名値の大きさの順に並べて，「hash(それら署名の結合値)%有効ブロック数」番目のブロックを次ブロックとして決定する．以上により課題1，2の攻撃を防止する．また seed は 1slot 前の 1 つのブロックではなく投票で有効になった全てのブロック内の次回 seed 値を結合して更新する手法[4]を適用する．多数のノードが結託しても他ノードが生成するブロックにより seed がランダム化されるため，課題3の連続当選予見を防止する．

表 1　既存手法と提案手法の主な差分

	既存手法	提案手法
投票での合意対象	1 有効ブロック選定	ブロック毎の締切前受信有無
次回 Seed への影響	1 有効ブロック	締切前受信ブロック全て

5. まとめと今後の課題

本稿では既存の主要な公衆ブロックチェーンの合意形成手法について DoS 攻撃関連の課題を挙げ，解決案を示した．今後定量評価を行う．また提案手法との組み合わせに適した投票手法についても検討を進める．

参考文献

[1] Kwon, Jae. "Tendermint: Consensus without mining." *Draft v. 0.6,* 2014.

[2] Y. Gilad, et al., "Algorand: Scaling Byzantine Agreements for Cryptocurrencies," SOSP'17, Oc. 28–31, 2017, Shanghai, China.

[3] Ethereum development documentation, https://ethereum.org/en/developers/docs/, 2024.1.2 参照

[4] Ogawa, Takeshi, et al., "Proposal of proof-of-lucky-id (PoL) to solve the problems of PoW and PoS," IEEE Blockchain-2018, Jul 30-Aug 3, Halifax, Canada.