JeChain

By: Nguyen Phu Minh

Email: nguyenphuminh09876543@gmail.com

What is JeChain and what problem is it solving?

In the modern era, centralized currencies systems are starting to raise their ugly heads, since it give all the power to third-party providers, which also mean that they can have full power over your money - they can take all your money, print more money, or lock your account with no authority. And because it is a centralized entity, if the system is hacked, which is 100% possible, then all of your money will be at risk. That's why Bitcoin - the first decentralized cashing system utilizing the use of blockchains and the proof-of-work consensus mechanim had been released to fix this problem, bringing fairness and freedom to every users. Following its philosophies, JeChain is built to be a decentralized peer-to-peer currency network, but added a little spice - a decentralized application platform.

A payment system

Basic information

People will access the network as `nodes`, nodes can send messages to each others, all nodes will hold an agreed ledger containing payment history, from that, we can identify one's balance. The ledger will be represented as multiple "blocks" chained together, thus the term `blockchain` and the name JeChain.

Transactions

JeChain's transactions will contain basic information like the amount of money to be sent and addresses from the sender and the recipient.

The problem is, in a decentralized network, it's everyone's game, people can fake transactions from other users to enrich themselves. To prevent this, we have two added properties - a cryptographic signature and a timestamp.

Now, how do these two props solve problems of decentralized transactions? First, let's look at the problem, people can create multiple transactions that take money away from others, right? So we just need a randomly generated key pair, with the first one being the private key, which is used to generate a signature based on information from the transaction, and the public key which can be used for verifying the signature and can act as a public address. With this system, people can no longer create transactions from other addresses if they don't have their private key. But, there is still one problem, what if people take a signed transaction and continuously recreate it, since it would still be available, right? We can fix this by adding a `nonce`, but JeChain takes an approach of using timestamps, bringing several benefits. First, with this problem specifically, it make the signature come out differently every time since time always changes. Therefore, we can just discard any new transactions with duplicated timestamps from one address. Second, it can be used for knowing when the transaction was made.

Blocks

Blocks are entities that keep the blockchain immutable, it contains information like its creation timestamp, transactions, a cryptographic hash generated from a block's information (block header) and the hash of the previous block which is also in the block header. If a block is changed, its hash will be changed, and the following block's hash will also be changed, and the following of that will also be changed. Repeat this process and you can easily recognize if one's chain is changed or not.

Timestamps also play an important role, it records public actions from nodes.

Genesis block

Genesis block is the first block in the blockchain. It might contain a transaction acting as an initial coin release (not to be mistaken with ICOs).

Consensus

But the thing is, nodes can cheat any time, not just attackers, even normal users. So we need a way to make nodes not become attackers. We can solve this using a consensus mechanism called proof-of-work. Basically, you add a `nonce` value into one block. You increment `nonce` by 1 continuously until the block's hash starts with a required amount of zeros. This process is often known as `mining`. Blocks can now no longer be created randomly, you would need a proof of your work to make a block valid. "The majority decision is represented by the longest chain, which has the greatest proof-of-work effort invested in it. If a majority of CPU power is controlled by honest nodes, the honest chain will grow the fastest and outpace any competing chains." - said the Bitcoin whitepaper, which has brought out one of the keypoints from proof-of-work consensus. But, what keeps the honest nodes mining? Why would they mine for us? This can be simply solved with rewards, if a miner successfully produces a valid block, he/she will be awarded with minted (newly released) coins, so this creates an effect which keeps the nodes honest - if they cheat, they wouldn't get money, which is less beneficial than if they did not. This system is also decentralized, since the hashing function is completely random, and each blocks from each miners will have a different mint transaction pointing to their address.

The required amount of zeros is also determined by a variable called `difficulty`, which rises if miners are mining too fast, falls if miners are mining slower than before.

The network will be in the hand of attackers if they have more than approximately 51% computational power of the whole network, which is unlikely.

State

State is like a result created by blockchain where you can get accounts' information like balance or used timestamps from. This will play a big role in making JeChain a decentralized application platform.

JeChain follow an account-based model, which is better for smart contracts (we will talk about this in the next part of this document) and also used by Ethereum, while Bitcoin and many other networks use the UTxO (unspent transactions' output) model. This model works like a key-value database, with the key being an address, and the value is its information.

Every time a new block is submitted, the state will be changed according to transactions from the block.

Network

In the JeChain network, any people, appeared as nodes, can broadcast their transactions to all nodes, which are then put into a mempool called transaction pool, miners then grab transactions from the pool, add it into a new block and start mining. Mined transactions are then removed from the pool. When there is a winner, all nodes will update the chain state according to the newest block.

The problem with a decentralized network is that it's relatively slow compared to centralized network, this is due to a period of time for all nodes to reach to consensus, so it is always vulnurable to DDoS attacks (to the blockchain itself, not to nodes, since attacking every single nodes is practically impossible). To prevent attacks from happening, each transactions must add a fee called "gas fee" so no one can spam transactions continuously, infinitely. This also born a whole new use of this "gas fee", miners will always pick transactions with a higher gas fee, since message's size in a decentralized network is limited, so something more beneficial is always more favorable.

An application platform

Smart contracts

Smart contract is the key point to achieve decentralized applications on a blockchain network. It is just a piece of code that is attached to an address (this kind of address is also called "contract address"). Every time some one create a transaction pointing to a contract address, the contract will be executed. This open an opportunity for decentralized applications, using the blockchain as a database (which is the chain state mentioned before).

There is this one problem though, if the programming language used for development is turing-complete, people can just create infinite loops to halt the network. Furthermore, people can store data on the blockchain continuously, making nodes' storage full. There are many solutions to this, one is making the language turing-incomplete, limiting dapp's functionalities, other is what Jechain is doing. JeChain has fixed this with a similar approach with Ethereum - using gas fees. By making every instructions cost a small amount of money, people can no longer create infinite loops, and storage costs money.

Applications

With the use of applications, people have come up with crazy, decentralized technology like decentralized marketplaces, DAOs, decentralized finance, NFTs, etc.

Conclusion

Overall, we have proposed a decentralized peer-to-peer currency network, also a decentralized application platform with the hope of bringing freedom and independence to every person, ending the reliant to third-party authorities.