

イーサリアム 2.0 のステートシャーディングにおける共謀攻撃問題の研究

A Study on the Collusion Attack Problem in State Sharding of Ethereum 2.0

LIANG XIAOTIAN† 川橋 裕‡

1. 研究背景

ブロックチェーン技術はビットコインシステムで誕生し、分散化、情報の透明性、改ざん防止などの特徴を持っている^[1]。近年、様々な応用シーンで広く使用されている。応用範囲の拡大に伴い、ブロックチェーンシステムにはより高い性能が求められるようになってきている。しかし、現在最大規模のブロックチェーン基盤であるビットコインおよびイーサリアムには依然として性能のボトルネックが存在し、大規模な応用に対応することが困難である。ビットコインのスループットは毎秒 7 件の取引であり、イーサリアムは毎秒 10~20 件^[2]で、VISA の毎秒 2000 件の取引と比較すると非常に低いである。(図 1 で示す)

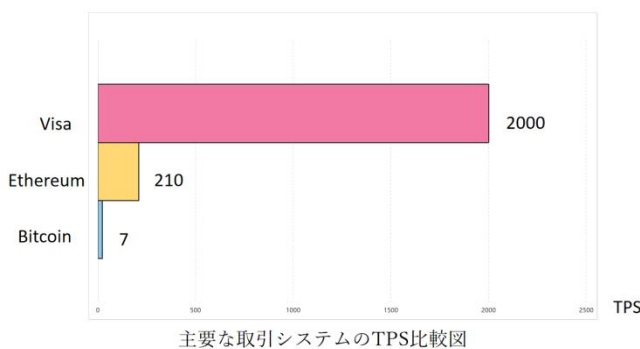


図 1

そのため、拡張性の向上はブロックチェーン研究における重要な課題の一つとなっている。ただし、拡張性の向上はシステムの安全性を犠牲にしてはならず、安全性を確保しつつ効果的な拡張を実現する方法が、現在解決すべき重要な課題である。

2. 先行研究

最近、多くの研究者がブロックチェーンの拡張性を強化する方法を提案している。その中には、ブロックサイズを増やすことで拡張性を改善する方法もある^[3]。しかし、この方法は拡張性を高める際に、拡張性、分散性、安全性の三つの属性を同時に満たすことができない。

そこで、分散性と安全性を犠牲にせずに拡張性を実現するために、従来のデータベース分野で広く用いられてきたシャーディング技術^[4](図 2 で示す)の導入が注目されている。

しかし、シャーディングにおける共謀攻撃の問題に関しては、依然として有効な解決策が提案されていない。

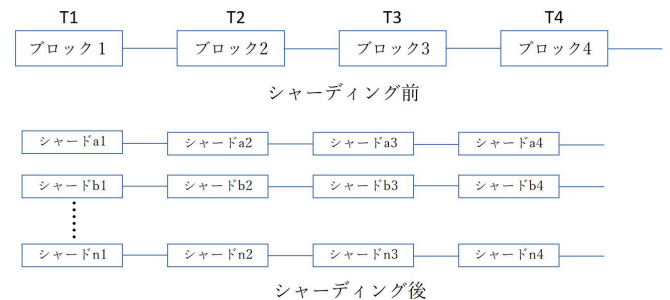


図 2

3. 研究目的

本研究は、現在のブロックチェーンの拡張性のニーズを分析した上で、イーサリアム 2.0 のステートシャーディングにおける共謀攻撃問題に対して、共謀攻撃に対抗する多段階検証方法を提案する。

4. 研究方法

1. 取引をマッピングルールに従って対応するシャーディングに割り当てる。
2. 検証ノードは自身のランダム分配アルゴリズムを使ってランダム数を生じ、マッピングルールに従い対応するシャーディングに入り、取引のコンセンサス検証を行う。
3. 検証結果が一致すれば、2 のステップを繰り返し、同じ検証結果が n 回達成されるまで取引をパッキングする。一致しない場合、2 のステップを繰り返し、多段階の回数が T 回に達しても一致しない場合、その取引を放棄する。(図 3 で示す)

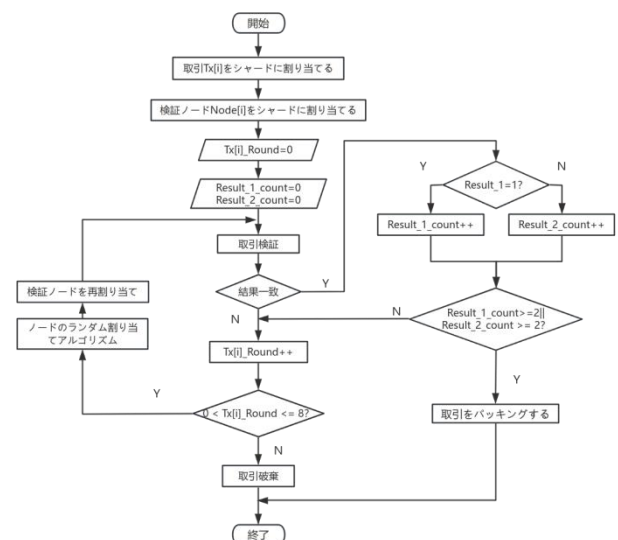


図 3

†和歌山大学

‡和歌山大学学術情報センター

5. 結論予測

本研究で提案する共謀攻撃に対抗する多段階検証方法は、共謀攻撃の発生確率を効果的に低減し、コンセンサスのタイムアウト回数を制限する。連続して多段階コンセンサスがタイムアウトすると、取引が放棄され再分配されるため、DDOS 攻撃、Sybil 攻撃、51%攻撃は実行できない。これによりシステムの正常な運用が保証される。

6. 未解決の課題

イーサリアム 2.0 のステートシャーディングでは、バリデータノードは一部のシャーディングのみを担当する将来的な研究では、ステートシャーディングにおけるバリデータノードの状態選択の最適化に焦点を当て、さらなる研究を行う。

7. 参考文献

- [1] SUN Y, FAN L J, HONG X H. Technology development and application of blockchain: current status and challenges [J]. Strategic Study of CAE, 2018, 20 (2) : 27-32.
- [2] WOOD E. A secure decentralised generalised transaction ledger[J]. Yellow Pap ,2015(151):1.
- [3] WANG ZP, CHALIASOS S, QIN K H, et al. On how zero-knowledge proof blockchian mixers improve, and worsen user privacy[J]. IEEE Network.2022(9):220.
- [4] Luu L, Narayanan V, Zheng C, et al. A Secure Sharding Protocol for Open Blockchains[C]// the 2016 ACM SIGSAC Conference. ACM, 2016.