



Bitcoin Exchange Application

Final Presentation

INFO 5100

Pengfei Wang
Jiahua Li
Shujun Lei



Description

Bitcoin (₿) is a cryptocurrency and worldwide payment system. It is the first decentralized digital currency, as the system works without a central bank or single administrator. These transactions are verified by network nodes through the use of cryptography and recorded in a public distributed ledger called a blockchain. Bitcoins can be bought on digital currency exchanges.

Our goal is to design an application to fulfill the bitcoin exchange. This application can create a platform with high security achieved by full trace verification, which can be used by buyers and sellers. We try to simulate bitcoin exchange in the real world, which ranges from mining and writing bitcoins, trading them under authentication to depositing and withdrawing money, etc.





Enterprises



EcoSystem



Miner

1. Mine bitcoins;
2. Write bitcoins into specific depository;
3. Sell bitcoins on the platform.



Bank

Build connections between the customer's platform account with its local account.



Depository

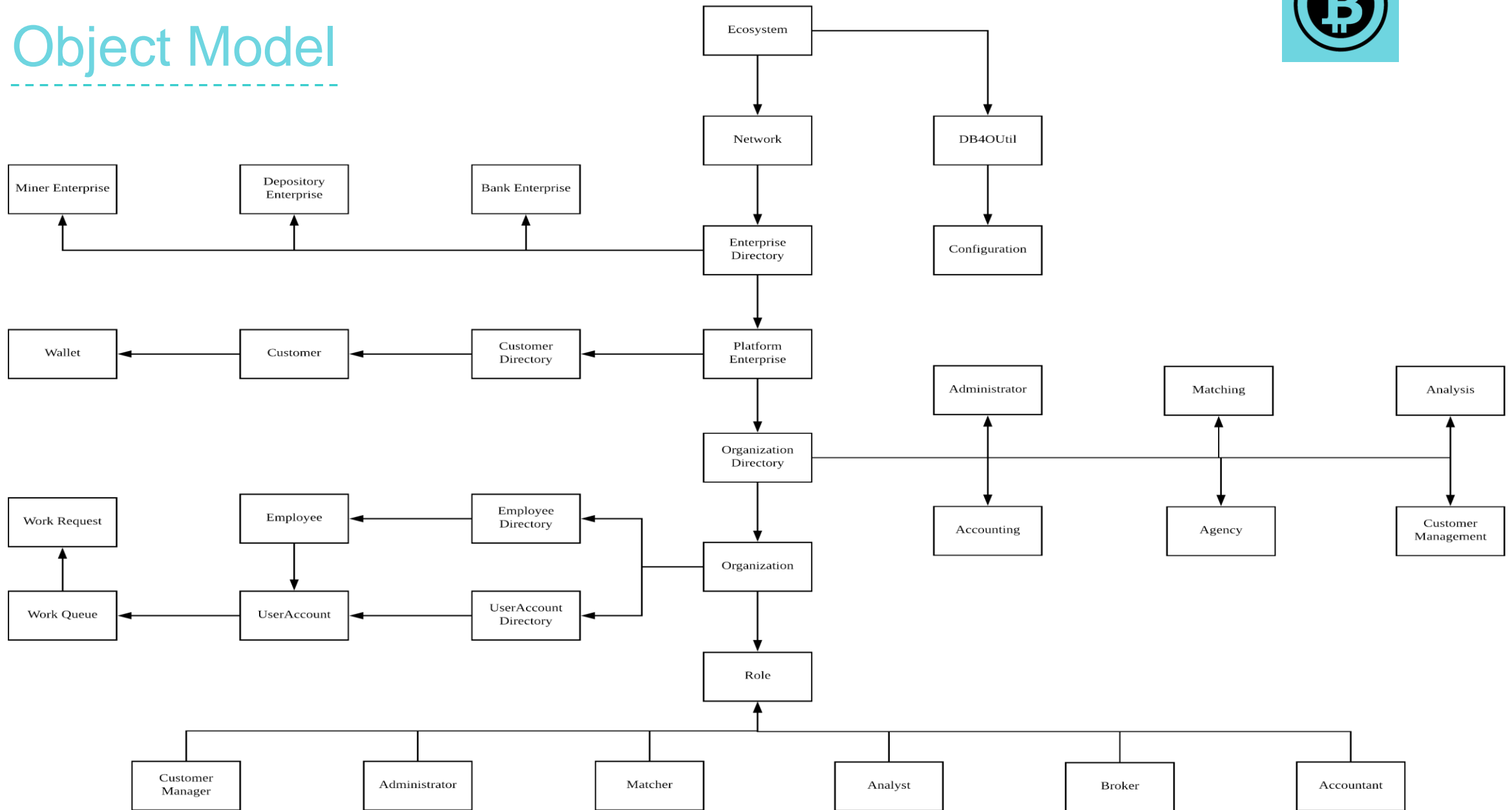
1. Authenticate trading records and bitcoins;
2. Keep records of all trading information;
3. Restore the bitcoin history.



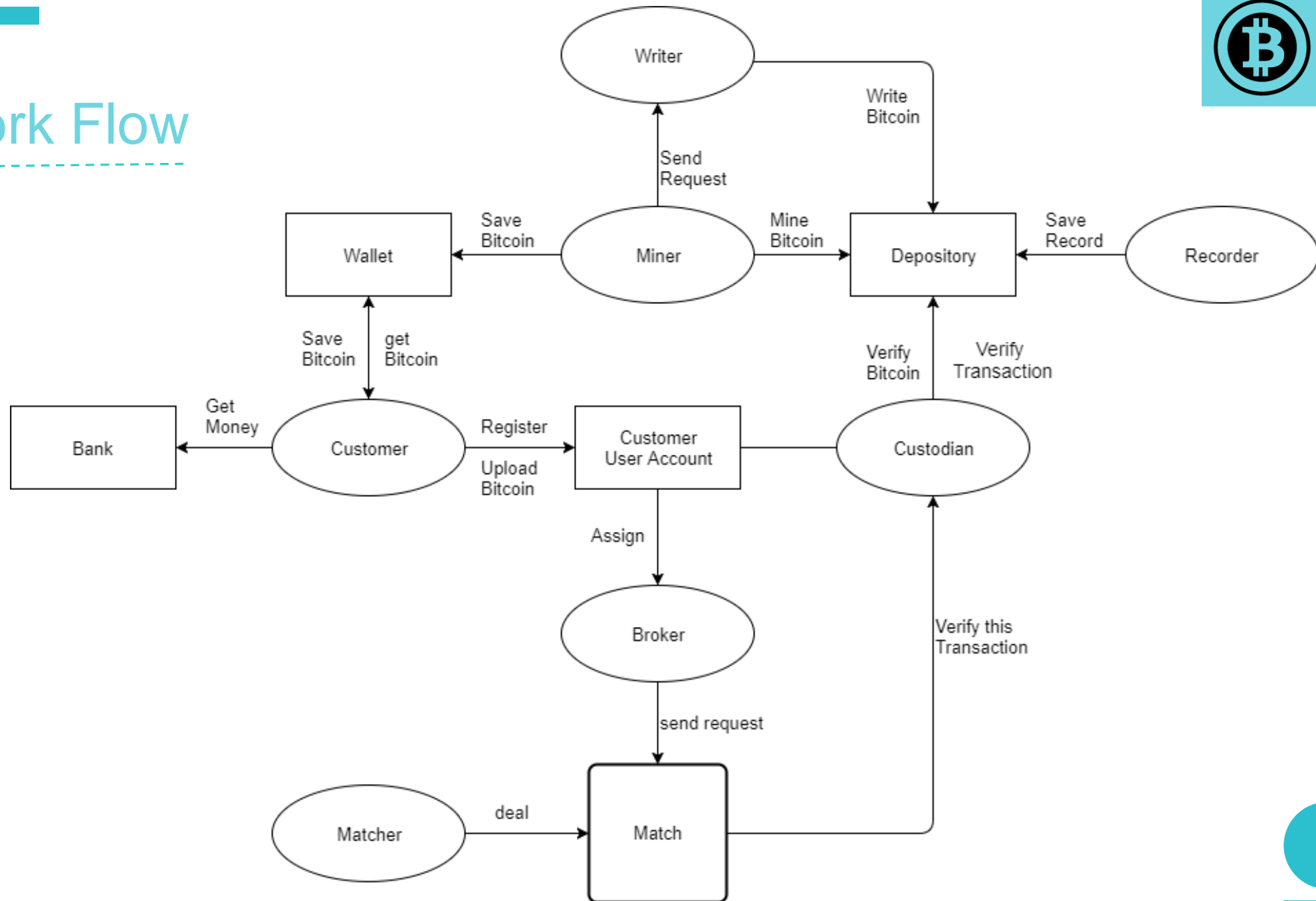
Exchange Platform

1. Buy and sell bitcoins;
2. Help customers to trade and manage bitcoins and money
3. Provide analysis report.

Object Model



Work Flow





Key Roles



Platform Administrator

Manage the user accounts in platform



Miner

Mining the bitcoin and get the private Key



Customer

Invest fiat money to buy bitcoins or trade its bitcoins on the platform



Bitcoin Matcher

Match the buying and selling request



Bank Accountant

Responsible for connections between the platform wallet and local wallet.



Custodian

Supervise the transaction and verify the private Key of Bitcoins



Bitcoin Broker

Represent customers to do the transaction, each investor has a Bitcoin Broker.

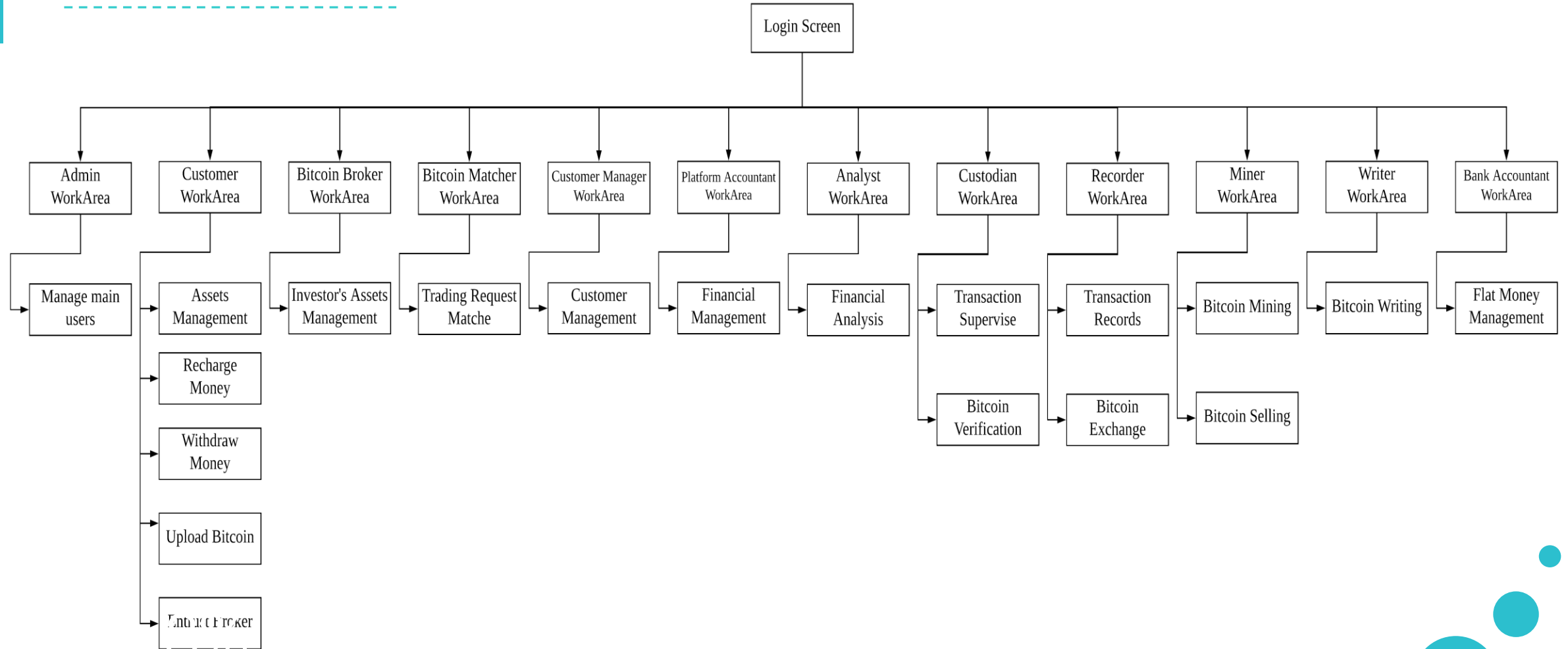


Analyst

Analyze the trading volume and turnovers within a certain period



System Flow





**Register Account
by E-mail**

Additional Features



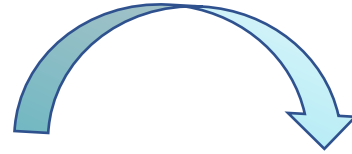
Match Algorithm



High Security



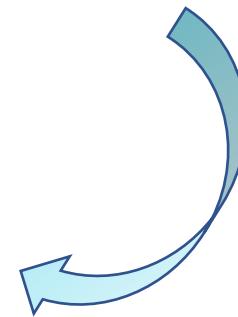
Match Algorithm 1



Investor	Price	Quantity
Seller A	110	2
Seller B	70	1
Seller C	60	4
Buyer A	120	3
Buyer B	110	2
Buyer C	105	5

Investor	Price	Quantity
Seller A	110	2
Seller B	70	1
Seller C	60	4
Buyer A	120	3
Buyer B	110	2
Buyer C	105	5

Investor	Price	Quantity
Seller A	110	2
Seller B	70	1
Seller C	60	1
Buyer B	110	2
Buyer C	105	5





Match Algorithm 2

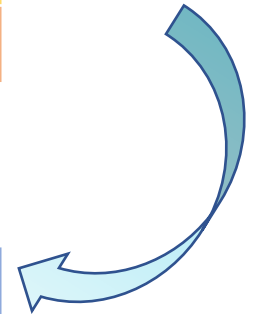


Investor	Price	Quantity
Seller A	110	2
Seller B	70	1
Seller C	60	1
Buyer B	110	2
Buyer C	105	5

Investor	Price	Quantity
Seller A	110	2
Seller B	70	1
Buyer B	110	1
Buyer C	105	5

Deal Price:
 $(110 + 70) / 2 = 90$

Investor	Price	Quantity
Seller A	110	2
Buyer C	105	5





High Security

1. Customers registration would be verified via personal emails.
2. All transactions is under custody of depository.
3. Bitcoins would be written into depository and verified after being mined.
4. Money depositing and withdrawing would be supervise by bank.
5. Bitcoins uploading and withdrawing would be also under supervision of platform.





Screenshots 1

User Name

55

Password

55

Login

Logout

Sign Up

Customer Related Information

Basic Information

Assets Management

Recharge Money

Withdraw Money

Local Wallet

Entrust

Order History

Withdraw Bitcoin

Name

CustomerB

Person ID

20

Bank Account

55

User Name

55

Password

55

Change Password

Save

User Name

14

Password

55

Login

Logout

Sign Up

Matcher Work Area

Unprocessed Requests

Processed Requests

Authenticate Transaction

Seller Request List

Message	Broker ID	Broker Name	Quantity	Max Biding Pri...	Statu	To be sold
Sell Bitcoin	7	BO	1	10000	Pending	1
Sell Bitcoin	7	BO	1	10005	Pending	1
Sell Bitcoin	7	BO	2	10050	Pending	2
Sell Bitcoin	11	BA	1	10020	Pending	1
Sell Bitcoin	11	BA	1	10003	Pending	1
Sell Bitcoin	11	BA	1	10030	Pending	1

Deal Price

Buyer Request List

Message	Broker ID	Broker Name	Quantity	Min Selling Pr...	Statu	To be bought
Buy Bitcoin	7	BO	1	10005	Pending	1
Buy Bitcoin	7	BO	1	10090	Pending	1
Buy Bitcoin	7	BO	1	10100	Pending	1
Buy Bitcoin	11	BA	1	10020	Pending	1
Buy Bitcoin	11	BA	1	10030	Pending	1
Buy Bitcoin	11	BA	1	10009	Pending	1

Sort

Match

Confirm



Screenshots 2

User Name

11

Password

==

Login

Logout

Sign Up

Customer Management Work Area

Authentication

Customer List

Withdraw Bitcoin

Unresovled Request

Message	Id	Sender	Quantity	Statu
---------	----	--------	----------	-------

Submit

Resovled Request

Message	Id	Sender	Receiver	Quantity	Status
True	16	Ep	CM	9450	Authenticated
True	16	Ep	CM	10557	Authenticated
True	16	Ep	CM	9228	Authenticated
True	16	Ep	CM	3967	Authenticated
True	16	Ep	CM	10357	Authenticated

User Name

31

Password

==

Login

Logout

Sign Up

Bank Accountant Work Area

Deposit

Recharge

Withdraw

Customer List

Recharge

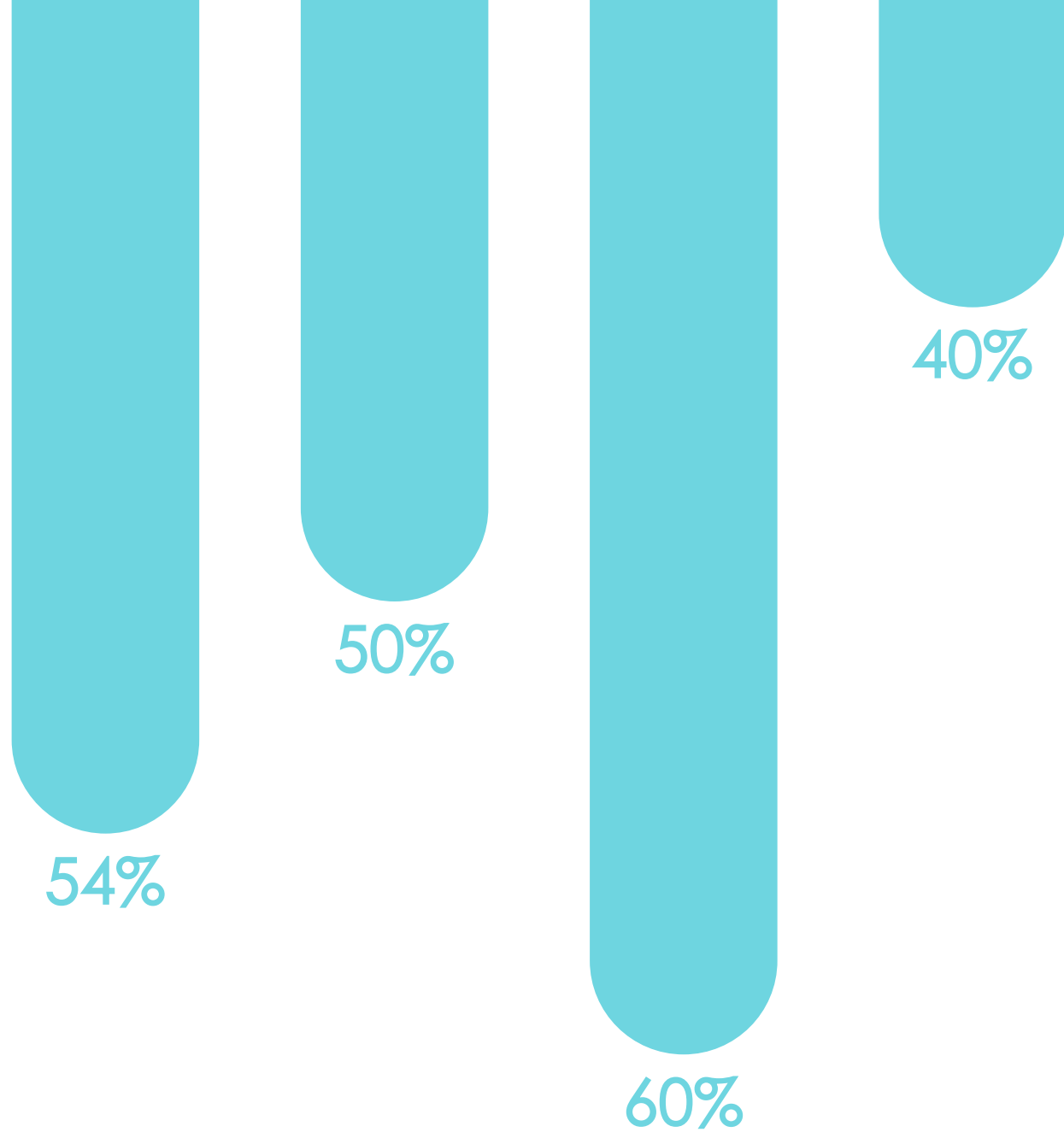
Message	Amount	Sender	Receiver	Status
Recharge Money	60000.0	66	31	Completed
Recharge Money	60000.0	55	31	Completed

Check

Available Money:

Recharged Money:

Process



Demo



Thank You