proceedings

MDPI

Proceedings

Optimal Transaction Throughput in Proof-of-Work Based Blockchain Networks †

B. Swaroopa Reddy * and G. V. V. Sharma *

Department of Electrical Engineering, Indian Institute of Technology Hyderabad, Telangana 502285, India

* Correspondence: ee17resch11004@iith.ac.in (B.S.R.); gadepall@iith.ac.in (G.V.V.S.)

† Presented at the 3rd annual Decentralized Conference, Athens, Greece, 30 October–1 November 2019.

Published: 22 October 2019

Abstract: As of today, Bitcoin suffers with restrictive transaction throughput of 3–7 transactions per sec and the transaction confirmation takes several min as bitcoin blockchain was designed with a block creation time of 10 min and each block is restricted with less blocksize for fast transmission. In this paper, we obtained the optimal transaction throughput for a Proof-of-Work (PoW) based longest chain rule blockchain network (called bitcoin protocol). This is done by modeling the delay diameter (D) and double spending attack in a Erdös-Rényi random network topology as constraints. Through numerical results, it is shown that the throughput can be significatly improved without compromising the fairness of the network.

Keywords: block creation rate; delay diameter; probability of successful double-spend; throughput; rewards

1. Introduction

Blockchain was introduced by Satoshi Nakamoto as a peer-to-peer network for cryptocurrencies like bitcoin [1]. It has also found application in smart contract based decentralized applications (DApp) like medical records [2] and IoT applications [3].

Blockchain involves creation of blocks by solving a computationally hard problem called Proof-of-Work (PoW) and validation of transactions through local copies of the blocks at each node. The difficulty of this task is adaptively set so that a block is created approximately once every 10 min in the entire network. Some calculations for the average delay in the bitcoin network are available in [4].

The bitcoin's consensus rule [1] has severe scalability limitations in terms of number of transactions processed per second (TPS). This is due to the significantly large amount of time assigned for block creation and solving PoW task for which miners get rewards in terms of the crypto-currency. Another major issue with the bitcoin protocol is the double spend attack [5], where a bitcoin is used fraudlently for multiple transactions.

A GHOST (Greedy Heaviest Objervable Sub-tree) rule was proposed in [6] to address this, where, instead of a longest chain consensus rule, the path of the subtree with the combined hardest PoW is chosen. However, the TPS for this protocol is still quite less [7].

A Spectre protocol is proposed in [8] which builds upon the the Directed Acyclic Graph (DAG) idea to achieve low confirmation time by interpreting the reference links as votes to compare between pairs of blocks. This protocol provides the pair-wise ordering of the blocks but not the complete ordering of the blocks. While the TPS is much better compared to [1,6,8] cannot be used for smart contracts.

A permissioned blockchain, Hyperledger Fabric was proposed in [9] with Practical Byzantine Fault Tolerant (PBFT) distributed consensus protocol for running distributed applications. PBFT achieves high transaction throughput, but is limited to only a few nodes due to communication overhead.

In this paper, we propose a mathematical model for optimizing the TPS for a bitcoin network by using the double spending attack as a constraint. The TPS is obtained as a function of the of

block creation rate(λ), block size(b) and delay diameter of the network (D). The delay diameter (D) is modeled by assuming the blockchain as a Erdös-Rényi random network topology [10]. Our model ensures an increase in the block creation rate resulting in improved throughput. Through numerical results, it is shown that this is achieved without disturbing the balance between the hashrate and rewards for miners in the network.

The rest of the paper is organized as follows. Section 1 describes the System model and system parameters, Section 2 describes the preliminaries of End-to-End delay and mainchain growth rate in Blockchain network considered as in Erdös-Rényi random network. In Section 3, we formulate the optimization problem for maximizing the block creation rate and the transaction throughput. In Section 4, we present the analytical and simulation results. In Section 5, we conclude the paper and gave future directions of research.

2. System Model

We refer to the models in [6,10] where the bitcoin network is considered as a directed graph with parameters given in Table 1.

Table 1. System parameters for the model in [6].

Symbol	Description
V	Set of nodes in the network
E	Set of edges between a pair of node
n	Number of nodes in the network
p_v	Computational power at the v^{th} node
λ	Block creation rate
β	Main chain growth rate
q	Fraction of the attacker's computational power
b	Block size in kB
K	Number of transactions per kB
D	Delay diameter (end-to-end delay) in the network
h	Depth of the tree in [11]
N_t	Number of nodes connected to a given node
N_h	Number of confirmations required for a Txn
N_a	Number of blocks found by the attacker
P_d	Prob. of successful double-spend attack

Lemma 1. *The end-to-end block propagation time in the bitcoin network [10,11] where the degree of the node is derived from a binomial distribution is*

$$D = h\left(T_p + \frac{b}{R}N_t\right) \tag{1}$$

where

$$N_t = (n-1)P_e \tag{2}$$

$$h = \lceil \log_\mu \left(n(N_t - 1) + 1\right) \rceil \tag{3}$$

Lemma 2. *For a blockchain network generating blocks at a rate λ and delay diameter D, the lower bound of the main chain growth rate β is*

$$\frac{\lambda}{1 - \frac{3}{\sqrt{N}} + \lambda D} \tag{4}$$

Proof. See Appendix A.

Corollary 1. For $N \to \infty$

$$\beta \geq \frac{\lambda}{1+\lambda D}. \tag{5}$$

3. Optimal Throughput

Theorem 2. *In a blockchain network with throughput $TPS(\lambda, b)$ and end-to-end delay D, the optimal block creation rate is*

$$\lambda = \frac{1}{D} \tag{6}$$

and the optimal transaction throughput is given by

$$TPS(\lambda, b) = \frac{bK}{2h\left(T_p + \frac{b}{R}N_t\right)} \tag{7}$$

Proof. Our goal is to maximize the number of transactions per second $TPS(\lambda, b)$ with very low probability of successful double-spend attack. So, the optimization problem can be framed as

$$\max_{\lambda} \quad TPS(\lambda, b) \tag{8}$$

$$\text{s.t} \quad q < \frac{\beta}{\lambda} \tag{9}$$

$$\frac{1}{\lambda} > D \tag{10}$$

where $q\lambda$ is the attacker's chain growth rate and $\frac{1}{\lambda}$ is the block creation interval. ∵

$$TPS(\lambda, b) = \beta bK, \tag{11}$$

substituting for β from (4) in (8), the optimal λ is obtained by solving

$$\max_{\lambda} \quad \frac{\lambda}{1 - \frac{3}{\sqrt{N}} + \lambda D} \tag{12}$$

$$\text{s.t} \quad q\left(1 - \frac{3}{\sqrt{N}} + \lambda D\right) < 1 \tag{13}$$

$$\lambda D < 1 \tag{14}$$

The solution to the optimization problem is provided in Appendix B.

Proposition 1. *If q_h is the probability the attacker will ever catch up from z blocks behind the honest nodes [1] is*

$$q_h = \min\left(\frac{q}{1-q}, 0\right)^{\max(N_h, 0)} \tag{15}$$

$$= \begin{cases} 1, & \text{if } z < 0 \text{ or } q > (1-q). \\ \left(\frac{q}{1-q}\right)^z, & \text{if } z \geq 0 \text{ and } q \leq (1-q). \end{cases} \tag{16}$$

then the probability of successful double-spend attack is

$$\sum_{N_a=0}^{N_h-1} \frac{\left(N_h \frac{q}{p}\right)^{N_a} e^{-N_h \frac{q}{p}}}{N_a!} \left(\frac{q}{1-q}\right)^{N_h - N_a} \tag{17}$$

Proof. If the honest nodes create N_h (see Table 1) number of blocks in an average time of $\frac{N_h T}{p}$, then the attacker found N_a number of blocks in the same time interval follows poisson distribution with expected value

$$\alpha = N_h \frac{q}{p} \tag{18}$$

Since attacker's chain growth rate is less than the main chain growth rate ($q\lambda < \beta$ from (9)) $N_a < N_h$.

$$P_d = \sum_{N_a=0}^{N_h-1} \frac{\alpha^{N_a} e^{-\alpha}}{N_a!} q_h \tag{19}$$

By substituting (16) with $z = N_h - N_a$ and (18) in (19) yields (17) .

4. Results and Discussions

Table 2 lists the values of the parameters used for generating the results in this section. See Table 1 for a description.

Table 2. Parameter values for the case of Bitcoin.

Parameter	Value
n	10,000 [12]
N_t	8 [12]
P_e	$8.0/(n-1) \approx 0.0008$
T_p	30 msec
b	4 MB
R	>25 Mbps [13] but chosen 10 Mbps
q	<0.5
K	4 txn's/KB for bitcoin [14]

(7) is used for computing the TPS plotted in Figure 1 with respect to the block size b. The TPS increases slowly with b since increasing block size results in an increase in the delay D. This reduces the block creation rate in (6) and main chain growth rate (4).

Figure 1 shows that the minimum achievable throughput is around 400 TPS whereas existing bitcoin networks have a throughput around 3–4 TPS [14].

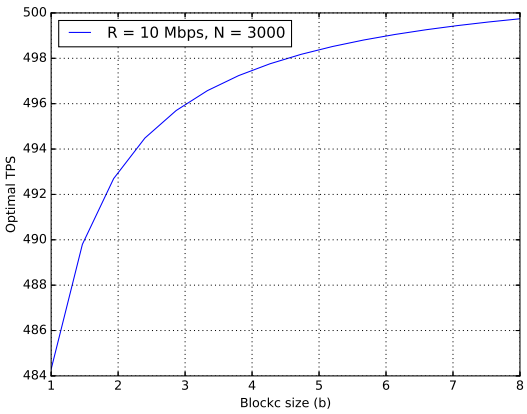


Figure 1. Block size (b) Vs TPS

Figure 2 shows the number of confirmations required with increase in the attacker's hash rate q. It shows that the P_d is less compared to the original bitcoin framework [1] as $q\lambda < \beta$ in (9).

We have conducted an event-driven simulation using python by generating events for 1 day as per the information propagation protocol in [4] for bitcoin blockchain network with n = 10,000 nodes

and 13 miners having the Hashrate distribution shown in [15]. We generated the events for creating a block, broadcating the block to neighbours and adding the block after verifying the block height and hash of the previous block. The timing information for block generation event of each miner was drawn from exponetial distribution with mean equals to λ times the fraction of the hashrate of the corresponding miner. The simulation was performed such that end-to-end delay should be equal to $D \approx 17$ s calculated for parameter values shown in Table 2 using (1). These results shown that, with an optimal block creation rate of $\lambda = \frac{1}{D}$, the longest-chain rule PoW blockchain network will performs similar to the system with block creation rate of $\frac{1}{600}$.

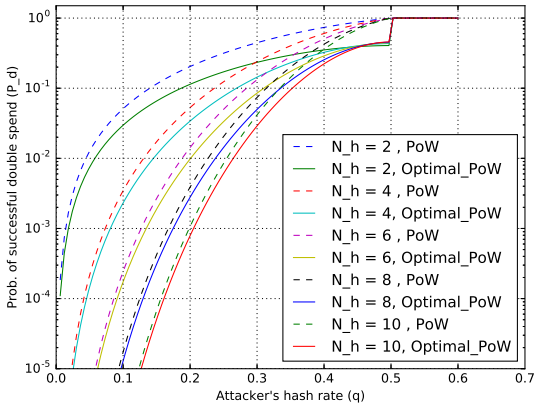
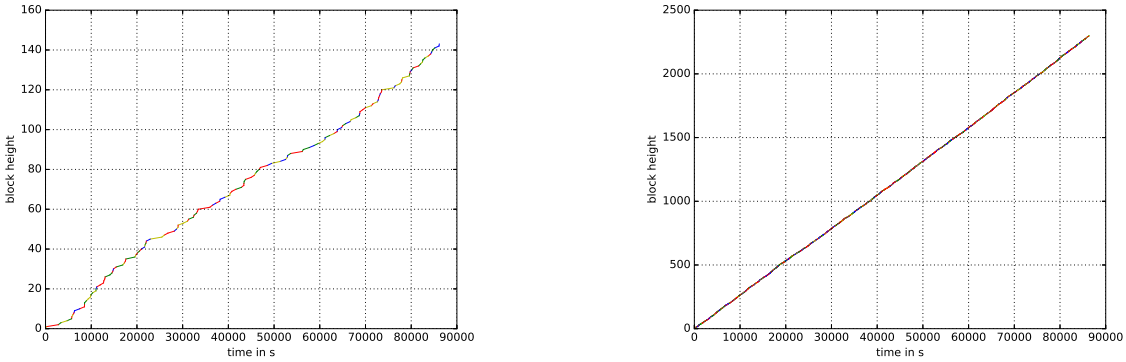


Figure 2. Attacker's rate (q) Vs P_d.

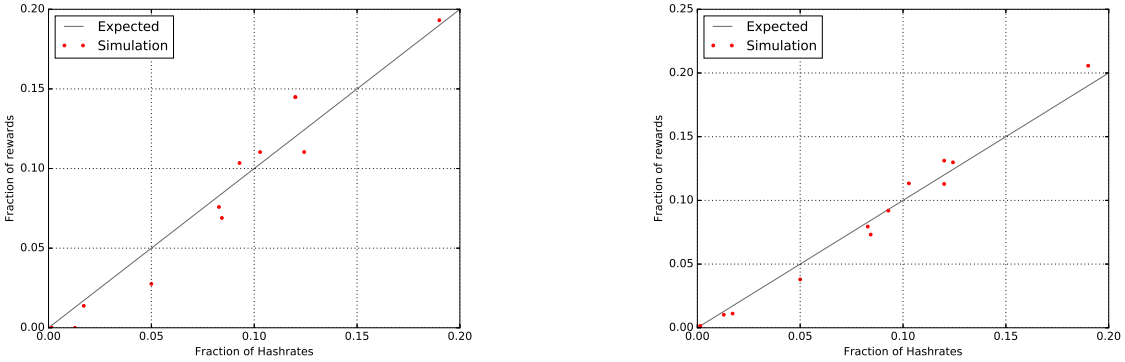
We have chosen the optimal block creation rate $\lambda = \frac{1}{20}$ ($\frac{1}{\lambda} < D$). Figure 3a,b shows the block height w.r.t time of creation. In both cases $\beta > \frac{\lambda}{1+\lambda D} = \frac{1}{2D}$ is satisfied. From Figure 3b, $\beta = 0.0266$ and optimal throughput is ≈425 txn's/sec which is comaparable with analytical resulsts shown in Figure 1.



(**a**) $\lambda = \frac{1}{600}$ (**b**) $\lambda = \frac{1}{20}$

Figure 3. Time in sec Vs Block height for 1 day. In (**a**) and (**b**) you can see the blocks created by different miners in different colours.

Figure 4b shows the proportion of the rewards (shown by red dots) of each miner are nearly equal to their proportion of the hash rates (shown by a line) in the network and is comparable with the rewards proportion for $\lambda = \frac{1}{600}$ shown in Figure 4a. These results shown that, with an optimal block creation rate of $\lambda = \frac{1}{D}$, the longest-chain rule PoW blockchain network will performs similar to the system with block creation rate of $\frac{1}{600}$.



(**a**) $\lambda = \frac{1}{600}$ (**b**) $\lambda = \frac{1}{20}$

Figure 4. Hashrate Vs Rewards proportion for 1 day.

5. Conclusions and Future Research

In this paper, we obtained an analytical expression for the optimal block creation rate and optimal throughput by considering the bitcoin network in [10,11]. Our numerical results show that the achievable throughput can be a hundred times more than the current throughput in the existing blockchain network. The simulation results show that the proportion of the rewards of the miners are comparable to their hash distribution with the optimal block creation rate. This opens up immense possibilities for research in blockchain technology in distributed consensus protocols and security.

Funding: This research was funded by 5G Research and Building Next Generation Solutions for Indian Market Project, Dept. Information Technology, Govt. of India.

Abbreviations

The following abbreviations are used in this manuscript:

PoW	Proof-of-Work
TPS	Transactions processed per second

Appendix A. Proof of Lemma 2

The main chain growth rate [6]

$$\beta \geq \left[\frac{1}{N}\sum_{i=1}^{N} X_i\right]^{-1} \tag{A1}$$

$$\{X_i\}_{i=1}^{N} = D + Y, (i\text{th Block creation time}) \tag{A2}$$

$$\{z_j\}_{j=1}^{m} \sim poiss(\lambda_j), (\text{jth miner creates blocks with a rate of } \lambda_j) \tag{A3}$$

$$\sum_{j=1}^{m} z_j \sim poiss(\lambda), (\text{Blocks are created with a rate of } \lambda \text{ in the entire network}) \tag{A4}$$

$$Y \sim \exp(\lambda), (\text{Block creation interval}) \tag{A5}$$

Thus,

$$E[X_i] = D + \frac{1}{\lambda}, \text{var}(X_i) = \frac{1}{\lambda^2} \tag{A6}$$

Let

$$S_N = \frac{1}{N}\sum_{i=1}^{N} X_i \tag{A7}$$

Using the central limit theorem [16] and (A6),

$$S_N \sim \mathcal{N}\left(\mu, \sigma^2\right), \quad \mu = D + \frac{1}{\lambda}, \sigma^2 = \frac{1}{N\lambda^2} \tag{A8}$$

$$\therefore \Pr\left[\frac{1}{S_N} \leq \beta\right] = Q\left(\frac{\sqrt{N}}{\sigma}\left(\frac{1}{\beta} - \mu\right)\right) \tag{A9}$$

where $Q(\cdot)$ is the Q-function [17]. From Figure A1, it is obvious that the maximum value of $Q(x) \approx 1, x < -3$. Thus, $\Pr\left[\frac{1}{S_N} \leq \beta\right]$ is maximum for

$$\frac{\sqrt{N}}{\sigma}\left(\frac{1}{\beta} - \mu\right) \leq -3 \tag{A10}$$

$$\implies \beta \geq \frac{\lambda}{1 - \frac{3}{\sqrt{N}} + \lambda D} \tag{A11}$$

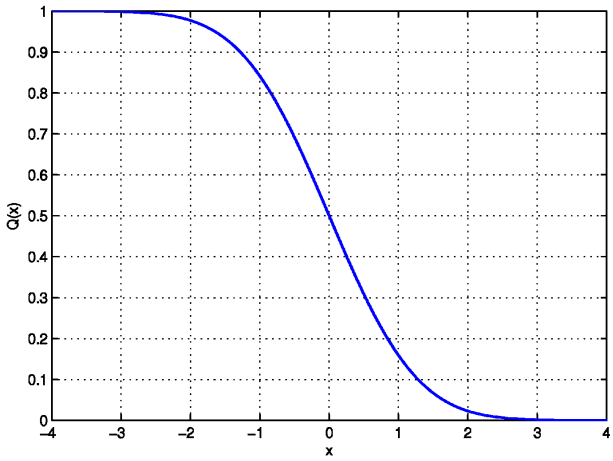


Figure A1. The Q function.

Appendix B. Proof of Theorem 2

In (8), The objective function

$$f(\lambda) = \frac{\lambda}{1 - \frac{3}{\sqrt{N}} + \lambda D} \tag{A12}$$

is concave and and the constraints

$$g_1(\lambda) = q\left(1 - \frac{3}{\sqrt{N}} + \lambda D\right) - 1 \tag{A13}$$

$$g_2(\lambda) = \lambda D - 1 \tag{A14}$$

are affine. The lagrangian of the optimization problem is given by

$$L(\lambda,\alpha)=\frac{\lambda}{1-\frac{3}{\sqrt{N}}+\lambda D}-\mu_1\left(q\left(1-\frac{3}{\sqrt{N}}+\lambda D\right)-1\right)-\mu_2(\lambda D-1) \tag{A15}$$

The optimal solution is obtained by solving

$$\frac{\partial L(\lambda,\alpha)}{\partial\lambda}=0 \tag{A16}$$

$$\implies \frac{1}{1-\frac{3}{\sqrt{N}}+\lambda D}-\frac{\lambda D}{\left(1-\frac{3}{\sqrt{N}}+\lambda D\right)^2}-\mu_1 qD-\mu_2 D=0 \tag{A17}$$

$$\implies \frac{1-\frac{3}{\sqrt{N}}}{\left(1-\frac{3}{\sqrt{N}}+\lambda D\right)^2}=\mu_1 qD+\mu_2 D \tag{A18}$$

and

$$\frac{\partial L(\lambda,\alpha)}{\partial\mu_1}=0 \tag{A19}$$

$$\implies q\left(1-\frac{3}{\sqrt{N}}+\lambda D\right)-1=0 \tag{A20}$$

$$\text{or}\quad 1-\frac{3}{\sqrt{N}}+\lambda D=\frac{1}{q} \tag{A21}$$

and

$$\frac{\partial(\lambda,\alpha)}{\partial\mu_2}=0 \tag{A22}$$

$$\implies \lambda D-1=0 \tag{A23}$$

From (A21) and (A23),

$$\lambda=\frac{1}{D}\left(\frac{p}{q}+\frac{3}{\sqrt{N}}\right) \tag{A24}$$

$$\lambda=\frac{1}{D} \tag{A25}$$

From (A24),

$$g_2(\lambda)>0 \tag{A26}$$

So, $g_1(\lambda)<0$ is an inactive ($\mu_1=0$) and for $q=0$, $g_1(\lambda)$ no longer become a constraint. These can be observed in Figure A2.

From (A18) and (A25)

$$\lambda=\frac{1}{D} \tag{A27}$$

$$\mu_2=\frac{1-\frac{3}{\sqrt{N}}}{\left(2-\frac{3}{\sqrt{N}}\right)^2}\frac{1}{D} \tag{A28}$$

Since $\mu_2 > 0$ for after creating sufficiently large number of blocks (N), λ in (A27) yields the optimum throughput in (7) for sufficiently large N.

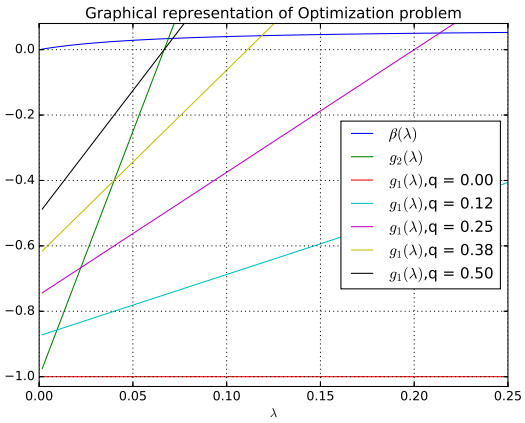


Figure A2. Graphical representation of Optimization problem.

References

1. Nakamoto, S. *Bitcoin: A Peer-to-Peer Electronic Cash System*; 2009. Available online: https://s3.amazonaws.com/academia.edu.documents/54517945/Bitcoin_paper_Original_2.pdf?response-content-disposition=inline%3B%20filename%3DBitcoin_A_Peer-to-Peer_Electronic_Cash_S.pdf&X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIWOWYYGZ2Y53UL3A%2F20191022%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20191022T021937Z&X-Amz-Expires=3600&X-Amz-SignedHeaders=host&X-Amz-Signature=992637af757aa82a8300d0f2a7033364283d92821e52e8b3039e32818dbd7717 (accessed on 31 October 2008).
2. MedicalChain. Available online: https://medicalchain.com/en/ (accessed on 10 February 2019).
3. Dorri, A.; Salil S.; Kanhere, R.J.; Gauravaram, P. Blockchain for IoT security and privacy: The case study of a smart home. In Proceedings of the IEEE PERCOM Workshop On Security Privacy And Trust In The Internet of Things 2017, Kona, HI, USA, 13–17 March 2017; pp. 618–623.
4. Decker, C.; Wattenhofer, R. Information propagation in the Bitcoin network. In Proceedings of the IEEE P2P 2013 Proceedings, Trento, Italy, 9–11 September 2013; pp. 1–10.
5. Rosenfeld, M. Analysis of Hashrate-Based Double Spending. *CoRR* **2014**, *abs/1402.2009*, 1–13.
6. Sompolinsky, Y.; Zohar, A. Secure High-Rate Transaction Processing in Bitcoin. In Proceedings of the Financial Cryptography; International Financial Cryptography Association (IFCA), FC'15, San Juan, Puerto Rico, 26–30 January 2015; pp. 1–20.
7. Ethereum. Available online: https://etherscan.io (accessed on 15 March 2019).
8. Sompolinsky, Y.; Lewenberg, Y.; Zohar, A. SPECTRE: A Fast and Scalable Cryptocurrency Protocol. Cryptology ePrint Archive, Report 2016/1159. 2016. Available online: https://eprint.iacr.org/2016/1159 (accessed on 18 December 2016).
9. Androulaki, E.; Barger, A.; Bortnikov, V.; Cachin, C.; Christidis, K.; Caro, A.D.; Enyeart, D.; Ferris, C.; Laventman, G.; Manevich, Y.; et al. Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains. *CoRR* **2018**, *abs/1801.10228*, 1–15.
10. Erdös, P.; Rényi, A. On the Evolution of Random Graphs. In *Publication of the Mathematical Institute of the Hungarian Academy of Sciences*; Mathematical Institute of the Hungarian Academy of Sciences: Budapest, Hungary, 1960; pp. 17–61.
11. Noh, J.; Baccichet, P.; Hartung, F.; Mavlankar, A.; Girod, B. Stanford Peer-to-peer Multicast (SPPM): Overview and Recent Extensions. In Proceedings of the 27th Conference on Picture Coding Symposium, PCS'09, Chicago, IL, USA, 6–8 May 2009; IEEE Press: Piscataway, NJ, USA, 2009; pp. 517–520.
12. Bitnodes. Available online: https://bitnodes.earn.com/ (accessed on 1 July 2019).
13. Speedtest. Available online: https://www.speedtest.net/global-index (accessed on 1 July 2019).

14. Blockchain Charts. Available online: https://www.blockchain.com/charts/n-transactions? (accessed on 1 July 2019).
15. Blockchain Luxemberge S.A. Available online: https://www.blockchain.com/pools (accessed on 1 July 2019).
16. Papoulis, A. Probability, Random Variables and Stochastic. In *Probability, Random Variables and Stochastic*, 3rd ed.; McGraw-Hill: New York, NY, USA, 1991; pp. 182–240.
17. Proakis, J.G.; Salehi, M. Digital Communication. In *Digital Communication*, 5th ed.; Michael Hackett, L.K.B., Ed.; McGraw-Hill: New York, NY, USA, 2008; pp. 40–44.