EAI Endorsed Transactions
on Scalable Information Systems
Research Article EAI.EU

Enhanced Bitcoin Protocol with Effective Block Creation and Verification by Trusted Miners

R. Bala[1],* and R. Manoharan[1]

[1]Department of Computer Science and Engineering, Pondicherry Engineering College, Pondicherry, India.

Abstract

The Distributed nature of Bitcoin introduces security issues that necessitate security-specific enhancements in Bitcoin protocol. Therefore, proposing a method of incorporating criteria check and verification process for miners to participate in the mining process and join the mining pool respectively. The proposed idea mitigates double spending, block withholding, and 51 percentage attacks. In addition, an increase in the rate of Bitcoin users necessitates performance improvement. Hence, proposing an effective approach of refining the existing block creation and verification strategy for improving transaction rate without compromising security.

Keywords: anonymity, decentralization, Double Spending; Block withholding, 51% Attack, transaction rate, memory pool, block.

Received on 21 December 2019, accepted on 15 March 2020, published on 19 March 2020

doi: 10.4108/eai.13-7-2018.163836

1. Introduction

The drastic growth of Internet makes e-shopping a key fragment of commercial web activities and its main attribute is online payments. It deals with electronic fund transfers from customers to merchants using existing electronic payment mechanisms like card payments and Internet banking. For performing transaction verifications, the system requires a third-party mediator (ex. PayPal) through which user's sensitive data are exposed leading to sensitive information leakage. Consequently, there is a need for a secure payment system that does transactions without requesting any sensitive details from users and without a third party for verifications.

A decentralized digital currency named Bitcoin [1] gives a solution for the above-stated problems, stating everyone is a bank. The Bitcoin transactions are peer-to-peer and it uses the concept of Blockchain [2], a sequence of blocks so called distributed ledger for handling all transactions and ownership without involving any financial institution through which it preserves the privacy of the users. Figure 1. Shows attributes of a block and dependency between the blocks.

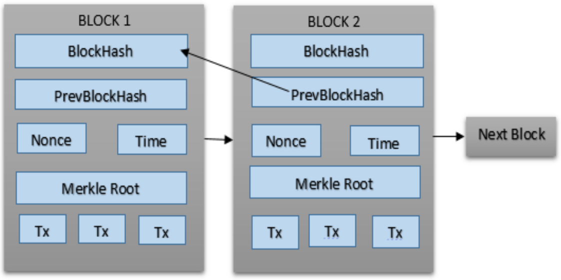

Figure 1. Chain of blocks

Bitcoin users are denoted as Bitcoin nodes and special Bitcoin nodes having high computational power which can participate in transaction and block verification process are denoted as miners.

Bitcoins do not exist as physical coin instead, ownerships and amounts are maintained as a transactions sequence in

*Corresponding author. Email:balasekar.bs@gmail.com user's digital wallet [2], a secure software application for storing Bitcoins. At present, value of one Bitcoin is, 1 BTC = 7219.9 $ and its INR value is 1 BTC = 472052.11 ₹. Its value may change with time. It is also feasible to transfer segments of Bitcoin and one Satoshi (10^{-8} BTC) is the minimum transferable amount.

A digital wallet should be installed in user's system before start transferring Bitcoins and each wallet produces a pair of the public-private key. The Public key of the user is utilized to generate Bitcoin address [3] to which the Bitcoins are transferred. The overall flow of Bitcoin protocol for transferring Bitcoins from user A to user B is as follows: User A first creates a transaction (TX) [2] specifying receiver B's Bitcoin address, amount in BTC and digitally signs it with A's private key. The transaction created is broadcasted in Bitcoin network followed by the verification by the miners against a set of validation rules [4]. The verified transactions for a specified duration are combined to form a block [2] of size 1 MB. A block is referred as a leaf of the distributer ledger i.e. the blockchain. The created block is verified by the mining process (Proof of Work [1]) and on success the solution is published in the network for verification and added to the block chain. Remaining miners validate the solution and on receiving six confirmations the transferred Bitcoin is credited to B's account.

Bitcoin protocol excludes the third-party intervention by the concept of decentralization, leading to security issues like double spending [10], block withholding [11] and 51 % attacks [12]. For handling the security issues [13] [14], the protocol does a tough mining process named Proof-of-Work which affected the performance of the system resulting in very low transaction rate of 7-8 tps.

The transaction rate [5] of Bitcoin protocol is the transactions count affixed to the block chain per second. The determined size of a block is 1 MB, transaction size is ≈ 200 KB and average time taken is 10 minutes to attach a block to the block chain. Based on these figures the average transaction rate of the existing system computes to 7-8 tps. In real-time, the transaction rate varies from 1.5 to 7 tps.

2. Related Works

In 1988, David Chum proposed first E-cash scheme [6] with untraceability termed as Digital Cash. It is a system of purchasing cash credits in a small amount and storing the credits in the respective storage such as computer systems, mobiles etc. Then using those credits for online payment and transactions. Chaum's Blind signature [7] and Zero knowledge proof [8] techniques are utilized in Digital cash for maintaining the anonymity of users. Even though it maintains anonymity, it is a digital currency that represents the centralized system that requires a banking module for generating and maintaining the E-cash credits.

This leads to the Bitcoin [1] invention on Nov 2008 by Satoshi Nakamoto that provides an appropriate solution by eliminating the requirement for a central bank. That is, each Bitcoin user maintains an individual copy of the record which would be handled at the central bank. To maintain those records in a distributed way, mechanisms are required and it should also handle Bitcoin creation and management. In Bitcoin network, block chain concept [2] does the job of distributer ledger for maintaining the Bitcoin transactions. It also logs the owner and timestamp of each transaction.

A concept named Proof of Work (PoW) [15] is used in Bitcoin for maintaining the distributed ledger in a secured way. PoW is like Adam Back's Hash cash [9]. It is the process of sequentially varying and finding the nonce value which on hashing with block header using SHA 256 produces the hash value having a pre-defined zero's in beginning. Large computational power is required to find the solution for the puzzle and it is the sequential process. That is, each block header which is included in the puzzle has a value called preBlockHash, which points to previous block. So, if an attacker wants to attack any of the blocks and change its hash, should also solve that block and the forthcoming blocks to make the attack successful.

Transaction rate [5] is a metric for analysing the Bitcoin system performance. It is the transactions count attached to the blockchain per second. Series of activities [16] are involved in processing a transaction and adding it to the blockchain. First the transaction is created by user A, followed by the verification against a set of rule. Once the transaction clears the verification process [17] a set of transactions are added to a block and undergoes mining process [1]. Transaction is said to be processed only if it succeeds block verification. Transaction rate is the time taken for a transaction to complete the above-said process. Theoretically the maximum possible transaction rate of Bitcoin system is 10 tps with a block size of 1MB and minimum transaction size of 166 bytes. The transaction rate can be increased a bit by the user if they combine and process their transactions leading to a reduction of 10 bytes in the transaction size.

Even though Bitcoin preserves the obscurity of the users, it has some open issues that require attention. Notably, the transaction rate of Bitcoin protocol computes to 7-8 tps which is minimal when compared to other electronic payment mechanisms (VISA – 2000 tps, PayPal – 100 tps). The main difficulty Bitcoin users face nowadays is the delay in confirming the unconfirmed transactions.

3. Motivation

Proof-of-Work concept used for achieving security degrades its performance leading to a minimal transaction rate (number of transactions appended to the memory pool per second) of 7-8 tps. Notably, the transaction rate of Bitcoin protocol is minimal when compared to other electronic payment mechanisms (VISA – 2000 tps, PayPal – 100 tps). The main difficulty of the Bitcoin users is the delay in confirming the unconfirmed transactions. Therefore, motivated to propose a solution for performance improvement with enhanced security.

4. Proposed Work

The Proposed work concentrates more on enhancing security by refining the mining process (Proof of Work module). Currently, computational power is the only criteria for the miners to take part in the mining process. This is the reason why attackers easily enter as miners/join the mining pool to solve Proof of Work puzzle and perform attacks like 51%, double spending, and block withholding. Proposed work also concentrates on increasing throughput of Bitcoin protocol by refining block creation and verification strategy without compromising security.

4.1 Proposed Mining Process

To counter the issue, we propose a solution that includes criteria check for Miners to participate in the mining process and verification process for miners to join the mining pool. Criteria check/ verification process includes set of rules to verify the trustworthiness of the users which shall act as a barrier for the attackers to participate in the mining process. Figure 2 depicts the modules of proposed mining process.

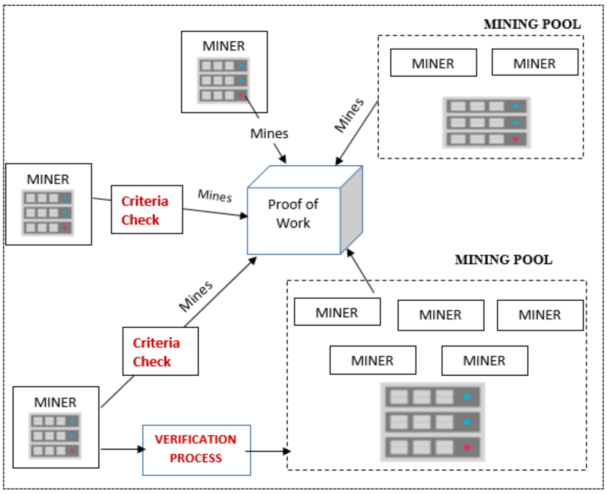

Figure 2. Proposed mining process

Verification Process

The verification process is to prevent attackers from joining mining pool by verifying miners against a list of verification rules. The validation rules are as follows,

- Rule1: Checking the attack history of miners i.e. no. of forks [2] created so far in the blockchain.
- Rule2: Checking the balance Bitcoins in their digital wallet [2], because users having more no. of Bitcoins shall have the more responsibility to build trusted network.

Since only trusted miners enter the pool based on above two rules, there is no possibility of retaining the solution obtained for the Proof of Work puzzle. This could be mitigation for block withholding attack (BWH).

- Rule3: Checking whether the sum of pool's computational power (CP_p) for which miners are requesting and miners computational power (CP_m) is not more than 50 % of total computational power.

This could be the mitigation for 51% attack. The check for rule 3) is done using equation 1,

$$CP_p + CP_m \leq 0.5 * \sum_{i=1}^{p} CP_{p_i} + \sum_{i=1}^{m} CP_{m_i} \quad -(1)$$

Criteria Check

This module is for miners to participate in the mining process. It checks with a list of criteria to permit only the honest miners to perform mining process which could be the mitigation for the double-spending attack. The rule 1 and 2 mentioned in the verification process is also applied for this module since they are created for individual miners.

4.2 Transaction Rate

The transaction rate of existing payment mechanisms like PayPal and VISA are high when compared with Bitcoin protocol. It processes the transactions at the rate of 7-8 tps. Transaction Rate is the Bitcoin transactions count added to block chain per second and equation 2 can be used to compute its value.

$$Transaction\ Rate\ (TR) = \frac{B_{nT}}{B_t}\ tps \quad --(2)$$

Where, B_{nT} –Transactions count per Block. B_t – Processing time of a block in seconds.tps – Transactions per second. Equation 3 can be used for calculating the number of transactions per block.

$$B_{nT} = \frac{B_s}{\frac{1}{n} * \sum_{i=1}^{n} T_i} \quad --(3)$$

Where, B_s – Maximum block size. T_i - i^{th} Transaction size i = {1, 2, 3…n}

For a sample data with Bitcoin block size limit as 1 MB (B_s), Proof of Work verification time for single block as 10 minutes (B_t), Bitcoin transaction average size as 250 bytes. The transaction rate can be computed using equation 2 & 3 and the calculation is as follows,

$$B_{nT} = \frac{1000000}{250} = 4000\ transactions$$

$$TR = \frac{4000}{10 * 60} = 6.666 \ \simeq\ 7\ tps$$

4.3 Effective Block Creation and Verification Strategy

Proposing an effective process for increasing the transaction rate of existing system resulting in performance improvement of Bitcoin protocol without compromising security. This is achieved by refining block creation and verification strategy of the protocol which targets at reducing the block processing time (B_t) for few (requires normal level of security) of the blocks. The blocks are classified into premium and normal based on the threshold value. The premium block holds the transactions that entails high level of security and it undergoes existing Proof of Work process. The normal block holds the transactions that requires medium level of security and undergoes Proof of Work with reduced challenge. Since block processing time and transaction rate are inversely proportional as given in equation 2, the above said refinement improves the transaction rate.

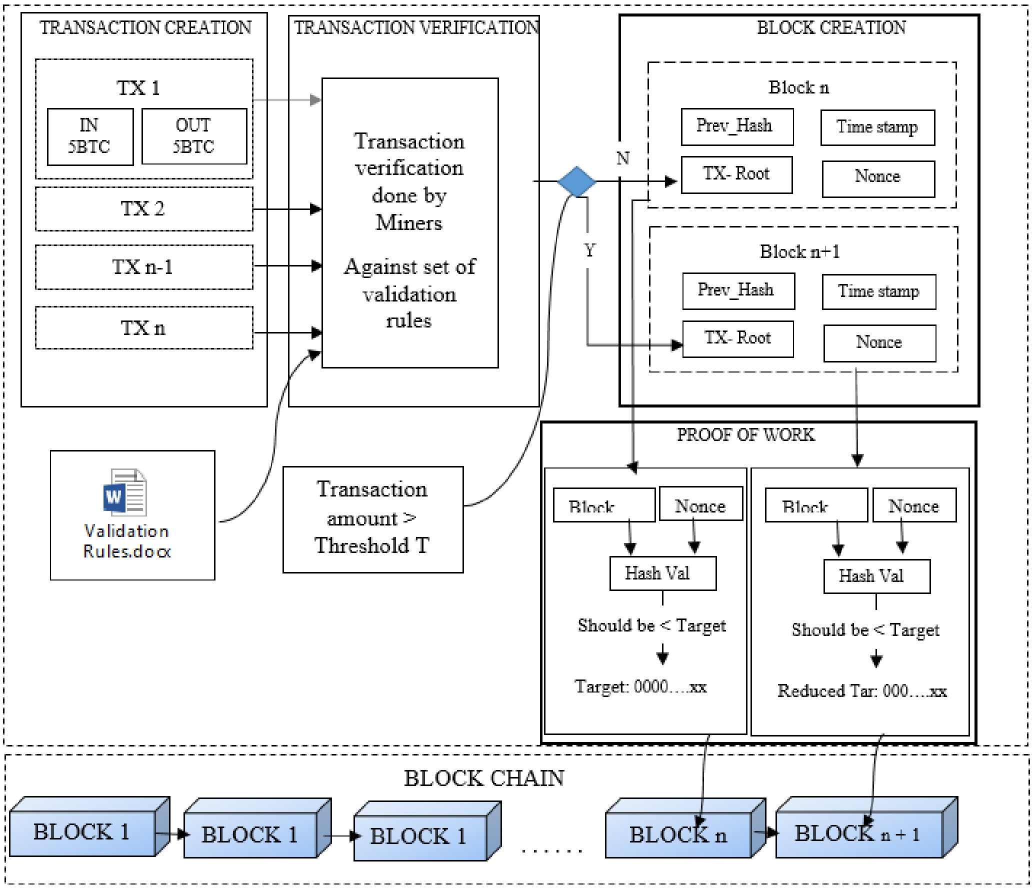

Figure 3. Effective block creation and verification strategy.

Figure 3. Shows the proposed protocol with effective block creation and verification strategy. The changes are proposed in Block Creation and Proof of Work modules that are tuned to handle transactions in two different blocks, one with challenge that can be met at 10 minutes and the other with reduced challenge that can be processed at 5 minutes.

4.4 Setting Threshold

Threshold value is the Bitcoin amount and the idea is to provide high security for the transactions having amount above threshold and medium level of security for the transactions having amount less than threshold. Threshold value is decided by carrying out the study on the logs of main-net transactions with their amount and frequency. Main-net is the real time Bitcoin network that does Bitcoin transactions around the globe. The real time transactions can be simulated in the proposed system and the system performance can be studied for different threshold values for finalizing on the threshold.

4.5 Proof of Work – Target

The main reason to utilize Proof of Work consensus in Bitcoin protocol is to provide anti-double spending attack and Denial of Service attack defense. The process of Proof of Work is varying the nonce to find the hash using SHA-256 from block header information that meets the target set for a block. The target is calculated for every block based on the difficulty and Bitcoin network hashing power. Equation 4 can be used to compute its value.

$$Target = \frac{D * 2^{32}}{H_p} - - -(4)$$

Where D – difficulty, H_p- Hash power of the network.

The difficulty D is calculated taking into account the preceding block attributes of the block chain and with complexity which can be cracked in an average time of 10 minutes. The target is usually calculated as a 256 bit number leading with specified number of zeros and represented in 32 bits by performing compact encoding on 256 bit target. For Block 0, the 256 bit target calculated from the block attributes is "000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f" and it is represented as "1d00ffff". The difficulty of above target is 1 i.e. the block hash should have 4 bytes leading zeros.

4.6 Reduced Target

It is the value of the target with a reduced number of leading zeros. Reducing the target by level one is removing a leading zero with reduces the processing time by half. Here the complexity is also reduced but the reduced target is applied only for transactions that requires medium level of security. Level two reduction is the process of removing two leading zeros in proof of work target.
The following algorithm describes the steps involved in the proposed block creation and verification strategy for improving the transaction rate of Bitcoin protocol without compromising security.

Effective block creation and verification algorithm

```
Input   : List of transactions $TX_n$ created for a
          Specified time interval, n = {1, 2 . . ., n},
          Threshold T
Output: blocks $B_m$ created from $TX_n$ , m = {1, 2}
1.  Foreach $TX_j$ j from 1 to n
2.      If $TX_j$.amount A > threshold T
          //block that need to be verified under //normal
          security level
3.          Add $TX_j$ to block $B_1$
4.      Else
          //block can be verified with reduced target
5.          Add $TX_j$ to block $B_2$
6.  End
7.  Verify block $B_1$ with normal PoW. // takes 10
    minutes for verification.
8.  Verify block $B_2$ with PoW with reduced target. //
    take less than 10 minutes for verification since target
    is easy to achieve.
```

The proposed algorithm is to improve the transaction rate of Bitcoin protocol. Before starting the enhanced process, the Threshold T is to be defined i.e. the transaction amount above which the security level required is high for the transactions. The threshold value T is obtained by performing a study on the amount transferred in transactions created so far in Bitcoin network. Once threshold is fixed, the group of transactions for a particular duration of time are categorized and grouped together as block 1 and block 2. Block 1 with transactions having amount A above the threshold T. Block 2 with transactions having amount A below the threshold T. After grouping the transaction into two blocks, block 1 is verified under normal Proof of Work process with target calculated as in existing Bitcoin protocol. Block 2 is verified under Proof of Work process with reduced target with the aim of reducing verification time. It does not compromises security since the transactions in block 2 requires medium level of security.

5. Experimental setup

Bitcoin protocol experimentation has been carried out using ***BitcoinJ***, a complete Java library of protocol implementation that can maintain a wallet and send/receive transactions. For experiment 1, The Proof-of-Work module present in that library was enhanced to adopt the proposed block creation and verification strategy. For experiment 2, the verification and criteria check modules are implemented with set of rules proposed. The experiment was conducted with simulated Peer-to-Peer Bitcoin network of 850 sq. m. area with 25 Bitcoin nodes and 9 miners. And utilized ***Testnet3*** for conducting real time testing which is the Bitcoin testing network.
The system performance was evaluated with below evaluation metrics,

- Transaction Rate: Number of transaction added to block chain per second and its value can be calculated using equation no.2.
- Chain Quality (CQ): The proportion of blocks in any k long subsequence produced by an attacker is < µk and it can be evaluated using equation no.5.

$$B_A < \mu k \quad --(5)$$

B_A- Blocks created by Attacker, µ ϵ (0, 1) and k ϵ N.

6. Results

With configured setup of 25 Bitcoin nodes and 9 miners within the nodes, the proposed system processes transactions at the rate of 12.685 tps by reducing the target of mining process (Proof-of-Work) by one level. The sequence of experiments conducted are as follows,
Experiment 1 was conducted to evaluate the performance of proposed system without any threshold set and Figure 4 shows the transaction rate of proposed system considering medium level of security for all transactions.

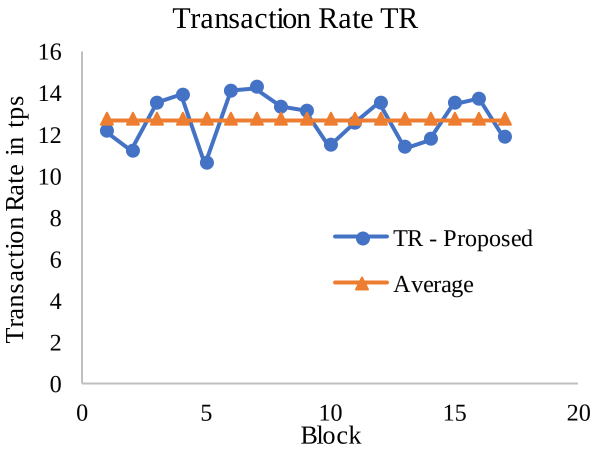

Figure 4. Transaction Rate of proposed system without threshold

In experiment 2, the threshold value T is identified by monitoring the performance of the proposed system for different values of T (T1, T2 ... Tn) starting from 1 until it reaches saturation. The optimal value of T was set as threshold. Table 1. Shows the progress in the transaction rate for different threshold values.

Table 1. Transaction Rate for various threshold values

Threshold	Premium Transactions	High Transactions	Average TR
1	239576	26962	7.3337011
2	218698	47956	7.8577574
3	199297	67447	8.3440005
5	165654	101067	9.1836345
7	137583	129184	9.8851565
10	106758	159993	10.654569
12	90888	175877	11.050903
13	84134	182640	11.219596
20	51607	215165	12.031628
30	28839	237934	12.600036
40	17388	249386	12.885902
50	10795	255980	13.050506
60	6902	259873	13.147695
70	4569	262206	13.205936
80	2961	263814	13.246076
90	1997	264778	13.270148

Figure 5. Shows the graph of improved transaction rate for various threshold value. From graph the optimal point was chosen as 30 (Threshold value).

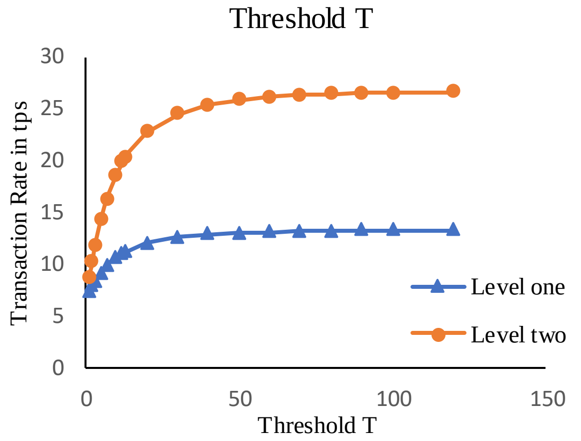

Figure 5. Threshold for performance enhancement

The optimal result was achieved with a threshold value of 30 and implementing the proposed enhancement in mining process (Proof-of-Work). As per the proposed verification process,

Level one – At level one, the optimal transaction rate was 12.600 tps which is increased by 77.46% when compared with existing protocol. The transactions with amount > T, i.e. the premium transactions that requires high level of security are processed at the rate of 6.66 tps and transactions with amount < T are processed at a rate of 13.3 tps.

Level two – At level two the optimal transaction rate was 24.480 tps. Premium transactions are processed at the rate of 6.66 tps and transactions with amount < T are processed at a rate of 26.64 tps.

Experiment 3 was conducted to compare the performance of existing and the proposed system and Figure 6 shows the comparison. Experiment 4 was conducted to implement proposed criteria check and verification modules for blocking untrusted miners from participating in mining process and to join mining pool that mitigated Block withholding, double spending and 51 % attacks.

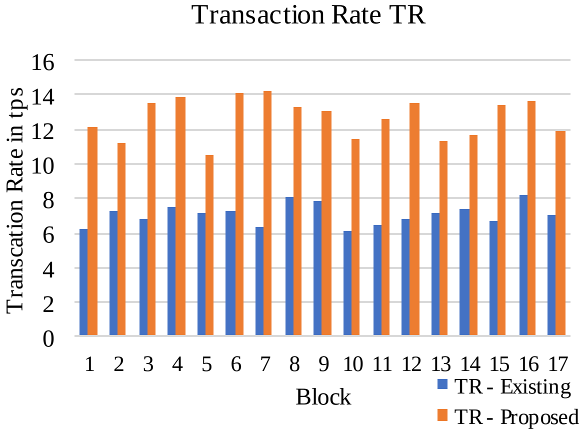

Figure 6. Existing and proposed protocol comparison.

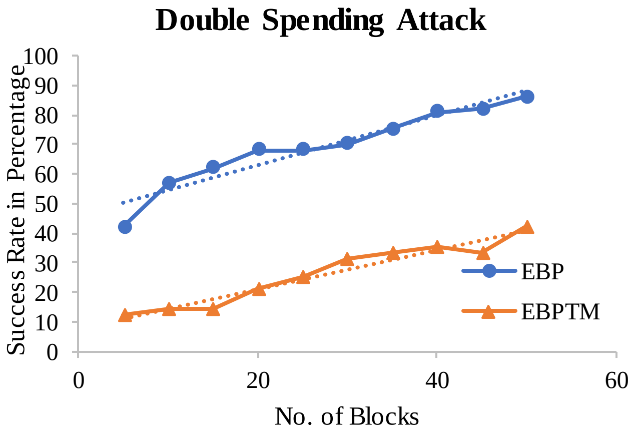

Figure 7. Success Rate of Double spending attack – a comparison.

Figure 7 shows the comparison of success rate of Double Spending attack with increasing number of blocks. Without any doubt it proves that the Enhanced Bitcoin Protocol by Trusted Miner (EBPTM) outperforms the Existing Bitcoin Protocol (EBP) by showing 63.60 % reduction in the attack success rate.

Figure 8 and 9 shows the comparison of success rate of Block Withholding and 51% attacks respectively with increasing number of blocks. Without any doubt it proves that proposed protocol EBPTM outperforms the Existing Protocol EBP by showing 54.64 % and 46.07 % reduction in the success rate of the Block Withholding and 51% attacks respectively.

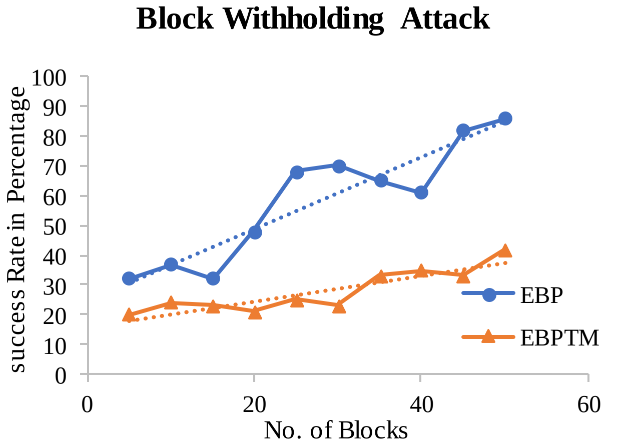

Figure 8. Success Rate of Block Withholding attack – a comparison.

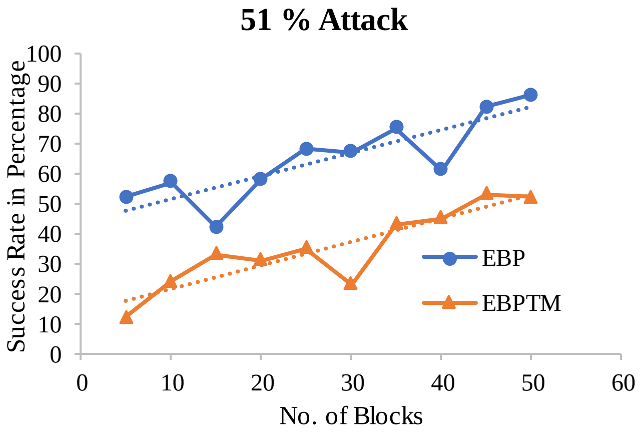

Figure 9. Success Rate of 51% attack – a comparison

Table 2 shows the percentage reduction in the success rate of various attacks for increasing number of blocks. And average percentage reduction in success rate of Double Spending, Block Withholding attack and 51 % attack.

Table 2. Percentage Reduction in success rate of Double Spending, Block Withholding and 51% attacks

No. of Blocks	Double Spending	Block Withholding	51%
5	71.42	93.75	76.92
10	75.43	35.13	57.89
15	77.41	28.125	21.42
20	69.11	56.25	46.55
25	63.23	63.23	48.52
30	55.71	67.14	65.67
35	56	49.23	42.66
40	56.79	42.62	26.22
45	59.75	59.75	35.36
50	51.16	51.16	39.53
Average	63.601	54.6385	46.074

6. Conclusion

In this paper, an effective block creation and verification strategy was proposed for increasing the transaction rate of Bitcoin protocol from its current rate 7.1 tps to 12.600 tps without compromising security. The proposed system was implemented using BitcoinJ and the results were evaluated using standard evaluation metrics. The results obtained confirm that the proposed strategy outperforms the existing protocol in terms of throughput (transaction rate). In an average the proposed strategy improves the transaction rate by 77.46% when compared with existing protocol. Further it is evident that the performance is optimal at a threshold value of 30 and was depicted in the results. Also, an efficient pre-mining module is proposed which permits only trustworthy miners to participate in mining process for mitigating security attacks namely 51%, double spending, block withholding. This is made possible by introducing criteria check and the verification modules in the mining process, which can block attackers entering Bitcoin mining network. It resulted an average reduction in success rate of Double Spending, Block Withholding and 51% attacks by 63.60%, 54.64% and 46.07% respectively.

7. Future Enhancement

The proposed mining process helps to mitigate attacks like double spending, 51 %, block withholding. The proposed system can be further enhanced to counter unhandled attacks like DDoS, transaction traceability etc. In addition, there is a scope for scalability issues because of surgical increase in Bitcoin users. The Bitcoin scalability problem denotes the limits on the amount of transactions the Bitcoin system can process. The transaction processing capacity of the Bitcoin network is limited by the average block creation time of 10 minutes and the block size limit of 1MB. The scalability directly affects the transaction rate, hence improving transaction rate along with scalability consideration is also a key focus area in Bitcoin protocol.

References

[1] Nakamoto, Satoshi. (2008) “Bitcoin: A peer-to-peer electronic cash system”. White Paper, 1-28.

[2] Tschorsch, F., & Scheuermann, B. (2016) “Bitcoin and beyond: A technical survey on decentralized digital currencies”. IEEE Communications Surveys & Tutorials, Vol. 18, no. 3: 2084-2123.

[3] Bitcoinwiki. Technical_background of Bitcoin address, (2017) https://en.bitcoin.it/wiki/Technical_background_of_version_1_Bitcoin_addresses

[4] Bitcoinwiki. “Protocol rules (tx messages, block messages , (2017) https://en.bitcoin.it/wiki/Protocol_rules

[5] Bitcoinwiki. Maximum Transaction Rate, (2014) https://en.bitcoin.it/wiki/Maximum_transaction_rate

[6] Fan, Chun-I., and Vincent Shi-Ming Huang. (2010) “Provably secure integrated on/off-line electronic cash for flexible and efficient payment”. IEEE Trans on Systems, Man, and Cybernetics, Part C (Applications and Reviews), Vol. 5: 567-579.

[7] Kang, Baoyuan, and Jinguang Han. (2010) “On the security of blind signature and partially blind signature”. In 2nd IEEE Int. Conf. on Education Technology and Computer (ICETC), Vol. 5: 206-208.

[8] Jaafar, Abdullah M., and Azman Samsudin. (2010) “Visual Zero-Knowledge Proof of Identity Scheme: A New Approach”. In 2nd IEEE Int. Conf. on Computer Research and Development, 205-212.

[9] A. Back, (2002) “Hashcash - a denial of service counter-measure”, http://www.hashcash.org/papers/hashcash.pdf

[10] Bag, Samiran, Sushmita Ruj, and Kouichi Sakurai. (2017) "Bitcoin block withholding attack: Analysis and mitigation." IEEE Transactions on Information Forensics and Security, Vol. 8: 1967 – 1978.

[11] Pinzón, Carlos, and Camilo Rocha. (2016) "Double-spend Attack Models with Time Advantange for Bitcoin." Electronic Notes in Theoretical Computer Science, 79-103.

[12] Bastiaan, Martijn. (2015) “Preventing the 51%-Attack: a Stochastic Analysis of Two Phase Proof of Work in Bitcoin.” Proc. 22nd Student Conf. IT Available online at https://fmt.ewi.utwente.nl/media/175.pdf, 1-10.

[13] Lin, Iuon-Chang, and Tzu-Chun Liao. (2017) "A survey of blockchain security issues and challenges." IJ Network Security, Vol. 19, no. 5: 653-659.

[14] Wang, Qin, Bo Qin, Jiankun Hu, and Fu Xiao. (2017) "Preserving transaction privacy in bitcoin." Future Generation Computer Systems, Vol. 107: 793-804.

[15] Shanaev, Savva and Shuraeva, Arina and Vasenin, Mikhail and Kuznetsov, Maksim. (2019) Towards Proof-of-Work Cryptocurrency Valuation: Mining Games, Network Effects and the Social Value of Blockchain. Available at SSRN: https://ssrn.com/abstract=3352098 or http://dx.doi.org/10.2139/ssrn.3352098.

[16] Gupta, Suyash, and Mohammad Sadoghi. (2019) "Blockchain Transaction Processing.” Encyclopedia of Big Data Technologies Vol. 1: 366-376.

[17] Liu, Zhenhua, Yuanyuan Li, Dong Yuan, and Yaohui Liu. (2019) "Effective Privacy Preservation and Fast Signature Verification in Bitcoin Transaction." International Journal of Network Security 21, Vol. 5: 741-750.