Command Chain Protocol

Blue Print

ILCOIN

Definition

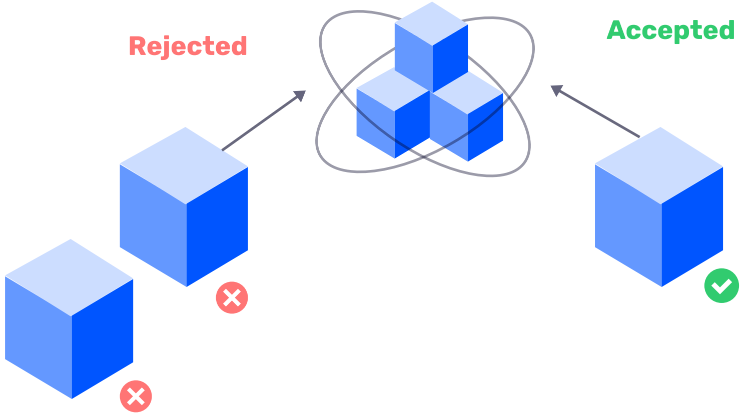
Introduction

As we are all aware, a 51% attack is a reality and a possible danger for all cryptocurrencies. However, we contemplated for a solution in order to prevent what Bitcoin Gold, Ethereum and some others already suffered. Command Chain Protocol is the solution we achieved. With this, we are not only preventing current but also future attacks whenever quantum computing will become an achievable asset for the crypto mining entities as well as for non-ethical hackers.

Definition

How C2P was Created

As thought became reality and we began to test our new design, we thought, **"We have to see if this protocol/protection really works."** We set a certain hash rate for our ILCOIN blockchain. Then, we set up more miners to achieve double the amount of hash rate as an attacker would. This is an attack which can be performed easily by anyone. Someone could simply rent some capacity for a short term to have at least 51%. In the end, none of the blocks outside of our chain were able to be forged; even with double the hashing power. When a miner finds a solution, it is supposed to be broadcast 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; thus, creating 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. The majority of the miners add blocks to their version of the blockchain faster than the rest of the network (i.e. longest chain = majority). This is how the blockchain determines which 3/4 version of its chain is correct, and in turn, what all balances of wallets are based on. From the point a corrupt miner enters a block, whoever has the most hashing power will add blocks to their version of the chain faster. **For this reason, we implemented a certification-based defence mechanism.** By employing this mechanism, no matter how a block is forged, the block becomes invalid due to its lack of certification. This certificate is impossible to replicate because it uses references from previous blocks as well as random data from the computers themselves.



Certification-based defence mechanism

Definition

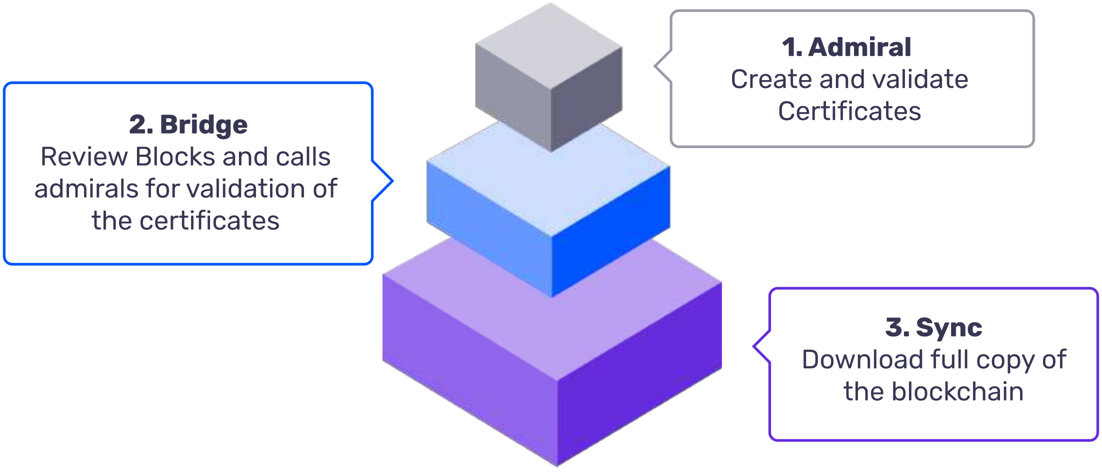
What is C2P

As the name indicates, we have a set of rules and policies carved into the source code which allow or block different types of activities. This also helps us to prevent any blockchain corruption like the double spending issue and prepares our chain for having safer and more stable smart contracts. We use 3 different, unique layouts of nodes so our network is very secure.

The nodes we call **“Admirals”** (there are many of them) need to sign every block; giving an extra layer of verification. Without this signature, the block is invalid. Thus, we are convinced that our system is truly protected.

“Bridge Nodes” work to communicate between Admirals and Sync nodes, and their most important job is to recognize if the block is a valid or a malicious one.

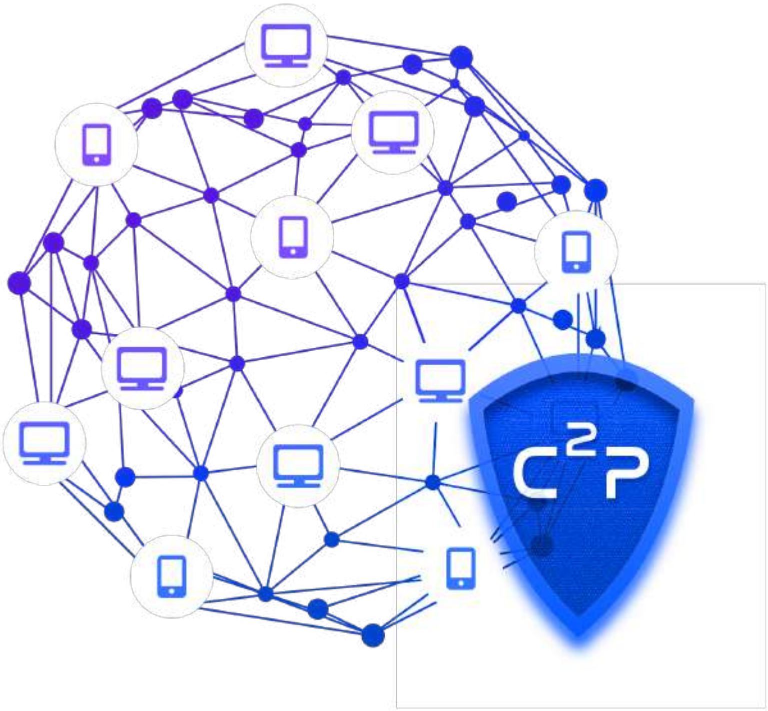
“Sync Nodes” have the ability to read the network as well as send and receive transactions. As the name implies, these sync with the ILCOIN blockchain.


1. Admiral
Create and validate Certificates
2. Bridge
Review Blocks and calls admirals for validation of the certificates
3. Sync
Download full copy of the blockchain

Definition

Implementation of the 3 levels of security creates a safe environment for the user. Beginning with a solid SHA-256, we applied a security layer so no one can double spend, roll back, or corrupt the network. What is more, with these 3 levels we spread the stress of the network by giving different tasks to complete to every full node. Therefore, our chain can be more stable, stronger and faster.

In C2P, every block not only contains the hash of the last block but also contains a set of certificates which the nodes can read in order to double or even triple check the origin of the block and inputs. This way, it determines if that container is a valid or a corrupt one. With the latter, that block and its inputs will be rejected from the entire network. This new protocol prevents the 51% attack with its unique certificate stamp in every block since only non-malicious nodes can deliver that certificate. In addition to this, it has consequently implemented a unique blocking mechanism which prevents the theft of coins or the spending of lost coins in case a user loses their wallet or control thereof. C2P is a unique asset of ILCOIN, and with these new security additions, has made ILCOIN the most secure coin to have ever existed.

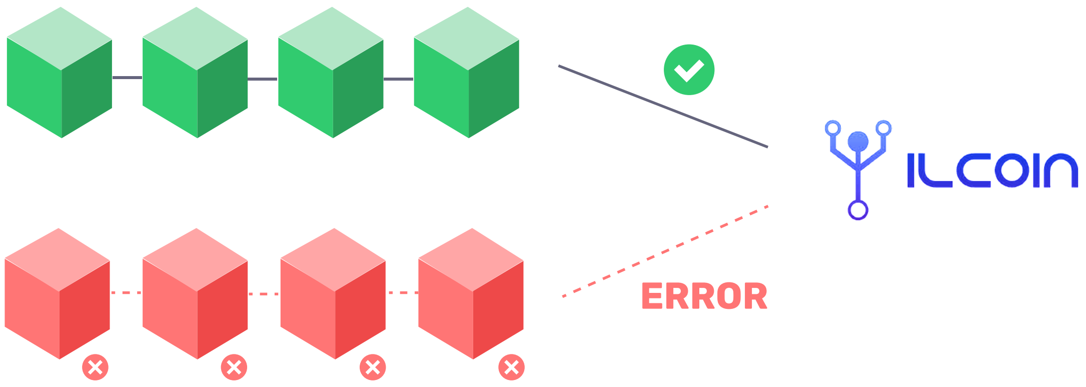


Definition

C2P guarantees that the validation may only occur on our blockchain. Even though someone created a corrupt blockchain, our system would not communicate with it. Think of it as if thieves were printing money which, at first glance, might seem very similar to real money. However, with the aid of a simple inspection (C2P), it becomes obvious the money is falsified. In the case of the blockchain, it is even more obvious as our blockchain does not communicate with false solutions. Based on this, ILCOIN's value is guaranteed as long as people are using one of our official wallets from our home page.

C2P protocol is the basis of the protection against hash power attacks which are based on quantum technology. It doesn't mean we operate on a quantum technological base. It only means we are resistant to it. Consequently, even if the strength of the hash power utilized in the attack is based on quantum technology, it will not let the attackers reach their goals as they have no chance of falsifying our customized digital signature. Think of it as if someone is standing in front of a door with the most powerful object to break in with, but it turns out there is no door. We removed the door that might have given the possibility to attack the PoW system. We have neutralized the possibility that an attacker can harm our system even with an unlimited hash rate.

C2P is the next step for security in the cryptocurrency world in order to reject the unethical hackers who, for example, attempt to take advantage of back doors by way of faulty codes or by overpowering a lesser hashing power; those who, at the same time, end up hurting a specific cryptocurrency and consequently the trust of this entire new market.



ILCOIN

ilcoincrypto.com