Chapter 1. Introduction / Overview

Locus Chain aims to solve the problem of current-generation Blockchain technologies like transaction speed, quantity, and resource consumption, while keeping beneficial properties of fairness and transparency.

An embodiment of Blockchain technology widely adopted in the real world is Crypto-Currency. The critical point accelerated the adoption of Crypto Currency is the decentralized nature of Blockchain. A technological mean enables perfectly fair participation without any central intervention is unprecedented in human history.

▪ Key Points of Blockchain

Blockchain enables the security, fairness, equality, transparency between users by managing (or non-managing) the whole army of independent and autonomous network nodes without any central authority. The key technological means enables this magic includes P2P network technology, cryptographically signed transactions, and fair consensus algorithm.

The P2P network and Gossip protocol are central means of communication. This combination of technology enables secure distributed communication that cannot be controlled by any single party. Cryptographically signed transactions ensure equality and transparency of data management to all participants while preventing control of data by any single party. Also, Blockchain encourages every contributor to keep the whole integrity by offering fair incentives to contributors.

Moreover, Smart Contract implemented on Blockchain accomplishes a mechanism of establishing automated and forced digital alternatives of real-world contracts.

▪ The Limitation of Current Generation Blockchain Technology

The technological properties of first-generation Blockchains are well studied and widely acknowledged. Especially the following points are worth mentioning.

First, the speed and volume of transaction processing should be addressed. Well-known current generation Blockchain system requires tens of minutes to confirm a transaction. Also, there is a limitation in the number of transactions can be confirmed in a single process. This limitation is due to the nature of consensus algorithm design.

The limitation of transaction speed and volume leads to the problem of processing fees. Transactions that pay higher processing fees get higher priority of processing. With the limitation of the processing volume makes small transactions with small fees unfavorable for processing, which can be problematic to the fairness of the total system.

The limitation of speed and volume of transactions also becomes the limitation of participants. The capacity for possible transactions is the same regardless of the growing number of participants, which effectively limits the growth of participants.

In spite of the limitation of transaction capacity, the use of computing resources still grows according to the number of participants. Particularly the Blockchains which incorporate Proof-of-Work scheme consume an enormous amount of computing resources in the form of electricity, which became a kind of environmental problem.

▪ The Approaches of Locus Chain

Our Locus Chain tackles the problem of previous-gen Blockchain technologies with practical technological designs. Our system aims to achieve high speed and a massive amount of transactions by parallelized processing of transactions over distributed nodes, while linearly scalability of total processing power with a growing number of participants. Additionally, we aim for a highly efficient software system even could be run on battery-powered, portable devices.

Some of the key technologies of our system to achieve these goals are “Direct-Acyclic-Graph data structure”, “Sharding”, “Round Consensus”.

First, Locus Chain incorporates the data-structure of Account-Wise-Transaction-Chain (AWTC), which organizes transactions logically in a kind of Directed-Acyclic-Graph (DAG). In this scheme, only the account owner can append transactions to its own chain, which makes the dependencies between transactions explicit. By this, the processing of transactions became independent for each account, and the verification of transaction validation became clean and straightforward.

Each independent AWTC can be processed independently. Locus Chain splits the whole network into several properly sized subgroups, as known as Shards, and assigns proper number of AWTCs to each shard. The total capacity of transaction processing grows if shards are divided because each shard has a roughly equal capacity of transaction processing. If the number of participants grows, the number of shards also grows, which means grown capacity of total transaction processing.

Each shard makes consensus about the contents of new transactions, in regular interval. In each Round, which is an interval between two consensuses, the shard fairly elects a certain number of committee nodes. Then the elected committee nodes try to agree on the new transactions. If the committee reached a consensus, then it means the transactions are fixed irreversibly.

In summary, Locus Chain incorporates clever consensus algorithm scheme to speed up transaction processing and incorporates sharding to process a large number of transactions. To support these ideas, Locus Chain uses the AWTC, which is a DAG-style structure of transactions.

In advance, Locus Chain also incorporates expandable Crypto Facility for transactions and accounts, which can become an excellent way to keep up with Post-Quantum Cryptography era.