SCDO Stem Subchain Introduction

SCDO is developing a layer2 protocol called Stem subchain protocol. It is designed to be highly scalable. Another technology we use to improve SCDO's transaction capacity is sharding. This Stem subchain protocol is also an architecture to empower the SCDO application ecology. If you imagine a SCDO main chain as the trunk of a tree, then the subchains are just like the branches of the tree. The subchains may have very different settings with respect to the SCDO main chain. For example, they could have their own consensus algorithms, applications, and ecologies. But they have a close connection with the SCDO main chain. In the first phase, we are going to support subchains with PBFT consensus. For example, users can build a tendermint subchain and connect with our main chain via the Stem subchain protocol. Subchains can have a much faster transaction speed than the SCDO main chains. Therefore, applications that require high TPS can be deployed on subchains. Applications that require large data traffic can be deployed on subchains. But you may ask why do we need SCDO main chains? Here is the answer. Since the subchains may have more centralized consensus, they are less secure compared to the SCDO main chains. We need to protect the users' assets with the SCDO main chains.

Our target is to build a main chain and subchain ecology that can support various applications such as fast asset transfer, gaming, logistics and data sharing. Recently, Decentralized finance (DeFi) has become a hot movement in the blockchain space. In the following, I would like to talk about how SCDO is going to build a DeFi ecology with our main chain and subchain infrastructure.

DeFi is an important application of blockchains. Centralized finance is still the cornerstone of modern society. But it has some problems like the transaction fees could be high and there could be a lack of transparency. The centralized financial organizations have large operational costs. For that reason they have to charge customers high fees to cover part of their costs. They also have a target to make profits. We have seen many times that the centralized financial organizations underestimated the market risk and credit risk to pursue high profits. There is also unpredictable risk from the organizations themselves and their employees. Especially in scenarios where no proper regulations exist, it's likely to have fraud.

The target of DeFi is to build a more transparent financial market. It should be decentralized and open to everyone. It should be controlled by the algorithms and programs to avoid man-made risk. It should meet the financial needs of people who can't get help from centralized financial institutes. Before the invention of blockchain, nobody talked about defi because we didn't know how it could be done. But with blockchains, it's becoming clear that DeFi is not only possible but also very promising. We don't expect DeFi to replace the centralized financial system. But it can solve some problems that can't be solved by the centralized financial system.

There are many DeFi projects in the market, like uniswap, bancor, dYdX. But in general DeFi is still at an early stage. Theoretically, more sophisticated economic models and algorithms are needed to provide equilibrium, improve market liquidity and control the risk. The models and algorithms should have good consistency and make sense economically. Because DeFi projects rely on computer programs that execute automatically, the quality of computer programs is very

important. Especially when the project codes are made public to everyone, they become the target of many hackers. We have seen some projects fail just because of one or two bugs in the smart contracts. For security reasons, DeFi projects should be developed by good engineering teams, be tested extensively. Code audits before the launch of the projects can also reduce the risk. Although DeFi is still quite new and immature compared to centralized finance, I think eventually there will be some solid DeFi frameworks becoming the industry standards.

SCDO has many ideal features to support the DeFi applications. SCDO is compatible with EVM. Therefore the DeFi applications on Ethereum can be migrated to SCDO main chain easily. We will provide SDKs and attract developers from our community. Security is important for the DeFi applications. SCDO is a secure blockchain powered by a new PoW algorithm. Our engineering team put a lot of effort in optimizing our consensus, p2p networking, and transaction logic to provide the best security to the users.

As mentioned earlier, SCDO is building the layer2 subchain ecology. The subchains can have their own consensus, networks, applications and digital assets. We find that the value transfers between main chain and subchains should be part of our DeFi ecology. The assets on main chain and the assets on subchains are heterogeneous. They may have different total supplies, They are used in different applications and circulated in different communities. For all these reasons, the assets on different chains should have different values. The exchange rates between these assets should be flexible and determined by the market.

Here we can use a mechanism similar to uniswap to determine the exchange rates between assets. But there is something different in our case. In uniswap, the assets are Ethereum or ERC20 tokens. They are assets on the same chain, easy to validate. Generally speaking, the Ethereum Defi ecology is based on Ethereum main chain. In our case, the assets are on different chains. This is one important feature of SCDO DeFi ecology. To exchange assets in a smart contract, assets on other chains must be represented with local tokens. A mechanism is required to guarantee there is a true relationship between local tokens and the underlying assets. This mechanism could be a cryptographic proof, a reward-and-punishment mechanism, or governance by a third-party. We need a certain method for cross-chain validation. Cross-chain validation is tricky. Different chains could have different sets of block validators. Since the main chain doesn't keep the full ledgers of subchains, it's possible that subchain block validators conspire and lie to the main chain. It's important to have a mechanism to prevent the malicious behaviors of block validators. The SCDO Stem subchain protocol is designed to make sure the main chain knows the status of subchains well. It has various settings depending on the subchain applications. Usually, a Stem smart contract needs to be deployed on SCDO main chain to manage the interaction between main chain and the subchains.

The value transfer between chains could be more than a simple exchange. It can be a collateral loan. Here is one example. User A wants to borrow 100 subchain tokens. He locks 10 SCDO in a main chain smart contract. The algorithms in the smart contract determines that the exchange rate is 1 SCDO for 10 subchain tokens. Now another user B is going to make a deal with user A.

He will release 100 subchain tokens to A on the subchain. After one month, A needs to pay 100 subchain tokens back to B. Since A borrows B's subchain tokens for one month, he needs to pay B some SCDO as interest. Therefore A may only get 9 SCDO back from the main chain smart contract.

We can also exchange the assets of multiple subchains in one smart contract. The key is the mathematical model to provide liquidity and the mechanisms to provide cross-chain validation.