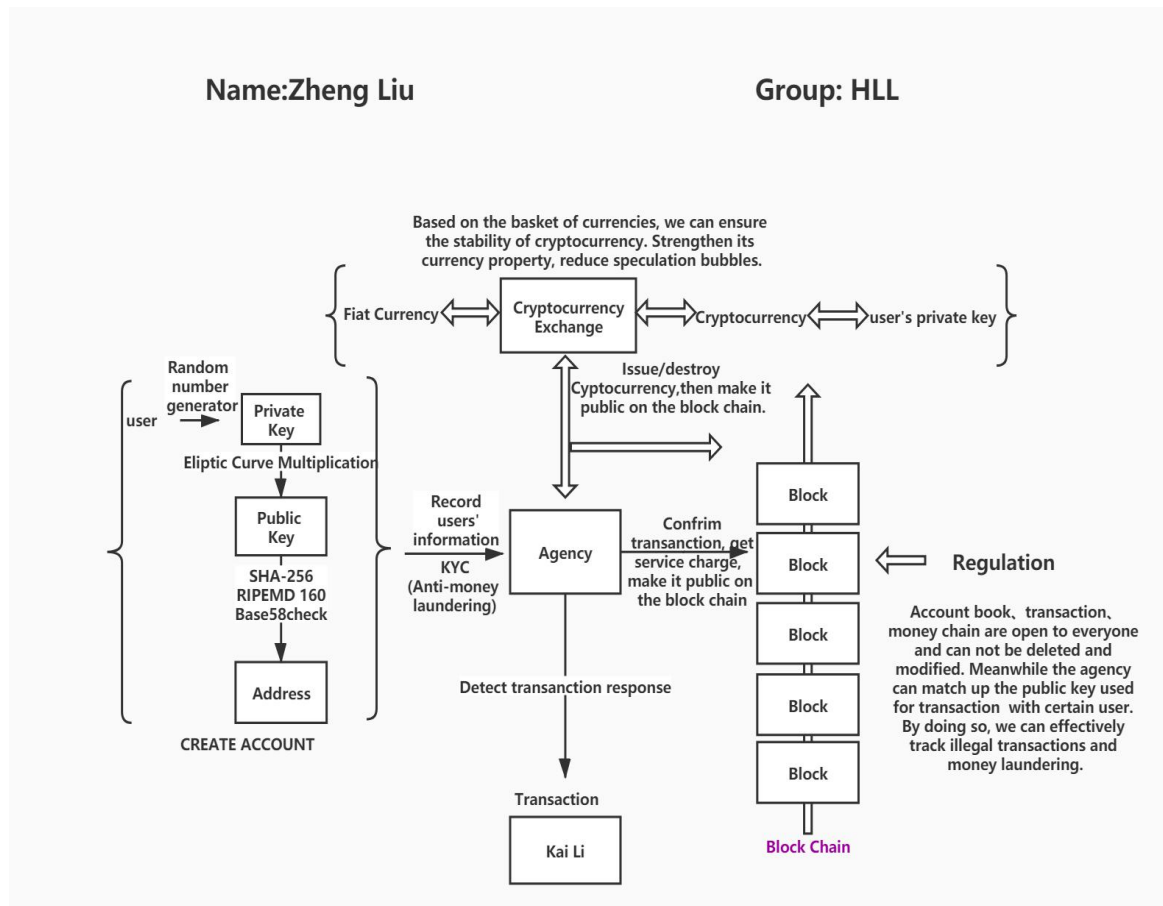# Team Name: HLL

Project Name:

Data structures and algorithms needed for regulating cryptocurrency

Project Description:

Regulating cryptocurrency so that only allowed users and organizations can mine. Establishing a regulatory authority so that the circulation of cryptocurrency needs to be monitored by this authority
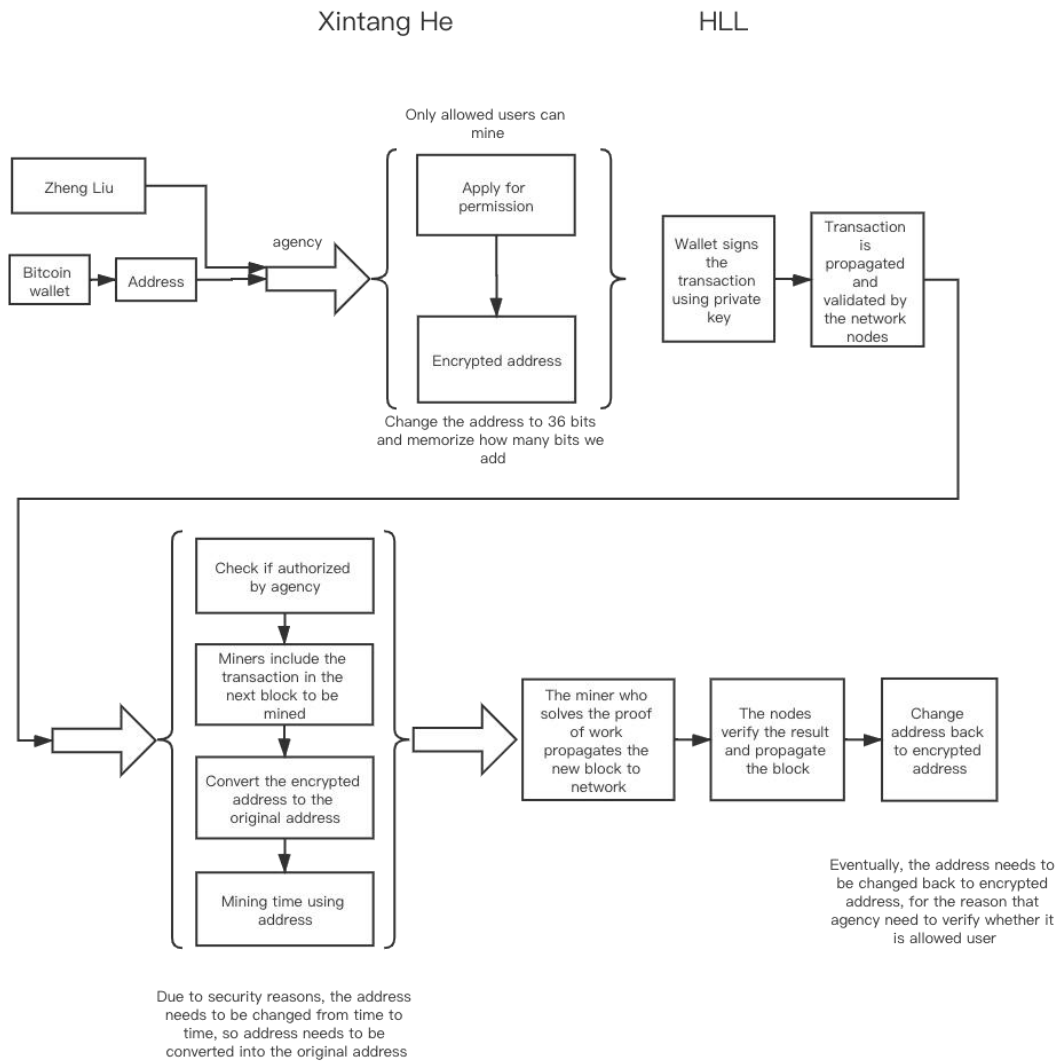
Cryptocurrency Structure:

Our cryptocurrency structure as shown above. We create an agency to regulate the cryptocurrency and prevent it from being used for illegal act. And it also can keep the stability of our cryptocurrency, make it possible to replace fiat currency.

Progress:
The structure has been done. Research papers are being studied.Code is being written.

Xintang He's diagram shows how the agency works. Kai Li's diagram shows how the transaction works.
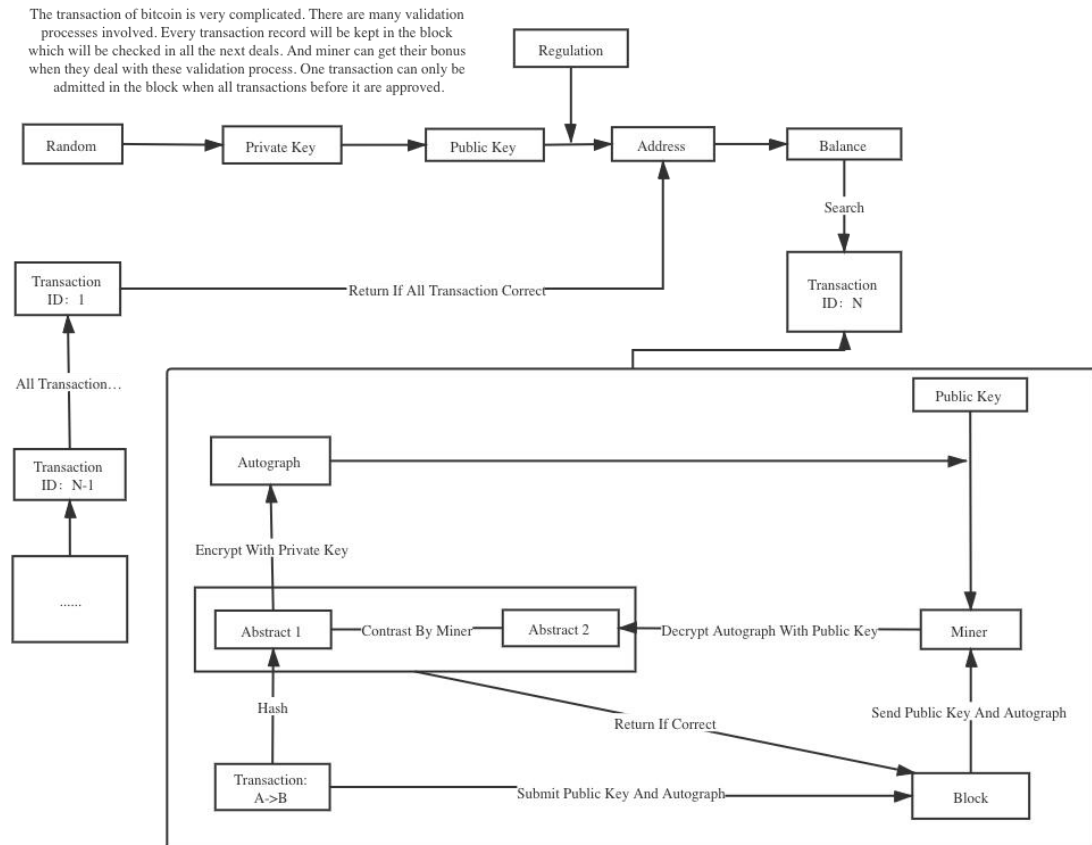
Agency:

I think we can use hashmap to store the information of original address and how many bits we add. Then determine the user's legitimacy by determining whether the address is 36 bits.

Transaction:

Name: Kai Li   **Team: HLL**

The transaction of bitcoin is very complicated. There are many validation processes involved. Every transaction record will be kept in the block which will be checked in all the next deals. And miner can get their bonus when they deal with these validation process. One transaction can only be admitted in the block when all transactions before it are approved.

Regulation

Random → Private Key → Public Key → Address → Balance

Search

Transaction ID: 1 — Return If All Transaction Correct

Transaction ID: N

All Transaction…

Transaction ID: N-1

......

Public Key

Autograph

Encrypt With Private Key

Abstract 1 — Contrast By Miner — Abstract 2 — Decrypt Autograph With Public Key — Miner

Hash

Return If Correct

Send Public Key And Autograph

Transaction: A->B — Submit Public Key And Autograph — Block

In my opinion, if we want to make the system of Bitcoin run under regulation like Libra but keep its non-centralization. The best way is to find an algorithm that can transform the public key of those who voluntarily accept regulation to a new one. In order to get the new under-regulation key, you have to submit an application attached with your personal information to the agency and wait for approval and your new key. Those who get a new under-regulation key can do everything with their bitcoin and others may get some restriction.