

# ブロックチェーンプラットフォームをもとに生成された活動記録システムの調査研究

電子商取引研究室 阪本 翔

## 1. 序論

Blockchain を用いた活動記録を Bitcoin に記録する Blockcerts や OpenBadge と呼ばれるシステムがある。しかし、Bitcoin の検索は可能だが本来収集したい Bitcoin のブロック情報が十分に得られない。そこで、ダウンロードした 70 万個のブロックをもとに Blockcerts や OpenBadge を検索をするシステムを作成する。最終的には、検索から得た結果から Blockcerts や OpenBadge がどの程度含まれているかについてグラフ化しどのような利便性があるのかについて調査を行う。

## 2. 研究内容

本研究は、Blockchain 技術を用いて活動を記録するような Blockcerts や OpenBadge と呼ばれるシステムを検索するために、まず仮想通貨である Bitcoin に対し API を取得し API を利用しブロックチェーンのブロックの情報を JSON 形式で取り出す。取り出した JSON 形式の情報を MongoDB と呼ばれる分散型データベースに保存し、保存したデータ全てに対し検索を行うシステムを作成し実行する。検索する対象は Blockcerts や Open Badget のような活動記録システムが全ブロックに対しどのくらい含まれているかについてである。ブロックチェーンのトランザクションの構造はいくつかのブロック内に複数のトランザクションが形成されており、その一番前のトランザクションにビットコインのブロックを識別する公開鍵のハッシュ値を文字列表現したビットコインアドレスがある。この文字列をもとに、Bitcoin 内に実装されている String の文字列 OP \_\_ RETURN というメッセージを検索する。OP \_\_ RETURN は Bitcoin の Blockchain 内に文字列を書き込むという命令である<sup>1)</sup>。そこで、この OP \_\_ RETURN というメッセージを検索することで Blockcerts や OpenBadge のようなシステムが Blockchain 内に活動記録を文字列で保存されていて全ての Bitcoin の Block の情報に対しどのくらい記録されているのかを調査することを目的とした。図 1 は現在までで取得できた 70 万個の Bitcoin ブロックのトランザクションを過去のデータを 24 時間のブロックあたりで平均を取ったトランザクション数をグラフ化したもので、図 1 を見ると 2009 年に運用を開始し 2010 年から 2018 年まで順当にトランザクション数が増加傾向にあったがコロナや容量を超えた送金などが原因でトランザクション数が急激に減少した。しかし、2015 年 12 月に提唱された Segwit と呼ばれる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<sup>2)</sup>が普及したことによりデータ容量が改善され再びトランザクションが増加していることが図 1 よりわかる。このことより Segwit がどのようなものである

かについて、さらにトランザクションにてどのように記録されているかについて調査を行う。

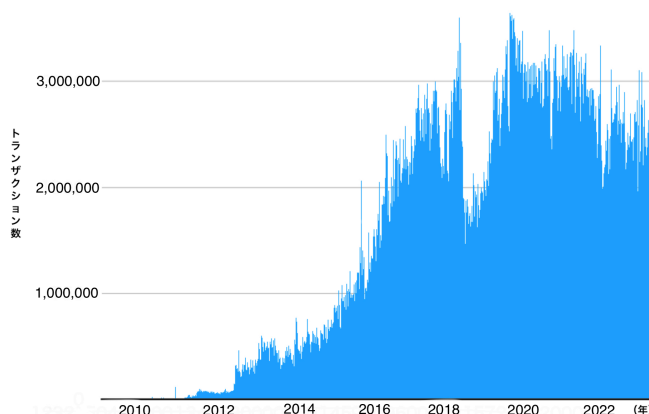


図 1 過去 24 時間のブロックあたりの平均トランザクション数

## 3. 完了までの研究計画

現時点 (10/19) での進捗状況は、Bitcoin のブロック 70 万個の情報をダウンロードしている段階である。次の段階は 10 月中にブロック 70 万個を MongoDB に保存し、11 月に Blockcerts や Open Badget がどの程度含まれているか検索しそれらをグラフにまとめる。12 月には、ブロックチェーンをサポートする技術である Segwit について調査しまとめる。

## 参考文献

- 1) Bitcoin の ブ ロ ッ ク チ ェ ー ン に 任 意 の 80byte デ ー タ を 刻 み こ む:<https://qiita.com/yyu/items/8650563126380d813e8e> (閲覧日:2022/10/19 時点)
- 2) セ グ ウ ィ ッ ト (Segwit) と は ? : <https://coinpost.jp/?p=2931> (閲覧日:2022/10/18 時点)