Task 1: Emerging Technologies Coursework

Charles Read | C1646151 CM3202

Introduction:

Bitcoin is built upon the blockchain architecture which is a distributed system with no centralised point of authority. Many crypto currencies have emerged from blockchain due to the many benefits of a having a system with no centralised functionality, these include security, anonymity, satiability and for economical reasons as the role of a 'middle-man' that could potentially take a cut from transactions doesn't exist.

Structure of Bitcoin

As I mentioned before, bitcoin has no centralised power that has more privileges than the rest of the nodes on the network. Instead of a bank or government holding information on everyone's transactions and identity, that information is given to all nodes on the bitcoin network, so each node will have all transactions that has ever happened as well as all user's identifier (their public keys).

Once a transition has taken place, for example person A has now received 3 bitcoin and person B has now lost 3 bitcoin, the transaction is broadcast across the world to all the nodes with many techniques used to ensure validity, integrity and security. Digital signatures are used to prevent malicious users/nodes fabricating transactions for their own gain. These digital signatures authenticate transactions, as each person on the bitcoin network has a unique public and private key that is computationally impossible to forge this making it impossible to forge or copy a transaction. The public keys for the digital signatures are used as the address for which to send bitcoin to.

Transactions are passed from node to node, however because of factors including latency and node failure, order is a concern as a new transaction arrival to a node may not necessary be the most recent. If this problem wasn't solved, double spending could occur as person A could spend their bitcoin twice and there would be no way to prove which transaction was first, e.g. a retailer could send out an item that wasn't paid for.

To solve the problems relating to order, bitcoin uses a block chain where nodes place unauthorized transactions into a pool which are then eventually placed into a block. Each block references the previous block by hashing the previous block's output with itself. These linked blocks that date all the way to the first set of bitcoin transactions in 2009. To find the next block in the chain, all the nodes make suggestions on the next block and one is selected at random via a race to solve a cryptographic hash puzzle.

A brute force solving technique is used by each node to find the solution to the hash and thus to nominate the next block in the chain. All the nodes processing power on the network are combined until some node eventually solves the hash and the new block is formed. A new block is formed every 10 minutes. Once the new block has been created and broadcast to the network, it's added to the block chain via it's hash being included. Each block references the block before it, making it a long chain of blocks with an order. Nodes that create the block are rewarded with bitcoin; this is called bitcoin mining.

More than one block chain branch could potentially be formed if two blocks were created at once. This would cause disagreement within the network, however, nodes always add blocks to the longest branch. Thus after a new branch/s is formed, it is unlikely another set of two or more blocks will be formed at the same time so one branch will once again be longer, leading to all nodes adding to that specific block chain.

Bitcoin node types

The majority of nodes on the bitcoin network are honest, meaning the person behind that node isn't trying to damage the system or gain anything maliciously for themselves for example, the double spend attack. An honest node will contribute to the network by receiving and sharing transactions and working towards the creation of blocks.

Rewards are given to honest nodes in the means of bitcoin payment. Node hosts are paid in bitcoin for each time they create a block that ends up on the long-term consensus branch. The reward is fixed and reduces by half every four years, the next time the block reward will be halved will be on 23/05/2020. Transaction fees can also be created which act like a tip to the original block creator, this payment is only a 'donation' and not mandatory.

Malicious cannot fabricate transactions due to the use of digital signatures which cannot be forged in feasible time. Malicious nodes also cannot skip certain transactions in order to skip a payment due to the fact that other honest nodes will contain the transaction that was skipped. Double spending attacks could be possible if there are a large number of malicious nodes working together but due to most nodes being honest, it is very unlikely it would be possible.

How the Double-Spend attack is normally countered in a correctly functioning bitcoin system

Assuming the transaction is valid without any new blocks (confirmations) being created can allow double spending to occur as the branch may not be the longest (consensus branch). The chance of a double spend attack is reduced when the amount of confirmations of valid transactions increases. It is recommended sellers wait for 6 valid confirmations (6 new blocks) before trusting that the transaction is valid. However, there is always a chance that the transaction isn't on the consensus branch, the more valid confirmations the better however more confirmations means a longer transaction time.

Because of the difficulty of solving the cryptographic hash, the chance of an attacker being able to create a block is extremely low. For an attacker to successfully deploy a double spend attack, they would need to create 6 blocks in a row (to get around the recommended waiting period of an hour). So it is possible but highly unlikely that an attacker would have enough processing power to achieve the creation of 6 blocks in a row as it is much more likely any other honest node on the network will create the next one.

If an attacker had the processing power of 50% of the whole network, then the malicious node would have a 50% chance of solving the next block. This is the reason why the block chain structure works as even with a room of computers or even a super computer, the power is still minuscule over the whole of the networks processing power.

The likely success of a double-spend attack in correlation to the length of potential network outage.

If the bitcoin consensus branch split into two equal branches, the likelihood of a double spend attack directly corresponds to how long it takes for the system to be fixed. As mentioned previously, the recommended time for a merchant to wait for a transaction to be considered valid is 6 blocks, or 1 hour (as a new block is formed every 10 minutes).

We also need to consider that all nodes will use the longest branch of the block chain as the consensus branch (main) which is important because the blockchain has been split into two equal branches due to the outage.

Because the consensus branch has been split approximately equally, someone could use this to their advantage by spending the same coin on each branch, one to themselves (transaction A) and one to a merchant (transaction B). Since the branches are equal, the same amount of hash power is required thus both transactions on each branch get confirmations at the same time. When the outage is fixed, a smaller amount of processing power is required to complete the proof of work to make the branch containing transaction A longer, thus making it the consensus branch thus making that transaction valid. This causes transaction B on the parallel branch invalid. This would result in a successful double spend attack. Of course, this requires allot of processing power to be able to produce the next block on the blockchain to make it the longest, and the amount of time taken to fix will help this.

With 5 minutes of downtime, the effect will be minimal because the time to fix is small enough to fit between creations of blocks, so once the blockchains have been fixed the next node to find a block will add it to the specific blockchain branch that they hold. The rest of the nodes will then use that branch as it is now the longest. A double spend attack wouldn’t be feasible as long as the merchant still waits for 6 confirmations. If an attacker was trying to use the split to their advantage, they would need to complete the proof of work for at least 6 blocks to catch up with the fixed consensus chain. This would be computationally infeasible and extremely unlikely of happening without a large stake in global power. Likelihood: extremely unlikely.

With 20 minutes to fix the problem, a double spend attack is possible but still relatively unlikely (more likely than a 5-minute fix). 20 minutes until a fix would allow for two new blocks to be created, thus if a merchant trusts a transaction based on the last two blocks, there is a chance that a double spent attack could still happen. If an attacker could somehow create two blocks making their branch the longest then a double spent attack could be possible. Likelihood: unlikely.

If the time taken to fix the network problem is 2 hours, then the chance of a double spent attack being successful is very high. This is because an attacker could have potentially made the favourite branch much longer if enough computation power was used. Causing transactions on the attackers preferred branch valid, and all the others invalid. Likelihood: likely.

References

CuriousInventor. 2013. How Bitcoin Works Under the Hood. Available at: https://www.youtube.com/watch?v=Lx9zgZCMqXE&list=LLEbJF_0skXqqPKCkThan2qQ&index=2&t=0s[Accessed: 12 April 2019].

DXChain, 2018. A Deep Understanding of the Double-Spending Problem in Bitcoin. Available at: https://medium.com/dxchainglobal/a-deep-understanding-of-the-double-spending-problem-in-bitcoin-86b73aaefc36 [Accessed: 12 April 2019].