Blockchain Attacks, Analysis and a Model to Solve Double Spending Attack

A. Begum, A. H. Tareq, M. Sultana, M. K. Sohel, T. Rahman, and A. H. Sarwar

Abstract—**Blockcahin is such a technology that helps us to use a shared ledger. Although the ledger is in shared manner, the total system is quiet secure. Bitcoin is a crypto currency which uses blockchain technology. Value of blockchain is very high than dollar or some other expensive currency. This is one of the reasons of encouraging theft attack on the blockchain technology. In this paper, we want to show the attacks on blockchain, their targeted area, reason and their possible proposed solution as review. Besides this, Double spending attack is a major attack on blockchain which is occurred twice till now and caused a huge loss of crypto currency. In this paper, we also want to represent the reasons of these attacks and propose one solution that can prevent Double Spending Attack. Our findings will provide some future direction for new researchers and also help the crypto business analysts to predict about present security in the aspects of blockchain network.**

Index Terms—**Blockchain, bitcoin, attacks, double spending attack & solutions.**

I. Introduction

There are a lot of researches occurred in various section of computer attack [1],[2]. We have got the first concept about Blockchain and Bitcoin from a published paper of “Sathoshi Nakamoto” named as “A peer to peer electronic cash system”. Blockchain as a secure ledger is the current digital platform and takes attention to it academically and industrially. In 2015 and 2016 Bitcoin was the best performing currency [3] but in 2017 ripple reach to best position [4]. It is used in Transportation and data management system this transaction allows for decentralized, immediate and dependable, and there is no need of third party, such as dealer negotiator, etc. Consensus mechanism is making this network more secure [5]. Though it is a secure system, but due to some vulnerability a huge number of Bitcoin is stolen from 2010 to 2018. In the first six months of 2018 micro researcher detect more than 787000 of malicious crypto currencies mining software [6]. In May and June 2018 Double spending attack occurred which was constructed by equihash algorithm and effect on POW consensus mechanism. By this attack $18.6 million US bitcoin was stolen [7]. So, we keep our focus on bitcoin security, their risk, real attack, loss, effect and countermeasures. In this research, we have divided our work into two parts. First of all, we will complete our work with the review of Blockchain attack which is shown in “Result and Discussion part” depending on our data collection from research papers and some official web links. Then as per our target, in section ‘V’ we have discussed the general process of Double Spending Attack and its existing solution. Then in the section ‘VI’ we have given our proposed model solve the problem of first solution of Double Spending Attack. In “Result and Discussion” part we also showed the Discussion of our proposed model.

II. Backgroudn Study

We have studied more than 59 research papers and web links to find out the data about Bloackchain Attacks and their solutions. We also look at the general research confirmation [8]. In Table I we have shown the types, examples and Transection mediums that we have find out.

TABLE I: Various Type of Blockchain Network

Type	Examples	Transaction medium
Blockchain 1.0	Financial transaction	Bitcoin
Blockchain 2.0	Facilitation, verification, enforcement	Ethereum
Blockchain 3.0	Decentralized storage and communication	Ethereum storage
Blockchain 4.0	Making Blockchain technology useable to industry 4.0 demands	

TABLE II: Consensus Types and Their Marked Capitalization of Various Kinds of Crypto Currencies

Name of Crypto	Consensus	Market cap
Bitcoin	Pow	$71,890454,161
Ethereum	Pow	$12,092,653,223
Ripple	Ripple protocol	$14,796,628,442
Bitcoin cash	Pow	$3,023,721,859
Steller	Steller consensus	$3,121,437,638
Litecoin	Pow	$1,990,487,368
Cardano	Pos	$1,066,100,559
EOS	Pos	$2,660,752,236

A block is a size number to specify how much data is coming next. It is composed of a header and a long list of transactions as shown in Fig. 1. In the Table II we have listed types and their market capitalization and the market value of crypto currencies at December, 2018 are shown in table 3 [9]. Table III represents the market value of bitcoin at different time. From the data we can see that bitcoin is very expensive and at February 2018 is was very expensive.

Manuscript received May 13, 2019; revised January 22, 2020. This work was supported in part by the Daffodil International University, Department of Software Engineering.

The authors are with the Daffodil International University, Dhaka, Bangladesh (e-mail: afsana.swe@ diu.edu.bd, tareq677@diu.edu.bd, mahmuda667@diu.edu.bd, khaledsohel@daffodilvarsity.edu.bd, tasnim.swe@diu.edu.bd, afjal.swe@diu.edu.bd).

doi: 10.18178/ijmlc.2020.10.2.942

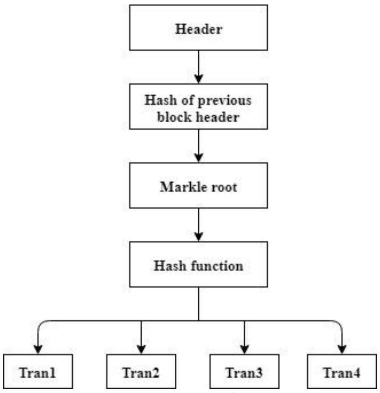

Fig. 1. Structure of a block.

TABLE III: MARKET VALUE OF BITCOIN IN DIFFERENT TIME (FROM STARTING TO RUN TIME)

Date	Value of Bitcoin in Us $
Jan 2009	0.00
July 2010	0.08
Feb 2011	1.00
July 2011	31.00
Dec 2011	2.00
Dec 2012	13.00
April 2013	266.00
June 2013	100.00
Jan 2014	800.00
April 2014	440 – 630
March 2015	200 – 300
June 2016	450 – 750
Jan 2017	800 – 1150
Sept 2017	5000
Dec 2017	17900
Feb 2018	6300
Nov 2018	3778

III. LITERATURE REVIEW

We go through at most 80 papers/web links to find out the attacks that already happened on the Blockchain network. We found 19 different attacks as follows:

1) Spam Attack: A spam attack effects a committed transaction by slowing the network and making the block creation delay [10]-[13].

2) Double Spending Attack: Double spending attack refers to that a different number of transactions occurred where the crypto currencies are same [14], [15].

3) Eclipse Attack: To enlarge and store information about other peer, a node chooses eight peers randomly in a network and eclipse attack invasions on that node to take benefit from peer-to-peer (P2P) network [16].

4) Time Jacking Attack: Time jacking attack may divide the network into various parts [17], [18].

5) Finney Attack: If, vendor confirms the transaction only once then the Finney attack occurs [19].

6) DAO Attack: The DAO stand for "Decentralized Autonomous Organization'' [20], [21].

7) Brute- Force Attack: A Brute-force attack is used to collect secret information [22]-[25].

8) Sybil Attack: In Sybil attack the attacker makes many pseudonymous identities in peer to peer network by hijacking an insecure computer. Here, an attacker presents these identities in distinct node [26], [27].

9) Targeted DDOS Attack: Targeted DDOS attack relates to overflowing the network with more info in a procedure it develops an insensible exploit [28].

10) Block withholding Attack: In General Block withholding attack formed a block mining by few pool components but they don't express any blocks [29].

11) Nothing at Stake Attack: Debut of proof of stake, a big element of the crypto group was hesitant that is just a liability for sign and plenty of obstacles misconduct manner [30].

12) The Long Range Attack: In Long range attack, the history of blockchain is modified by a fork which is already exists in a current block [30], [31].

13) Research Gap: In the aspect of Blockchain, as there are a lot of attacks had happened, and for beginners if anyone wants to know the all attacks in a link, then he or she feel difficulties to get all the information at a glance. It motivates us to write a review paper. Moreover, our target was to also list down all the possible solution. As Double Spending attack was occurred several times, there is a solution of this attack. So here is a gap that we can propose a new model so that we can reduce the chance to occur this attack.

IV. METHODOLOGY

In this paper as our first target was to create a complete review of blockchain so that researcher can get a proper review about blockcahin at a glance, so we have created our dataset from more than 70 web links and research papers. By analyzing these data manually, we have created Table IV to get a review. Each and every attack was occurred to the intention of money theft. We have also found the total amount of currency loss due to different attacks, which is shown in Table V. Then by using excel we have uploaded our data and find out some result such as, in which year how much attacks were happened as shown in Fig. 3, year wise crypto currency hacked in Fig. 4, how many times network was hacked in Fig. 5. By analyzing our data, we have also shown the date wise stolen amount with different network name, as shown in Table VI.

In this research, our target was to ensure more security of blockchain network. As Double Spending attack occurs several times after implementing one solution. We have analysed the fault with the existing procedure and proposed a hypothetical solution of this vulnerability, as shown in Section VI.

V. DUBLE SPENDING ATTACK EXISTING PROCESS

To reach our goal at first we need to understand how Double Spending attacks had happened. There are five stages that represents how a double spends occur.

Stage 1: Block adding process. At first user sign off and request for transaction through their user wallet. This unconfirmed transaction takes place in a pool of unconfirmed transaction from where the miner picks transactions and solve complicated mathematical problem through POW consensus to get hash output as unique one and broadcast them to add the block to blockchain. If other miners verify these hashes, only then, the block will be added.

Stage 2: As long as the good miners verify the block and the block is being added to the real blockchain, on that time the corrupted miner starts his own chain with the verified block. This time corrupted miner spends all his currency and sends this information to the real blockchain but not to his own isolated chain.

Stage 3: In this stage the corrupted miner picks transactions and add block to his isolated chain by verifying them by him with strong computational power faster than the good miners add block to the real blockchain.

Stage 4: The corrupted miner broadcast isolated blockchain's transaction to the real blockchain when isolated chain is larger than the real one and the miner of real chain try to add their block to the isolated one.

Stage 5: The democratic governace rule states that the blocks will add to the larger one by reemoving the previous records that they have. As the real blockchain's block had the information about the transaction where the corrupted miner spent his currency but the isolated one don't know about the transaction. So, when the blocks try to add the isolated chain then they would remove the previous transaction informatin. So, in the new isolated chain, the corrupted miner would be able to spend all of the currencies that he had spent once in the real blockchain.

VI. Proposed Model for Double Spending Attack

As we stated before, double spending problem starts in stage (3), when the corrupted miner starts to make his chain larger than the real blockchain with his strong computational power. Suppose, a corrupted miner M1 spends all his bitcoins (B1) to purchase a product from vendor V1. This corrupted miner adds this transaction to his block and spread the information to the real blockchain and other miners of the real blockchain verified this transaction, but this corrupted miner does not add the transaction T1 to his own isolated chain. As a result, the owner of the block in isolated chain does not know about the transaction T1.

When the corrupted miner would be able to make his chain larger, than, to the real chain, on that time, would spread information about a transaction to the real blockchain that exists in the isolated one. When the miner would go to verify the transaction, then miner will find that, the isolated chain is larger.

As democratic governance protocol rules, the larger chain will be defined as real and miner from the smallest one would like to add in the larger one by removing their previous record and update the information according to the new chain.

That means, as the block in isolated chain and does not have the information about transaction T1, but real blockchain blocks have, so when the old block add to the new chain, that time they would remove the information about transaction T1. That is how the corrupted miner would be able to spend the bitcoin B1 that has already been spent. To solve this problem when the block tries to add the new chain, on that time if a block does not remove its previous memory, rather updates its information with keeping the previous one.

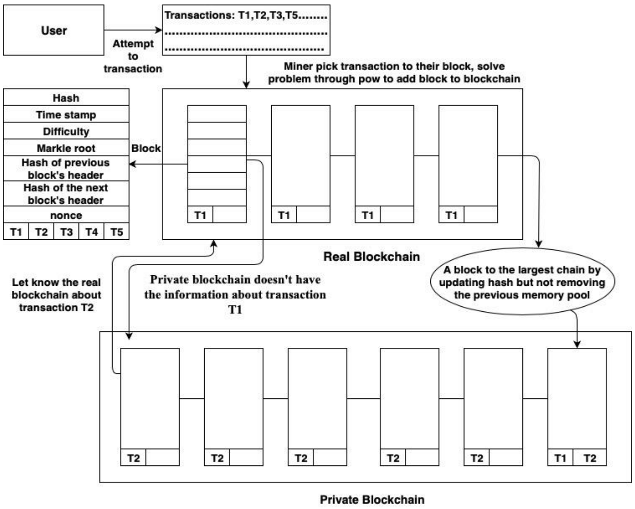
User
Attempt to transaction
Transactions: T1,T2,T3,T5........
Miner pick transaction to their block, solve problem through pow to add block to blockchain
Hash
Time stamp
Difficulty
Markle root
Hash of previous block's header
Hash of the next block's header
nonce
T1 T2 T3 T4 T5
Block
T1
T1
T1
T1
Real Blockchain
Let know the real blockchain about transaction T2
Private blockchain doesn't have the information about transaction T1
A block to the largest chain by updating hash but not removing the previous memory pool
T2
T2
T2
T2
T2
T1 T2
Private Blockchain

Fig. 2. Proposed model to overcome the double spending problem.

By following our proposed rule, whenever a block from smaller chain would add to the isolated chain, which has the hash of transaction T1, it updates its transaction information with keeping previous one. That means if isolated one has the transaction information T2, T3, when block A would add to isolated chain who has the information T1, after being added it would have the information about T1, T2 and T3 and beside it will also spread the information of T1 to the new chain. Thus, if one transaction has ever been occurred, will be recorded permanently, and all of the blocks of chain would have the information about all transaction. The combined process of our proposed model is shown in Fig. 2.

TABLE IV: Attack Date and Their Losses the According Attack

No	Attack Name	Attack Time/Date	Currency loss due to attack
1.	Wallet Attack	2013, 2016	US $70 million [32], [33]
2.	Double Spending Attack	March 2013 , 2018	Rapidly drop off bitcoin prices, US $175 million [34]
3.	BGP Hijacking	2014	US $83000 [35]
4.	Spam Attack	2015 to 2017, 2018	Effect on 80000 transactions [36]
5.	Dao Attack	28th may 2016	US $60 million
6.	DDOS Attack	16 times in 2016, 2017	Staminus network down for 20 hours, peaking at over 650 Gbps US $123000 [37]
7.	Selfish Mining Attack	May 2018	US $90,000 [38]

VII. Result and Discussion

From our data set we have found 15 different attacks during this survey where 4 attacks are "POW consensus based". These 4 attacks are double spending attack, Finney attack, brute force attack and block withholding attack. Five attacks of these attacks targets on network, three are on blocking protocol and the others are on computing power as well as database. In Table VI, the survey results are given. We also find out the targeted area for each attack so that a researcher can easily find out the category of a specific attack. Table IV also shows the effects of all specific attacks and their countermeasure that was proposed by various researchers as we found from our survey.

From these above 15 attacks, we found only seven attacks that occurred in several time.

Table V shows the date or time and the total amount of losses due to the attacks. Wallet Attack, Double Spending Attack, DDOS Attack, BGP Hijacking, Spam Attack, Dao Attack, Selfish Mining Attack all are the attacks that occurs from 2 to 16 times and causes a loss of dollars from US$70 to US $123000 as shown in the Table V. The entries are total up to 818,485.77 stolen Bitcoins, presently worth like USD 502,081,166.11. [39].

TABLE V: ATTACK NAME, THEIR TARGETED AREA OF ATTACK, EFFECT FOR THE ATTACH AND POSSIBLE COUNTERMEASURES FROM SURVEY

No	Attack Name	Targeted Area	Effect of Attack	Possible Countermeasure found
1.	Brute Force Attack	Computing Power, Pow Consensus	Data encryption	inserting observers in the network, notify the merchant about an ongoing double spend[40]
2.	Refund Attack	Payment protocol	Lose money, reputation	publicly verifiable evidence[41][42]
3.	Wallet Attack	Private key	Lose of bitcoin	threshold signature based two-factor security, hardware wallets [43], Password-Protected Secret Sharing (PPSS)[44]
4.	Time Hijacking Attack	Network	Fake peers	constraint tolerance ranges, network time protocol (NTP) or time sampling on the values received from trusted peers [45]
5.	Long Range Attack	Database[	Alter transaction history	Nodes trust identity provider, implementation of trusted hardware[46]
6.	BGP Hijacking	Database, Protocol	Fake transaction	Human driven process consisting of altering configuration or disconnecting the attacker.[46]
7.	Sybil Attack	Network	Pseudonymous identities, threatens user privacy	Xim (a two-party mixing protocol)
8.	DDOS Attack	Network	Generates huge unnecessary responses about transaction	Proof-of-Activity (PoA) protocol[47]
9.	Eclipse Attack	Network	inconsistent view of the network and blockchain	Use whitelists, disabling incoming connections[47],[48]
10.	DAO Attack	Computing Power	Fake transaction	Hard fork proposal, Soft fork proposal [49]
11.	Nothing at Stake Attack	Block	Slow consensus time	Slasher Protocol [50]
12.	Pool Mining Attack	Block, Computing Power	Slow verification time, fake transaction	Not Found
13.	Double Spending Attack	Bitcoin transaction, Pow Consensus	lose products, create forks	Recipient oriented transaction[51]
14.	Selfish Mining Attack	Block, Computing power	Increase personal share on transaction	Address bitcoin protocol and raise threshold, computing branches are same length and propagate all of them, Zero Block technique[52]
15.	Spam Attack	Network	Slow transaction, network and computing Power	permanent nominal transaction fee [53]

Moreover, we have calculated the total number of attacks occurred in Blockchain Network are shown in Fig. 3. It shows that in 2016 four different attacks were happened, in 2018 three attacks, in 2013 and 2017 two attacks, in 2012 and 2015 one attack were happened. In Fig. 4, we can see the stolen amount of bitcoin with respect to year. Here we can see that in 2014 suddenly the stolen amount was too high, 850000 bitcoins. Moreover, we can also see that bitcoins stolen are happening as a regular basis. Table VI shows our findings on date wise stolen amount in various networks. From this table we can state that, hackers are trying to attack in different aspects of network.

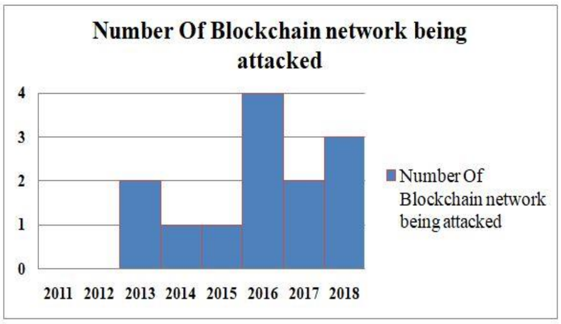

Fig. 3. Number of blockchain network being attacked yearly from 2011 to 2018.

TABLE VI: THE STOLEN AMOUNT WITH DATE AND HACKED NETWORK NAME

Date	Stolen amount	Blockchain Network
June 2011	16,120 bitcoins worth $500,000	Allinvain[54]
August 2011	Wallet service was disappeared	Mybitcoin[54]
March 2012	46,703 bitcoin	Linode user[54]
May 2012	18,000 bitcoin	Bitcoinica[54]
September 2012	24,000 bitcoin	Bitfloor[54]
February 2014	850,000 bitcoins	collapse of Mt. Gox[54]
January 2015	19,000 bitcoins	Bitstamp[54]
August 2016	102,666 bitcoins worth $77 million	Bitfinex[54]
2013	1000 bitcoins worth $100,000	WIRED [55]
March 2014	100,000 bitcoins	Poloniex [56]
2017	240,000 bitcoins worth $1.2 billion [57]	
First half of 2018	174,603 bitcoins worth $1.1 billion [58]	
September 2018	5966 bitcoins	Japan based cryptocurrency exchange [59]

Moreover, as hackers always target to different networks.

In Fig. 5 we can see that in 2012 three networks had been affected. In 2011, 2013, 2014 and 2018 2 different networks were attacked by attacker. In 2015, 2016 and 2017 only one network was affected by the attacker. After analyzing all our data, we can conclude that 33% attackers target on network protocol, 26% on computing power mechanism and 20% on block history. Moreover, we found within these 15 attacks 85% on them are on POW based consensus.

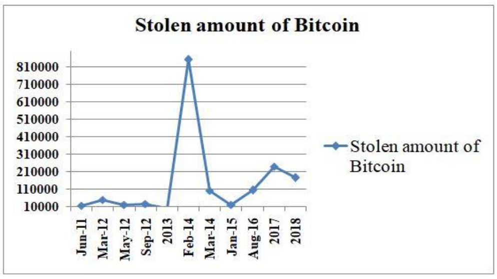

Fig. 4. Stolen amount of bitcoin in with respect to time.

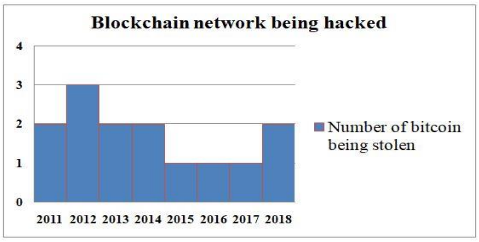

Fig. 5. Number of blockchain network being hacked to steal bitcoins from 2011 to 2018.

Bitcoin stole rate was high at the first period of blockchain history (in year 2011- 2014) and protocol targeted attack happened frequently in the recent years (2016 – 2018), even in 2016- 4 different types of attacks happened and only DDOS attack hit 16 times on blockchain network.

Again, we have shown our proposed model in Section V where we have discussed how double spending attack may be prevented with a simple changing in governance protocol. We have constructed only the hypothesis of the proposed model. Due to lack of fund we could not implement it in the real world. Ccb18628344470

VIII. Conclusion and Future Work

We have shown a survey on blockchain, its attacks, and their solutions as described before. We have analyzed the affected area and conducted area, and also we have analyzed double spending attack. After showing the limitation of Double Spending Attack, we have provided a possible solution. We make a pattern of real attacks on blockchain. It will help new researcher in this area. On the other hand, if we can gather fund and implement our proposed model in real world, it could protect our bitcoins form Double Spending Attack.

In this paper, we had some limitations also. We have studied 70 to 80 resources, if we used more sources then it could happen that there may add some more information. Besides this, we have proposed a solution model of double spending prevention, but due to lack of funding we could not prove it. Our future work will be collect fund and apply this model in real world so that we can strongly prevent Double Spending Attack.

Conflict of Interest

The authors declare no conflict of interest.

Authors Contribution

Begum and Tareq done literature review and find out research gap. Begum, Sohel and Sultana collected the data. Begum, Tareq, Sultana and Rahman analyze the data. Begum, Tareq, Sultana, Bhuiyan and Sarwar has written the paper.

References

[1] A. Begum, M. M. Hassan, T. Bhuiyan, and M. H. Sharif, 2016, “RFI and SQLi based local file inclusion vulnerabilities in web applications of Bangladesh,” in *Proc. International Workshop on Computational Intelligence (IWCI)*, Dhaka, Bangladesh, 2016, pp. 21-25.

[2] T. Bhuiyan, A. Begum, S. Rahman, and I. Hadid, “API vulnerabilities: Current status and dependencies,” *International Journal of Engineering and Technology*, vol. 3, pp. 9-13, 2018.

[3] Sophos. [Online]. Available: https://medium.com/@BambouClub/best-and-worst-performing-currencies-in-2015d1e62088bc29?fbclid=IwAR0IR7KZWvdk7QeLIFzt7W_1tynjAqUaoOQ5zHJdxSoahjs3RNrJ-thqg

[4] Quartz. [Online]. Available: https://qz.com/1169000/ripple-was-the-best-performing-cryptocurrency-of-2017-beating-bitcoin/

[5] D. K. Tosh, S. Shetty, X. Liang, C. Kamhoua, and L. Njilla, “Consensus Protocols for Blockchain-based Data Provenance: Challenges and Opportunities,” in *Proc. IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference*, New York, 2017.

[6] Coindesk. (2018). [Online]. Available: https://www.coindesk.com/

[7] H. Yan, R. Oliveira, K. Burnett, D. Matthews, L. Zhang and D. Massey, “BGPmon: A Real-Time, Scalable, Extensible Monitoring System,” *IEEE*, Washington, DC, USA, 2009.

[8] J. L. D. L. Rosa, V. Torres-Padrosa, D. Gibovic, and O. Hornyak, “A Survey of blockchain technologies for open innovation,” *Research Ghate*, 2017.

[9] L. Matsakis, “How WIRED lost $100,000 in Bitcoin,” *Wired*, 2018.

[10] L. Parker, “Bitcoin ‘spam attack’ stressed network for at least 18 months, claims software developer,” *Brave Newcoin*, 2017.

[11] NEO blockchain experiences transaction spam attack, *Neo News today*, 2018.

[12] Steemit. (2018). [Online]. Available: https://steemit.com/cryptocurrency/@superfreek/btc-spam-attack-200-000-unconfirmed-transactions-halts-bitcoin

[13] K. Nakayama, Y. Moriyama and C. Oshima, “An algorithm that prevents spam attacks using blockchain,” *IJACSA*, vol. 9, 2018.

[14] . D. K. Toshi, S. Shetty, X. Liang, C. A. Khamhua, K. A. Kwiat and L. Nijilla, “Security implications of blockchain cloud with analysis of block withholding attack,” *IEEE Press Piscataway*, USA, 2017.

[15] M. Rosenfield, *Analysis of Hashrate-Based Double-Spending*, Cornell University, 2014.

[16] Y. Marcus, E. Heilman, and S. Goldberg, “Low-resource eclipse attacks on ethereum’s peer-to-peer network,” *IACR Cryptology ePrint Archive*, 2018.

[17] Culubas. Blogspot. (2011). [Online]. Available: http://culubas.blogspot.com/2011/05/timejacking-bitcoin_802.html

[18] M. Apostolaki, A. Zohar, and L. Vanbeber, “Hijacking bitcoin: Routing attack on bitcoin,” *IEEE*, San Jose, CA, USA, 2017.

[19] Topic: ZNCoin[Secured-Fast-Untraceable][Platforms][POS 60%][NO ICO][AIRDROP][BOUNTY] (Read 4655 times), "Bitcointalk". Bitcoin Forum. (2018). [Online]. Available: https://bitcointalk.org/index.php?topic=4437539

[20] X. Zhao, Z. Chen, X. Chen, Y. Wang, and C. Tang, “The DAO attack paradoxes in propositional logic,” *ICSAI*, Hangzhou, China, 2017.

[21] SLOCK.IT. (2018). SLOCK. [Online]. Available: https://slock.it/

[22] Medium. (2018). Upright. [Online]. Available: https://medium.com/@UnibrightIO/blockchain-evolution-from-1-0-to-4-0-3fbdbccfc666

[23] Techopedia. (2018). [Online]. Available: https://www.techopedia.com/definition/18091/brute-force-attack

[24] J.-S. Cho, S.-S. Yeo, and S. K. Kim, "Securing against brute-force attack: A hash-based RFID mutual authentication protocol using a secret value," *Elsevier*, vol. 34, no. 3, pp. 391-397, 2011.

[25] M. Conti, S. Kumar, C. Lal and S. Ruj, A survey on security and privacy issues of Bitcoin," *IEEE*, vol. 20, no. 4, pp. 3416-3452, 2018.

[26] G. Bissias, A. P. Ozisik, B. N. Levine, and M. Liberatore, "Sybil-resistant mixing for Bitcoin," *ACM*, New York, USA, 2014.

[27] Torproject, Tor. (2018). [Online]. Available: https://blog.torproject.org/tor-security-advisory-relay-early-traffic confirmation-attack

[28] R. R. O'Leary, "Bitcoin gold website down following DDoS attack," *Coindesk*, 2017.

[29] D. K. Tosh, S. Shetty, X. Liang, C. A. Kamhoua, K. A. Kwiat, and L. Njilla, "Security implications of blockchain cloud with analysis of block withholding attack," *IEEE Press Pisctaway*, Madrid, Spain, 2017.

[30] W. Li, S. Andriena, J.-M. Bohli, and G. Karamme, *Securing Proof-of-Stake Blockchain Protocols*, Springer, pp. 297-315, 2017.

[31] E. Deirmentzoglou, "Rewriting history: A brief introduction to long range attacks," *Positive*, 2018.

[32] Bitcoin. (2018). [Online]. Available: https://en.bitcoin.it/wiki/July_2015_flood_attack

[33] K. Karagiannis, "Hijacking Blockchain," *RSA*, 2017.

[34] E. Bonadonna, *Bitcoin and the Double-Spending Problem*, Cornell University, 2013.

[35] A. Toonk. Bgmon. [Online]. Available: https://bgpmon.net/bgp-routing-incidents-in-2014-malicious-or-not/

[36] Bitcoin. [Online]. Available: https://en.bitcoin.it/wiki/July_2015_flood_attack

[37] T. B. Lee, "Arstechnica," *Technica*, 2017.

[38] W. Zhao, "Crypto exchange zaif hacked in $60 Million Bitcoin Theft," *Coindesk*, 2018.

[39] Cloudflare. [Online]. Available: https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/

[40] T. Bamert, C. Decker, L. Elsen, R. Wattehofer and S. Welten, "Have a snack, pay with bitcoins," *IEEE*, Trent, Italy, 2013

[41] P. Mecorry, S. F. Shahadashti, and F. Hao, "Refund attacks on bitcoin's payment protocol," *Springer Link*, 2017.

[42] E.-R. Latifa, E. K. M. Ahemed, E. G. Mohamed, and A. Omar, "Blockchain: Bitcoin wallet cryptography security, challenges and countermeasures," *JIBAC*.

[43] T. Bamert, C. Decker, R. Wattenhofer, and S. Welten, "Bluewallet: The secure bitcoin wallet," *Springer Link*, vol. 8743, pp. 65-80, 2014.

[44] S. Jarecki, A. Kiayias, H. Krawczyk, and J. Xu, "Highly-efficient and composable password-protected secret sharing," *IEEE*, Saarbrucken, Germany, 2016.

[45] D. Mills, J. Martin, J. Burbank, and W. Kasch, "Network time protocol version 4: Protocol and algorithms specification," *IETF*, 2010

[46] A. Gkaniatsou, M. Arapinis and A. Kiayias, "Low-level attacks in bitcoin wallets," *Spinger Link*, pp. 233-253, 2017

[47] Y. Marcus, E. Heilman, and S. Goldgberg, *Low Resource Eclips Attacks on Ethereum Peer-to-Peer Network*, 2018.

[48] JOE STEWART. Bravenewcoin. (2018). [Online]. Available: https://bravenewcoin.com/insights/bitcoin

[49] BENNETT GARNER. Coincentral. (2018). [Online]. Available: https://coincentral.com/sybil-attack-blockchain/

[50] Hackernoon. (2018). [Online]. Available: https://hackernoon.com/protocol-evolution-and-the-future-of-blockchain-governance-24ffd53c052b

[51] H. Lee, M. Shin, K. S. Kim, Y. Kang, and J. Kim, "Recipient-oriented transaction for preventing double spending attacks in private Blockchain," *IEEE*, Hong Kong, China, 2018.

[52] I. Eyal and E. G. Sirer, "Majority is not enough: Bitcoin mining is vulnerable," *ACM*, New York, USA, 2018

[53] Dave Gutteridge, "Japanese cryptocurrency monacoin hit by selfish mining attack," *CCN*, 2018.

[54] Arstechnica. (2018). Technica. [Online]. Available: https://arstechnica.com/tech-policy/2017/12/

[55] Andrew Quenston. (2018). Hacked. [Online]. Available: https://hacked.com/biggest-bitcoin-hacks-thefts-time/.

[56] CNBC. (2018). [Online]. Available: https://www.cnbc.com/2018/06/07/1-point-1b-in-cryptocurrency-was-stolen-this-year-and-it-was-easy-to-do.html

[57] BUSINESSINSIDER. (2018). [Online]. Available: https://www.businessinsider.com.au/how-many-bitcoins-have-been-stolen-2014-3

[58] REUTERS. (2018). [Online]. Available: https://www.reuters.com/article/us-crypto-currency-crime-idUSKCN1IP2LU

[59] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, *A Survey on the Security of Blockchain Systems*, ELSEVIER, 2017.

Afsana Begum was born in Bangladesh on January 1, 1991. She has completed her B.Sc in telecommunication and electronic engineering from Hajee Mohammad Danesh Science and Technology University, Dinajpur, Bangladesh at 2011. Then she has completed her maters in information technology from Institute of Information Technology, University of Dhaka, Bangladesh at 2015. Now she is working as a senior lecturer at Software Engineering Department, Daffodil International University, Dhaka, Bangladesh. Before that, she worked as a senior programmer in a software fir "Live Technologies".

A. H. Tareq was born in Sherpur, Mymensingh, Bangladesh on October 7, 1994. He has completed the B.Sc in software engineering from Daffodil International University, Dhaka. Besides, he received two other degrees, first one is Secondary School Certificate(SSC) from Saint Andrews High School Haluaghat, Mymensingh, the last one is Higher Secondary Certificate(HSC) from Najmul Smrity University College Nalitabari, Sherpur.

M. Sultana was born in Brahmanbaria, Bangladesh on February 6, 1994. She received her bachelor's degree (B.SC) in software engineering from Daffodil International University, Bangladesh in 2018. She completed higher secondary certificate (HSC) from Agricultural University College, Mymensingh, Bangladesh in science background in 2012.

M. K. Sohel was born in Mymensingh, Bangladesh in 1972. He received his M.S in management information system from Daffodil International University, Dhaka, Bangladesh in 2007. He pursued his B.Sc. (Hons.) in computing and information systems from London Metropolitan University, UK. Currently he is working as an assistant professor in the Department of Software Engineering under the Faculty of Science and Technology at the Daffodil International University, Dhaka, Bangladesh. His Research area includes RFID technology, computer networks, distributed database system, blockchain technology, information systems management. Mr. Mohammad is a member of Bangladesh Computer Society; member of Bangladesh AOTS Alumni Association. He took part in the International Conference on Cyber Security and Computer Science in 2018 in Karab ük University, Karab ük, Turkey and had been assigned as a session chair.

T. Rahman was born in Dhaka, Bangladesh on November 26, 1992. She has completed her bachelor and masters both in software engineering from Institute of Information Technology (IIT), University of Dhaka, Bangladesh in 2013 and 2014 respectively. She has also done a masters in innovative computing from the University of Buckingham, UK on 2018.

A. H. Sarwar was born in Bangladesh. He has completed his B.Sc in Software Engineering Department from Daffodil International University, Bangladesh. Now he is working as a research associate in Software Engineering Department from Daffodil International University, Bangladesh.