

Evaluating the Performance of Bitcoin Scaling Test Network

Akihiro Fujihara and Takaaki Yanagihara

Abstract Bitcoin Scaling Test Network (STN) は、ビットコインのスケーラビリティ問題を On-chain 技術で解決する為の実験ネットワークである。P2P ネットワーク上には常に大量の取引が送信されており、巨大ブロックを生成する実験が行われている。本研究では STN ノードを構築することで、取引処理の稼働率やブロックチェーンの分岐確率の推定を行った。その結果、推定稼働率は約 1.04、推定分岐確率 8.5% となった。更に OP_RETURN スクリプトを含む取引を 1 分に 1 回の高頻度で 1 週間の期間転送することで取引処理性能を実験的に評価した。その結果、取引が BC に取り込まれる確率は 98% となった。また取引が取り込まれるまでにかかる時間分布は長期的には冪分布に従う傾向を確認した。以上より、STN においても優先権付き待ち行列理論による考察が有効であると考えられる。(Tantative) Bitcoin Scaling Test Network (STN) is an experimental network to solve the scalability problem of Bitcoin by using on-chain technology. A large number of transactions are constantly sent over the P2P network, and miners generate huge blocks. In this study, we estimated the occupancy rate of transaction processing and the fork probability of the blockchain by constructing STN nodes. As a result, the estimated occupancy rate was about 1.04 and the estimated fork probability was 8.5%. In addition, we experimentally evaluated the transaction processing performance by transferring many transactions containing the OP_RETURN script once per minute for one week. As a result, the transaction processing probability was 98%, and the latency distribution for transaction processing tends to follow a power distribution in the long period. These results suggest that the priority queueing theory is also effective for STN.

Akihiro Fujihara

Chiba Institute of Technology, 2-17-1 Tsudanuma, Narashino, Chiba 275-0016, JAPAN, e-mail: akihiro.fujihara@p.chibakoudai.jp

Takaaki Yanagihara

Chiba Institute of Technology, 2-17-1 Tsudanuma, Narashino, Chiba 275-0016, JAPAN, e-mail: s1522313qq@s.chibakoudai.jp

1 Introduction

ビットコイン [1] は 2008 年に P2P 電子貨幣システムとして提案され、翌 2009 年 1 月 3 日に創始ブロックが生成されて以来、利用され続けている。Bitcoin の本質的に新しい利用価値は、取引にかかる手数料を極度に安くする事によって実現できる (1 円や 1 セント以下の) 超小額決済 (Micropayment) にある。このことによってインターネット上の様々なサービスの利用時に、ほぼ 0 に近い (人々が支払いを行ったことを気にしないレベルの) 課金を沢山のユーザから集めることによってサービス運営の為のコストを回収することが可能となる。つまり超小額決済は、これまでにない新しい分散型経済の仕組みを作ることができる潜在能力を持っている。

一方、ビットコインやブロックチェーン (BC) を用いたビジネスは新しい分散経済の仕組みを構築する方向には全く進化していない。Bitcoin Core (BTC) [2] は電子貨幣システムではなく、投機目的の価値の貯蔵システムと化してしまった。その背景には、現状のビットコインでは多数の超小額決済の実行が事実上困難であるという理由がある。

BTC のブロックサイズの上限は 1MB に決まっている。これより大きなサイズのブロックは不当なものとみなされ、マイナーに拒否されることになっている。またビットコインの平均ブロック生成時間は 10 分になるように難易度調整アルゴリズムによって制御されている。従って、平均 10 分に 1MB 以下のブロックに取り込めるだけの取引しか処理することができない。これは 1 秒あたり 5~7 取引しか処理できない計算になることが知られている。単純に平均ブロック生成時間を 10 分より短くしたり、ブロックサイズの上限を 1MB より大きくすれば、この問題が解決するように思われる。しかし、ブロックサイズを大きくすると、ブロックを P2P ネットワーク上の全ノードに転送して共有する過程により時間がかかってしまう。従って、平均ブロック生成時間を 10 分より長くしないとブロックが P2P ネットワーク全体に行き渡る前に別のブロックが生成される確率が上がる。従って、単純にブロックサイズを大きくしても BC の分岐を引き起こすことになる。分岐が起これば Proof of Work (PoW) を行ってブロックを生成するノードのハッシュレート (単位時間あたりにハッシュ関数の計算を実行できる回数) が二種類のブロックのものに分断されてしまい、将来的に排除されてしまうブロックの生成に大量のハッシュパワーをかけてしまうことにつながり、ネットワーク全体のブロック生成効率も下がる。逆に平均ブロック生成時間を 10 分よりも短くしても、そのうち BC の分岐が起こりやすくなり、同様の困難が生じる。これらの理由により、単位時間あたりの取引処理性能を向上することには技術的な困難がある。この技術的な課題のことをスケーラビリティ問題と呼ぶ。

ビットコインのスケーラビリティ問題を解決する方法も様々なものが提案されている [3]。その中でも Lightning network[4] のように、BC 外で多量の取引をまとめて実行し、その最終結果のみを BC に書き込むことで、ブロックに取り込む取引量を減らすことによってスケーラビリティ問題を回避する手法に注目が集まっている。このような解決手法は BC 以外の部分を工夫して困難を回避することから、Off-chain のスケーリング技術と呼ばれる。Off-chain 技術は一見良いように見えるが、個々の取引処理が BC に残らない。従って、Off-chain で処理した取引の改ざんが可能になってくる。また、BC を導入することで取

引の監査はブロック内の取引のみを確認すれば良い為、自動化が可能になるメリットがあったが、Off-chain 技術を適用すると、BC 外の取引のチェックが既存と同じく手動になってしまう為、BC のメリットを活かすことができなくなる。つまり Off-chain 技術はビットコインの元来の発想である、全取引を公開することで監査可能性を最大限に発揮する考え方に逆行している。

一方、ビットコインはダークネット・マーケットにおける違法な取引を行う手段として利用されてきた歴史がある。しかし、近年これらのマーケットの支配人や利用者が逮捕される事例が数多く報告されている [5, 6, 7]。これらの逮捕はビットコインが全取引を改ざん耐性を持たせて公開している為に、法的な証拠として利用可能であることに起因する。この観点から考えると、Off-chain 技術が普及するほど、政府等が追跡して監査することが不可能な取引が増えてしまい、ダークネット・マーケットのような違法な取引の取り締まりが難しくなったり、マネーロンダリングの温床となりうる。法と倫理とのバランスを考えた時、究極的には BC 上で全取引を処理する On-chain 技術によってスケーラビリティ問題を解決することが求められる。

また IoT や AI と BC を組み合わせることで多様なデータやプログラムを透明性の高い On-chain で統合管理する応用も期待されている [8]。IPFS などの分散ストレージ技術を使うことも可能ではあるが、On-chain 技術の発展によって取引処理性能が向上するほど、データやプログラムの扱い方の自由度が広がる側面もある。

On-chain でスケーラビリティ問題を解決する為には、BC が分岐しないようにうまく制御しながら平均ブロック生成時間を短くするか、ブロックサイズを大きくする必要がある。bloXroute[9] は、Blockchain Distribution Network (BDN) という名称の、より大きなブロックをより短時間で伝搬させることが可能なネットワーク層 (Layer 0) を P2P ネットワークに接続することで、スケーラビリティ問題を改善しようとする提案を行っている。

ブロックサイズを拡大する取り組みは Bitcoin SV (BSV) [10] のスケーリングテストネットワーク (Scaling Test Network, STN) で実験的な試みが行われている [11]。巨大ブロックを生成するために大量の取引を送信する負荷テストも行っている。上述の通り、BTC のブロックサイズの上限は 1MB であるのに対し、BSV ではブロックサイズの上限を撤廃した。そのことにより、24 時間あたりの平均取引処理数が 1,059 Transactions Per Second (TPS)、これまでに採掘された中で最も大きなブロックサイズは 2.9GB と報告されている (2021 年 2 月 9 日閲覧確認)。

本研究では STN のノードを構築することで、ブロックサイズの上限を撤廃した環境における取引処理に関するデータ分析や性能評価実験を行った結果について報告する。本研究の貢献を以下に示す。

- ・待ち行列理論を用いることで取引処理の稼働率の時間変化を調べた。その結果、推定稼働率は殆どの時間帯で 1 を超えていることが分かった。
- ・bitcoin-cli の機能を用いることで、BC の分岐確率の推定を行った。その結果、BTC では分岐確率が約 2% であることが計算されているが、BSV STN では約 8.5% に増加していることが分かった。このことから、P2P ネットワークのノード全体にブロックを転送する時間は約 53 秒となることも計算により推定できた。

- OP_RETURN スクリプトを含む取引を 1 分に 1 回の高頻度で転送した時に BC に取り込まれるまでにかかる時間を実測した．その結果，取引が BC に取り込まれる確率は 98% であり，その時間分布は冪分布に従うような傾向が確認できた．また優先権付き待ち行列の理論と矛盾しない $3/2$ の冪指数に従う傾向も確認できた．

2 Related Works

2.1 BC の分岐確率の計算

ビットコインのブロック生成時間は指数分布に従うことが知られている．

$$F(t) = P(T \leq t) = \int_0^t \lambda e^{-\lambda t'} dt' = 1 - e^{-\lambda t}. \quad (1)$$

ここでパラメータ λ は平均ブロック生成時間の逆数である．ビットコインの場合，平均ブロック生成時間は $1/\lambda = 10$ 分 = 600 秒と決まっている．

また BTC の P2P ネットワークの 90% のノードにブロックが拡散されるまでにかかる時間は $t = \tau_{fork} \doteq 12$ 秒であることが実測値として知られている [9]．あるブロックがネットワーク全体に拡散される前に，別のブロックが生成された時に BC が分岐してしまう．従って，ビットコインの BC が分岐する確率は以下のように計算できる．

$$\begin{aligned} F(\tau_{fork}) &= P(T \leq \tau_{fork}) = 1 - e^{-\lambda \tau_{fork}} = 1 - e^{-12/600} \\ &\doteq 0.02. \end{aligned} \quad (2)$$

以上より，BTC の BC の分岐確率は約 2% であることが分かる．

2.2 優先権付き待ち行列の理論

優先権の高い客に対して先にサービスを行う優先権付き待ち行列において稼働率 $0 < \rho \leq 1$ の時，優先権の低い客の待ち時間が冪指数 $3/2$ の冪分布に従い，その裾野が指数分布のカットオフを持つことが理論解析の結果から知られている [12]．

$$P(\tau) = \frac{A}{\tau^{3/2}} \exp(-\tau/\tau_0), \quad (3)$$

$$\tau_0 = \frac{1}{\mu(1 - \sqrt{\rho})^2}, \quad (4)$$

$$\rho = \lambda/\mu. \quad (5)$$

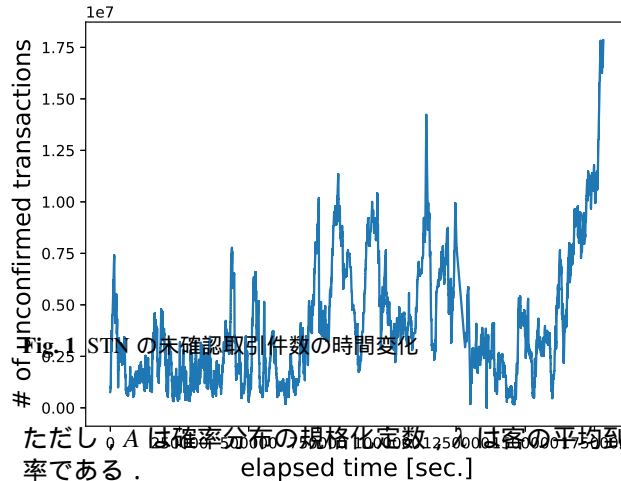


Fig. 1 STN の未確認取引件数の時間変化

ただし、 A は確率分布の規格化定数、 λ は客の平均到着率、 μ は平均サービス率である。

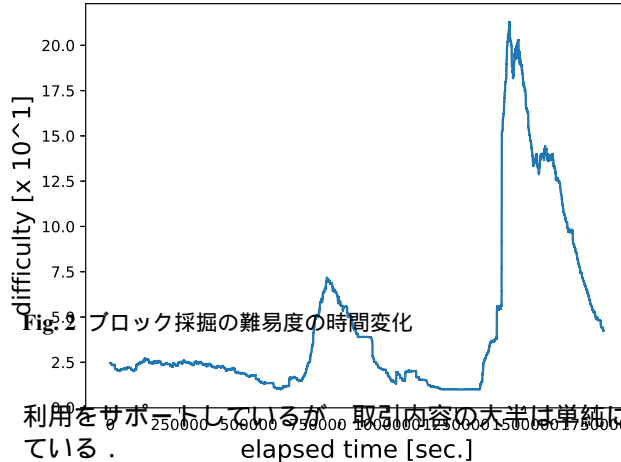
また稼働率が超臨界状態 $\rho > 1$ をとる時も同じ冪分布に従うことが報告されている。 $0 < \rho \leq 1$ の場合と異なる点は、 $1 - 1/\rho$ の割合で待ち時間が無限の（サービスを永遠に受けることができない）客が現れることである。

ビットコインにおける取引が BC に取り込まれるまでにかかる時間は取引手数料に依存した優先権付き待ち行列理論で説明できることが先行研究によって分かっている [13]。このことから、BSV STN においても取引が BC に取り込まれるまでにかかる時間分布も同様の性質を持つことが期待される。

3 Bitcoin Scaling Test Network

ビットコインのスケーラビリティ問題を On-chain 技術で解決する為の実験場として、BSV では RegTest, Testnet 以外の第 3 のテストネットとして STN が用意されている。Testnet では取引数が少ない為、ブロックサイズは小さい傾向にあるが、STN では巨大ブロックを作るために大量の取引が定期的に送信されている。STN の未確認 (=BC に取り込まれていない) 取引件数の時間変化を図 1 に示す。

ちなみにこの図を作成する元となったデータは whatsonchain [14] で報告されているものを収集して利用している。図 1 より、定常的に 1,000,000 以上の取引が Transaction pool に存在していることが分かる。また時々、取引数が 10,000,000 以上に達することも分かる。BSV では OP_RETURN スクリプトの



利用をサポートしているが、取引内容の大半は単純にアドレス間の送金になっている。

STNのネットワークは一般に公開されており、誰でもノードを構築してP2Pネットワークに参加することができる。ただしノード構築の為のシステム要求として、CPUは8~16コア、メモリは64GB(+64GB Swap)、ハードディスクは3TB以上、インターネット接続は上り下りとも1Gbit以上の性能が要求されている。BCの総容量は2021年2月9日時点で2.4TBとなっている。BSVのTestnetでは22GB、Mainnetでも284GB程度である為、比較するとBCの容量が非常に大きいことが分かる。またSTNのBCのブロック高は2021年2月9日時点で15,216となっており、小さい。これは過去にBCの再編成(=ブロック高を下げて再開)を何度か実施している為である。BSVのgithubの情報では2020年4月と11月にBCの再編成が行われたことが記録されている。

またシステム要求からも分かるが、STNはCPUによるブロック採掘が可能になっている。ブロック採掘の難易度の時間変化を図2に示す。難易度は1~数十の範囲で変化しており、容易に採掘が可能となっている。

STNでは最大ブロックサイズが10GBになるように設定することが推奨されている。またBitcoin scriptが使用可能なメモリの上限も2GBに設定することが推奨されている。これまでに採掘されたブロックのサイズ分布を調べた結果を図3に示す。STNのブロックサイズ分布は指数分布に従っているように見える。またこれまでに採掘された最大ブロックサイズは2.9GBになっている。一方、図3の下図はMainnetでのブロックサイズ分布になるが、興味深いことに指数分布よりも冪分布に従っているように見える。また冪指数の傾向からPareto-Zipf則(=冪指数2の冪分布)に従っているようにも見える。STNのコインには市場価値はないが、Mainnetでは市場価値を持つ。分布にこのような差が生まれる理由については、よく分かっていないが、市場価値を持つコインが入手できる場合、何らかの経済原理が働くことが影響していると考えられる。

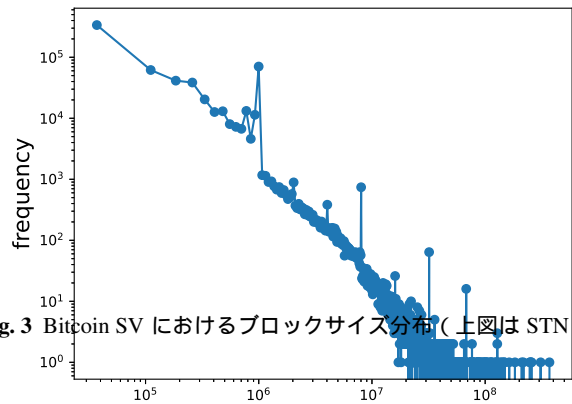
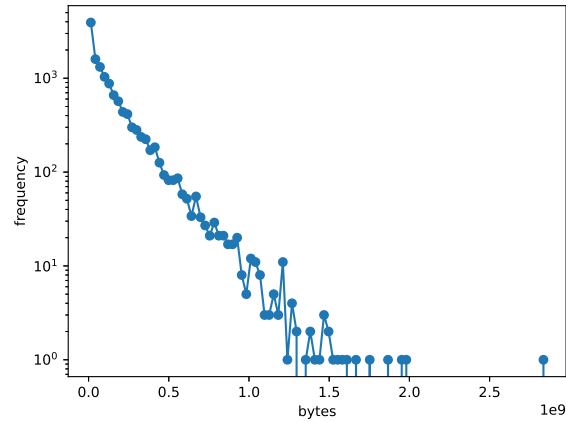


Fig. 3 Bitcoin SV におけるブロックサイズ分布 (上図は STN , 下図は Mainnet)

BSV は採掘者の評判を評価する観点から採掘したブロックに採掘者 ID を記録することを推奨している。この採掘者 ID を参考にしてブロック採掘頻度のランキングを計算した結果を図 4 に示す。こちらは STN と Mainnet の両方とも冪分布に従っていることが確認できる。

4 Performance Evaluation Experiments

https://github.com/cit-fujihalab/stn_experiments

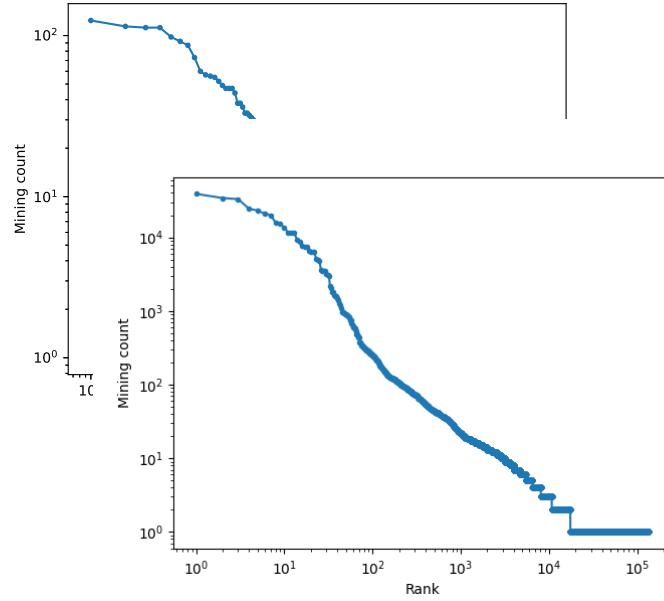


Fig. 4 採掘者 ID を参考にして計算したブロック採掘頻度ランキング（上図は STN，下図は Mainnet）

4.1 Experiment 1:

図 1 における未確認取引件数の時間変化から，STN の稼働率を推定した．待ち行列理論に基づいて，STN の推定稼働率 $\bar{\rho}$ の時間変化を計算した結果を図 5 に示す．推定稼働率は殆どの時間帯で 1 を超えていることが分かる．この結果は BC に取り込まれない取引が存在することを示唆している．また 2020 年 11 月 4 日～2021 年 2 月 9 日までのデータを用いて推定稼働率の時間平均を取ると $\bar{\rho} \doteq 1.04$ となった．この結果より， $1 - 1/\bar{\rho} \doteq 0.0387$ の確率で BC に取り込まれない取引が出現していると考えられる．

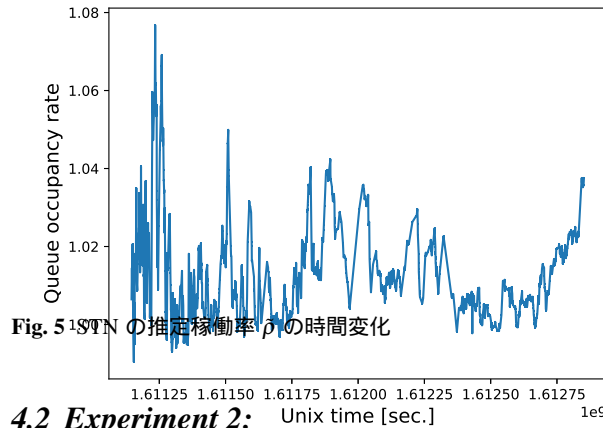


Fig. 5 STN の推定移動率 ρ の時間変化

4.2 Experiment 2:

STN のノードを構築して P2P ネットワークに接続すると分かるが、大きなブロックが生成されたと思われるタイミングで BC の大きな分岐が起きて Safe mode となり、bitcoin-cli コマンドを使って送金ができなくなることがある。また一度大きな分岐が起こると解消までに半日近くかかる場合もある。そこで bitcoin-cli getinfo の errors の値を取得することで分岐が起きている時間から分岐確率を推定する実験を行った。

2020 年 11 月 4 日～2021 年 1 月 13 日の期間において、10 秒に 1 回の頻度で errors の値を収集した（合計 594,880 回）。また BC が分岐している警告が出た回数を数えた。その結果、以下の 2 種類の警告が出た。

- Warning: The network does not appear to fully agree! We received headers of a large fork. Still waiting for block data for more details. (出現頻度は 32,724 回、全体に占める割合は約 5.5%)
- Warning: The network does not appear to fully agree! Some miners appear to be experiencing issues. A large valid fork has been detected. (出現頻度は 17,782 回、全体に占める割合は約 3%)

以上の結果より、分岐確率は約 $(5.5 + 3) = 8.5\%$ と推定することができる。これは BTC の約 2% の 4 倍超であることが分かる。ちなみに同じ手法で BSV Mainnet の分岐確率を評価すると 0% となった。また、式 (1) において $F(t) = 0.085$ と $\lambda = 1/600$ を代入した時、 $t = \tau_{fork} \doteq 53$ 秒となることから、STN における平均ブロック転送時間は約 53 秒になっていると推定することができる。

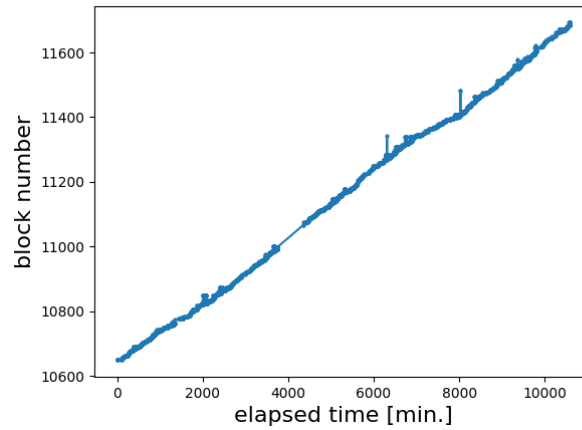


Fig. 6 経過時間と取引が取り込まれたブロック番号の対応関係

4.3 Experiment 3:

常に沢山の取引が Transaction pool にある状態で、取引が BC に取り込まれるまでにどの程度の時間がかかるかを実験により性能評価した。実験期間を 2021 年 1 月 7 ~ 14 日の 1 週間に設定し、期間中に分岐による取引送信ができない場合を除いて常に 1 分に 1 回の頻度で、前の 1 分間に Flightradar24 [15] の ADS-B データの収集ノードから千葉工業大学のある津田沼周辺を飛行する民間航空機の位置情報を収集し、OP_RETURN スクリプトとしてデータを含めた取引の送信を行った。1 取引あたりのサイズは 63KB 未満になるようにした。また取引手数料は 0.001BSV に固定した。ちなみに BSV の取引手数料は 1 satoshi/byte 以上となっている。昼間は民間航空機が多く飛行する為、取引データのサイズが大きくなるが、夜間は殆ど飛行がない為、書き込むデータが無かった場合は取引の送信は行わなかった。実験結果に関するその他の詳細情報は Github (https://github.com/cit-fujihalab/stn_experiments) に掲載した。

実験期間の経過時間と取引が取り込まれたブロック番号の対応関係を図 6 に示す。経過時間と共に取引が定期的にブロックに取り込まれていることが確認できる。一方、たまになかなか BC に取り込まれない取引があることも確認できる。

実験期間中に合計 6,828 取引を送信したが、そのうち 104 取引は BC に取り込まれなかった。このことより、取引が BC に取り込まれない確率が $(104/6828 \approx 0.02)$ と計算できる。この結果は??節で計算した $1 - 1/\bar{\rho} \approx 0.0387$ の確率で BC に取り込まれない取引が出現していると推定した結果とほぼ同じ値になっていることが確認できる。

次に取引送信から BC に取り込まれるまでにかかる時間のヒストグラムを図 7 に示す。ブロック生成時間分布が指数分布に従うことから、半日程度の短期間では BC に取り込まれる時間は指数分布に従うが、1 週間程度の長期間になると指数分布から外れてくる。実際に図 7 のとおり両対数プロットで直線的な

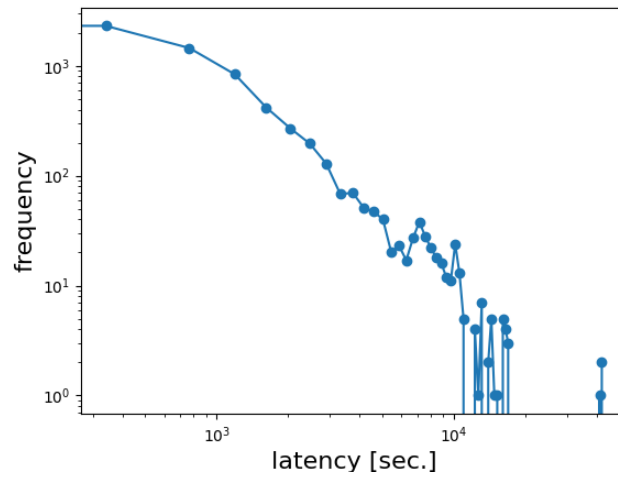


Fig. 7 取引送

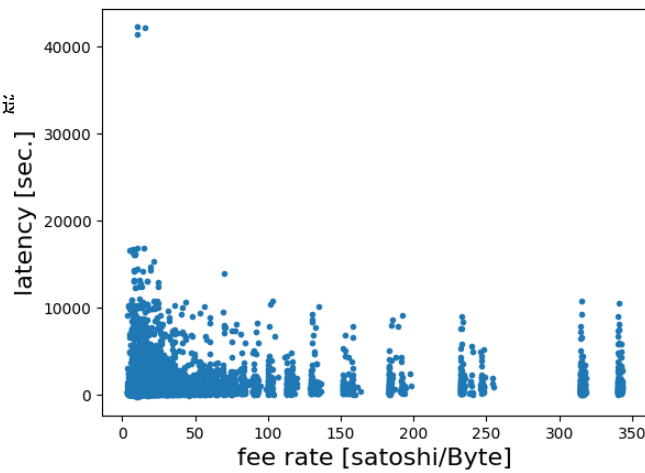


Fig. 8 取引サイズに対する取引手数料の割合と取引が BC に取り込まれるまでにかかった時間の関係

傾向が現れる為、冪分布に従う傾向が現れていることが確認できる。また冪指数を両対数プロットの傾きから見積もると $3/2$ に近いことが分かる。これらの結果は優先権付き待ち行列の理論解析結果と矛盾しない。このことから手数料の低い取引が優先度が低くなり、BC に取り込まれるまでに時間がかかっていることが予想される。

取引サイズに対する取引手数料の割合と取引が BC に取り込まれるまでにかかった時間の関係を図 8 に示す。割合 (fee rate) が低いと BC に取引が取り込ま

れるまでに時間がかかっていることが分かる．このことから STN においても優先権付き待ち行列理論による考察は有効であると考えられる．

5 Discussion

6 Conclusion

本研究では Bitcoin STN のノードを構築し，ブロックサイズの上限を撤廃した環境における取引処理に関するデータ分析や性能評価実験を行った．取引処理の稼働率の時間変化を調べた結果，推定稼働率は殆どの時間帯において 1 を超えていることが分かった．bitcoin-cli の機能を用いて BC の分岐確率の推定も行った結果，STN では約 8.5% となり，BTC の 4 倍超の確率となっていることが分かった．また P2P ネットワークの平均ブロック転送時間も約 53 秒と推定できた．OP_RETURN スクリプトを含む取引を 1 分に 1 回の高頻度で 1 週間の期間，転送することで取引処理性能を実験的に評価した．その結果，取引が BC に取り込まれる確率は 98% であり，その時間分布は長期的には冪分布に従うような傾向が確認できた．また優先権付き待ち行列の理論と矛盾しない $3/2$ の冪指数に従う傾向も確認できた．このことから STN においても優先権付き待ち行列理論による考察は有効であると言える．

今後の課題としては，より大量な数の取引を長期間に渡って送信し続けた時の処理性能について確認することが挙げられる．

Acknowledgements This work was partially supported by the Japan Society for the Promotion of Science (JSPS) through KAKENHI (Grants-in-Aid for Scientific Research) Grant Numbers 17H01742 and 20K11797.

References

1. S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System” (White paper), 2008 <https://bitcoin.org/bitcoin.pdf> <https://craigwright.net/bitcoin-white-paper.pdf> (2021 年 2 月 9 日閲覧確認)
2. Bitcoin Core <https://github.com/bitcoin/bitcoin> (2021 年 2 月 9 日閲覧確認)
3. Q. Zhou, *et al.*, “Solutions to Scalability of Blockchain: A Survey” IEEE Access, Vol. 8, pp.16440-16455, IEEE, 2020.
4. J. Poon and T. Dryja, “The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments,” (2016) <https://lightning.network/lightning-network-paper.pdf> (2021 年 2 月 9 日閲覧確認)
5. FBI, “Manhattan U.S. Attorney Announces Seizure of Additional \$28 Million Worth of Bitcoins Belonging to Ross William Ulbricht, Alleged Owner and Operator of “Silk Road” Website,” 2013. <https://archives.fbi.gov/archives/newyork/press-releases/2013/manhattan-u.s.-attorney-announces-seizure-of-additional-28-million>

- n-worth-of-bitcoins-belonging-to-ross-william-ulbricht-alleged-owner-and-operator-of-silk-road-website (2021 年 2 月 9 日閲覧確認)
6. The US Department of Justice, "AlphaBay, the Largest Online 'Dark Market,' Shut Down," 2017. <https://www.justice.gov/opa/pr/alphabay-largest-online-dark-market-shut-down> (2021 年 2 月 9 日閲覧確認)
 7. The US Department of Justice, "South Korean National and Hundreds of Others Charged Worldwide in the Takedown of the Largest Darknet Child Pornography Website, Which was Funded by Bitcoin," 2019. <https://www.justice.gov/opa/pr/south-korean-national-and-hundreds-others-charged-worldwide-takedown-largest-darknet-child> (2021 年 2 月 9 日閲覧確認)
 8. K. Salah, M. Habib Ur Rehman, N. Nizamuddin, and A. Al-Fuqaha, "Blockchain for AI: Review and Open Research Challenges" IEEE Access, Vol. 7, pp.10127-10149, 2019.
 9. U. Klarman, *et al.*, "bloXroute: A Scalable Trustless Blockchain Distribution Network" (White paper), 2018. <https://bloxroute.com/wp-content/uploads/2018/03/bloXroute-whitepaper.pdf> (2021 年 2 月 9 日閲覧確認)
 10. Bitcoin SV (Satoshi Vision) <https://github.com/bitcoin-sv/bitcoin-sv> (2021 年 2 月 9 日閲覧確認)
 11. Bitcoin Scaling Test Network <https://bitcoinscaling.io/> (2021 年 2 月 9 日閲覧確認)
 12. J. G. Oliveira and A.-L. Barabási, "Darwin and Einstein correspondence patterns," Nature 437, 1251, 2005.
 13. S. Kasahara and J. Kawahara, "Effect of Bitcoin fee on transaction-confirmation process," Journal of Industrial and Management Optimization, 15 (1): 365-386, 2019.
 14. WhatsOnChain.com, BSV Explorer - STN, <https://stn.whatsonchain.com/> (2021 年 2 月 9 日閲覧確認)
 15. Flight Tracker — Flightradar24 — Track Planes in Real-time, <https://www.flightradar24.com/> (2021 年 2 月 9 日閲覧確認)