一般社団法人　電子情報通信学会
THE INSTITUTE OF ELECTRONICS,
INFORMATION AND COMMUNICATION ENGINEERS

信学技報
IEICE Technical Report
NS2019-208(2020-03)

コンパクトブロックリレーとインターネット高速化を考慮したビットコインネットワークシミュレーション

永山流之介† 　首藤　一幸† 　坂野　遼平†

† 東京工業大学　〒152–8550 東京都目黒区大岡山 2–12–1
E-mail: †nagayama.r.ac@m.titech.ac.jp

あらまし　トランザクションスループットの改善は，Bitcoin にとって重要な課題である．しかし，スループットの改善のためにブロック生成間隔を短縮し，ブロックサイズを大きくすると，ブロックの共有が遅くなり，孤立ブロックが増加する．そのため，スループットの改善には，ブロック伝搬遅延を短縮する必要がある．近年，インターネット高速化やコンパクトブロックリレーの実装によって，ブロック伝播遅延は短縮した．しかし，これらの遅延短縮に対する貢献の定量的な分析は為されていない．本研究では，シミュレータを用いてブロック伝播遅延を測定し，2015 年から 2019 年のインターネット高速化とコンパクトブロックリレーの影響を調査した．実験では，インターネット高速化により，ブロック伝播遅延の 50 パーセンタイルが 64.5%，90 パーセンタイルが 63.7% 短縮し，コンパクトブロックリレーにより，50 パーセンタイルが 90.1%，90 パーセンタイルが 87.6% 短縮した．
キーワード　Bitcoin，ブロックチェーン，伝播遅延，シミュレータ

Simulation of the Bitcoin Network Considering Compact Block Relay and Internet Improvements

Ryunosuke NAGAYAMA†, Kazuyuki SHUDO†, and Ryohei BANNO†

† Tokyo Institute of Technology　2–12–1 Ookayama, Meguro-ku, Tokyo, 152–8550 Japan
E-mail: †nagayama.r.ac@m.titech.ac.jp

Abstract　Improving transaction throughput is an important challenge for Bitcoin. However, shortening the block generation interval or increasing the block size makes sharing blocks within the network slower and increases the number of orphan blocks. Therefore, to mitigate this, it is necessary to reduce the block propagation delay. Because of the contribution of compact block relay and evolution of the Internet, the block propagation delay has been shortened in recent years. However, there is no quantitative analysis of these contributions. In this study, we measure the block propagation delay on the Bitcoin network using a simulator, and investigate the effect of compact block relay and Internet improvements from 2015 to 2019. The experimental results reveal that the block propagation delay is reduced by 64.5% for the 50th percentile and 63.7% for the 90th percentile due to Internet improvements, and by 90.1% for the 50th percentile and by 87.6% for the 90th percentile due to compact block relay.
Key words　Bitcoin, blockchain, propagation delay, simulator

1. はじめに

ブロックチェーンはビザンチン障害耐性を持つ分散システムである．ブロックチェーンは集中システムを用いず，分散台帳を管理することができ，データの改竄が困難であることから，暗号通貨の基盤技術として利用されている．しかし，Bitcoin をはじめ，多くのブロックチェーンで使われるアルゴリズムである Proof–of–Work（PoW）[1] は一定期間に少数のトランザクションしか処理できないという問題がある．

一つの解決法は，ブロック生成間隔を短縮することであるが，これはブロックチェーンのセキュリティを犠牲にする [2]．ブロック生成間隔を短縮した場合，次のブロックが生成されるまでにネットワーク内にブロックを共有することが困難になり，ブロックチェーンの分岐が発生する．そのため，ブロック生成

This is an unrefereed paper.

間隔を短縮するためには，短時間でブロックをネットワーク内で共有する必要がある．

近年，Bitcoin のブロック伝播遅延は短縮している [3], [4]．伝播遅延の 50 パーセンタイルは 2015 年は 5 秒以上であったが，2019 年には 1 秒以下になっている．また，伝播遅延の 90 パーセンタイルは 2015 年は 15 秒以上であったが，2019 年には約 2 秒になっている．

ブロック伝播遅延の短縮には以下のような理由がある [4]．

- Falcon [5] や FIBRE [6] などのリレーネットワークの利用．
- コンパクトブロックリレー（Compact Block Relay, CBR）[7] などの Bitcoin プロトコルの拡張．
- ネットワーク遅延の短縮や帯域幅の拡大によるインターネットの高速化 [8], [9]．

大月ら [10] はブロックチェーンネットワークシミュレータ SimBlock [11], [12] 上で Bitcoin ネットワークを再現し，ブロック伝播遅延やフォーク率に対するリレーネットワークの影響を調査した．しかし，CBR やインターネットの高速化がブロック伝播遅延の短縮に与える影響の定量的な分析はない．本研究では，CBR と 2015 年から 2019 年にかけてのインターネットの高速化をシミュレータ上で再現し，ブロック伝播遅延とフォーク率を測定した．

本報告の構成は以下の通りである．次章では，Bitcoin の概要を述べ，3 章では利用するシミュレータとシミュレーションで用いるパラメタの算出方法や CBR のモデル化について述べる．4 章では，実験結果を元に，CBR とインターネットの高速化の影響について考察する．5 章では，まとめと今後の課題について述べる．

2. Bitcoin ネットワーク

2.1 ブロック生成

Bitcoin はトランザクションを記録するためにブロックと呼ばれるデータ構造を用いる．ノードはブロードキャストされたトランザクションを受信すると，メモリプールに格納し，それらからブロックを生成する．生成されたブロックは，ネットワークにブロードキャストされ，受信ノードはそのブロックを検証し，ブロックチェーンに追加する．ブロックはトランザクションに加えて，一つ前のブロック（親ブロック）のハッシュ値を保持するため，ブロックチェーンは連続したトランザクションの履歴となる．また，ブロックはナンスと呼ばれる値を保持する．Bitcoin で用いられる PoW では，ブロックの生成はナンスを調整して，全体のハッシュ値がある閾値を下回るようなブロックを発見することと等しい．このブロック生成のプロセスをマイニングと言う．現在，ブロック生成間隔が 10 分になるように，ハッシュ値の閾値の逆数である難易度は調整されている．

しかし，同じ親ブロックから複数のブロックが生成され，ブロックチェーンが分岐することがある．この場合，ノードは，そのブロックまでの難易度の合計が最大であるブロックを先頭ブロックとし，先頭ブロックを含むブロックチェーンを正当なブロックチェーンとする．

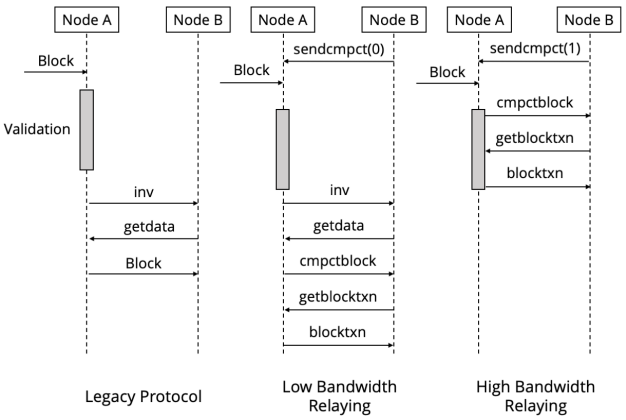

図 1　レガシープロトコルとコンパクトブロックリレーのブロック伝播のフロー．

Fig. 1　Block propagation flow in legacy protocol and compact block relay.

悪意のあるノードが過去のブロックで承認されたトランザクションを変更しようとした場合，現在の正当なブロックチェーンよりも難易度の合計が大きくなるまでブロックを生成しなければならない．よって，変更しようとしているトランザクションを承認したブロックと現在の先頭ブロックのブロック高（先祖ブロックの数）の差が大きいほど，トランザクションの変更は困難になる．

2.2 ブロック伝播

ノードはマイニングによってブロックを生成すると，隣接ノードにブロックを送信する．受信ノードはそのブロックを検証し，ブロックを伝播する．現在，Bitcoin のブロック伝播プロトコルは最初に実装されたレガシープロトコルと CBR がある．

レガシープロトコルでは，ノードはブロックに含まれるトランザクション全体を伝播する．そのため，伝播するデータのサイズは 1MB 近くになり，多くのネットワークリソースを必要とする [13]．一方，CBR はブロック伝播に必要な帯域幅を削減する．

図 1 にレガシープロトコルと CBR のブロック伝播のフローを示す．レガシープロトコルではブロックを受信し検証した後，ノード A はブロックのメタデータを含む `inv` メッセージをノード B に送る．ノード B はそのブロックをまだ受け取っていない場合，ノード A に `getdata` メッセージを送り，ブロック全体を要求する．`getdata` メッセージを受け取ったノード A はトランザクション全体を含むブロックをノード B に送信する．CBR では，トランザクション全体でなく，ブロックヘッダとトランザクションの ID のみを含むコンパクトブロックを送信する．ノード B はブロックの再構築に失敗した場合，つまり，メモリプールにブロックに含まれるトランザクションがなかった場合，ノード A に不足しているトランザクションを要求する．

CBR には low bandwidth relaying と high bandwidth relaying の 2 つのプロトコルがある．Low bandwidth relaying ではノード A が `inv` メッセージを送るのに対し，high bandwidth relaying ではノード A はブロックを受信するとブロックの検証が完了する前に，コンパクトブロックをノード B に送信する．

表 1　Bitcoin ネットワークのパラメータ．
Table 1　Parameter settings of bitcoin network.

ノード数	6000 (2015) or 9000 (2019)
ブロック生成間隔	10 分
ブロックサイズ	534 KB (2015) or 1.0 MB (2019)
ハッシュパワー	ガウス分布
次数分布	Miller ら [14] の測定結果
ノード分布	6 地域のノード分布
帯域幅	6 地域の帯域幅
ネットワーク遅延	6 地域間のネットワーク遅延

表 2　ネットワークパラメータの出典．
Table 2　Sources of network parameters.

	2015	2019
ノード分布	Bitnodes [15]	Bitnodes [15]
ネットワーク遅延	Verizon [16]	WonderNetwork [8]
帯域幅	testmy.net [9]	testmy.net [9]

3. ブロック伝播のシミュレーション

シミュレータを用いてブロック伝播遅延を測定した．実際のネットワークではなく，シミュレータを用いて測定した理由は以下の 3 点である．

- ノードを立ててネットワークを構築するよりもコストが低い．
- ノード数や帯域幅，ネットワーク遅延などのパラメータを簡単に変更できる．
- ブロック伝播遅延の短縮の要因それぞれ区別して評価できる．

Bitcoin ネットワークのシミュレーションにはブロックチェーンネットワークシミュレータ SimBlock [11] [12] を用いた．SimBlock はノード間のブロック伝播をシミュレートできるため，ブロック伝播遅延を測定できる．表 1 にシミュレーションで使用する Bitcoin ネットワークのパラメータを示す．

3.1　ネットワークパラメータの算出方法

2015 年のネットワークパラメータは [11] のパラメータを用い，2019 年のネットワークパラメータは新しく計算した．表 2 に 2015 年と 2019 年のネットワークパラメータの出典を示す．2019 年のネットワークパラメータの算出方法を以下に示す．

（1） ノード分布：Bitnodes [15] から各国のノード数のデータを取得した．SimBlock は 6 地域（北アメリカ，ヨーロッパ，南アメリカ，アジア，日本，オーストラリア）でノードの分布が表現されるため，ノード分布は各地域のノード数から算出した．

（2） ネットワーク遅延：各国の主要都市を一つ（アメリカのみ東西で 1 都市ずつ）選び，その都市間のネットワーク遅延を WonderNetwork [8] から取得した．ノード数による重みづけ平均を各地域間のネットワーク遅延とした．

（3） 帯域幅：各国の帯域幅を testmy.net [9] から取得した．ノード数による重みづけ平均を各地域の帯域幅とした．

3.2　コンパクトブロックリレーのモデル化

表 3 に CBR に関するパラメータを示す．Bitnodes から各ノードのプロトコルのバージョンを取得し，CBR を実装しているプロトコルを使用していれば，そのノードは CBR を使用しているとして，CBR を使用するノードの割合を算出した．

表 3　コンパクトブロックリレー（CBR）のパラメータ．
Table 3　Parameter settings of compact block relay (CBR).

CBR を使用するノードの割合	0.964
コンパクトブロックサイズ	18 KB
チャーンノードの割合	0.976
チャーンノードのブロック再構成失敗率	0.27
コントロールノードのブロック再構成失敗率	0.13

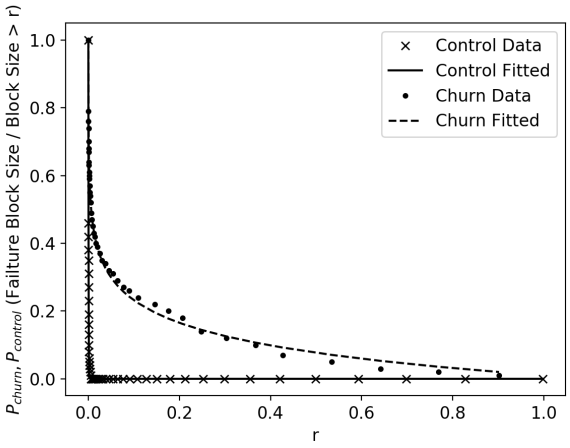

図 2　再構成失敗時に不足するトランザクションのデータサイズの累積分布．
Fig. 2　Cumulative distribution of the failure data size.

CBR を使用するノードは low bandwidth relaying を使用するとする．Imtiaz ら [17] によると，ネットワークに常に接続しているノード（コントロールノード）とネットワークへの参加・離脱を繰り返すノード（チャーンノード）ではブロックの再構成失敗率が異なる．コントロールノードとチャーンノードのブロック再構成失敗率は [17] の測定結果を用いた．また，コントロールノードとチャーンノードでは，ブロックの再構成失敗時に不足するトランザクションのデータサイズの分布も異なる．図 2 に再構成失敗時に不足するトランザクションのデータサイズの累積分布を示す．この累積分布は [17] で測定された再構成失敗時に不足するトランザクション数から算出した．累積分布の近似式を以下に示す．P_{churn} と $P_{control}$ は再構成失敗時に不足するトランザクションのデータサイズとブロックサイズの比がある割合 r よりも大きくなる確率を表す．

$$P_{churn} = e^{-2.12\times10^3 r} \quad (r \geq 0) \quad (1)$$

$$P_{control} = 1 - 0.0964\log(2.89\times10^4 r + 1) \quad (r \geq 0) \quad (2)$$

4. 実験結果と考察

ここでは，3 章のシミュレーションモデルを検証し，ブロック伝播遅延，フォーク率のシミュレーション結果について述べる．

表 4　Bitcoin ネットワークのブロック伝播遅延の 50 パーセンタイルと 90 パーセンタイルの実験値と実測値.
Table 4　50th and 90th percentile of block propagation delay in real networks and a simulation.

	2015	2019
50 パーセンタイルの実測値	7,988 ms	401 ms
50 パーセンタイルの実験値	9,673 ms	1,340 ms
90 パーセンタイルの実測値	16,835 ms	2,353 ms
90 パーセンタイルの実験値	14,056 ms	2,364 ms

4.1　モデルの検証

我々がシミュレーションで用いたモデルを実験的に検証するため，2015 年と 2019 年の実験値を実測値と比較する．2015 年の Bitcoin のシミュレーションでは，ノード数を 6000，ブロックサイズを 535KB とし，インターネットのネットワークパラメータは 2015 年のものを用いた．2019 年の Bitcoin のシミュレーションでは，ノード数を 9000，ブロックサイズを 1.0MB とし，インターネットのネットワークパラメータは 2019 年のものを用い，CBR も再現した．

表 4 にシミュレーションのブロック伝播の実験値と [3] で測定された実測値を示す．実測値は 2015 年 7 月と 2019 年 10 月の月間平均値である．

90 パーセンタイルは 2015 年と 2019 年ともに実験値は実測値と近い結果が得られた．しかし，50 パーセンタイルは実験値が実測値よりも大きいと言う結果が得られた．

これは，リレーネットワークの影響であると考えられる．リレーネットワークは，リレーサーバを介して効率よく参加ノードにブロックを伝播することができ，別地域であっても参加ノードはブロックを早く受け取ることができる．我々のシミュレーションでは，リレーネットワークのないランダムネットワークを想定していたため，リレーネットワークを利用するよりも 50% のノードへのブロック伝播にかかる時間が長くなる．一方で，リレーネットワークが存在するネットワークでも，リレーネットワーク非参加ノードへのブロック伝播はランダムネットワークである．よって，リレーネットワークはブロック生成ノードがリレーサーバを介してリレーネットワーク参加ノードに効率よく伝播するため，伝播遅延の 50 パーセンタイルは短縮する．一方，リレーネットワーク非参加ノードへの伝播はランダムネットワークであるため，リレーネットワークの参加率が多くない場合，90 パーセンタイルの短縮への影響は小さいと考えられる．実際，リレーネットワークの一つである Falcon の 2019 年 7 月 27 日の Bitcoin ノードに占める参加ノードの割合は 2.65% である [5].

このことから，90 パーセンタイルでは実験値と実測値が近い値であり，50 パーセンタイルでは実験値が実測値よりも大きな値になったというシミュレーション結果は，我々のモデルが CBR とインターネットの高速化を考慮した Bitcoin ネットワークをよく表現できていることが確認できた．

4.2　ブロック伝播遅延

ここでは，ブロック伝播遅延に対する CBR とインターネットの高速化の影響について述べる．実験では，CBR を使用しない 2015 年と 2019 年の Bitcoin ネットワークのシミュレーションと CBR を使用する 2015 年と 2019 年の Bitcoin ネットワークのシミュレーションを行った．ノード数を 9000，ブロックサイズを 1.0MB とする．

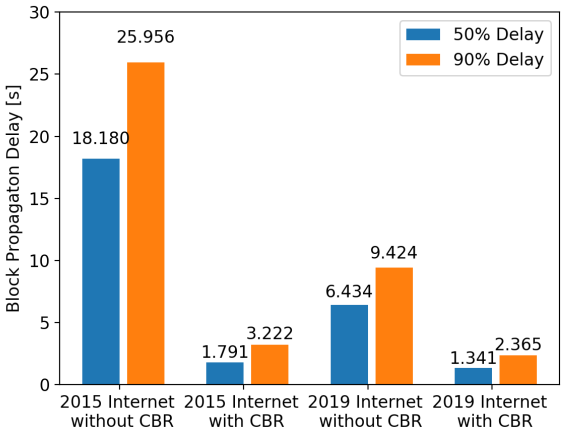

図 3　ブロック伝播遅延の 50 パーセンタイルと 90 パーセンタイルのシミュレーション結果.
Fig. 3　50th and 90th percentile of simulated block propagation delay.

図 3 にシミュレーションの実験結果を示す．CBR を使用しない 2015 年の Bitcoin ネットワーク（1 列目）と CBR を使用する 2015 年の Bitcoin ネットワーク（2 列目）のシミュレーション結果を比較すると，50 パーセンタイルは 90.1%，90 パーセンタイルは 87.6% 短縮した．また，CBR を使用しない 2015 年の Bitcoin ネットワーク（1 列目）と CBR を使用しない 2019 年の Bitcoin ネットワーク（3 列目）のシミュレーション結果を比較すると，50 パーセンタイル は 64.6%，90 パーセンタイルは 63.7% 短縮した．これらの結果から，CBR はインターネットの高速化よりもブロック伝播遅延の短縮に対する影響が大きい．

2015 年から 2019 年のインターネットの高速化では，ネットワーク遅延が平均 0.889 倍に短縮し，帯域幅は 2–3 倍大きくなった．一方，CBR によってブロックサイズはレガシープロトコルの 0.018 倍になった．伝播遅延の大半は帯域幅と送信するデータサイズの積が占めるため，CBR はブロック伝播遅延の短縮への影響が大きい．

さらに，CBR を使用する 2019 年の Bitcoin ネットワーク（4 列目）は CBR を使用する 2015 年の Bitcoin ネットワーク（2 列目）よりブロック遅延が短縮している．これは，CBR でブロックの再構築が失敗した場合，送信するデータサイズは依然として大きいため，インターネットの高速化により伝播遅延が短縮している．

4.3　フォーク率

フォーク率への影響も調査した．フォーク率は，生成されたブロック全体に対する正当なブロックチェーンに含まれないブロックの割合を表す．図 4 にフォーク率の測定結果を示す．

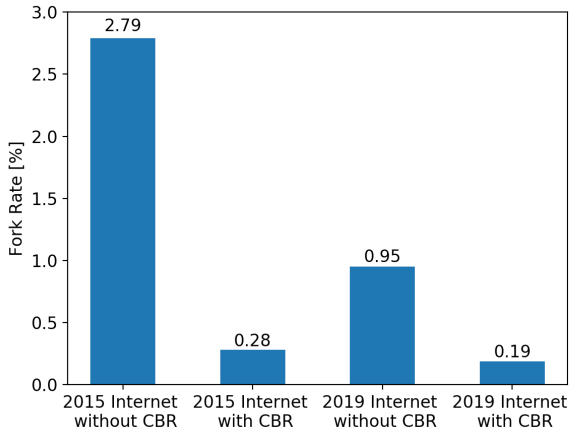

図 4　フォーク率のシミュレーション結果.
Fig. 4　Simulated fork rates.

フォーク率はブロック伝播遅延の短縮によって改善している．よって，Bitcoin ネットワークのセキュリティは 2015 年から 2019 年にかけて改善していることがわかる．

5. ま と め

本研究では，ブロック伝播遅延の短縮に対する CBR とインターネットの高速化の影響を調査した．実験結果から，CBR はインターネットの高速化よりもブロック伝播遅延の短縮に貢献していることかわかった．これは，CBR によるブロックサイズの圧縮率がインターネットの高速化によるネットワーク遅延の短縮率と帯域幅の増加率に比べて大きいためである．

さらに，2015 年と 2019 年の Bitcoin ネットワークのシミュレーションでは，ブロック伝播遅延の 90 パーセンタイルは実測値と近い値が得られたが，50 パーセンタイルは実測値よりも大きな値であった．これは，シミュレーションがランダムネットワークを想定していたためである．実際の Bitcoin ネットワークの一部はリレーネットワークである．

今後の課題は，SimBlock 上でリレーネットワークのトポロジやノードの振る舞いを再現することである．これによって，より実際の Bitcoin ネットワークに近いシミュレーションが可能になる．

謝辞　本研究は（公財）セコム科学技術振興財団 一般研究助成の支援を受けたものです．

文　献

[1] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash Sys-tem,” bitcoin.org, https://bitcoin.org/bitcoin.pdf.
[2] Y. Sompolinsky and A. Zohar, “Secure high-rate transaction processing in bitcoin,” in International Conference on Financial Cryptography and Data Security (FC 2015). Springer, 2015, pp. 507–527.
[3] “Bitcoin Network Monitor - DSN Research Group, KASTEL @ KIT,” https://dsn.tm.kit.edu/bitcoin/, Accessed: Nov. 1. 2019.
[4] T. Neudecker, “Security and Anonymity Aspects of the Network Layer of Permissionless Blockchains,” Ph.D. thesis, Karlsruhe Institute of Technology (KIT), 2018.
[5] “Falcon - a fast bitcoin backbone,” https://www.falcon-net.org/, Accessed: Jan. 27. 2019.
[6] “Fibre fast internet bitcoin relay engine,” https://www.bitcoinfibre.org/, Accessed: Jan. 27. 2019.
[7] M. Corallo, “Compact Block Relay (BIP 152),” https://github.com/bitcoin/bips/blob/master/bip-0152.mediawiki, Accessed: Nov. 10. 2019.
[8] “Global Ping Statistics - WonderNetwork,” https://wondernetwork.com/pings, Accessed: Oct. 20. 2019.
[9] “Top Countries for Bandwidth,” https://testmy.net/country, Accessed: Oct. 20. 2019.
[10] K. Otsuki, R. Banno, and K. Shudo, “Effects of a Simple Relay Network on the Bitcoin Network,” in Proc. 15th Asian Internet Engineering Conference (AINTEC 2019), August 2019.
[11] Y. Aoki, K. Otsuki, T. Kaneko, R. Banno, and K. Shudo, “SimBlock: A Blockchain Network Simulator,” in Proc. Workshop on Cryptocurrencies and Blockchains for Distributed Systems (CryBlock 2019, In conjunction with IEEE INFOCOM 2019), April 2019.
[12] R. Banno, and K. Shudo, “Simulating a Blockchain Network with SimBlock,” in Proc. IEEE International Conference on Blockchain and Cryptocurrency (ICBC 2019), May 2019.
[13] “Bitcoin Charts & Graphs - Blockchain,” https://www.blockchain.com/en/charts, Accessed: Oct. 10. 2019.
[14] A. Miller, J. Litton, A. Pachulski, N. Gupta, D. Levin, N. Spring, and B. Bhattacharjee, “Discovering bitcoins public topology and influential nodes,” 2015.
[15] “Bitnodes: Global Bitcoin Nodes Distribution,” https://bitnodes.earn.com/, Accessed: Oct. 20. 2019.
[16] “Verizon latency,” http://www.verizonenterprise.com/about/network/latency/, Not availble at Oct. 20. 2019.
[17] M. A. Imtiaz, D. Starobinski, A. Trachtenberg and N. Younis, “Churn in the Bitcoin Network: Characterization and Impact,” 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC 2019), 2019, pp. 431–439.