Bitcoin and Cryptocurrency in P2P network

Cryptocurrency is defined as securely exchanging virtual currency or transactions digitally and verify the transfer of funds, which operates independently of central authority. Virtual currencies like Bitcoin, altcoin, namecoin have become famous to send fast payment digitally. Bitcoin is the first most digital de-centralized peer-to-peer approach using cryptocurrency.

Bitcoin is an electronic payment system, a kind of virtual currency. It allows multiple peers to securely exchange information in form of electronic cash, which consist of simultaneously sending and receiving online payment without going to a central authority such as central bank or the government. It follows the P2P or peer to peer network architecture. The underlying P2P network must verify the network's integrity, transaction consistency in order for two network nodes to intermittently exchange currency.

The peer or Bitcoin users, also known as miners have a unique identification which is hidden using pseudonym (public keys) to form *bitcoin addresses[1]*. A *Pseudonym* is a base-58 encoding of hash of public key for bitcoin address. Pseudonym is similar to IP Address in real-world entity which uniquely identify the host. Since Bitcoin uses a P2P network, there is no centralized database that keep track of users pseudonym. Therefore, the bitcoins are stored into an electronic ledger (Block Chain) .Ledger is broadcasted on the entire network, in order to prevent cyber frauds such as double spending, 51% Attack, DDoS Attack. The Block-Chain[1] consist of entries in form of blocks which has a 80-byte block header and record set of legitimate transactions that are packed together. Bitcoins are also stored in Bitcoin Wallets. Now, bitcoins need to mined (extracted). But how? Let's discuss.

Bitcoin mining is performed to check everything is in the proper order. Mining is cumbersome process and hence raises many queries. How to verify that bitcoin users doesn't perform double spending?? How does network prevent other users from generating new bitcoins?? How to determine whether the blocks of data are valid or invalid?

The process of adding resource or transactions records into *shared electronic ledger* is called Mining. The miners need to solve a complex mathematical puzzle to get authority to publish a block in block-chain. The miners uses a cryptography to hash a block in block chain using SHA-

256, popularly known as *nonce* and if they are successful in mining blocks they get reward in form of new (mined) Bitcoins. The premium amount[4] for reward is 25 Bitcoins ($17,000), and this amount is portioned into half after every four years. Secure Hash Algorithms(SHA) are one way functions that is we cannot follow reverse-predict operation on the input from resulted outcome. The minimum rate between entering two consecutive block is 10 minutes/block and the network difficulty is altered after every two weeks (2,016 blocks) and also controlled by leading zeros in nonce. If nonce has increasing number of leading zeroes it increases the difficulty level of mining them. The mining platform was shifted from cost inefficient CPU to Graphic Processing Unit (GPU), and next was Field Programmable Gate Arrays(FPGA)[4], and lastly to ASIC. *Application Specific Integrated circuits (*ASIC) processors maximize the energy efficiency and implement reliable power delivery.

BITCOIN PEER-TO-PEER- NETWORK

Bitcoin users (peers) in the network are connected to other peers as shown in Fig 1 and they have a underlying TCP Channel which is unencrypted, i.e. without any authentication function in web of networks. Therefore, every user need to keep a record set consisting of Internet Protocol addresses associated with its neighboring nodes.

The protocol designed for Bitcoin restrict the volume of information transmitted by peers, as to avoid DoS Attack. It transmit legitimate transactions and block, on the other hand discard the illegitimate blocks. It applies a protocol in which every node has to keep a *penalty score* for every connection that is established in the network. Whenever the network detect the distorted message it inflates the penalty-score of connection .If penalty score reaches a value of 100,it prohibits the "disobedient" IP address for next 24 hours.

Bitcoin peers can be grouped into inbound connections (Servers) and not inbound connections (clients) that are behind Network Address Translation. Initially there were about 8,000 servers and 100,000 clients but now there are millions of peers (clients and servers). By default each peer has total 125 connections (8 outbound connections and 117 inbound connections). The 8 users to which client initiates connection is called entry-nodes whereas server can accept random number of total connections from one IP address till it reaches threshold. Let's discuss how bitcoins are exchange between bitcoin users and principles its clients and server have to follow to broad-cast their address and transactions.

Block Chain[1]: It consists of a series of blocks .Every block, contains transaction data and 80-byte Header field. Header consist of performing the 256-bit hash of last(previous) block B(j-1), time-stamp T(j) ,32-bit nonce N(j) ,difficulty parameter d(j) and hash of transaction data T X(j)

$$\mathbf{B(\,j) = SHA\text{-}256\ (\,SHA\text{-}256\ (\,B(j\text{-}1)\ \|\ T(j)\ \|\ TX(j) \| d(j)\ \| N(j) \| \,)))\ <\ function(d(\ j)).}$$

The d (j) must be greater than double hash of block header, which d(j) difficulty parameter and it is linear function. The benefit of block chain is that it offers **tamper-detection.** If intermediator tries to modify data in one of network nodes, then hash value changes and no longer consistent with hash value reported in hash pointer as shown in Fig 3. Therefore, bitcoin user who stores the most recent hash pointer, can validate the entire history of transactions made in bitcoin.

Address Propagation[1]: Each peer maintains record set consisting of addresses of other neighboring peers in web-network and every address has a time-stamp. Peers can broadcast address using ADDR messages and request addresses using GETADDR messages. There are two restriction on broadcasting address to its neighboring peers. First, the count of addresses in ADDR message of neighboring peer should never exceed 10. Secondly, the timestamp value must be less than 10 minutes. If both condition satisfy then address become reachable otherwise categorized as unreachable. Bitcoin users recognize IPv4, IPv6 and onion-cat addresses.

Bitcoin node perform hash of the following items: secret salt, address that will be forwarded, present day, and memory address of data structure. Then it make sure that hash remain same for the next 24 hours. The peers sorts the neighboring nodes according to calculated hashes and choose first entry node or two first entries, these nodes are also known as responsible nodes. In order to increase efficiency of system, peers randomly select one neighbor every 100 milliseconds, which become part of network nodes and added to queue for outgoing ADDR messages .This node is called Trickle node and mechanism is called Trickling as shown in Fig 2. This is similar to “optimistically un-choking” node in Bit-Torrent. Finally, peers receiving GETADDR messages, but sends back only 23% of total addresses and do not return more than 2500 addresses.

Transaction Propagation[1]: In order for a transaction to occur between two peers, Sender forwards an INVENTORY MESSAGE by performing hash function on the current transaction. On the other side, receiver carry out several validation checks on the transaction, if the transaction passes the validation test then it can request actual transaction by using command as GETDATA message. Sender replies in form of TRANSACTION message.

Possible Attacks in Bitcoins

Fast Payment Double Spending: Double Spending is an attack that consists in online payment to two distinct vendors with same bitcoins as shown in Fig 4.This is known as Cyber Fraud, hence one of the two transaction won't be legitimate and will be declined. But the vendors already have offered his service for free to the illegitimate client. The solution consist of long payments rather than fast payments. In case of long payment[2], the vendor has to wait for about an hour for the transaction to be assured positive and validated, so that vendor is confident about providing services to authorized clients. Hence double spending becomes impossible for long payments but fast payments bypass this validations and attack become possible.

In fast payments[2] (generally in few seconds), the vendor doesn't wait for validation of transaction and hence viable to double spending attack. Example for this is fast food restaurants, coffee shops .The cybercriminal can use the same bitcoins twice to pay two distinct sellers and receive two services before even one of the two payments is validated. Indeed, one possible high-risk attack[2] can be that the attacker tries to get his bitcoins back by sending a transaction to himself. We can say that if TR(x) denotes transaction from I to X and TR (I) denotes transaction from I to itself, then both have distinct destination but same source. In order to perform fast payment, the cybercriminal tries to spread TR (I) faster than TR(X) but the vendor should receive TR(X) before TR (I). If the vendor condition not satisfied, he will reject TR(X) and know that fallacy is being performed. Hence the cybercriminals have one or more Helpmate H, which are communicating using a secured channel (TCP) and are used as intermediators between I and X.I sends TR (I) to H and H broadcasts it into the network nodes. Hence X will indirectly receive TR(I) and will automatically rejects it .Hence the conclusion is that the more Helpmate's H the cybercriminal has, the easier is to perform TR(I). The solution is to accept fast payments only for small-scale money transfers and halt for few seconds to validate that same inputs arrive at node X.

51% Attack: If a single user controls the majority of network's hash-rate of mining, they would have total control of network's nodes and would modify the ledger (block-chain) as per their will. It is possible only when bitcoin user has high computational power .Example- Ghash.io has twice attacked the network's hashing algorithm and gain 42 percent access of the network. The owner nodes of 51% attack can carry out many risky tasks such as preventing random transaction to gain any confirmations, preventing bitcoin users to share addresses, reverse transactions leading to double spending, preventing other miners to mine new blocks. The solution to this attack is to perform Bitcoin's proof-of-work system, i.e. number of confirmation requirements can be increased. The more number of confirmations lead to larger number of transactions to be 'reversed' by the attacker. Therefore the time required to access the ledger (block-chain) increases and hence become more expensive to overtake the shared ledger.

Dos Attack (Denial of Service attacks): It consist of sending a large amount of data to a node such that node become so occupied that it cannot be able to process normal Bitcoin transactions [3]. It eventually lead to slow down the response time, leading to system crash because it cannot handle such large amount of data. The inventor of bitcoins-Santoshi suggested some techniques to prevent DoS Attack [3]. First, the transactions that are larger than 100kbytes should be declared as non-standard (rejected).Second, UXTO (Unspent Transaction Output Set) should only be stored in memory and all the remaining data should be stored on disk. Third, whenever client fetch transaction from disk to main memory, he should check that all inputs are not exhausted up till now.

Now a day, number of bitcoins users are increasing tremendously, hence the attackers and the network is becoming vulnerable to these attacks. There are various other attacks such as Wallet vulnerable to theft, packet sniffing, Sybil attack, illegal content in block chain, bugs, energy consumptions, coin destruction [7].

Conclusion

In this paper, I have summarized about Bitcoins. I discussed about 'how the bitcoins works and rules bitcoin users has to follow in order to broadcast their addresses and transactions'. I discussed various bitcoin terms such as Bitcoin Wallet, block chain, miners, mining bitcoins strategy, nonce, ledger .Then we discussed three rules for connection to Bitcoin clients: Block-Chain, Address Propagation, and Transaction Propagation. Finally, I outlined the various strategies that are adopted by attackers to unauthorized access to bitcoins for their own benefit .It consist of double spending fast payment, 51% Attack, denial of Service attack. While the network can be exploited due to small unnoticeable attacks but the ideal solutions can lead to preventing threatening attacks.

REFERENCES

1. Alex Biryukov and Dmitry Khovratovich, *Deanonymisation of Clients in Bitcoin P2P Network (*Luxembourg: University of Luxembourg, 2014), 1405.
2. Ghassan O. Karame and Elli Androulaski, Double Spending Fast Payments in Bitcoin (Switzerland: ETH Zurich, 2012*),* 906-917.
3. T. Neudecker and P. Andelfinger, *A simulation model for analysis of attacks on the Bitcoin peer-to-peer network* (Germany: University Munich, 2015) 1327-1332.
4. J. Barkatullah and T. Hanke, *Goldstrike 1: CoinTerra's First-Generation Cryptocurrency Mining Processor for Bitcoin*,(USA: ASIC Engineering Department ,2015),68-76.
5. Muhammad Aslam Zahid, *Bitcoins: Mining, Transaction, Security Challenges and Future of This Currency*, (Florida: Boca Roston, 2015), 192-250.
6. A. Biryukov and I. Pustogarov, *Bitcoin over Tor isn't a Good Idea*, (San Jose, CA, 2015)134.
7. Bitcoin wiki. "https://en.bitcoin.it/wiki/", 2014.

Bibliography

Biryukov, Khovratovich and Ivan Pustogarov. "*Deanonymisation of Clients in Bitcoin P2P Network"* .Luxembourg: University of Luxembourg, 2014, 1405

Karame, Androulaski, and Srdjan Capkun. *"Double Spending Fast Payments in Bitcoin"*. Switzerland: ETH Zurich,2012*)*,906-917

Neudecker, Andelfinger and H. Hartenstein, ," *A simulation model for analysis of attacks on the Bitcoin peer-to-peer network"* .Germany: University Munich, 2015. 1327-1332.

Figures

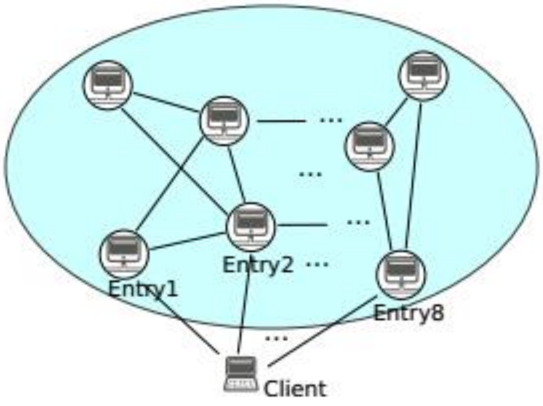

Figure 1: Bitcoin network

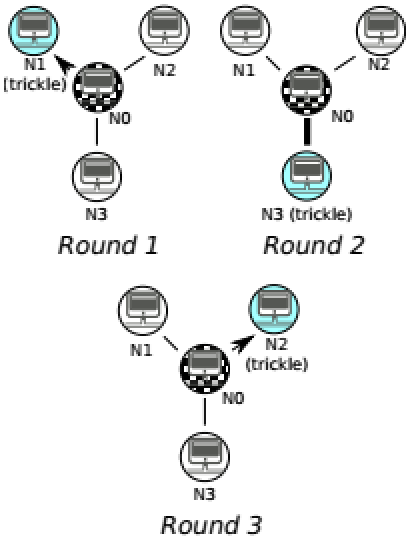

Figure 2: Trickling of ADDR messages

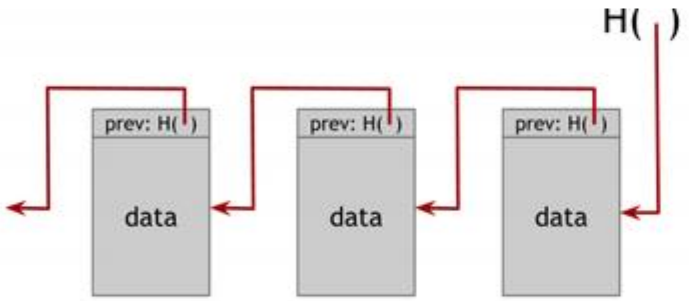

Figure 3 ***Block chain.*** A block chain is a linked list that is built with hash pointers instead of pointers.

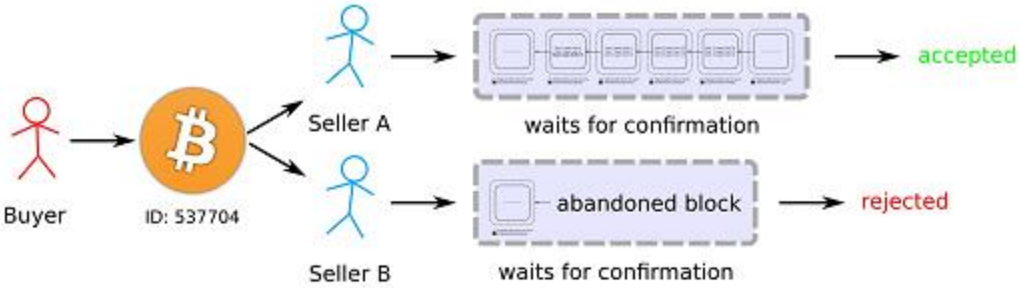

Figure 4: Sketch of a double spending attack