Pakistan Journal of Engineering and Technology, PakJET
ISSN (p): 2664-2042, ISSN (e): 2664-2050
Volume: 5, Number: 2, Pages: 1- 10, Year: 2022

Investigating the Impact of Delayed Mining upon Scaling Blockchain Applications under Malleability Attack—An e-Voting Scenario

Kashif Mehboob Khan[1], Shafaque Khan[2]

[1]Department of Software Engineering, NED University of Engineering & Technology, Karachi, Pakistan
[2]Department of Pharmaceutical Chemistry, Jinnah Sindh Medical University, Karachi, Pakistan

Corresponding author: Kashif Mehboob Khan (e-mail: kashifmehboob@neduet.edu.pk).

Received: 5/02/2022, Revised: 10/04/2022, Accepted: 20/04/2022

***Abstract*-Blockchain is a disruptive technology and has attracted significant attention with prominent applications across finance, medical and many other systems. Electronic voting or e-voting is one of the emerging applications of blockchain leveraging benefits such as integrity, and non-repudiation of data. Whilst existing research has focused on using blockchain for e-voting applications to achieve transparent and verifiable solutions, there exists a gap in study with respect to an in-depth investigation for the challenges surrounding the trade-off for scalability versus security in the context of transaction malleability attack when mining capability is compromised for the blockchain network. In order to present our research, we have used e-voting as an example application to demonstrate our investigations regarding the mentioned gap. The paper does not focus on building a blockchain based e-voting system. The study carries out empirical analysis by establishing blockchain networks with varying mining strength under an extreme load of incoming transactions to achieve a real world scenario of large blockchain based system. The developed system has then been exposed to transaction malleability attack while scaling throughput up to thousands of transactions. The findings reveal that blockchain networks upon scaling, are more vulnerable to transaction malleability attack while operating under lower mining strength as compared to the networks having higher mining power under same conditions. These research outcomes would help researchers and application architect to build highly secured and large scaled applications. To the best of our knowledge, there has not been any published empirical investigation present in the given context.**

Index Terms—Blockchain, e-Voting, Scalability, Transaction Malleability Attack

I. INTRODUCTION

Voting has undoubtedly been one of the most significant pillars of human society. Many efforts have been made by the technology specialists to aid the voting process for actual empowerment of the society. The era of information and communication technology has already started its impact to bring the characteristics of verifiability and transparency in the voting process. Since the early adoption of technology in the form of punched-card ballots, electronic voting has been making a quick and progressive journey with the latest emerging technologies [1]. This includes the installation of electronic voting machines at polling stations, and digital voting with the use of portable electronic devices. The paper presents research to investigate the impact of mining strength in blockchain-based applications upon scaling when they are under transaction malleability attack. We have used e-voting as an application scenario not only due its significance and its increasing adaption of blockchain technology but also due to its scaling and security requirements. Such investigation will lead towards a better utilization of blockchain technology in many real world applications in general and in the context of e-voting in particular.

In the recent years, blockchain has been able to mark its impact on many domains of real world other than only cryptocurrency mainly due to its transparent and decentralized nature of record keeping structure, which is available to the peers of the network. The blockchain stores the transaction's data through its hashes in the form of separate blocks, which are connected to each other through their block hashes. In this way, a temper evident chain of data in the form of blocks is kept and maintained in the blockchain network by the peers. Each peer stores and maintains its own copy of data locally as well. This local copy is kept synchronizing by the peers who actually run the network [2]–[4]. The blockchain is also powered by strong cryptographic scheme to restrict any malicious and unwanted access to the data [4]–[6]. Although, bitcoin has been the most known and probably the most accomplished application of blockchain but at the same time, the researchers have already started to explore the potential of this technology in other areas.

Although current research in the area of blockchain technology has revealed its various new dimensions to

contribute in the applications areas other than cryptocurrency, but still we believe that the challenge of scalability has been increasing day by day not only in the domain cryptocurrency (such as Bitcoin) but also in other real world use-cases where the data has been growing rapidly such as healthcare, road transport, ware houses and many others [7]. Scalability, therefore demands further investigation under certain realistic conditions. This paper specifically takes into account the impact of mining resources and capabilities, which can cause the scalability of blockchain network to behave differently when it is under transaction malleability attack. This study is extremely significant in the cases where controlling the challenges of scalability is the primary focus.

The core contributions of this research study is as follows;

i. A thorough investigation and empirical analysis where we have been able to practically demonstrate how mining may increase or decrease the chances for a successful transaction malleability attack when the system is receiving a higher number of transactions. To the best of our knowledge, such empirical analysis that takes into account mining resources, scalability, and transaction malleability has never been done before.
ii. A formal analysis and mathematical modelling have been performed to model the event for success and failure of attack.
iii. Development of the fully functional prototype to implement the presented voting model bearing the capability to initiate transaction malleability attack under rigorous testing of incoming bulk transactions.

The paper has been structured as follows: Section II illustrates a summary of the current research work related to e-voting and existing efforts to study the significance of scalability of blockchain based solutions. Section III presents an overview of our proposed system based upon blockchain technology for public e-voting model we have developed as part of efforts detailed in [8]. Architecture and execution of our e-voting system is presented in section IV along with details of our blockchain setup including hardware used, the type of blockchain created as well as methods and techniques used to implement client applications. Section V details the experimentation conducted along with the technical discussion of the experiments' outcome observed in the following Section. Summarizes of the investigation has been presented in Section VII.

II. RELATED WORK

Since there has not been much published work that specifically carryout research investigation towards the impact on delayed mining upon scaling blockchain applications under malleability attack, therefore in this section we present the scientific research that is closed to our investigation for e-voting and scalability challenges. As presented in [9], the authors propose a voting process which does not need any intervention from a single central authority to count votes . This scheme does not also use any secure channel communication. In [10], the process of tallying votes is performed by the protocol in two different steps. This scheme also does not demand any secure path for voters or a dedicated central authority for the approval or rejection of vote. As far the computational power and network bandwidth utilization is concerned, the performance of the protocol is very satisfactory but at the same time the lacking in robustness and fairness in [10] was then later on improved in [11]. The constraints in DRE-i in [12] was addressed and resolved by [13] by empowering DRE-I with DRE-ip (DRE-I with enhanced privacy). In [13], rather than calculating ciphertext in advance, the same is calculated when the voting process is continued. This [13] scheme helps performing end-to-end verification. In [14], verification from end to end is performed by the Mixnet protocol [15] that mixes servers in a chain to randomize the ciphertext. Scantegrity solution in [12] makes use of confirmation codes to let the voters know the inclusion of their votes as it as. In another approach which was presented in [16] and inspired from [14], works on the privacy of the voting process by dividing the ballot into two separate sections for voting options and choices. In [17], the use of scratch stripes was done for making off-line audit of ballots using homomorphic tabulation. Other known systems include Bingo Voting [18], Helios [19], DRE-i [20], Star-Vote [21] and as it is presented in [22].

Majority of the existing work in the domain of scalability, has been done for blockchain based cryptocurrency applications. For instance, as highlighted by authors in [23], blockchain applications such as bitcoin can motivate miners to pick up the transaction that has more transaction fee. If in such a case, the size of block increases, it may result in delaying the creation of new blocks for transaction confirmation. This may ultimately lead towards blockchain forking. The authors further highlighted limitations in processing transactions at increasing on-demand speed by real-life examples. Since the size of block in a conventional application of bitcoin had initially been kept at 1 MB and the chain is tuned to process only seven transactions in a second, it took on average one hour to get a confirmed status of a transaction. Consequently, if the block is allowed to handle higher number of transactions by expanding its memory space, maintaining rate of block generation at an appropriate level will be a challenge. This also depends upon the application, which is being run blockchain platform. Similarly, authors in [24] investigated the role of transaction throughput and its impact over the delay in the network to find the relationship between the size of the block and its rate of generation for achieving an optimum level of performance. Furthermore, efforts including [25] and [26] have focused on achieving more scalable blockchain solutions by investigating alternate consensus algorithms to replace the standard proof of work algorithm used by bitcoin. Through our study of existing literature, we have identified that the challenge of scalability for blockchain based application is significant and is acknowledged by research community. However, our study has also revealed the gap in existing research with respect to a rigorous investigation of scalability with respect to security against blockchain based transaction malleability attack. Although some empirical studies such as in [27], and [28] have been conducted on transaction malleability attack and scalability but these studies do not cover the aspect of mining

resources of blockchain network. Transaction malleability attack was successfully conducted in Bitcoin based Mt. Gox exchange and resulted in a loss of millions of dollars [27]. This situation demands to assess the scalability of blockchain based solutions in the context of well-known transaction malleability attack, backed by extensive experimentation.

III. A BLOCKCHAIN BASED E-VOTING SYSTEM

Fig. 1 shows how different entities work together in our proposed e-voting model to facilitate voting mechanism. We have explained this model in detail in [27]. Here, we have extended our model to capture the success rate of transaction malleability attack when it is being operated with a higher number of transaction throughput and variable mining strength. We have given a comprehensive implementation of our voting model to thoroughly investigate the impact of scalability and security vulnerabilities under controlled and delayed mining.

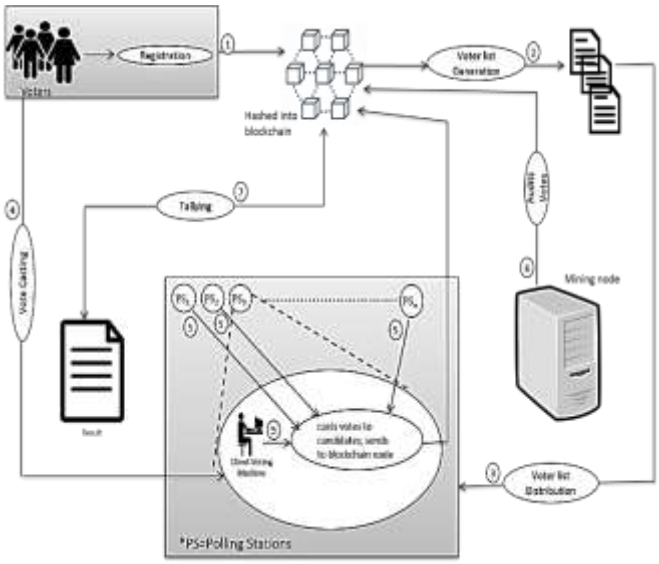

Figure 1: A Blockchain based e-voting architecture

Figure 1 represents our proposed voting model that has been implemented on blockchain platform to investigate the impact of delayed mining over scalability. The process starts with the registration of voters by generating their public wallet addresses on voting blockchain. These wallet addresses will act as a Voter ID in the entire voting process model. Data for voters' registration (along with some metadata) would become a part of blockchain in the form of hashes. We have used these voters' IDs (public wallet addresses of voters) to generate voter lists (csv files) based upon the individual polling stations. These voter lists will automatically be distributed through API's based services that are responsible for interacting with voting blockchain and forwarding the voters list to the respective polling station identified by voting machines at each polling station. We have created a pool of 10 mining nodes that are responsible for confirming voting transactions into the main consensus blockchain for voting. We will investigate the behaviour of our developed system using different number of active miners and its impact on transaction throughput in the context of security. This will enable us to monitor and control the length of operational time window for confirmation of transactions. There has been an observed relationship between rate of incoming transactions per unit time and the number of active miners. The higher the number of transactions demands a respective increase in the number of active mining processes to timely confirm the voting transactions into the chain. If there is a mismatch (reasonable delay) in the ratio of incoming transactions and their confirmations into the block, time window of that delay may then be used by an attacker to get his own version of (malleable) transaction confirmed in place of the original transaction. Our study takes into consideration the parameters which are critical in this regard.

IV. IMPLEMENTATION AND SETUP

In order to execute the voting model as presented in Fig 1, we designed and developed a testbed as illustrated in [8]. The testbed consists of permissioned blockchain network having seed node (or root node), peer nodes, mining nodes, and JSON based RPC remote clients. The remote clients have been written to programmatically scale up our proposed decentralized network of blockchain with thousands of transactions. This raises transaction throughput (scalability) to tens of thousands of transactions per second. We have tested our system with hundreds of thousands of transactions from multiple remote clients to observe a real time empirical response of the state of the system against bulk remote voting transactions. At this moment, the system behaves as the real world public voting scenario does in peak hours under stress of bulk transactions. The decentralized blockchain network has been created using an open source blockchain platform, Multichain [28] (Alpha 4) which was released by Multichain community in 2016. The specifications of the machine in the network running blockchain seed and connected nodes have been shown in Table III JSON based Remote clients have been written in java to access blockchain via APIs for sending bulk voting transactions. This has been done to apply and monitor the impact of delayed mining when the system is tuned to be scaled. Table I illustrate the state of our operational blockchain with and without delayed mining (using mining diversity) respectively.

The paper aims to investigate how scaling up the system with varying number of active mining nodes (to adjust the rate of confirmation of transactions) may increase the chances for an attacker to successfully carryout the transaction malleability attack.

Algorithm 1 Transaction Malleability Attack

```
1: procedure SENDMALLEABLETRANSACTIONS(VotingChain, VoterList)
2:     VoterAddress ←VotcrList[ArrayIndcx]
3:     VoteCount ← 1
4:     while VoterAddress ≠ EOF do
5:         if VoteCount DIVISIBLEBY 1000 then
6:             CALL PushEncodedMetaDataForMalleableTransaction
           (OriginalTransaction) with AddedMetaData;
7:             RETURN TransactionID
8:             VoteCount ←VotcCount+1 =0
```

V. EXPERIMENTATION

As mentioned in the Section IV, a public voting scenario has been used here as an application use case to demonstrate the scenario of transaction malleability attack. Overall, the evaluation was performed using a voter population of over 100,000. In order to observe the impact of scalability upon mining strength of the system to ultimately determine the impact of transaction malleability attempt under such conditions (with and without delayed mining), evaluations were performed using different remote clients against each set of mining diversity (see table I). RPC remote API clients have been programmed to send bulk voting transactions to the blockchain network. These clients have been given access to the voter lists of the respective polling station using (.csv) files and have access to blockchain through JSON based RPC remote APIs. The system has been implemented with following a public voting model where only voting transactions may only be made through registered wallet addresses available in the voters' lists. This helps to develop a real voting scenario for making observations.

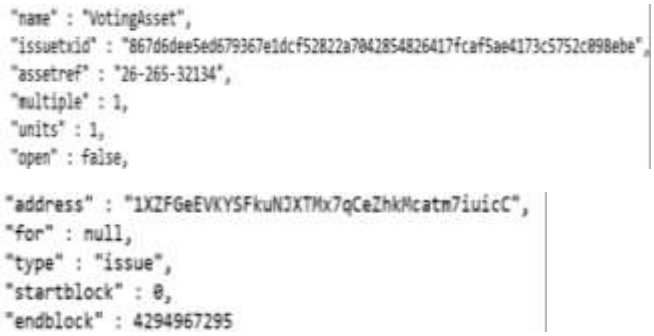

Figure 3: Node Wallet Address for Issuance of Voting Assets

Table I shows the master configuration of the node which initiated the blockchain network. Consequently, this environment does not allow everyone to actively participate in the election process unless the relevant rights are not granted to respective voters, candidates or even to miners. For a voter, the rights are granted for receiving of a single asset of voting token to be used against the candidate of his choice.

Figure 4 shows the transfer of voting assets to voters. In the same way, the candidates' accounts have been configured to receive voting tokens from voters' public wallet addresses.

Figure 2: Example voting asset within the proposed system

Figure 4: Transfer of voting asset to voters

Transactions for casting votes are confirmed by a controlled number of miners, which have been allowed to actively participate in the mining process through mining diversity. We have taken control over the mining capability of our decentralized network using mining diversity (a parameter in the configuration file of blockchain network). This parameter accepts inputs from 0.1 to 1.0. In the first set of experiment here, the value has been set to 0.3. This implies that in this case three randomly selected miners from a pool of 10 available miners (0.3 * 10 = 3) will be actively mining the incoming transactions while the rest of the available miners will not participate [28]. In this way, we can find the impact of delayed mining (by reducing the mining capability) against increased scalability using a higher number of consecutive transactions via JSON based RPC remote clients and then observe its behaviour for randomly generated incoming malleable transactions. This will enable us to determine whether delayed mining (It will happen when bulk transactions will be entering into the system and there are not enough miners to confirm the transactions into the block quickly, so it would enforce some transactions to be delayed) is a factor of consideration for an attacker to open an attack window (utilizing delay of time for confirmation of some transactions) for artificially injected malleable transaction into the block through the pool of unconfirmed transactions. This is achieved by taking the chance that such malleable transactions would be picked up by the miners in place of their original transactions. The second new parameter, which is used in this case, is *Mining Turnover* (value between 0 and 1) which manages the turns among the miners using a round robin scheme. If this value

is set to 1 then every miner will add the block to the blockchain [28], potentially leading to forks and increasing computational overhead. Similarly, if the value is set to 0, then there is no turnover and a simple round robin scheduling algorithm adopted. In our experiments, the value of mining diversity is set to 0.3 and 0.6 to monitor the impact of delayed and early mining.

```
"address" : "1AZh3Umi1Rs2CvEKV16sTCNob8PGeD6tz1RLg1"
"ismine" : true


"address" : "1RDVBxfkzhPpYueLEaJexEu2m19yVDFktaPgX3"
"ismine" : true
```

Figure 5: Candidates wallet addresses

```
multichain.HonestTransaction ) MakeMalleableTransaction ) Obj2 )
Debugger Console × Run (MalleabilityRun) ×
************************************************************
Voting Transaction is being sent at 2021-12-31T12:29:16.463 for voter 1CwuuFMgNgFHqp3pYQuE7avWw4FtUTpTKW33dp
Transaction for Voter Number 9 bearing address -->1CwuuFMgNgFHqp3pYQuE7avWw4FtUTpTKW33dp has been declined.
A failed Malleable Transaction
************************************************************
Voting Transaction is being sent at 2021-12-31T12:29:17.477 for voter 14pwgq5nnSB83uuTpKdcXhmK9PeZBEfwj28TdU
Transaction for Voter Number 10 bearing address -->14pwgq5nnSB83uuTpKdcXhmK9PeZBEfwj28TdU has been declined.
A failed Malleable Transaction
************************************************************
Total Number of attempts for Malleability attacks are 10
------------------------------------------------------------------------
```

Figure 6: Failed transaction malleability attack without delayed mining

Table I: Blockchain Setup for Delayed and Early Mining

Platform	Blockchain Parameters				
	Mining Diversity	No. of miners	Block generation Rate(secs)	Max. Allowable Size (MB)	Mining Turnover
Windows	0.3	10	15	8.3	0.5
Windows	0.6	10	15	8.3	0.5

Table II: Hexadecimal Encoded Meta-data of successful malleable transaction hash

Malleable Tx ID	Time Received	Time Added to Wallet	Decoded Hex Data of Tx (From Fig. 7)
4653f5ed5581e3ce6afe26672b29c8b36431e367fca1744af831a22e4702f57e	12:46:12.708 PM	12:46:12.715 PM	Malleable Tx for No. 2 at (Root Node)

Table III: Hardware and software specifications

Node Type	Platform	Hardware Specification		
		Processor	Memory	Page File
Seed Node	Windows 10 Home Single Lang. 64-bit (10.0, Build 17134)	Intel Core i7-7500U CPU @ 2.70GHz (4 CPUs) 2.9GHz	8076MB RAM	14346MB used 2836 available
Connected Node-I	Windows 10 Pro 64-bit (10.0, Build 10586)	Intel Core i3-4005u CPU @ 1.70GHz (4CPUs)	4096MB RAM	5586MB Used 1887MB available
Connected Node-II	Windows 10 Enterprise 64 bit	Intel(R) Core(TM) i7-7500U CPU @ 3.4GHz (4 CPUs), 3.4GHz	16384MB RAM	3809MB used 14901MB available

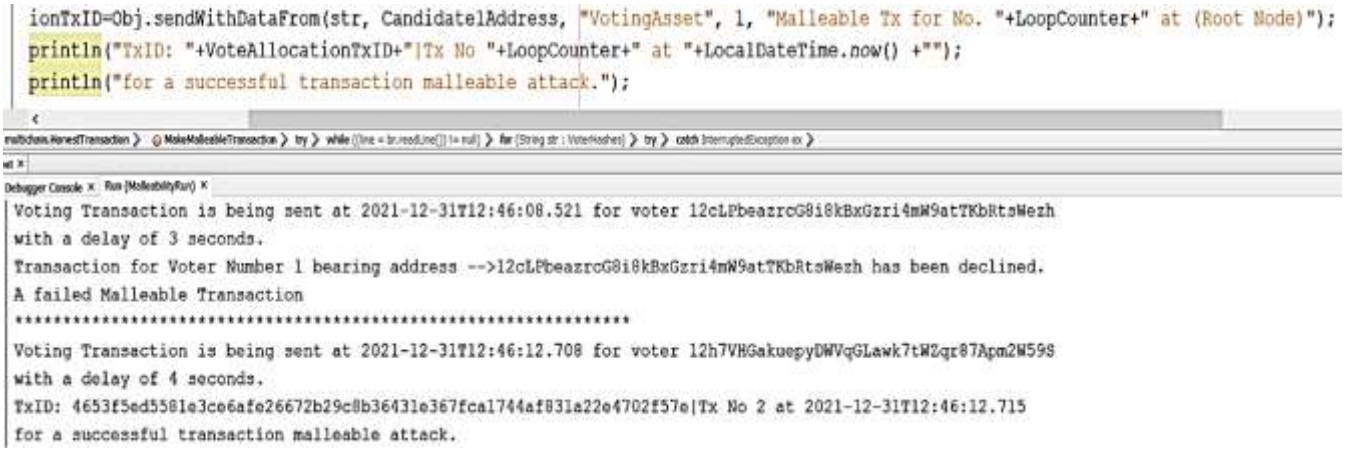

Figure 7: Successful transaction malleability attack with delayed mining


```
"myaddresses" : [
    "12h7VHGakuepyDWVqGLawk7tWZqr87Apm2W59S"
],
"addresses" : [
    "1AZh3Umi1Rs2CvEKV16sTCNob8PGeD6tz1RLg1"
],
"permissions" : [
],
"items" : [
],
"data" : [
    "4d616c6c6561626c6520547820666f72204e6f2e203220617420285 26f6f74204e6f646529"
],
"confirmations" : 0,
"txid" : "4653f5ed5581e3ce6afe26672b29c8b36431e367fca1744af831a22e4702f57e",
"valid" : true,
```


Figure 8: Successful malleable transaction in blockchain

Upon establishing an operational testbed for our experimentation, we started with the creation of voting token assets for our model on blockchain as shown in Fig. 2. The collection of voting token was generated using the default public wallet address of seed node as shown in Fig. 3. This address has full permission over the node include mining, creation of assets and sending and receiving of transactions to and from other peers over the network. (A seed node is the one where blockchain is initialized for the very first time in the network). All the other peer nodes, connected to seed node, are termed as connected nodes. Currently, we have two dedicated connected nodes as shown in Table III (other than seed node) which will be used to achieve decentralization of the network along with the pool of ten mining nodes. This pool serves as an agent to dynamically adjust mining power (through controlling number of actively participating miners) of the pool and observe its impact towards the success/failure of attack.

VI. FORMAL ANALYSIS OF ATTACK

In order to perform the impact of transaction malleability attack in our scenario, we would carry out formal analysis to find out the probability for a successful transaction malleability attack. Suppose T_{xh} and T_{xm} be the honest and malleable version of transaction. As mentioned before, we have setup multiple JSON based RPC remote clients. These software clients have been programmed to send bulk transactions (T_{xh} and T_{xm}). These bulk transactions have been sent under two different sets of experiments n for delayed and without delayed mining. We are interested to investigate and analyse the desired event where T_{xm} is able to beat its respective T_{xh} to become a part of the consensus chain containing voting transactions. Although, it is evident that T_{xh} would come earlier before its respective T_{xm} to the pool of unconfirmed mining transactions, but the miner may pick up any transaction from the pool [29]. Delayed mining would certainly be helpful to facilitate transaction malleability attack in a way that it limits the rate of picking up transaction from the pool by reducing mining power of the network. This causes the transactions to wait more in the mining pool to get their turn of being picked up by the miner [27]. Secondly, arrival of bulk transactions due to remote java based software clients with limited mining capability (delayed mining) is likely to make this wait even a bit longer. It is basically a competition between T_{xh} and T_{xm} to make it the chain first. It is important to understand that the addition of blocks in a blockchain by a miner is purely a random event and therefore may be modelled using Poisson's distribution. As mentioned before, we also need to take into consideration the number of blocks on the top of the block containing malleable voting transaction. This is very important to factor into the equation to determine the success or failure of attack. for example, if a block containing malleable transaction is added to a blockchain but the next following blocks do not connect themselves with the block containing malleable transaction, then this blockchain is going to become orphan blockchain and will no more be a part of the longest consensus blockchain. This means we

need n blocks on the top of block carrying T_{xm}. Let p be the probability of event for mining the new block by the honest node containing T_{xh} while q represents probability in case of attacking node for sending T_{xm}. Lets suppose α determines the predictable value for measuring the progress of attacker. This may be calculated as [5];

$$\alpha = n\left(\frac{p}{q}\right) \quad (1)$$

The interval for adding n blocks is very important as this reflects to the duration of time in which the election regulatory body needs to wait for the confirmation of voting transactions on order to ensure that the voting transactions reside on the longest chain. Suppose a miner is proposing p blocks containing honest transactions at an interval 't'. This implies that n blocks will be appended at the top of p blocks. This duration may then be calculated as;

$$duration = n\left(\frac{t}{p}\right) min \quad (2)$$

At the same time, the attacker 'A' would be generating 'q' blocks at the same interval to win the race against 'p' blocks. Mathematically,

$$A = \left(\frac{q}{t}\right) \quad blocks/minute \quad (3)$$

Hence, the average success outcome α, in the particular duration of time may then be expressed by multiplying eq. 2 and eq. 3 [5];

$$\alpha = n\left(\frac{t}{p}\right) * \left(\frac{q}{t}\right) = \left(\frac{nq}{p}\right) \quad (4)$$

Eq. 4 may be used to asses the overall expected probability for the success and failure of transaction malleability attack.

VII. RESULT AND ANALYSIS

We initially attempted to investigate how the variation in mining power may affect the capability of transaction throughput in a blockchain based system. Through our experimentation, we may infer that under our experimentation condition for hardware/software specification (see the Table III), transaction throughput may be increased reasonably by increasing the hashing power of mining (provided if the influx of incoming transactions increases in a proportion to be confirmed by

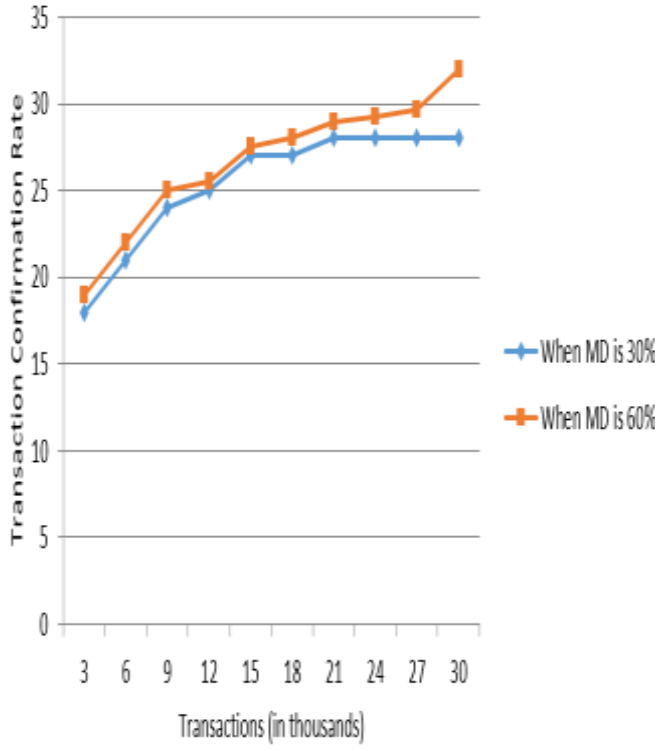

Figure 9: Tx processing speed vs no. of Tx for one client

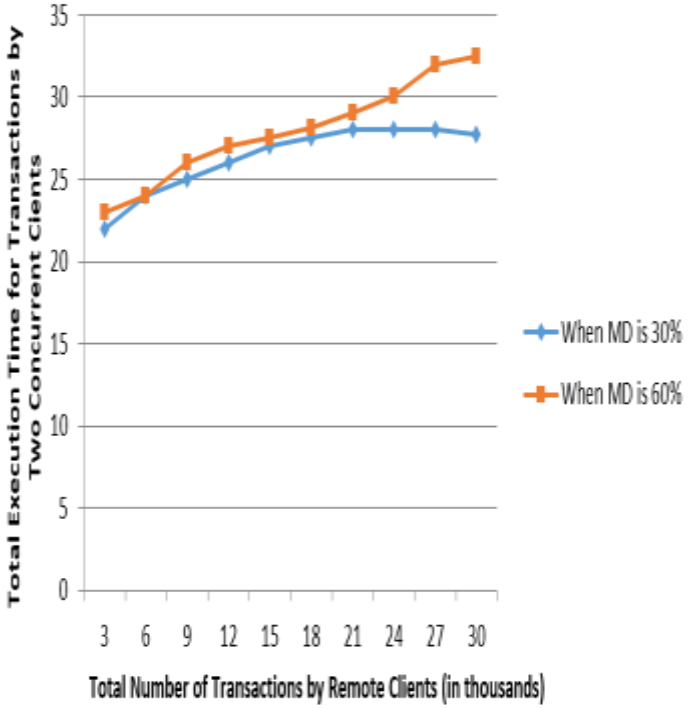

Figure 10: Tx processing speed vs no. of Tx for two clients

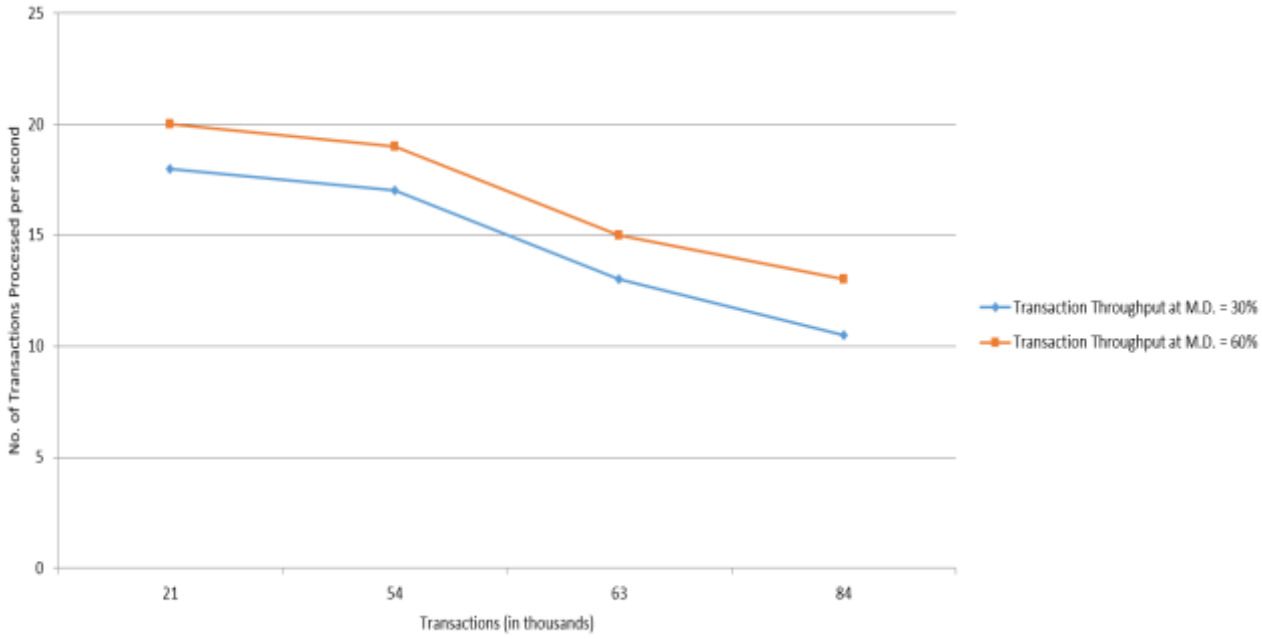

Figure 11: Tx processing speed vs number of Tx for Seven Clients

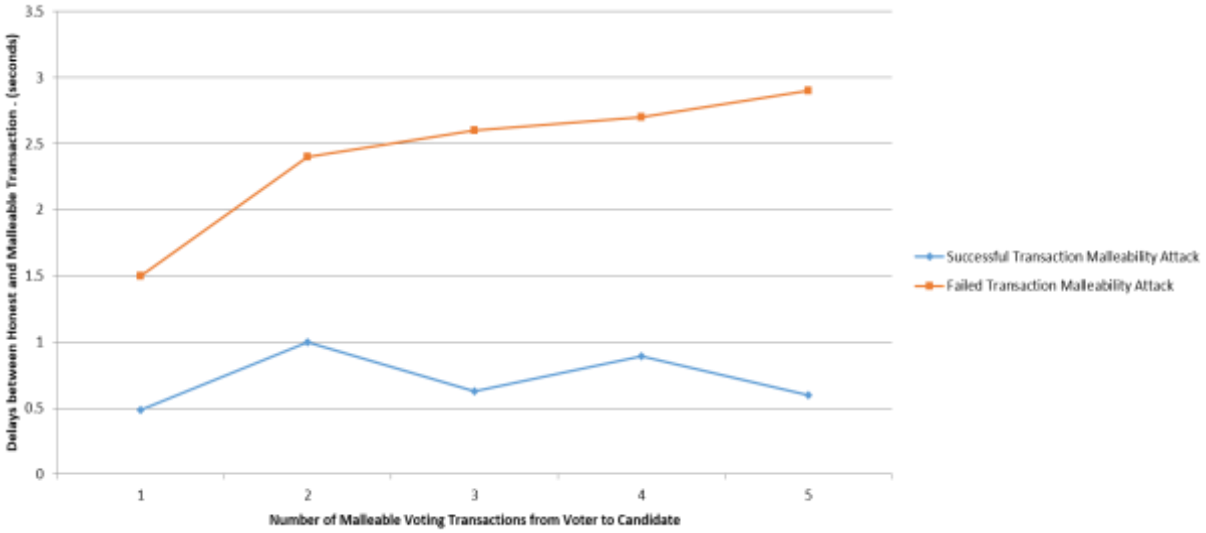

Figure 12: Successful (Delayed Mining) Vs. Failed (Without Delayed Mining) Malleability attack

the increased/added mining power). This implies that reducing mining capability against higher number of incoming transactions can certainly slow down the transaction throughput of the system which results in the increment of time for confirming transactions into the block.

Figure 9 demonstrates scalability in terms of transaction throughput when thirty thousand voting transactions were being cast from a single remote client to the blockchain master node with and without delayed mining. It can be seen here that when 30 percent of the mining power of network is utilized , maximum attained transaction throughput was a bit lower than in the case of 60% utilization of mining power under the same number of incoming transaction. Observing the peak value for delayed mining, system was operating at a frequency of 28 transactions per second i.e. in this case, a single voting transaction took 0.035 seconds (on average) to be mined. On the contrast, when mining capability (i.e. mining diversity) was increased from 30 percent to 60 percent, the three added mining nodes confirmed the incoming transactions more quickly and moved the transaction confirmation rate to 30k per second, eventually making a single transaction to wait for 0.033 seconds only.

Figure 10 shows clearly that increased scalability (in terms of incoming transactions) with reduced mining capability, gradually tends to open up the time-window for confirming transactions. Fig. 10 shows the state of the system when it is being flooded with thousands of transactions from seven different JSON based RPC remote clients. It can clearly be seen that increasing the scalability of the system would result in decreasing the transaction throughput. The effect is likely to be more obvious (and may result towards the motivation of attack as the

transactions start to take more time to get into the block and thereby creating a time-window to place malleable transactions within the unconfirmed transaction mining pool) if the hashing power of miners is not adequate with respect to the rate of incoming transactions.

Now we will show and discuss the result of transaction malleability attacks which have been carried out against delayed and without delayed mining. Figure 7 and Fig. 8 highlight output of failed and successful transaction malleability attack at real time using our proposed algorithm in Fig. 1. This helped us to finally investigate how scalability impacts transaction malleability attack. Our focus was to investigate how this time-window can be critical as an added advantage to let the attacker's version of transaction (malleable transaction) win race against its actual version of transaction. Figure 12 displays the results for the experimentation performed in Fig. 7 and Fig. 8. In this case, the time window may impact as a network latency. Analysing Fig. 12, we may infer that blockchain networks which are operating under delayed mining are more vulnerable to transaction malleability attack against the networks which have relatively higher mining diversity provided both the networks have been experiencing higher incoming rate of transactions. Fig. 12 shows the selected individual transactions (for successful transaction malleability attack) which were able to be picked up from unconfirmed mining pool and entered into the blockchain. Here, it is evident that under the same experimental conditions but with minor variation in connectivity strength (as shown in Fig. 13), the chain is more vulnerable to transaction malleability attack under delayed mining. Here, 5 out of approximately 100,000 transactions (50 percent of which were malleable through programmatically controlled JSON based RPC clients Fig. 7 and Fig. 8) were able to get their way into the block.

VIII. CONCLUSION

The paper empirically investigates and proves that delayed mining can certainly be a real big threat for blockchain based applications against transaction malleability attack. By observing our findings, (Fig. 9, Fig. 10, and Fig. 11) it may be inferred that delayed mining can increase the mining time of transaction (possibly due to network delay of remote clients and building up of queue for unconfirmed transactions in mining pool) and therefore not only opens up the attack window but also reasonably increases chances for carrying out a successful transaction malleability attack upon scaling.

FUNDING

This research received no external funding.

CONFLICT OF INTEREST

The authors declare that there is no conflict of interest.

REFERENCES

[1] J. Gobel, H. Keeler, A. Krzesinski, and P. Taylor, ¨ "Bitcoin blockchain dynamics: The selfish-mine strategy in the presence of propagation delay," Performance Evaluation, vol. 104, pp. 23 – 41, 2016. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S016653161630089X

[2] M. Rosenfeld, "Analysis of hashrate-based double spending," 02 2014.

[3] J. P. J. S. Kadam, M., "Double spending prevention in bitcoins network," International Journal of Computer Engineering and Applications, 2015.

[4] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," Cryptography Mailing list at https://metzdowd.com, 03 2009.

[5] B. J. F. E. M. A. Narayanan, A. and S. Gold, Bitcoin and Cryptocurrency Technologies,. Princeton, 2015.

[6] D. Kraft, "Difficulty control for blockchain-based consensus systems," Peer-to-Peer Networking and Applications, vol. 9, 04 2015.

[7] J. Yli-Huumo, D. Ko, S. Choi, S. Park, and K. Smolander, "Where is current research on blockchain technology?—a systematic review," PLOS ONE, vol. 11, no. 10, pp. 1–27, 10 2016. [Online]. Available: https://doi.org/10.1371/journal.pone.0163477

[8] K. M. Khan, J. Arshad, and M. M. Khan, "Secure digital voting system based on blockchain technology," Int. J. Electron. Gov. Res., vol. 14, no. 1, pp. 53–62, Jan. 2018. [Online]. Available: https://doi.org/10.4018/IJEGR.2018010103

[9] A. Kiayias and M. Yung, "Self-tallying elections and perfect ballot secrecy," in Public Key Cryptography, D. Naccache and P. Paillier, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2002, pp. 141–158.

[10] F. Hao, R. P. Y. A., and P. Zielinski, "Anonymous voting by two-round public discussion," IET Information Security, vol. 4, no. 2, pp. 62–67, 2010.

[11] K. Dalia, R. Ben, P. Y. A, and H. Feng, "A fair and robust voting system by broadcast," in 5th International Conference on E-voting, 2012.

[12] D. Chaum, A. Essex, R. Carback, J. Clark, S. Popoveniuc, A. Sherman, and P. Vora, "Scantegrity: End-to-end voter-verifiable optical- scan voting," IEEE Security Privacy, vol. 6, no. 3, pp. 40–46, 2008

[13] S. Shahandashti and F. Hao, "Dre-ip: A verifiable e-voting scheme without tallying authorities," vol. 9879, 09 2016, pp. 223–240.

[14] D. Chaum, "Secret-ballot receipts: True voter-verifiable elections," IEEE Security Privacy, vol. 2, no. 1, pp. 38–47, 2004.

[15] "Untraceable electronic mail, return addresses, and digital pseudonyms," Commun. ACM, vol. 24, no. 2, pp. 84–90, Feb. 1981. [Online]. Available: http://doi.acm.org/10.1145/358549.358563

[16] D. Chaum, P. Y. A. Ryan, and P. Y. A. Schneider, "A practical voter verifiable election scheme," in 10th European Conference on Research in Computer Security, ser. ESORICS'05. Springer-Verlag, 2005, pp. 118–139

[17] A. B. and R. L. Rivest, "Scratch & vote: Self-contained paper-based cryptographic voting," in 5th ACM Workshop on Privacy in Electronic Society, ser. WPES '06. New York, USA. ACM, 2006, pp. 29–40.

[18] J. M. Bohli, J. Muller-Quade, and S. Rohrich, "Bingo voting: Secure and coercion- free voting using a trusted random number generator," in 1st International Conference on E-voting and Identity, ser. VOTE-ID'07. Berlin, Heidelberg. Springer-Verlag, 2007, pp. 111–124

[19] B. Adida, "Web-based open-audit voting," in 17th Conference on Security Symposium, ser. SS'08. Berkeley, CA, USA: USENIX Association, 2008, pp. 335–348

[20] F. Hao, M. N. Kreeger, B. Randell, D. Clarke, S. F. Shahandashti, and P. H. J. Lee, "Every vote counts: Ensuring integrity in large-scale electronic voting," in 2014 Electronic Voting Technology Workshop/Workshop on Trustworthy Elections (EVT/WOTE 14).

[21] S. e. a. Bell, "Star-vote: A secure, transparent, auditable, and reliable voting system," in 2013 Electronic Voting Technology Workshop/Workshop on Trustworthy Elections (EVT/WOTE 13). USENIX Association, 2013

[22] D. Sandler, K. Derr, and D. S. Wallach, "Votebox: A tamper-evident, verifiable electronic voting system." 01 2008, pp. 349–364

[23] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: A survey," International Journal of Web and Grid Services, vol. 14, p. 352, 10 2018

[24] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in 2017 IEEE International Congress on Big Data (BigData Congress), June 2017, pp. 557–564

[25] X. Xu, I. Weber, M. Staples, L. Zhu, J. Bosch, L. Bass, C. Pautasso, and P. Rimba, “A taxonomy of blockchain-based systems for architecture design,” 04 2017.
[26] M. Vukolic, “The quest for scalable blockchain fabric: Proof-of-work vs. ´ bft replication,” in Open Problems in Network Security, J. Camenisch and D. Kesdogan, Eds. Cham: Springer International Publishing, 2016, ˇ pp. 112–125
[27] K. M. Khan, J. Arshad, and M. M. Khan, “Empirical analysis of transaction malleability within blockchain-based e-voting,” Computers & Security, vol. 100, p. 102081, 2021
[28] Multichain. Open platform for blockchain applications. [Online]. Available: www.multichain.com
[29] K. M. Khan, J. Arshad, and M. M. Khan, “Investigating performance constraints for blockchain based secure e voting system,” Future Generation Computer Systems, vol. 105, pp. 13 – 26, 2020.