Command Chain Protocol

ILCOIN

Saytama
you need we create

EURODIGITAL

paloalto NETWORKS
NEXTWAVE
TRAPS SPECIALIZED

paloalto NETWORKS
NEXTWAVE
SILVER PARTNER

The Command Chain Protocol (C2P)

The following tasks were conducted:

• Analyse the design plan of the C2P protocol.

• Validate the quantum resistance of the protocol.

The detailed description of the identified vulnerabilities, risk explanation and our recommendations can be found in the following section.

During the test, the C2P protocol was not exploited in any way. The protocol and the system components reacted properly and dropped or deactivated our attack attempts.

51% or Majority Attack

A majority attack is possible when a hacker gets control of 51% of the network hash rate and creates an alternative fork that finally takes precedence over existing ones. This attack was initially the only known blockchain vulnerability and seemed unrealistic in the near past. However, at least five cryptocurrencies — Verge, ZenCash, Monacoin, Bitcoin Gold, and Litecoin Cash — have already suffered from 51% attacks. In each of these cases, cybercriminals collected enough hashing power to compromise the network and pocket millions of dollars.

Unfortunately, all small cryptocurrencies are still at risk. Since they attract fewer miners, attackers can just rent computing power to create a majority share of the network. The developers of Crypto51 have tried to draw attention to the potential risks of hacking smaller cryptocurrencies.

Possible measures for preventing double-spending attacks include monitoring received transactions during a listening period, forwarding double-spending attempts, inserting other nodes to observe transactions, and rejecting direct incoming connections.

Moreover, there's an innovative technology called the lightning network that's designed to solve the problem of exploiting weaknesses in the transaction verification mechanism. This network allows users to instantly verify transactions through a network of bidirectional payment channels without delegating custody of funds.

Our first thought was: **"Does this protocol / protection really work? Let's keep it simple!"** We checked the current hashrate of ILCOIN. Then, we obtained double the amount of hashrate capacity and released our hashing beast against them. This is the attack which can be performed easily by anyone. This just requires a large sum of money to rent some capacity for a short term to have at least 51%. The result: We waited a while and found every block created our side was simply dropped in the end. We even tried some tricks, but to no avail. We could be an active participant in their network, and we could see that everything went well (from our perspective). However, in the end, we still had nothing; no valid block, no reward, nothing.

The total network had 10x hashrate capacity: our hashrate was 7x, and our customer had 3x capacity. After this attack method where the substantial part of the hashrate belonged to us, it did not make sense to attempt again using even more hashrate. It would not have been worth the effort.

Fork Attack with a Rollback Attack

A malicious miner can try to reverse existing transactions. When a miner finds a solution, it is supposed to be broadcasted to all other miners so that they can verify it whereafter the block is added to the blockchain (the miners reach consensus). However, a corrupt miner can create an offspring of the blockchain by not broadcasting the solutions of its blocks to the rest of the network. There are now two versions of the blockchain.

The blockchain is programmed to follow a model of democratic governance known as "the majority." The blockchain does this by always following the longest chain. After all, the majority of the miners add blocks to their version of the blockchain faster than the rest of the network (so; longest chain = majority).

This is how the blockchain determines which version of its chain is the truth, and in turn what all balances of wallets are based on. A race has now started. Whoever has the most hashing power will add blocks to their version of the chain faster.
Therefore, we used fork techniques. Some blockchains still might be vulnerable against a fork attack using a lower ID comparing the original ID from the blockchain. And also the preferred version using a bigger ID, which actually “overtakes” the original ID from the blockchain. Neither of them worked.

Design Flaw Type Attacks

Using design flaw type attacks, like in some smart contracts where the code is poorly written, the attacker can force flaws in the code to make some changes. Then, with these changes, he can execute the smart contract.
Although we had only received design related plans on paper, we could play a lot within this domain. Actually, we insisted that the way certificates were implemented was vulnerable. We believed that this certification-based defense mechanism can be bypassed.

Summary

The SHA-256 algorithm with POW consensus is generating the blocks. Obviously, the blocks include the ILCOIN and the Transactions. C2P protects the blockchain consensus with its protocol. The POW consensus and the C2P protocol that is protecting the blocks are inseparable because they were merged together.

What is the significance of “Quantum Resistance” for C2P?

Quantum technology is capable of breaking current coding and creating new rules in existing technology systems. However, this statement is irrelevant to our hypothesis. The significance of our statement is to eliminate the fundamental attack on the POW system. That means, it can compete against any kind of HASH power. Why? Because the 3-level node system has put our vision of HASH power on a new foundation.

Why does this mean Quantum Resistance?

If quantum technology breaks into the mining market, the currently known machines like AntminerS15 or newer versions of this series would be worthless. The quantum machines would be able to overcome any blockchain in no time at all; to the degree that the Bitcoin or Ethereum system would not be able to resist that kind of an attack. The attacker could easily take the control over the network.

Due to C2P, ILCOIN is not only protected against classic 51% attacks, but also against the above-mentioned quantum attack. It is clear that the attack would not be successful due to the Admiral Nodes.

What is the essence of this innovation? We thought about blockchain again, and the point where the system was most vulnerable was eliminated. We do not claim that the ILCOIN blockchain is perfect, but that no other system has the ability to refute these attacks. Currently, only C2P is able to do so, and the ILCOIN blockchain's quantum resistance gets absolute meaning and value. At this point, the ability of the ILCOIN system is indisputable.

The hypothesis and its proof are, therefore, extremely simple and clear:

You cannot make the ILCOIN blockchain corrupt with unlimited HASH Power. You cannot create a block that would not be rejected by the Command Chain Protocol. Falsified ILC cannot be created. If there is no digital signature, it’s impossible to forge a block, and without it the attacker cannot connect to the ILC blockchain.

Due to C2P, ILCOIN blockchain is 51% and quantum resistant. We claim this and prove it. that even an infinite amount of HASH power is useless to form an attack.

ilcoincrypto.com