Accounts on StarkNet & Mobile Ecosystem

Giwook Han

In 2018, I had interested in blockchain technology like everyone else. So, I participated in various conferences and meetups but I thought there were some problems with blockchain technology being widely used

Problems that I felt in 2018

First of all, Ethereum (and all of the other blockchains in 2018) has a scalability problem. It wasn't new It was a well-known problem that many people already knew and 'CryptoKitties' shows a lot of people about it. High transaction fees and slow transaction times may seem bad to choose Ethereum to create decentralized applications (hereinafter referred to as Dapps).

Second, uncomfortable user experience with their account. If user lost their private key to the crypto wallet, then they can't find their asset. Or, if I get someone's private key, then I can easily move his asset to any account. For example, you might know 'Stefan Thomas' who can't access his asset because he forgot his private key. He has a bitcoin in his wallet and the amount of it is 7,002. That is more than $147milion as of this week.

Third, in 2018, I thought that many people that interested in just money, not blockchain technology itself. Even though the technology is good enough, if only a few people have the interest to use that technology, then I believe there is a limit to the development of the technology.

Because of the problems above, my interest moved on to another technology. And earlier this year, I looked at blockchain again, and there was a huge improvement. Especially StarkNet's method of solving Ethereum's scalability problem is impressive.

Solutions

StarkNet is a zk-rollup solution to solve the first problem that I mention above of Ethereum, which is scalability. StarkNet makes a bunch of transactions into one single transaction on Ethereum. It uses zk proof called 'zk-STARKs' as a mathematical tool that allows systems to prove that certain transactions have been correctly settled and updated the state of the blockchain without actually processing those transactions.

And StarkNet also solves the second problem, uncomfortable user experience with their account. This occurs because EOA is not a contract and the private key of Ethereum's account is the same as a signer. Account on StarkNet is contracted, which means, you can make the account's private key not equal to the signer. Not only this, you can customize your wallet's design.

For example, you can make your wallet a multisig wallet. Multisig is, for example, you could have a wallet that has three keys, where any two of them are needed to send a transaction. This makes your account much safer, for instance, if a hacker stole a private key from one of your accounts, he can't make transactions because he doesn't know the other private key to make transactions.

Alternatively, you can make your accounts secure with the other way, it is social recovery. Social recovery could be much more convenient than multisig. In this method, you have one single signing key, and you must set at least 3 "guardians", of which a majority can cooperate to change the signing key of the account.
In normal circumstances, it works just like a normal wallet. If you want to sign a transaction, then you can sign it by just using a single signing key. But if a user lost their signing key, they can change their signing key with social recovery functionality. The user reaches out to their guardian and asks them to sign a transaction that changes the signing key registered in the wallet contract to a new one.
But in social recovery, the problem may remain. If a theft stole a user's private key, then the theft can send every asset that existed in that wallet. It can be solved by adding a vault. When a user makes their account, automatically adds a vault that the user can use. User can store their asset in the vault by making send a transaction to the vault's address, but they can be moved out of the vault only with a certain time delay (e.g. 1 day, 3 days, 1 week, etc.). of course, you can make this on Ethereum with smart contract, but social recovery needs many transactions so StarkNet is a better network to make this account.

And multicall could be also another powerful feature on the StarkNet account. Multicall allows an account to make multiple calls in a single transaction. If a user wants to send their asset to N people, then they can make it happen with a single transaction. Why is this a big deal? Because users need to sign only once, not N times. And also, they don't need to wait for confirmed N transactions. They only have to wait for one transaction to be confirmed. This gives us a huge improvement in user experience on account
There are many other examples besides what I wrote above, and all of these things give us a huge improvement in the user experience with the account.

About the Third problem

So, StarkNet solved the first and second problems that I wrote above, but the third problem remains, which is people's interest. I think even today, many people are only interested in Defi, coin trading, NFTs, and not in other Dapps. And I think the solution to this is to create a lot of Dapps on StarkNet so that people can experience it. Of course, there are many Dapps in Ethereum, but I think people's barriers to entry are high because of the high transaction fee of Ethereum. And also, there are great Dapps on StarkNet, and I believe many people keep working on creating Dapp on StarkNet, but I think we need more Dapps and we have to make lower the barriers to entry.

How to make lower the barriers to entry?

I think I can improve the accessibility of web3 by Expanding the mobile web3 ecosystem. Because mobile is much more accessible than desktop. There are no restrictions on places and many people have a mobile phone already.

So, my first goal is to make a mobile wallet on StarkNet so that the other mobile Dapps can make a transaction. (When I start this project, Braavos didn't have a mobile wallet)
I am working on making Android and iOS wallet applications by using Argent-X's wallet contract and StarkNet.js and React.

After this, as I wrote above, I truly believe that the mobile web3 ecosystem is important, so I'll go a make mobile Dapp, such as a mobile game on StarkNet.

Concluding

StarkNet is a great network to make Dapp because it solves scalability problems on Ethereum effectively and gives the user an enhanced user experience. So, it has the potential to bring many people who are not interested in Web3. And mobile Dapp can make the barriers to entry lower by improving accessibility. So, I think we should keep working on expanding the mobile Web3 ecosystem.