Bitcoin ノード国別ランキング

永田倖大†
明治大学総合数理学部　先端メディアサイエンス学科　菊池研究室†

1　はじめに

Bitcoin は Nalamoto の論文[1]に基づいたディジタル通貨であり 2009 年に運用が開始され，取引手数料が安い，匿名性が高いという特徴がある．しかし分散管理されているために，誰と誰が通信しているか，どの国で多く使われているかなどが不明であった．

そこで，本研究では Full Node のウォレットが Bitcoin ネットワークへコネクションを行う時の様子を長期間観測し，Bitcoin ノードの IP を収集した．収集したデータを解析するシステムを開発し，どの国で多く使われているか，どれくらいの IP が集まるのかを明らかにすることを目的とする．

2　実験

2.1　MultiBit と Bitcoin Core の違い

Bitcoin ノードには様々な種類があり[2]，そのなかに Full Node と SPV(Simplified Payment Verification)がある.そのクライアントであるウォレットには，表 1 で示す種類がある．

表 1.MultiBit と BitcoinCore の比較

	Bitcoin Core	MultiBit
種類	Full Node	SPV
ブロック情報	全て所持	ヘッダーのみ

Bitcoin Core と Multibit はビットコインの取引を行うことが可能である．しかしノードによって取引を行う機能を持たないクライアントを稼働しているものもある．

2.2　データ収集方法

Bitcoin の Full Node Client である Bitcoin Core を起動し，その時に通信を行った Bitcoin に関するパケットを観測するために解析システム BitcoinPcap を python を用いて開発した．

2.3　解析システム BitcoinPcap

BitcoinPcap は起動するとパケットキャプチャを始め，そのパケットを入力とし，IP データを抽出し，国判別を行い，表 3 のような csv ファイルを出力する．BitcoinPcap は特定のパケットだけを抽出することも可能である．例えば，図 4 の様な addr パケットだけを集め，addr パケットの Count を抜き出すことも可能である．

2.4　収集データ

収集した IP の総数は 2524 個であり，重複を除くと 1715 個である．表 2 に収集情報を示す．

表 2.収集情報

観測期間	2016 年 11 月 17 日～11 月 27 日(10 日間)
起動ウォレット	Bitcoin Core
ユニーク IP 数	1715 個
国数	69 国
観測場所	自宅(東京都国分寺市)
ISP	アルテリア・ネットワークス
bandwidth	最大 1Gbps
IP 上位オクテット	122.219.218.0/24

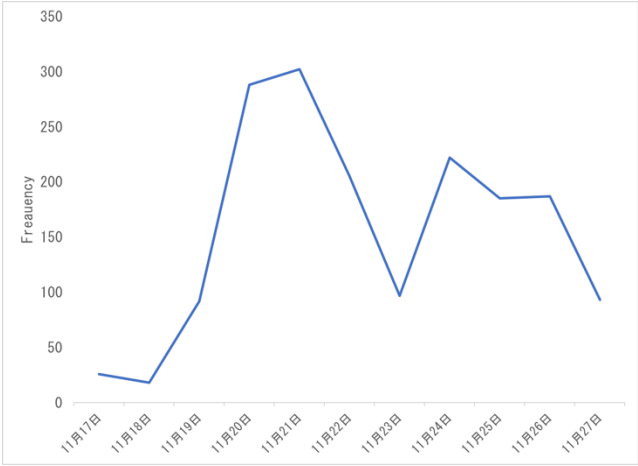

図 1:IP アドレス観測の分布

図 1 にユニーク IP の分布図を示す．11 月 17 日から 20 日の観測期間は，日に 7 時間ほど断続的に観測していたため収集 IP が少ない．11 月 20 日から収集数が増えたのは 24 時間連続して観測したためである．

表 3.収集データ一部

Time	IP	Country	Day
12 時	217.79.189.197	Germany	11/17
12 時	139.162.27.201	Singapore	11/17
13 時	173.170.76.60	United States	11/17
14 時	66.96.199.201	Singapore	11/17
15 時	50.206.138.178	United States	11/17
16 時	208.66.68.127	Canada	11/17
12 時	64.121.102.206	United States	11/18
12 時	46.101.192.63	Germany	11/18

† Kodai Nagata, Department of Frontier Media Science, School of Interdisciplinary Mathematical Science ,Meiji University, Kikuchi Laboratory.

表 3 に収集した IP の一部を示す．Country の判別には GeoIP を用いた．

2.5 実験環境

実験環境を表 4 に示す．

表 4. 実験環境

OS	macOS Sierra 10.12.1
メモリ	8GB
言語	Python 2.7.12

BitcoinPcap には python のライブラリである pyshark を使用した．pyshark はパケットキャプチャーソフトの thsark を python の環境で利用できるようにしたものである．プログラムの起動はターミナルで行う．

2.6 コネクション

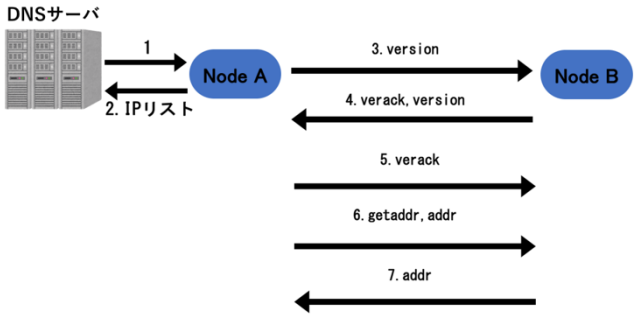

図 2:Bitcoin ネットワークへのコネクション方法

図 2 に Bitcoin ネットワークに接続するプロトコルを示す．1.DNS サーバに問いかけ Bitcoin ノードを稼働しているノードの IP アドレスリストを受け取る．そして，ノード A はリストの中から任意の IP を選び，3.version パケットを送信する．3.version パケットには A のクライアント情報や，どのブロック情報まで保持しているかなどが含まれている．3.version パケットを受けとるとノード B は 4.verack パケットを A に返信する．その後，ノード B に対して 6.addr パケットと 6.getaddr パケットを送信する．6.addr パケットには，A のノード情報や，他の Bitcoin ネットワークのノード情報が含まれている．6.getaddr パケットを B に送ることによって，7.addr パケットを返答として受け取る．7.addr パケットには，1 つだけノード情報が入っているものや，1000 個入っているものまで存在する．

2.6 パケットの分析

表 5.addr パケット統計情報

アドレスの個数	パケットの数
1	351
2	25
3	1
524	1
1000	9

表 5 に 387 個の addr パケットの統計情報を示す

```
Bitcoin protocol
    Packet magic: 0xf9beb4d9
    Command name: version
    Payload Length: 102
    Payload checksum: 0x40538f0e
    Version message
        Protocol version: 70012
        Node services: 0x0000000000000005
        Node timestamp: Dec 12, 2016
18:09:28.000000000 JST
        Address as receiving node
        Address of emmitting node
        Random nonce: 0x3bbd12a066ee8ce8
        User agent
            Count: 16
            String value: /Satoshi:0.12.0/
        Block start height: 443099
```

図 3:version パケット

図 3 に version パケットを示す．Protocol version は送信ノードが使用しているプロトコルバージョンを示しており，String value では使用しているソフトウェアのバージョン，Block start height には，現在どのブロック情報まで所持しているかが含まれている．

```
Bitcoin protocol
    Packet magic: 0xf9beb4d9
    Command name: addr
    Payload Length: 31
    Payload checksum: 0x3245bb2d
    Address message
        Count: 1
        Address:
5a694e5805000000000000000000000000000000000000ffff
...
            Node services: 0x0000000000000005
            Node address: ::ffff:209.188.18.142
(::ffff:209.188.18.142)
            Node port: 8333
            Address timestamp: Dec 12, 2016
18:09:46.000000000 JST
```

図 4:addr パケット

図 4 に addr パケットを示す．Count は addr パケットに含まれる IP アドレスの数を示し，Node address には Bitcoin ノードを稼働している IP アドレスが記されている．

```
Bitcoin protocol
    Packet magic: 0xf9beb4d9
    Command name: tx
    Payload Length: 191
    Payload checksum: 0xae049e31
    Tx message
        Transaction version: 1
        Input Count: 1
        Transaction input
        Output Count: 1
        Transaction output
            Value: 2435310
            Script Length: 25
            Script:
76a91469feb683ce891c508786fdb1d2ef29eb5304d34d88
...
        Block lock time or block ID: 0
```

図 5:tx パケット

図 5 にビットコインの送受信の取引を表す tx パケットを示す．Value は送金したビットコインの額であり，10^{-8} の額を表記している．

2.7 利用上位国

表 6 に観測 IP，上位 10 カ国を示す．

表 6. 上位 10 カ国 IP 数

順位	国	割合[%]	個数
1	United States	33	447
2	Germany	13	240
3	United Kingdom	6	115
4	France	5	93
5	Netherlands	5	86
6	Russia	4	81
7	Canada	4	74
8	China	3	53
9	Sweden	2	42
10	Ukraine	2	37

表 6 に含まれる IP は，自分のノードと通信を行ったものだけであり，Full Node と SPV のどちらも含まれる．

1 つだけ観測できた国では，モナコやヨルダンなどがあった．

2.8 考察

実験結果より，Bitcoin ネットワークへのコネクション方法，Bitcoin に関するパケットの内容，Bitcoin ノードがどの国で多く使われているかが明らかになった．

本研究で調査を行なったユニーク IP の 33 パーセントはアメリカのものであったので，世界で一番 Bitcoin ノードを稼働している国はアメリカではないかと考える．IP アドレス 2524 個中 809 個が重複していた．収集 IP の 32 パーセントと高いことから，ウォレットを起動し，通信を確立する相手ノードは常に稼働し続けていると考えられる．

3 おわりに

Bitcoin に関するパケットを収集し，情報を取得するプログラム BitcoinPcap を開発した．BitcoinPcap は取得したいパケットの種類や，パケットの一部を抽出することが可能であるため Bitcoin に関するパケットを観測，および解析するのに有益である．

本実験で収集した IP アドレスは，自分のノードと通信を行ったものだけであったが，DNS サーバーへ通信を行い IP リストを受け取る方法や，他のノードに向けて getaddr パケットを送り集める手法など，より効率よく多くの IP を集めることを検討中である．

本実験では tx パケットの解析は行わなかった．tx パケットに含まれる取引額と国の関係や，どれくらいの tx パケットが収集できるか，どの時間帯に取引がよく行われているかを分析することで，ビットコインの使用の特徴が明らかになるだろう．

4 先行研究紹介

先行研究[3]は，ビットコインの取引の際に使用される，アドレスをクラスタリングし再識別攻撃を行うことで管理者を明らかにすること，Bitcoin 市場の長期的な変化の分析，その変化による Bitcoin システムへの影響，安西や詐欺目的で使用されたビットコインの検知を目的としている．

図 6:クラスタリング手法 1

図 6 はアドレスのクラスタリングの手法の一つとして紹介されている．ビットコインの取引では入力アドレスの管理者は同一であるため，図 6 のように入力アドレスが 2 つ以上あるような取引 1,取引 2 があった場合，アドレス A,B,C の管理者は同一であると定めている．

アドレス間の変化を見るために，Change Address というクラスタ手法も用いている．

研究結果として，3,384,179 個のクラスターができ，その中で管理者が分かったものは 2197 個であり，1,800,000 個のアドレスの管理者を特定したといっている．

参考文献

[1] S.Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System” (https://bitcoin.org/bitcoin.pdf ,2016 年 4 月参照).

[2] Andreas M.Antonopoulos,“Mastering Bitcoin”,O’REILLY,pp.140-143,2014.

[3] S.Meiklejohn, M.Pomarole,G.Jordan,K.Levchenko, D.McCoy, G.M.Voelker, “A Fistful of Bitcoins:Characterizing Payments Among Men with No Names”,(Internet measurement conference),pp127-140,IMC’13,2013.