

IT Crypto Currency on Blockchain Demo

Author: Bhavin Pandya

Date: 8 April 2016

Email: PandyaB@rba.gov.au, bhavin6431@gmail.com

1 SUMMARY

This document outlines the Proof of Concept implemented for IT Crypto Currency based on Blockchain distributed database. This implementation contains set of user accounts between which the transactions are processed. Each user of the system has a user account and a local copy of the Blockchain distributed database. Each user is capable of paying another user and mining the transaction generated due to payments between user accounts. The implementation demonstrates the core concept of Blockchain distributed database, Cryptography and Transaction Mining. This is implemented using Core Java and Restful web services. There are certain limitations of this implementation which can be further looked into if required.

2 CONCEPTS

Following concepts are demonstrated in this implementations.

- Blockchain
 - Distributed transactions database is implemented as Java Collections.
 - It is distributed and maintained as part of the system transactions.
 - Knowledge of full list of transactions is needed for any user to generate valid transaction.
 - Each transaction has a key which is used to validate Blockchain. Any missing transaction or invalid key within transaction will mark the Blockchain as invalid.
 - Valid Blockchain is required to fully reconcile User Account balances.
- Storage
 - UserAccounts
 - Each user has a user account. User account contains the user details and account balance.
 - Account balance in User Account is used for payments and transactions.
 - Public key in User Account is used for Cryptography purpose.
 - Id in User Account identifies the account individually.
 - Transactions
 - Each payment is represented as transaction. Transaction contains the payment and mining details.
 - Key in transaction is used for Blockchain validation.

- Payer, Payee, amount and signature is also part of Transaction used for payments.
- o Serialization and deserialization
 - Transaction and UserAccounts are serialized on the file system at the exit and de-serialized at the startup.
- o MineRequest
 - Mine request is used for Proof of work system. Mine requests is send to each known user.
 - It is initiated by payer as part of the transaction generation.
 - Mine request contains key, result, operator and transaction itself.
 - It is required to find operand as part of mining process.
 - Mine requests and responses checked against the public-private key combinations of the payer and miner user accounts for crypto correct messages.
- o MineResponse
 - Mine response is used as a result of the mine request. It is send to payer by miner of the mine request as part of the Proof of work system.
 - All the details from mine request and operand, which is the result of the mining process, solver user id, timestamp and transaction.
 - Mine requests and responses checked against the public-private key combinations of the payer and miner user accounts for crypto correct messages.
- o UpdateChain
 - Update chain is validated mine response, by payer of the transaction, send to all the users of the system to update according to mine response details.
 - It is the last transaction as part of the processing of the payment.
- o UpdateAllUserAccounts
 - This option requests all users of the system to send any known user accounts to the requestor user. Requestor user then updates and merges all the account to its local user account storage.
 - This is required to have all the user accounts in sync in this implementation for any existing or new users.
- o UpdateAllTransactions
 - This option requests all transactions of the system to send any known transactions to the requestor user. Requestor user then updates and merges all the transactions to its local transactions storage.
 - This is required to have all the transaction in sync in this implementation for any new user.
- Mining
 - o In this implementation, mining is done by finding operand using key, result and operator provided.
As an example,
 - transactionKey = 3 (sum of all the keys in Blockchain)
 - result = 40
 - operator = "/"

Then miner has to go through all the possible operand values to find;
 $\text{possibleOperand} / 3 = 40$

In this case, possible operand is 120. Each miner has to go through various numbers or combinations or algorithms to effectively find the possibleOperand. The better the algorithm, the higher the chance of finding the possibleOperand quicker. Therefore winning the mining prize, 100 in this implementation, for the miner.

- PKI
Private and public key combination is used for cryptography to validate transaction, validate initiator and validate miner etc.
 - Private key
 - Each user has a private key that is private to the user and not shared.
 - This is used to generate signature in this case it's simply multiplying private key by random number generated from 1-10.
 - Public key
 - Each user has a public key that is public to all the users and shared.
 - This is used to validate signature in this case it's simply performing module operator on signature to find if it's zero.

3 TECHNOLOGIES

- Java
- Restful
- Maven
- Jetty
- Apache Common Collections
- GSON

4 LIMITATIONS

- Less secure
The implementation is less secure and only design for the demo purposes. However, security strategies for Cryptography and Blockchain implementation is pluggable and can further be strengthened.
- Manual User Account Sync
User accounts are synced between users using manual option and transaction. This could further be automated.
- Transactions and user account reconciliation
This implementation handles basic conditions to reconcile user accounts and transactions. More advanced conditions of mismatch between user accounts and transaction can be further developed.

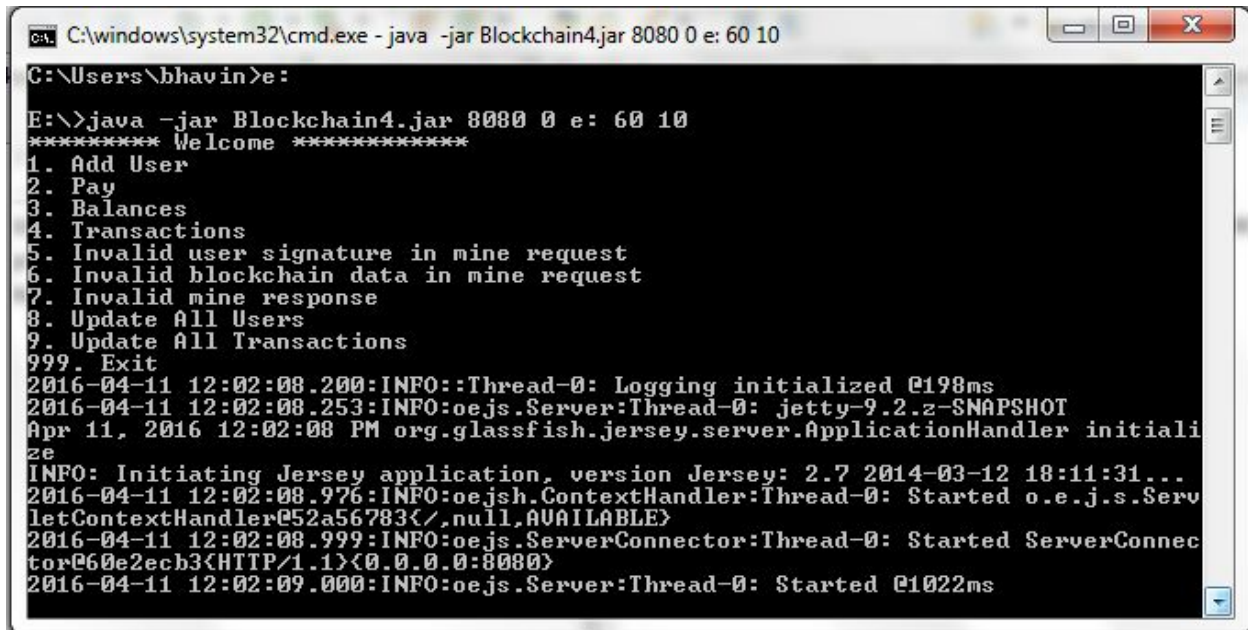
- Random sleep in mining

Random sleep is introduced in mining algorithm to provide unpredictability of solving the mining request.

5 USAGE

Following screen shot demonstrates the sample usage of the implementation

5.1 STARTUP



```
C:\windows\system32\cmd.exe - java -jar Blockchain4.jar 8080 0 e: 60 10
C:\Users\bhavin>e:
E:\>java -jar Blockchain4.jar 8080 0 e: 60 10
***** Welcome *****
1. Add User
2. Pay
3. Balances
4. Transactions
5. Invalid user signature in mine request
6. Invalid blockchain data in mine request
7. Invalid mine response
8. Update All Users
9. Update All Transactions
999. Exit
2016-04-11 12:02:08.200:INFO::Thread-0: Logging initialized @198ms
2016-04-11 12:02:08.253:INFO:oejs.Server:Thread-0: jetty-9.2.2-SNAPSHOT
Apr 11, 2016 12:02:08 PM org.glassfish.jersey.server.ApplicationHandler initiali
ze
INFO: Initiating Jersey application, version Jersey: 2.7 2014-03-12 18:11:31...
2016-04-11 12:02:08.976:INFO:oejsh.ContextHandler:Thread-0: Started o.e.j.s.Serv
letContextHandler@52a56783</,null,AVAILABLE>
2016-04-11 12:02:08.999:INFO:oejs.ServerConnector:Thread-0: Started ServerConnec
tor@60e2ecb3<HTTP/1.1><0.0.0.0:8080>
2016-04-11 12:02:09.000:INFO:oejs.Server:Thread-0: Started @1022ms
```

```
C:\windows\system32\cmd.exe - java -jar Blockchain4.jar 8081 1 e: 700 100

E:\>java -jar Blockchain4.jar 8081 1 e: 700 100
2016-04-11 12:04:02.997:INFO::Thread-0: Logging initialized @199ms
***** Welcome *****
1. Add User
2. Pay
3. Balances
4. Transactions
5. Invalid user signature in mine request
6. Invalid blockchain data in mine request
7. Invalid mine response
8. Update All Users
9. Update All Transactions
999. Exit
2016-04-11 12:04:03.052:INFO:oejs.Server:Thread-0: jetty-9.2.z-SNAPSHOT
Apr 11, 2016 12:04:03 PM org.glassfish.jersey.server.ApplicationHandler initiali
ze
INFO: Initiating Jersey application, version Jersey: 2.7 2014-03-12 18:11:31...
2016-04-11 12:04:03.740:INFO:oejsh.ContextHandler:Thread-0: Started o.e.j.s.Serv
letContextHandler@60f931b1</,null,AVAILABLE>
2016-04-11 12:04:03.763:INFO:oejs.ServerConnector:Thread-0: Started ServerConnec
tor@6ee1a701<HTTP/1.1><0.0.0.0:8081>
2016-04-11 12:04:03.763:INFO:oejs.Server:Thread-0: Started @1004ms
```

```
C:\windows\system32\cmd.exe - java -jar Blockchain4.jar 8082 2 e: 800 200

E:\>java -jar Blockchain4.jar 8082 2 e: 800 200
***** Welcome *****
1. Add User
2. Pay
3. Balances
4. Transactions
5. Invalid user signature in mine request
6. Invalid blockchain data in mine request
7. Invalid mine response
8. Update All Users
9. Update All Transactions
999. Exit
2016-04-11 12:04:43.660:INFO::Thread-0: Logging initialized @195ms
2016-04-11 12:04:43.711:INFO:oejs.Server:Thread-0: jetty-9.2.z-SNAPSHOT
Apr 11, 2016 12:04:44 PM org.glassfish.jersey.server.ApplicationHandler initiali
ze
INFO: Initiating Jersey application, version Jersey: 2.7 2014-03-12 18:11:31...
2016-04-11 12:04:44.397:INFO:oejsh.ContextHandler:Thread-0: Started o.e.j.s.Serv
letContextHandler@443c2e0b</,null,AVAILABLE>
2016-04-11 12:04:44.420:INFO:oejs.ServerConnector:Thread-0: Started ServerConnec
tor@5218f9d7<HTTP/1.1><0.0.0.0:8082>
2016-04-11 12:04:44.421:INFO:oejs.Server:Thread-0: Started @971ms
```

```
C:\windows\system32\cmd.exe - java -jar Blockchain4.jar 8083 3 e: 2000 1000

E:\>java -jar Blockchain4.jar 8083 3 e: 2000 1000
***** Welcome *****
1. Add User
2. Pay
3. Balances
4. Transactions
5. Invalid user signature in mine request
6. Invalid blockchain data in mine request
7. Invalid mine response
8. Update All Users
9. Update All Transactions
999. Exit
2016-04-11 12:05:28.003:INFO::Thread-0: Logging initialized @194ms
2016-04-11 12:05:28.055:INFO:oejs.Server:Thread-0: jetty-9.2.z-SNAPSHOT
Apr 11, 2016 12:05:28 PM org.glassfish.jersey.server.ApplicationHandler initialize
INFO: Initiating Jersey application, version Jersey: 2.7 2014-03-12 18:11:31...
2016-04-11 12:05:28.760:INFO:oejsh.ContextHandler:Thread-0: Started o.e.j.s.ServletContextHandler@443c2e0b</,null,AVAILABLE>
2016-04-11 12:05:28.783:INFO:oejs.ServerConnector:Thread-0: Started ServerConnector@65babc5c<HTTP/1.1><0.0.0.0:8083>
2016-04-11 12:05:28.784:INFO:oejs.Server:Thread-0: Started @990ms
```

5.2 UPDATE ALL USERS

```
C:\windows\system32\cmd.exe - java -jar Blockchain4.jar 8080 0 e: 60 10
9. Update All Transactions
999. Exit
2016-04-11 12:09:05.523:INFO::Thread-0: Logging initialized @192ms
2016-04-11 12:09:05.573:INFO:oejs.Server:Thread-0: jetty-9.2.z-SNAPSHOT
Apr 11, 2016 12:09:05 PM org.glassfish.jersey.server.ApplicationHandler initiali
ze
INFO: Initiating Jersey application, version Jersey: 2.7 2014-03-12 18:11:31...
2016-04-11 12:09:06.268:INFO:oejs.ContextHandler:Thread-0: Started o.e.j.s.Serv
letContextHandler@56c45846[/,null,AVAILABLE]
2016-04-11 12:09:06.292:INFO:oejs.ServerConnector:Thread-0: Started ServerConnec
tor@5fb80d14[HTTP/1.1]<0.0.0.0:8080>
2016-04-11 12:09:06.292:INFO:oejs.Server:Thread-0: Started @977ms
8
***** Welcome *****
1. Add User
2. Pay
3. Balances
4. Transactions
5. Invalid user signature in mine request
6. Invalid blockchain data in mine request
7. Invalid mine response
8. Update All Users
9. Update All Transactions
999. Exit
```

5.3 BALANCES

```
C:\windows\system32\cmd.exe - java -jar Blockchain4.jar 8080 0 e: 60 10
4. Transactions
5. Invalid user signature in mine request
6. Invalid blockchain data in mine request
7. Invalid mine response
8. Update All Users
9. Update All Transactions
999. Exit
3
[UserAccount [id=0, balance=10000, userName=TestUser, publicKey=10, port=8080],
UserAccount [id=1, balance=10000, userName=TestUser, publicKey=100, port=8081],
UserAccount [id=2, balance=10100, userName=TestUser, publicKey=200, port=8082],
UserAccount [id=3, balance=10000, userName=TestUser, publicKey=1000, port=8083],
UserAccount [id=4, balance=10000, userName=TestUser, publicKey=60, port=8084]]
***** Welcome *****
1. Add User
2. Pay
3. Balances
4. Transactions
5. Invalid user signature in mine request
6. Invalid blockchain data in mine request
7. Invalid mine response
8. Update All Users
9. Update All Transactions
999. Exit
```


5.4 UPDATE ALL TRANSACTIONS

```
C:\windows\system32\cmd.exe - java -jar Blockchain4.jar 8080 0 e: 60 10

UserAccount lid=4, balance=10000, userName=TestUser, publicKey=60, port=808411
***** Welcome *****
1. Add User
2. Pay
3. Balances
4. Transactions
5. Invalid user signature in mine request
6. Invalid blockchain data in mine request
7. Invalid mine response
8. Update All Users
9. Update All Transactions
999. Exit
9
***** Welcome *****
1. Add User
2. Pay
3. Balances
4. Transactions
5. Invalid user signature in mine request
6. Invalid blockchain data in mine request
7. Invalid mine response
8. Update All Users
9. Update All Transactions
999. Exit
```

5.5 TRANSACTIONS

```
C:\windows\system32\cmd.exe - java -jar Blockchain4.jar 8080 0 e: 60 10

5. Invalid user signature in mine request
6. Invalid blockchain data in mine request
7. Invalid mine response
8. Update All Users
9. Update All Transactions
999. Exit
4
[Transaction lid=0, signature=0, minedTimestamp=1460327041199, key=1, payerId=0,
payeeId=1, amount=200, comment=0-1], Transaction lid=1, signature=5600, minedTi
mestamp=1460327053129, key=2, payerId=1, payeeId=2, amount=300, comment=1-2], Tr
ansaction lid=2, signature=6400, minedTimestamp=1460327065102, key=4, payerId=2,
payeeId=3, amount=200, comment=2-3], Transaction lid=3, signature=14000, minedT
imestamp=1460327120485, key=8, payerId=3, payeeId=0, amount=200, comment=3-0]]
***** Welcome *****
1. Add User
2. Pay
3. Balances
4. Transactions
5. Invalid user signature in mine request
6. Invalid blockchain data in mine request
7. Invalid mine response
8. Update All Users
9. Update All Transactions
999. Exit
```


5.6 PAYMENT

```
C:\windows\system32\cmd.exe - java -jar Blockchain4.jar 8080 0 e: 60 10

6. Invalid blockchain data in mine request
7. Invalid mine response
8. Update All Users
9. Update All Transactions
999. Exit
2
Enter Payee Id : 1
Enter Amount : 200
Enter Comment: User 0 -> User 1
Mine Response : {"key":16,"result":40,"operator":"/","operand":640,"solverUserId":1,"transaction":{"id":4,"signature":540,"minedTimestamp":1460340796453,"key":16,"payerId":0,"payeeId":1,"amount":200,"comment":"User 0 -\u003e User 1"},"timestamp":1460340796453}
***** Welcome *****
1. Add User
2. Pay
3. Balances
4. Transactions
5. Invalid user signature in mine request
6. Invalid blockchain data in mine request
7. Invalid mine response
8. Update All Users
9. Update All Transactions
999. Exit
```

```
C:\windows\system32\cmd.exe - java -jar Blockchain4.jar 8081 1 e: 700 100

2016-04-11 12:09:26.522:INFO::Thread-0: Logging initialized @208ms
2016-04-11 12:09:26.576:INFO:oejs.Server:Thread-0: jetty-9.2.z-SNAPSHOT
Apr 11, 2016 12:09:26 PM org.glassfish.jersey.server.ApplicationHandler initialize
INFO: Initiating Jersey application, version Jersey: 2.7 2014-03-12 18:11:31...
2016-04-11 12:09:27.294:INFO:oejsh.ContextHandler:Thread-0: Started o.e.j.s.ServletContextHandler@4715407a{/,null,AVAILABLE}
2016-04-11 12:09:27.318:INFO:oejs.ServerConnector:Thread-0: Started ServerConnector@5218f9d7{HTTP/1.1}{0.0.0.0:8081}
2016-04-11 12:09:27.319:INFO:oejs.Server:Thread-0: Started @1021ms
Mine Request received : {"key":16,"result":40,"operator":"/","transaction":{"id":4,"signature":540,"minedTimestamp":0,"key":16,"payerId":0,"payeeId":1,"amount":200,"comment":"User 0 -\u003e User 1"}}
Mine request : MineRequest [key=16, result=40, operator=/, transaction=Transaction [id=4, signature=540, minedTimestamp=0, key=16, payerId=0, payeeId=1, amount=200, comment=User 0 -> User 1]]
Mine Response : MineResponse [key=16, result=40, operator=/, operand=640, solverUserId=1, transaction=Transaction [id=4, signature=540, minedTimestamp=1460340796453, key=16, payerId=0, payeeId=1, amount=200, comment=User 0 -> User 1], timestamp=1460340796453]
Update Chain Mine Response : {"key":16,"result":40,"operator":"/","operand":640,"solverUserId":1,"transaction":{"id":4,"signature":540,"minedTimestamp":1460340796453,"key":16,"payerId":0,"payeeId":1,"amount":200,"comment":"User 0 -\u003e User 1"},"timestamp":1460340796453}
```

```
C:\windows\system32\cmd.exe - java -jar Blockchain4.jar 8082 2 e: 800 200

9. Update All Transactions
999. Exit
2016-04-11 12:09:41.426:INFO::Thread-0: Logging initialized @196ms
2016-04-11 12:09:41.480:INFO:oejs.Server:Thread-0: jetty-9.2.z-SNAPSHOT
Apr 11, 2016 12:09:41 PM org.glassfish.jersey.server.ApplicationHandler initialize
INFO: Initiating Jersey application, version Jersey: 2.7 2014-03-12 18:11:31...
2016-04-11 12:09:42.169:INFO:oejs.ContextHandler:Thread-0: Started o.e.j.s.ServletContextHandler@205992c6</,null,AVAILABLE>
2016-04-11 12:09:42.192:INFO:oejs.ServerConnector:Thread-0: Started ServerConnector@222e289d<HTTP/1.1><0.0.0.0:8082>
2016-04-11 12:09:42.193:INFO:oejs.Server:Thread-0: Started @979ms
Update Chain Mine Response : <{"key":16,"result":40,"operator":"/","operand":640,"solverUserId":1,"transaction":{"id":4,"signature":540,"minedTimestamp":1460340796453,"key":16,"payerId":0,"payeeId":1,"amount":200,"comment":"User 0 -\u003e User 1"},"timestamp":1460340796453}>
Mine Request received : <{"key":16,"result":40,"operator":"/","transaction":{"id":4,"signature":540,"minedTimestamp":0,"key":16,"payerId":0,"payeeId":1,"amount":200,"comment":"User 0 -\u003e User 1"}}>
Mine request : MineRequest [key=16, result=40, operator=/, transaction=Transaction [id=4, signature=540, minedTimestamp=0, key=16, payerId=0, payeeId=1, amount=200, comment=User 0 -> User 1]]
Invalid blockchain request !!
Invalid mine request !!
```

```
C:\windows\system32\cmd.exe - java -jar Blockchain4.jar 8083 3 e: 2000 1000

9. Update All Transactions
999. Exit
2016-04-11 12:09:55.293:INFO::Thread-0: Logging initialized @197ms
2016-04-11 12:09:55.344:INFO:oejs.Server:Thread-0: jetty-9.2.z-SNAPSHOT
Apr 11, 2016 12:09:55 PM org.glassfish.jersey.server.ApplicationHandler initialize
INFO: Initiating Jersey application, version Jersey: 2.7 2014-03-12 18:11:31...
2016-04-11 12:09:56.042:INFO:oejs.ContextHandler:Thread-0: Started o.e.j.s.ServletContextHandler@2dfc180a</,null,AVAILABLE>
2016-04-11 12:09:56.065:INFO:oejs.ServerConnector:Thread-0: Started ServerConnector@43cd2ed4<HTTP/1.1><0.0.0.0:8083>
2016-04-11 12:09:56.066:INFO:oejs.Server:Thread-0: Started @985ms
Update Chain Mine Response : <{"key":16,"result":40,"operator":"/","operand":640,"solverUserId":1,"transaction":{"id":4,"signature":540,"minedTimestamp":1460340796453,"key":16,"payerId":0,"payeeId":1,"amount":200,"comment":"User 0 -\u003e User 1"},"timestamp":1460340796453}>
Mine Request received : <{"key":16,"result":40,"operator":"/","transaction":{"id":4,"signature":540,"minedTimestamp":0,"key":16,"payerId":0,"payeeId":1,"amount":200,"comment":"User 0 -\u003e User 1"}}>
Mine request : MineRequest [key=16, result=40, operator=/, transaction=Transaction [id=4, signature=540, minedTimestamp=0, key=16, payerId=0, payeeId=1, amount=200, comment=User 0 -> User 1]]
Invalid blockchain request !!
Invalid mine request !!
```

5.7 INVALID SIGNATURE MINING REQUEST

```
C:\windows\system32\cmd.exe - java -jar Blockchain4.jar 8083 3 e: 2000 1000

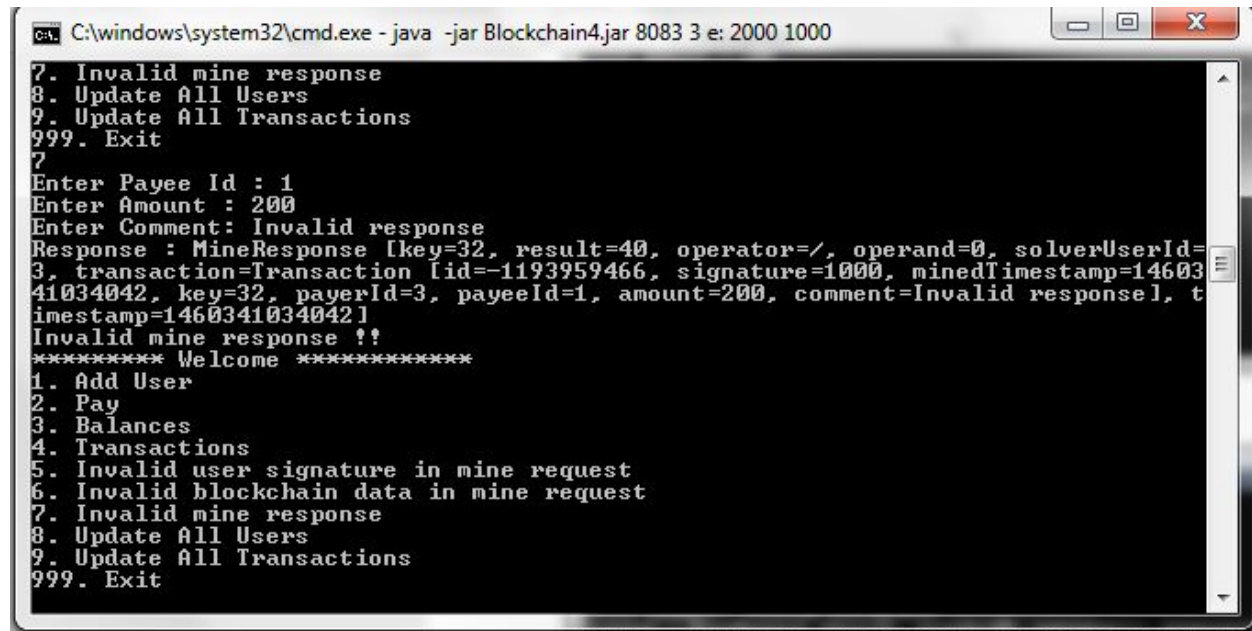
7. Invalid mine response
8. Update All Users
9. Update All Transactions
999. Exit
5
Enter Payee Id : 1
Enter Amount : 200
Enter Comment: Invalid signature
Request : MineRequest [key=32, result=40, operator=/, transaction=Transaction [i
d=-1193959466, signature=-2322, minedTimestamp=0, key=32, payerId=3, payeeId=1,
amount=200, comment=Invalid signature ]]
Unauthenticated user !!
Invalid user signature in mine request!!
***** Welcome *****
1. Add User
2. Pay
3. Balances
4. Transactions
5. Invalid user signature in mine request
6. Invalid blockchain data in mine request
7. Invalid mine response
8. Update All Users
9. Update All Transactions
999. Exit
```

5.8 INVALID BLOCKCHAIN MINING REQUEST

```
C:\windows\system32\cmd.exe - java -jar Blockchain4.jar 8083 3 e: 2000 1000

7. Invalid mine response
8. Update All Users
9. Update All Transactions
999. Exit
6
Enter Payee Id : 1
Enter Amount : 200
Enter Comment: Invalid blockchain
Request : MineRequest [key=32, result=40, operator=/, transaction=Transaction [i
d=-1193959466, signature=1000, minedTimestamp=0, key=204848473, payerId=3, payee
Id=1, amount=200, comment=Invalid blockchain]]
Invalid blockchain request !!
Invalid blockchain data in mine request!!
***** Welcome *****
1. Add User
2. Pay
3. Balances
4. Transactions
5. Invalid user signature in mine request
6. Invalid blockchain data in mine request
7. Invalid mine response
8. Update All Users
9. Update All Transactions
999. Exit
```

5.9 INVALID MINE RESPONSE



```
C:\windows\system32\cmd.exe - java -jar Blockchain4.jar 8083 3 e: 2000 1000
7. Invalid mine response
8. Update All Users
9. Update All Transactions
999. Exit
7
Enter Payee Id : 1
Enter Amount : 200
Enter Comment: Invalid response
Response : MineResponse [key=32, result=40, operator=/, operand=0, solverUserId=
3, transaction=Transaction [id=-1193959466, signature=1000, minedTimestamp=14603
41034042, key=32, payerId=3, payeeId=1, amount=200, comment=Invalid responsel, t
imestamp=1460341034042]
Invalid mine response !!
***** Welcome *****
1. Add User
2. Pay
3. Balances
4. Transactions
5. Invalid user signature in mine request
6. Invalid blockchain data in mine request
7. Invalid mine response
8. Update All Users
9. Update All Transactions
999. Exit
```