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。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．トランザクション情報検索システム

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（取引履歴）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 年 11 月 30 日時点）のビットコインブロックをダウンロードしブロック情報を全てデータベースに格納する。その後、データベースに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に用いられるアドレス（=addr）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

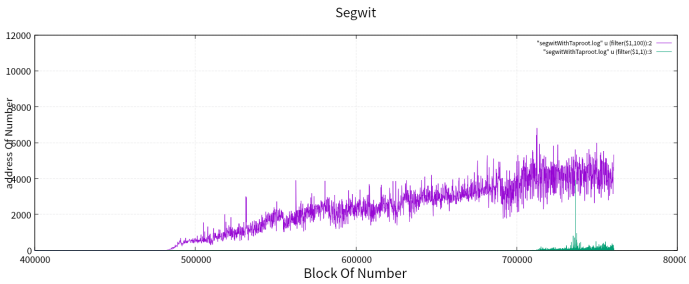

図 1　Segwit の使用率

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)