Journal of Convergence for Information Technology
Vol. 10. No. 10, pp. 65-70, 2020
e-ISSN 2586-4440
DOI : https://doi.org/10.22156/CS4SMB.2020.10.10.065

Data Volume based Trust Metric for Blockchain Networks

Seung Hyun Jeon
Researcher, School of Electrical Engineering, Korea Advanced Institute of Science and Technology

블록체인 망을 위한 데이터 볼륨 기반 신뢰 메트릭

전승현
한국과학기술원 전기및전자공학부 박사후연구원

Abstract With the appearance of Bitcoin that builds peer-to-peer networks for transaction of digital content and issuance of cryptocurrency, lots of blockchain networks have been developed to improve transaction performance. Recently, Joseph Lubin discussed Decentralization Transaction per Second (DTPS) against alleviating the value of biased TPS. However, this Lubin's trust model did not enough consider a security issue in scalability trilemma. Accordingly, we proposed a trust metric based on blockchain size, stale block rate, and average block size, using a sigmoid function and convex optimization. Via numerical analysis, we presented the optimal blockchain size of popular blockchain networks and then compared the proposed trust metric with the Lubin's trust model. Besides, Bitcoin based blockchain networks such as Litecoin were superior to Ethereum for trust satisfaction and data volume.

Key Words : DTPS, Trust Metric, Blockchain Size, Stale Block Rate, Average Block Size, Convex Optimization

요 약 Peer-to-Peer 망에서 디지털 콘텐츠를 거래와 암호화폐를 발행할 수 있는 신뢰망인 비트코인이 출현된 후, 거래 성능을 향상시키기 위해 많은 블록체인이 개발되었다. Joseph Lubin이 이런 Transaction Per Second (TPS) 만 강조한 블록체인 망에 탈중앙화 지수라는 개념을 최근 보완하여 Decentralization TPS (DTPS)를 제안하였지만, TPS에 대한 가중치가 여전히 크고 확장 트릴레마 중 하나인 보안 이슈를 충분히 고려하지 않았다. 본 논문은 블록체인 크기, 고아 블록률과 평균 블록 크기를 고려하여 새로운 신뢰 메트릭을 제안하고, 시그모이드 함수 및 최적화 기법으로 블록체인 망의 만족도를 극대화하기 위한 최적의 블록체인 크기를 제시했다. 인기 있는 블록체인 망들과 비교하여 기존 Lubin의 신뢰 모델보다 향상된 성능을 보였으며, 비트코인 계열의 블록체인 망이 이더리움 보다 나은 최적의 데이터 볼륨과 신뢰 만족도를 제공했다.

주제어 : 탈중앙화 TPS, 신뢰 메트릭, 블록체인 크기, 고아 블록률, 평균 블록 크기, 최적화

1. Introduction

With the advent of Bitcoin (BTC) on trading digital content between peers and storing distributed ledgers, a blockchain has been raising much interest as reliable overlay networks. However, as Vitalik Buterin first mentioned the scalability trilemma, the scalability in blockchain networks is still challenging[1]. The scalability trilemma, which consists of decentralization, security, and scalability, has the trade-off relationships among properties. After Vitalik Buterin first

*Corresponding Author : Seung Hyun Jeon(creemur@kaist.ac.kr)
Received August 31, 2020
Revised September 20, 2020
Accepted October 20, 2020
Published October 28, 2020

proposed Ethereum (ETC) with the concept of smart contract, most blockchain developers have struggled for improving the transaction performance, compared with Visa.

However, according to increasing the number of transactions such as BTC and ETC, adopting blockchain applications in real world is still difficult[2]. Generally, if transactions increase, volume of blockchain networks becomes large (e.g. blockchain size of BTC is around 300 GB). This blockchain scalability problem is not limited on BTC.

In order to discuss the scalability issue in blockchain networks, Joseph Lubin first proposed the concept of Decentralization Quotient (DQ), and he then emphasized decentralization more intensely than scalability in scalability trilemma. Even though literature on blockchain scalability and reliability has been primarily discussed in Section 2, a few studies on metrics has been worked to evaluate whether blockchain networks are enough trustworthy, according to huge blockchain data volume from increasing transactions

In this paper, we investigate a new trust metric that evaluate a blockchain network based on three properties of scalability trilemma. In detail, we propose a satisfaction function considering blockchain size, stale block rate (i.e. the ratio of blocks not included in the longest chain[3] as unapproved transaction), and average block size, involved with the DQ and performance of the existing Lubin's trust model. According to convex optimization and a sigmoid function we present the optimal blockchain size for popular blockchain networks. Therefore, we improve the Lubin's trust model in security and other data volume's manners.

2. Literature on Blockchain Scalability and Reliability

2.1 Scalability Trilemma

In fact, the scalability issue at the infancy of blockchain networks has not been discussed. EOS (referred as Everyone's Open Society from CEO of black.one, Brendan Blumer) with Delegated Proof of Stake (DPoS) as a consensus algorithm magnified the performance of the blockchain network due to having weighted transaction scalability[4]. EOS's transaction speed is 4,000 Transaction per Second (TPS)[5]. At the design to maximize transaction throughput, EOS did not consider unprocessed transaction[6]. Accordingly, EOS is doubtful that bots produce transactions about 75% of EOS Decentralized applications (Dapps)[7]. This means that EOS is not enough reliable as security in scalability trilemma. Essentially, since three properties of scalability trilemma have trade-off relationships, no blockchain network can satisfy all of the properties.

As already mentioned, trusting blockchain networks can guarantee to maximize all properties' gains the scalability trilemma. Lubin's trust model only considers decentralization and scalability.

Through previous studies, all transactions are stored in storage on blockchain networks. Surely, some stale blocks with unprocessed transactions continuously spend huge data storage. Increasing stale blocks involve the possibility of potential attacks[3,8]. Moreover, authors mention stale block rate is a security indicator of the blockchain network[9].

Moreover, If the limited block size is enlarged, blockchain scalability is helpful for fast transaction[3]. However, the bigger block may cause other security issues. Even though the block size is set to 4 MB given 10 minute block interval, the transaction performance was

improved till 27 TPS[10]. Hence, increasing the block size is good for scalability but can be not good for security.

2.2 Measurement of Satisfaction

The comparison of satisfaction is more relative than an absolute thing. In order to measure satisfaction, an utility function primarily is used traditionally. Authors used a logarithmic function for satisfaction of power allocation [11]. To obtain non-negative value in y axis, 1 in the log function is added.

As an another approach, a logistic function for measuring satisfaction can be used. The sigmoid function is a representative among logistic functions. Authors considered the sigmoid function for QoS satisfaction of time slot assignment[12]. Generally, the sigmoid function has often been utilized to classification and regression in machine learning. However, we consider it as a satisfaction function for increasing blockchain sizes.

3. System Model

3.1 Lubin's Trust Model

Joseph Lubin first mentions the concept of DQ and Decentralization TPS (DTPS) at the 2019 Deconomy Conference in Seoul[3]. DQ is a parameter which ranges from centralization (0) to decentralization (1). DTPS is a DQ parameter multiplied by TPS, which presents the performance on transaction of the blockchain. Table 1 shows measurement of DTPS in blockchain networks. DQ of dogecoin (DOGE) is anticipated at 0.5, because DOGE and litecoin (LTC) use the same script based cryptographic program for faster mining than BTC[13]. Hence, DTPS of DOGE can be calculated at 16.5[14]. Additionally, since DQ is defined as 0.1, EOS's DTPS is 400, as mentioned in Section 2.

Table 1. The existing Lubin's Trust Model for Blockchain Networks

Items	DQ	TPS	DTPS
BTC	0.8	7	5.6
ETH	0.7	15	10.5
LTC	0.5	56	28
DOGE	0.5	33	16.5

3.2 Proposed Trust Metric for a Blockchain Size

We assume a simple utility of satisfaction for a blockchain size as an application based data traffic model. We propose a trust metric for increasing the blockchain size (x), based on the sigmoid function[12] as follows:

$$U(x) = I_{DTPS}\sigma(\alpha x) - \frac{r_s}{s_b} \times \alpha x, \qquad (1)$$

where I_{DTPS} is a DTPS parameter, α is a scale-down factor. r_s and s_b are stale block rate (%) and average block size (KB), respectively[3]. $\sigma(\alpha x)$ is a satisfaction function for increasing blockchain size (x). Since I_{DTPS} has large priority for TPS, the added sigmoid function can be more balanced. Here, stale block rate is unsatisfactory due to spending storage as the thrown block for transaction. Moreover, according to increasing average block size, the amount of transaction per block is also increased. If the average block size is increased, the stale block rate can be alleviated. Here, $I_{DTPS}(\alpha x) < I_{DTPS}$, because $0 \le I_{DTPS} \le 1$ and $0 < \sigma(\alpha x) \le 1$. Considering the second term of (1) that is an unsatisfactory function for security risk, $U(x)$ is always less than I_{DTPS}.

Based on (1), we can define an optimization problem[15] relating to blockchain size as follows:

$$x^* = \underset{x>0}{\arg max}\, U(x), \qquad (2)$$

where $U(x)$ has a convex set[15] due to the

following reasons: when $x > 0$, 1st and 2nd terms of (1) are concave and affine, respectively.

For maximizing the trust metric of (1), the derivative of $U(x)$ is defined as followings:

$$\frac{\partial U(x)}{\partial x} = I_{DTPS}\frac{\partial}{\partial x}\left(\frac{e^{\alpha x}}{e^{\alpha x}+1}\right) - \frac{\alpha r_s}{s_b} = 0, \quad (3)$$

where assuming $e^{\alpha x} = t$, we can replace (3) with the following quadratic equation for t:

$$r_s t^2 + (2r_s - I_{DTPS}s_b)t + r_s = 0, \quad (4)$$

where $t > 0$ because $x > 0$. Here, the value of t is calculated by the followings:

$$t = \frac{\sqrt{(2r_s - I_{DTPS}s_b)^2 - 4(r_s)^2}}{2r_s} - \frac{2r_s - I_{DTPS}s_b}{2r_s}. \quad (5)$$

Hence, the optimal blockchain size (x^*, GB) is defined from t of (5):

$$x^* = \frac{1}{\alpha}ln(t). \quad (6)$$

4. Numerical Results

In this section, we present numerical analysis on the proposed trust metric for blockchain networks and compare the proposed trust metric with the Lubin's trust model. Here, we cannot include EOS blockchain in the proposed trust metric because current blockchain size, stale block rate, etc do not find proper references.

We consider the major parameters for analysis are referred as DTPS in Table 1, stale block rate/average block size[3], current blockchain size and expected range of x[16]. α as a slope factor for satisfaction is set to 0.015.

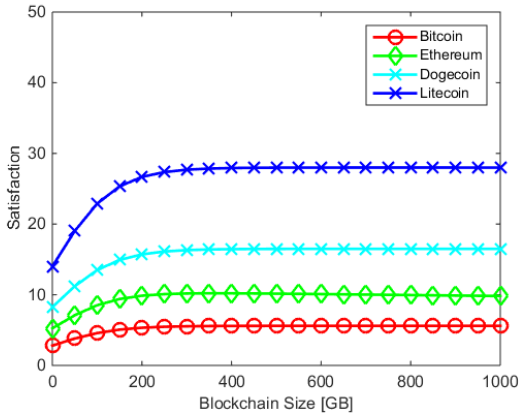

Fig. 1. Comparison among blockchain networks.

Fig. 1 shows the proposed trust metric according to increasing a blockchain size among blockchain networks. BTC and ETH show quite low satisfaction. However, DOGE and LTC present higher satisfaction than BTC and ETH. This means the output of Table 1 is similar to the proposed trust model, even though measured values are different in Fig. 1 as follows: LTC 〉 DOGE 〉 ETH 〉 BTC.

However, when we find the optimal blockchain size of each blockchain network like Fig. 2, we can obtain the information on which blockchain network is more trustworthy.

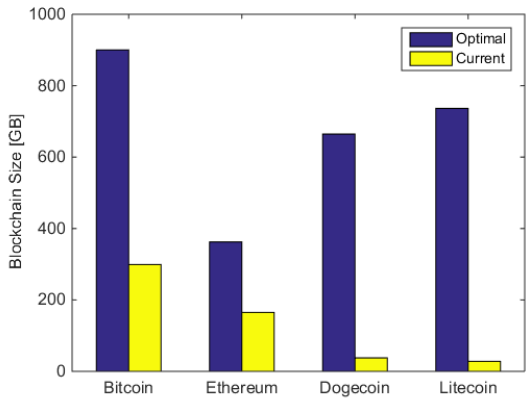

Fig. 2. The optimal and current blockchain sizes for blockchain networks.

Fig. 2 compares the optimal blockchain size of the proposed trust metric with the current blockchain size in blockchain networks. Here, the current blockchain size is brought from blockchair.com[16]. At this moment, volume on these blockchain networks still increases. According to considering the current blockchain size, ETH increases nearest to the optimal blockchain volume. However, LTC farthest to the optimal blockchain volume still remains at roughly 708 GB. Besides, BTC has the optimal (largest) blockchain data volume among other blockchain networks. Hence, the remaining storage considering the optimal blockchain size is shown as the following order: LTC 〉 DOGE 〉 BTC 〉 ETH.

Fig. 3 compares the proposed trust metric with the conventional Lubin's trust model. Due to the characteristic of the sigmoid function in (1), the proposed trust metric is less than I_{DTPS}. Nevertheless, satisfaction of ETH is slightly reduced by the higher stale block rate (i.e. 6.8 %) than that of other blockchain networks.

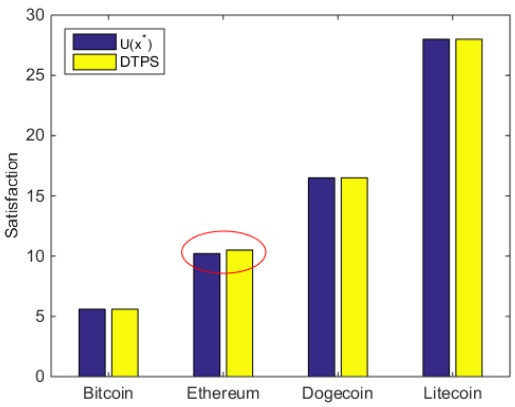

Fig. 3. Comparison between the proposed trust metric and the existing Lubin's trust model.

5. Conclusion

We propose a trust metric for blockchain networks, which consider a blockchain size, stale block rate, and average block size based on the sigmoid function. Through analyzing the proposed utility by the convex optimization, we compare the optimal blockchain size with the current blockchain volume for popular blockchain networks. Hence, the proposed trust metric is more improved than the existing Lubin's trust model for choosing trustworthy blockchain networks.

Obtaining more accurate trust metric as further works will become a challenging issues on comparing three properties for blockchain scalability fairly, even though weights of decentralization and security are reduced for scalability.

REFERENCES

[1] A. Hafid, A. S. Hafid & M. Samih (2020). Scaling Blockchains: A Comprehensive Survey. *IEEE Access, 8*, 125244-125262. DOI : 10.1109/ACCESS.2020.3007251

[2] A. Chauhan, O. P. Malviya, M. Verma & T. S. Mor (2018, July). Blockchain and scalability. In *2018 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C)* (pp. 122-128). New York : IEEE. DOI : 10.1109/QRS-C.2018.00034

[3] A. Gervais, G. O. Karame, K. Wüst, V. Glykantzis, H. Ritzdorf & S. Čapkun. (2016, October). On the security and performance of Proof of Work blockchains. *23rd ACM Conference on Computer and Communications Security,* (pp. 3-16). New York : ACM. DOI : 10.1145/2976749.2978341

[4] LiquidApps (Apr. 4, 2019). *Medium.* EOS + DAPP Network: How This Is The Key To Scalable Applications. (Online). https://medium.com/

[5] J. Lubin (Apr. 6, 2019). *Decrypt.* An Overview of the State of the Blockchain Ecosystem. (Online). https://decrypt.co/

[6] B. Xu, D. Luthra, Z. Cole & N. Blakely (2018). *EOS: An architectural, performance, and economic analysis.* Retrieved June, 11, 2019.

[7] D. Kuhn (2014). *Study: 75% of EOS Dapp*

Transactions Are Now Made By Bots. EOS: (Online). https://www.coindesk.com/

[8] N. Kannengießer, S. Lins, T. Dehling & A. Sunyaev. (2020). Trade-offs between distributed ledger technology characteristics. *ACM Computing Surveys (CSUR), 53(2)*, 1-37. DOI : 10.1145/3379463

[9] M. Alharby & A. van Moorsel (2020). Blocksim: An extensible simulation tool for blockchain systems. *arXiv preprint arXiv*:2004.13438.

[10] K. Croman et. al. (2016, February). On scaling decentralized blockchains. In *International conference on financial cryptography and data security* (pp. 106-125). Springer, Berlin, Heidelberg.

[11] S. H. Jeon, J. Lee & J. K. Choi. (2017). Energy outage-aware power distribution scheme for off-grid base station operation. *IEEE Communications Letters, 21(6)*, 1401-1404. DOI : 10.1109/LCOMM.2017.2676108

[12] J. S. Lee, Y. Yoo, H. S. Choi, T. Kim & J. K. Choi. (2019). Energy-Efficient TDMA Scheduling for UVS Tactical MANET. *IEEE Communications Letters, 23(11),* 62126-2129. DOI : 10.1109/LCOMM.2019.2936472

[13] D. Gilbert. (Dec. 20, 2013). *International Business Times*. What is Dogecoin? The Meme that Became the Hot New Virtual Currency(Online). https://www.ibtimes.co.uk/

[14] JcollinsVect (Apr. 20, 2018). *reddit*. Transactions Per Second (TPS)? (Online). www.reddit.com

[15] S. Boyd & L. Vandenberghe. (2004). *Convex Optimization*. Cambridge : Cambridge Univ. Press.

[16] N. Zhavoronkov (Sept. 13, 2020). *blockchair explorer*. blockchair. (online). blockchair.com

전 승 현(Seung Hyun Jeon) [정회원]

· 2009년 8월 : 한국과학기술원 정보통신공학과 졸업(공학석사)
· 2017년 2월 : 한국과학기술원 전기및전자공학부 졸업(공학박사)
· 2017년 3월 ~ 현재 : 한국과학기술원 전기및전자공학부 박사후 연구원

· 관심분야 : 최적화, 캐싱, 에너지 소모 모델, 분산망
· E-Mail : creemur@kaist.ac.kr