Midterm report

Project : Data structures and algorithms needed for regulating Bitcoin

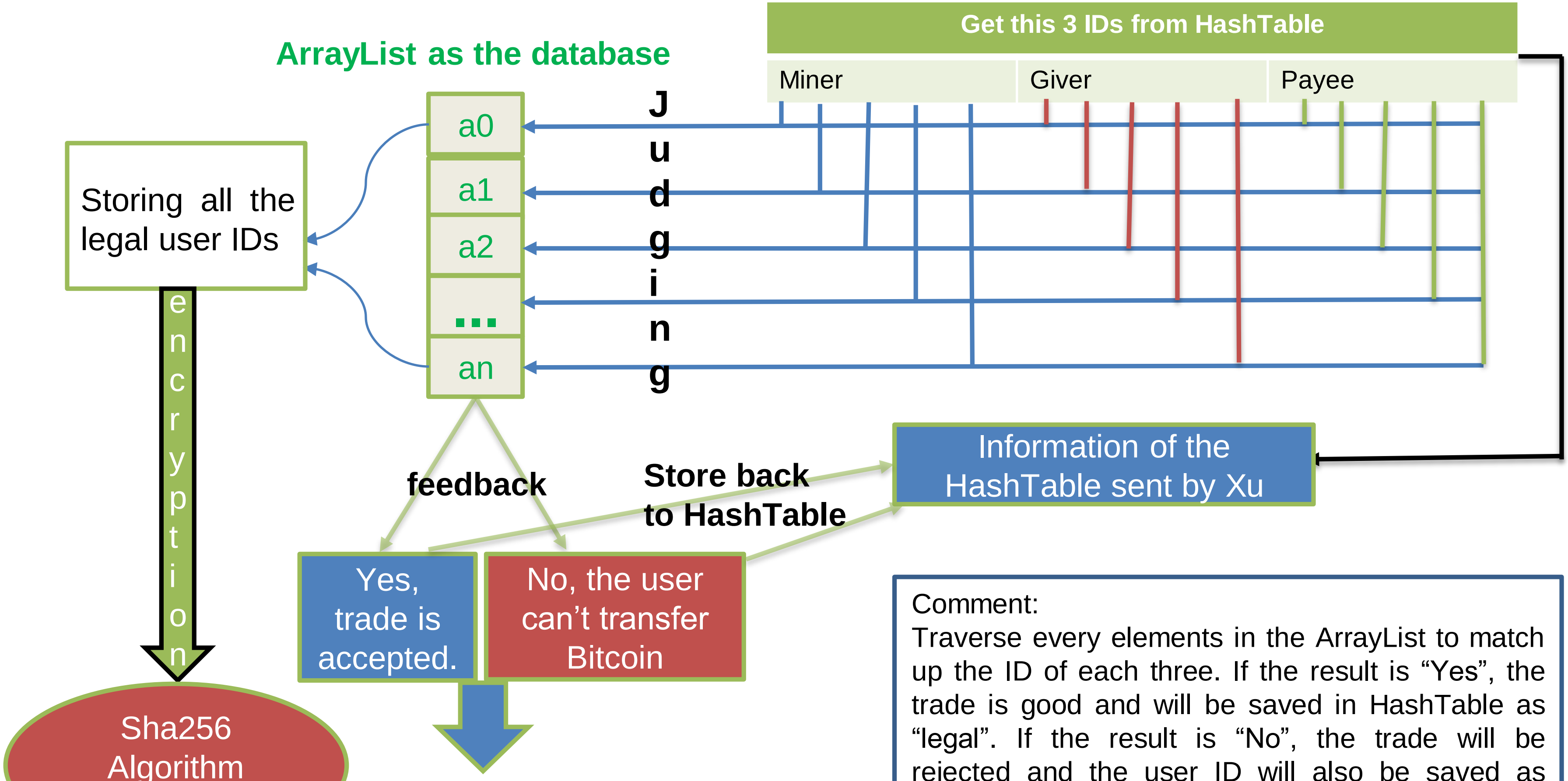
Team Name : XSWL

Team Member : Xiangyang Xu, Siyang Wu, Feng Liu

Description

In this report, we will demonstrate our idea for regulating Bitcoin according to the materials given by professor. Since Bitcoin is decentralized and everybody can package the information of the Blockchain, it’s very hard to control the deal made by every user without a third party. By realizing that, we attempt to use an ArrayList to store every user’s account which forcing them to create. As for privacy, we will use Sha256 Algorithm to encrypt their accounts and put the encoded information in the Blockchain. Finally, we will use a HashTable to save every transferring details relating to each account in order to fulfill the regulation such as tracking and searching the orders.

Siyang Wu’s Part : I will build a database which contains all of the information of the account(User’s ID) by using the ArrayList. Then use that to make the decision whether the ID of the user(giver and payee) match up one of the element in the stored data. And see if the Bitcoin trade is made by an eligible user.



ArrayList as the database
Get this 3 IDs from HashTable
Miner
Giver
Payee
a0
a1
a2
...
an
Judging
Storing all the legal user IDs
encryption
Sha256 Algorithm used by Liu
feedback
Store back to HashTable
Information of the HashTable sent by Xu
Yes, trade is accepted.
No, the user can’t transfer Bitcoin

Assume the whole process as a server’s operation.

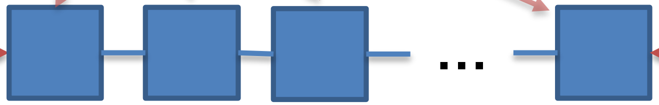
Comment:
Traverse every elements in the ArrayList to match up the ID of each three. If the result is “Yes”, the trade is good and will be saved in HashTable as “legal”. If the result is “No”, the trade will be rejected and the user ID will also be saved as “illegal” in HashTable.
Miner can be both the giver and payee because it also can be involved in the Bitcoin trade.

TEAM NAME : XSWL
THE CREATOR OF THIS PART : Siyang Wu

Feng Liu’s Part : If I get the trade information. And encode the ID of miner, giver and payee. Then store those value into the Blockchain and renew the information which has already inside Blockchain. The format of the information in the Blockchain will be like “**encoded ID + bill + time + random number**”. Thus, every Bitcoin user can know someone has made the deal but still can’t know the deal is made by whom.

How we make our works connected?

The Structure of the chain of Bitcoin :



Hash table block by Xu

This is the block(box), which including the information the user has traded.

Get this 3 values		
Miner	Giver	Payee

Using the algorithm of Sha256 to encode the User ID(including miner, giver, and payee)

This part is what I did.

Database by Wu (check if it is a good trade) and sending the User ID.

The name(ID) of miner, giver or payee

Decomposing into N 512-bits block

M1	M2	M3	…	Mn

Calculating the value of H0 to H7

TEAM NAME : XSWL

THE CREATOR OF THIS PART :
Feng Liu

Comments:
For the purpose of protecting user‘s privacy and preventing the database from being stolen by lawbreakers, I think it is impossible to correspond with the real users on the network by using encoded user’s name.
I have learned the security of this algorithm, and how it works. Besides, I saw the information of pseudocode for the SHA-256 algorithm.

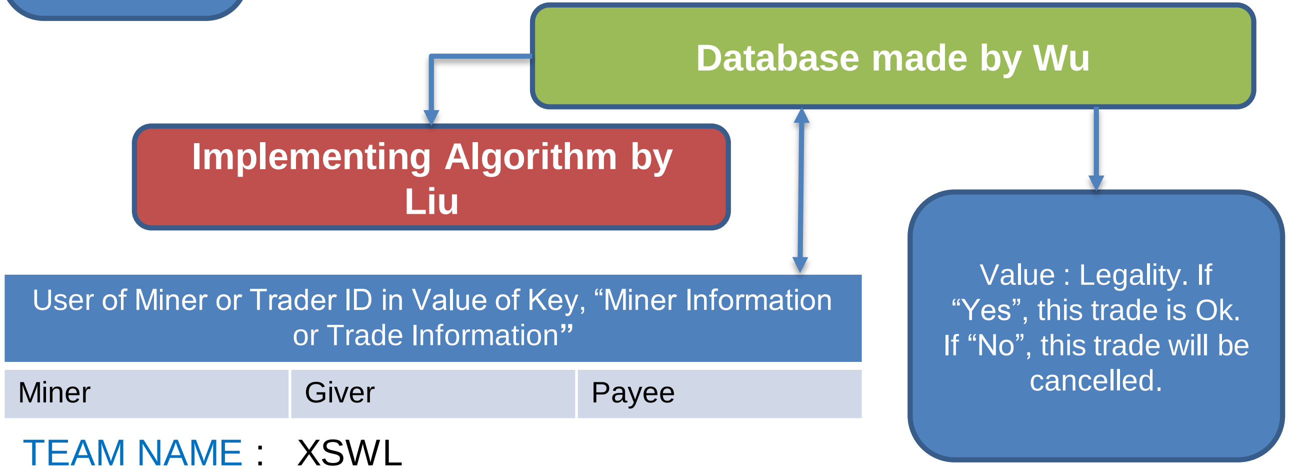
Xiangyang Xu Part : I will use a HashTable data structure to strengthen the regulation of Bitcoin. Then the information of trade will be easy to get. After that, I will send users ID to server and get their legality. Any trade without regulation will be cancelled.

Block n-1: You can know its id from value, “n-1 Block ID” of Key, “Block n ID”

Hash Table Block n and its neighbor chain

Key	Value			
Block n ID	n-1 Block ID	Miner	Block SHA256	
Miner Information	System	Reward Value	Miner ID	legality
Trade Information 1	Giver ID	Trade Value	Payee ID	legality
Trade Information 2	Giver ID	Trade Value	Payee ID	legality
….				
Trade Information N	Giver ID	Trade Value	Payee ID	legality

Block n+1: You can find block n ID from value “n Block ID of key”, Key “Block n+1 ID”



Database made by Wu

Implementing Algorithm by Liu

User of Miner or Trader ID in Value of Key, “Miner Information or Trade Information”

Miner	Giver	Payee

Value : Legality. If “Yes”, this trade is Ok. If “No”, this trade will be cancelled.

Comments:
By using hash table data structure we can easily and quickly know the basic information of giver and payee. Then we can send it to server to judge whether it’s a good trade or not. If not, its legality will be “NO” and this trade cannot be completed.

TEAM NAME : XSWL

THE CREATOR OF THIS PART : Xiangyang Xu