6D-06

ZK-rollups を活用した ブロックチェーンの相互運用性に関する検討

山本　周†　　山下　真一†

株式会社エヌ・ティ・ティ・データ 技術革新統括本部 技術開発本部 コンピテンシセンタ†

1. はじめに

Ethereum は高い分散性のもと、高信頼なネットワークが構成されており、デファクトスタンダードのブロックチェーンネットワークとなっている。しかし、エンタープライズ用途では public 型ブロックチェーンの利用についての障壁の一部として、情報の秘匿性やファイナリティの問題があり、public 型ブロックチェーンではなく、特定のノードのみ参加する consortium 型、private 型ブロックチェーン(以降まとめて consortium 型と呼ぶ)を利用しているのが実態である。consortium 型にも課題はあり、コンセンサスアルゴリズムの都合によっては性能制約から参加可能なノード数が限られるという問題も存在する。本検討では、エンタープライズブロックチェーンをより高分散で高信頼のものにすると同時に、consortium 型ブロックチェーン間を接続し、情報の秘匿性やファイナリティを保ったまま、より多くのノードと高信頼なやり取りを可能にする仕組みについて、ZK-rollups を活用する方法を検討する。

2. 現況

2.1. Public Ethereum Network

Ethereum では参加 Validator 数が 40 万を超え[1]非常に高い分散性がある public 型ブロックチェーンとなっている。一方でかねてより、トリレンマ(=分散性、スケーラビリティ、セキュリティ)を同時に満たすことは困難とされてきており、Public の Ethereum チェーンでは、スケーラビリティを犠牲に、高いセキュリティ(PoS)、高い分散性(40 万を超えるノード数)を優先する設計になっていると考えられる。

近年、Ethereum のロードマップでも肝とされている ZK-rollups の開発が盛んである。従来の Ethereum は、署名、実行、合意形成、記録等の役割を一つのクライアントによって担う仕組みとして設計されており、スケーラビリティに課題があるとされてきた。rollups は、これらの役割のうち、署名、実行を L2(合意形成や記録の役割を担うレイヤーを Layer-1(L1)と呼ぶのに対し、署名、実行を担うレイヤーを Layer-2(L2)と呼ぶ)で巻き取って(=rollup)実行することで、L1 の負荷を減らし、ネットワーク全体としてのスケーラビリティを向上させようという考え方である。そして、ZK-rollups は、この rollups の中でも、ゼロ知識証明を利用することで、署名や実行を簡潔に証明し、セキュリティにも悪影響なく、L1 の負荷を最大限小さくする手法である。この ZK-rollups は、長年の課題とされてきたトリレンマの同時成立の鍵と考えられている。

2.2. consortium 型ブロックチェーン

エンタープライズの一部の用途では、表 1 のような様々な理由から public 型ブロックチェーンの利用を避け、特定のノードのみ参加する consortium 型ブロックチェーンをカスタマイズ構成し利用するケースが多く存在する。

consortium 型ブロックチェーンについても課題がある。一つは、限られたノード数で運営するために、不正操作が比較的容易になりセキュリティ上の懸念が発生することである。もう一つは、コンセンサスアルゴリズムの設定次第で、性能制約から参加可能なノード数が限られ、大規模ネットワークを構成することについて制約があること[2]である。

表 1 中②や④の需要から引き続き consortium 型ブロックチェーンは今後も存続するものと考えられるが、一方で以上のような課題を解決することが望まれる。この解決策について本提案で検討する。

観点	課題	詳細	解決策
①業務上の課題	税制上の規制	public 型ブロックチェーンでの取引では仮想通貨等を扱うこととなり、租税の取り扱いに関して国内の法整備が遅れている。	法整備の動向あり[3][4]
②業務上の課題	情報公開範囲	エンタープライズ用途においてすべてのデータを第三者に公開することは忌避されるケースがある。限定されたメンバにのみ情報公開するための制御が必要である。	-
③技術上の問題	スケーラビリティ	現時点での public 型ブロックチェーンは急激に利用者が増加したため、トランザクション数が増加し、トランザクション実行に必要となる手数料(gas 代)が高騰している。	先述の通り、スケーラビリティ改善の動向が存在する
④技術上の問題	ファイナリティ	トランザクションの確定までに必要とする時間は、従来の DB によって構成されたシステムに比較して長くなる。	-

表 1 public 型ブロックチェーン利用の障壁

Examination on interoperability of blockchains by using ZK-rollups

† Research and Development dept., Technology and Innovation HQs., NTT DATA

3. ZK-rollups を活用した相互運用性

本提案では、ZK-rollups の検証 Contract が導入された L1 のもとで、複数の consortium 型ブロックチェーンを L2 として、L1 での transaction を介して相互に接続することのできる(=interoperability)構成(図 1)を提案する。それぞれの L2 は、coordinator を介して L1 に接続し、片方の L2 の transaction を L1 経由でもう片方の L2 に伝達する。実際に、privacy-scaling-explorations[5]を改造することで構成、実装を行った。この構成により、先述の consortium 型ブロックチェーンの課題を解決する。

セキュリティの向上: transaction 実行の最終的な合意形成は L1 にてとるため、L1 で Ethereum を採用することで高分散、高セキュリティを利用することができる。

大規模ネットワークの構成可能性: 複数 consortium 型ブロックチェーン間でのやり取りを可能にすることで、多数のノードとのやり取りを実現することができる。後述するがすべての transaction をブロックチェーン間でやり取りすることなく、必要な transaction のみチェーン間のやり取りを行う実装も考えられる。

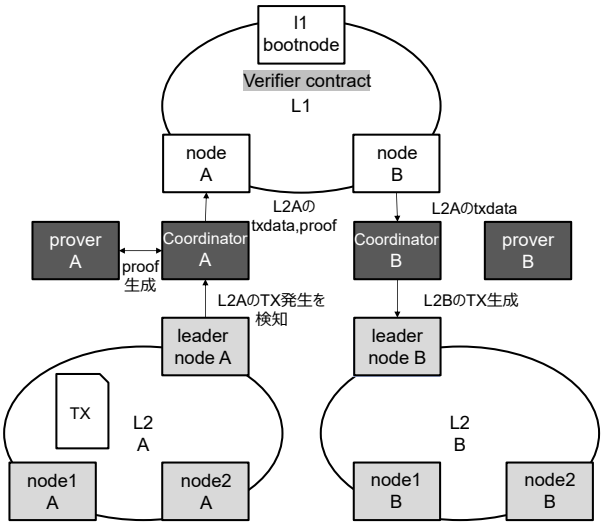

図 1 構成図

4. 評価

既存の consortium 型ブロックチェーンの利用形態に合わせたときに検討するべき他の観点としては、ファイナリティと、機密情報の限定公開可能性があった。ファイナリティについては、本提案実装では 2 段階に分かれると考えられる。1 段階目に L2 での合意形成、2 段階目に L1 で証明検証が行われる。1 段階目ではまだ coordinator が L1 に transactions data を post していない段階であるが、coordinator に異状ない限り内容は確定と考えられる。2 段階目に L1 に書き込まれることで最終的な確定となる。coordinator に異状が発生することは非常に稀にできるため、他チェーンとのやり取りを除いては基本的に 1 段階目でファイナリティとすることも可能であり、運用上の工夫によりこの観点については従来の consortium 型ブロックチェーン同様のユーザビリティがあると考えられる。

機密情報の限定公開の仕組みには整理の余地がある。基本的に本来の ZK-rollups ではすべての transaction の情報は L1 に post することとなっているが、セキュリティは犠牲になるものの、Validium のように transactions data を L1 に post しない手段を図 2 のように使い分けることで、業務上のユースケースに合わせることができる。

なお、Validium 方式を適用、もしくは併用する場合、L2 の transactions data を検証しないため、L1 の検証ロジックは ZK-rollups とは異なるものとなる。2 つの検証ロジックを組み合わせたとき、L1 の検証 Contract の実装として、純粋な ZK-rollup とは異なり注意が必要なのは以下の点である。

① L2 の状態遷移の検証については transactions data の有無に関わらず一貫して行うこと

② 送信側の L2 にとって不利な transaction の情報を L1 に post せずに秘匿することを防ぐ必要がある場合、予め送信側で L1 連携用の Contract を設定し、transactions data を L1 に公開しないときに限り、transactions の宛先が予め設定した連携用 Contract でないことの証明を別途検証すること

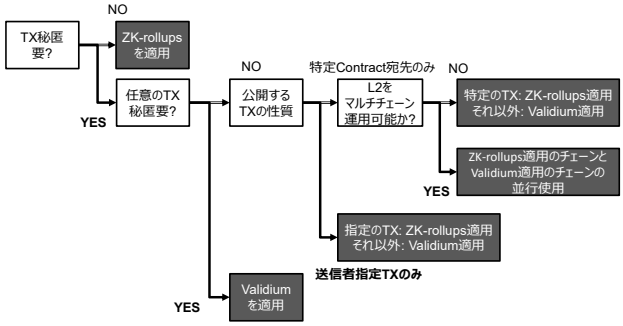

図 2 情報公開限定手法フローチャート

5. まとめ

今後、consortium 型ブロックチェーンはより業界横断で情報流通を行う基盤として発展していくだろう。そのような流通を促進する手段として、本提案では ZK-rollups を利用した情報流通を提起した。現時点で ZK-rollups は活発な検証段階にあるものの、高分散な public ネットワークが将来的にエンタープライズ利用しやすくなってきていると思われる。技術的困難から本検討では机上検討となった秘匿情報制御については今後実際に動作検証を行っていく方針である。

6. 参考

[1] Glassnode: The Merge: A Feat of Engineering, 2022, https://insights.glassnode.com/the-week-onchain-week-38-2022/, 最終アクセス日:2023/1/4

[2] H. Sukhwani, J. M. Martínez, X. Chang, K. S. Trivedi and A. Rindos: Performance Modeling of PBFT Consensus Process for Permissioned Blockchain Network (Hyperledger Fabric), 2017 IEEE 36th Symposium on Reliable Distributed Systems (SRDS), pp. 253-255(2017)

[3] 一般社団法人 日本ブロックチェーン協会: 暗号資産に関する税制改正要望 (2023 年度) https://jba-web.jp/cms/wp-content/uploads/2022/11/20221116_jbazeisei.pdf, 最終アクセス日:2023/1/4

[4] 一般社団法人 新経済連盟: 暗号資産に関する 2023 年度税制改正要望, https://jane.or.jp/app/wp-content/uploads/2022/09/220907document.pdf, 最終アクセス日:2023/1/4

[5] privacy-scaling-explorations/zkevm-chain: https://github.com/privacy-scaling-explorations/zkevm-chain, 最終アクセス日:2023/1/4