55　Bitcoin のトランザクションにおける Segwit と Taproot に関する分析

電子商取引研究室　阪本　翔

1．序論

Satoshi Nakamoto が 2008 年にビットコインを発表して以来、現在も暗号資産全体の約 39 %をビットコインが占めている[*1]。しかし、ビットコインには「スケーラビリティ問題」と「トランザクション展性」と呼ばれる問題がある。これに対し 2017 年 8 月に Segwit と呼ばれるビットコインプロトコルの拡張が行われ現在でもこの問題の改善に役立っている。また 2021 年 11 月に Taproot と呼ばれる Segwit をアップデートした形のビットコインプロトコルの拡張が行われ現在も実装されており今後のビットコインの脆弱な上記のような問題をカバーするものになると考えられている。そこで Segwit と Taproot に関する使用率を正確に調査することでビットコインに対する利便性がどの程度あるのかを調査し評価する。

2．ビットコイン問題

ビットコインにはデータ容量制限が原因の「スケーラビリティ問題」と外部からトランザクション ID によって改ざんが可能である「トランザクション展性」と呼ばれる問題があり、この問題に対しトランザクションを圧縮してデータ量を小さくする技術である Segwit が 2017 年 8 月に導入された。その後 Segwit のアップデート版となる Taproot は MAST とシュノア署名と呼ばれる技術 1) を融合し、さらなるスケーラビリティの向上とプライバシー機能の改善が実現される。そこで Segwit と Taproot の使用率を調査するにあたりビットコインを送金する際に生じるトランザクションの情報を取得するためにブロックチェーンの API を用いて 765,263 個（2022/11/30 時点）のブロックをダウンロード[*2]しブロック情報を全てデータベースに格納する。その後、格納したブロックのトランザクションに対し Segwit と Taproot を識別するために必要なビットコインを送金するためのアドレスを検索するシステムを作成し、システムを通して得た Segwit と Taproot が該当するアドレスの数をトランザクションのアドレスの全数で割ったものを Segwit と Taproot の使用率としグラフ化する。

3．結果・考察

図 1 のグラフより導入開始された Segwit は 2019 年の 600,000 ブロックで約 5 割の使用率となっており、2022 年時点では約 8 割の使用率となっているため増加傾向にあるとわかる。図 2 のグラフより Taproot はまだ 1 年間のみの実装と期間が短いため十分なデータが取れなく、ビットコインに対し有用的であるかどうかが判別しずらくなっている。しかし Taproot はこれまでビットコインに実装されることのなかった「スマートコンストラクト」の機能の拡張が実現されることが予想されており、近年アルトコインで普及している NFT がビットコインで普及すると考えられ多くのユースケースが実装されると予想される。

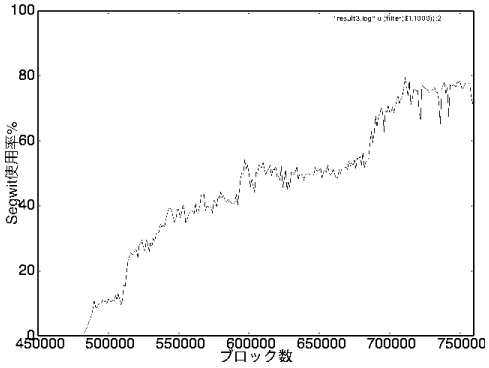

図 1　Segwit の使用率

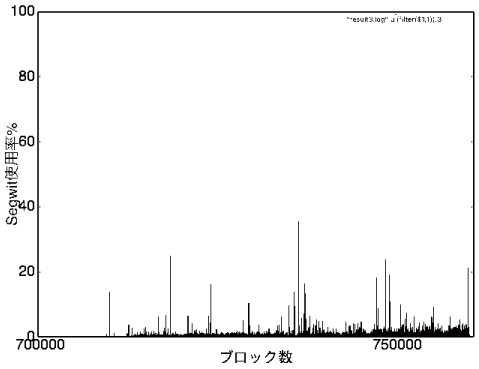

図 2　Taproot の使用率

4．結論

ビットコインの問題に対した改善案として挙げられる Segwit と Taproot の使用率を求める検索システムを提案し、ビットコインにおける Segwit と Taproot の使用率をグラフで可視化することで重要性が理解できた。また、Taproot のように未だ使用率がよくないのは実装期間が浅いためであり、Segwit と同様に先の 5 年〜10 年のデータをもとにグラフ化することで Taproot の有用性がわかると考える。

参考文献

1) Rewat Thapa, Pankajeshwara Sharma, Joschka Andreas Hüllmann, and Bastin Tony Roy Savarimuthu. Identifying influence mechanisms in permissionless blockchain communities: The bitcoin case. In *42nd International Conference on Information Systems (ICIS)*, pp. 1–17, 2021.

[*1] https://coinmarketcap.com/
[*2] https://www.blockchain.com/explorer/api