Demonstrating the security of a basic cryptocurrency

Sean Horgan - 2184253

Introduction

Cryptocurrency history

Why cryptocurrencies are important.

Goal for this project

Analysis

Requirements:

- Tamper-proof distributed ledger
- Proof of Work system
- Consensus mechanism

Other requirements and limitations

Design

Transactions

Blockchain

Consensus Mechanism

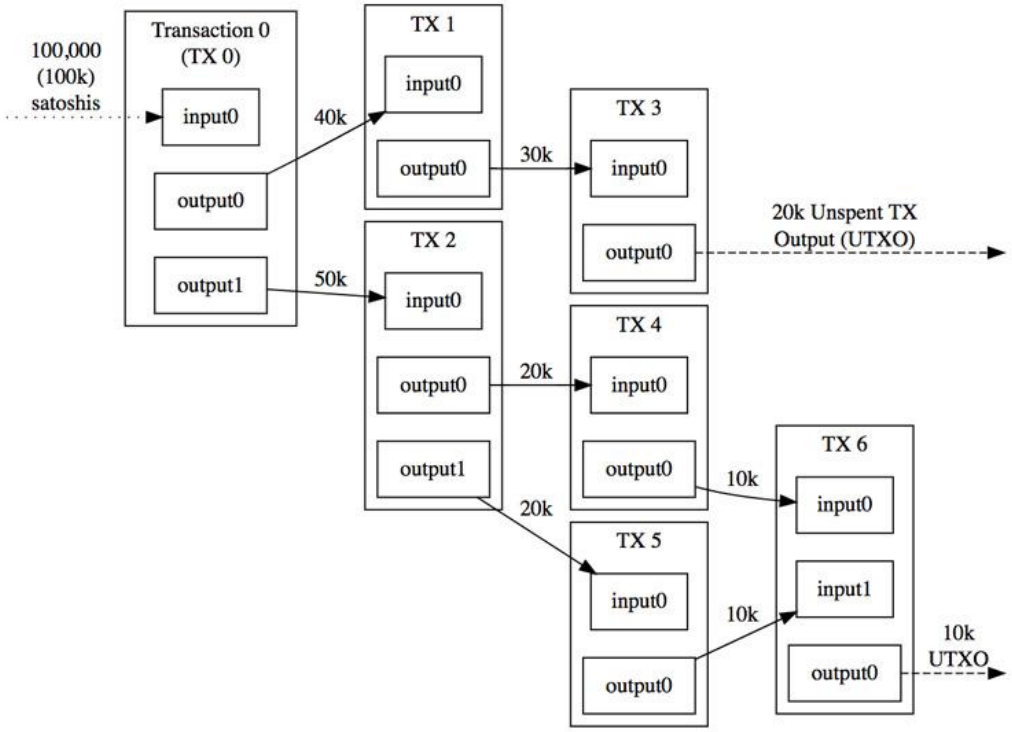
Test Harness

Transactions

Transaction inputs & outputs

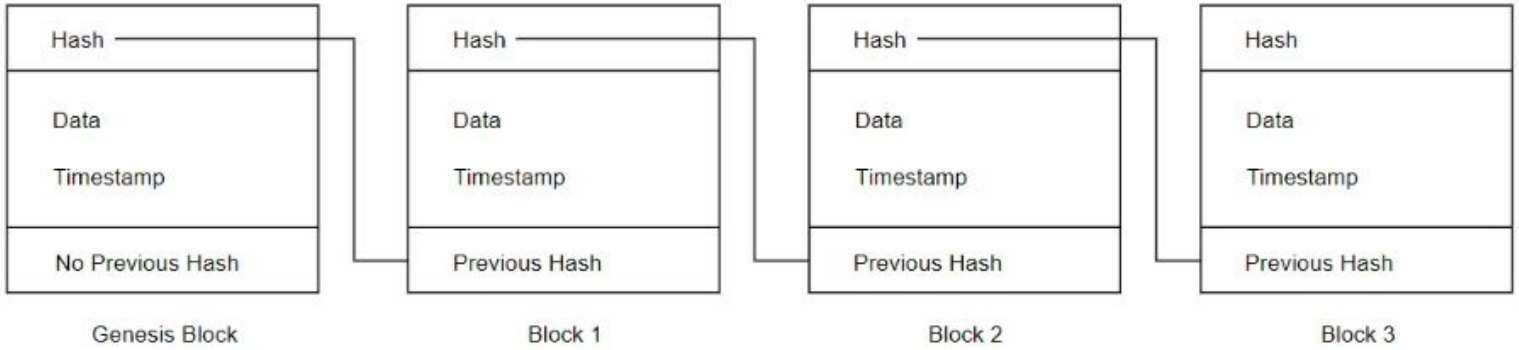
Process and checks

Currency creation



Triple-Entry Bookkeeping (Transaction-To-Transaction Payments) As Used By Bitcoin

Blockchain


Hash
Data
Timestamp
No Previous Hash
Genesis Block
Hash
Data
Timestamp
Previous Hash
Block 1
Hash
Data
Timestamp
Previous Hash
Block 2
Hash
Data
Timestamp
Previous Hash
Block 3

Implementation

Java and its Security Packages

Unspent Transaction Output list (UTXO)

Nearby nodes algorithm

Switching blockchains

Results

3 methods of evaluating the project

- Double Spending Attacks
- Sybil Attacks
- Blockchain Security

Results

Double spending attacks

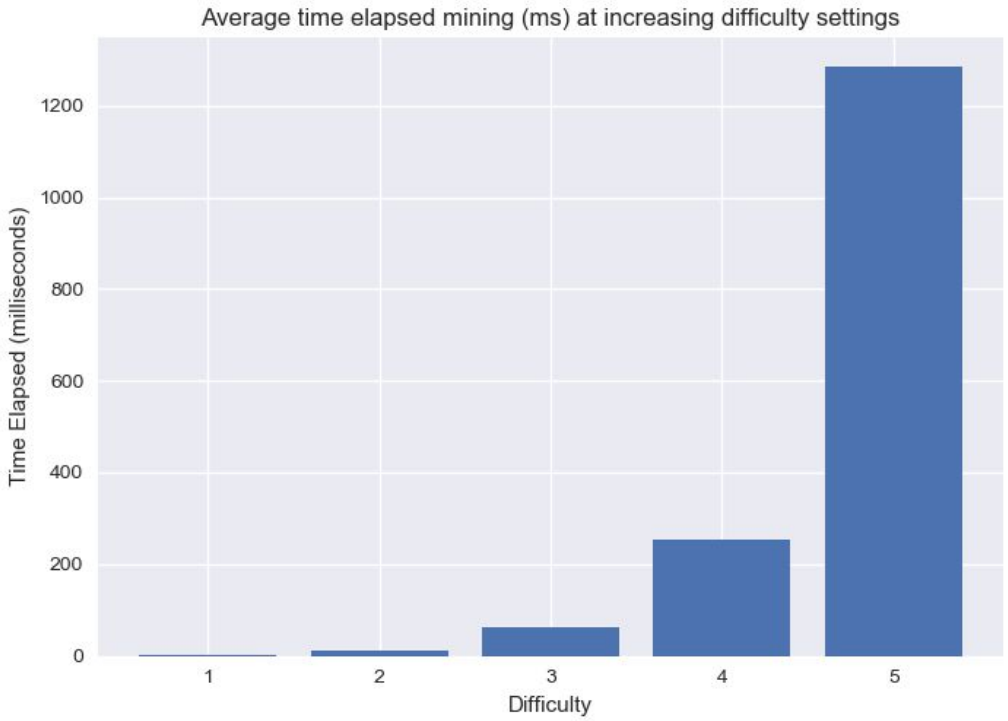
Tests showed the project successfully handled the attacks

```
---------TESTING------------
Value: 10.0, Inputsum: 0.0, Overpay: 0.0, ID: test
Block Mined: 00d6b4407be9b9cc5e702a73688169879c8578646c5a3be3497902da80361514
Time elapsed mining: 4747
TRANSACTION FAILED: This transaction is already included on the blockchain!
```

Results

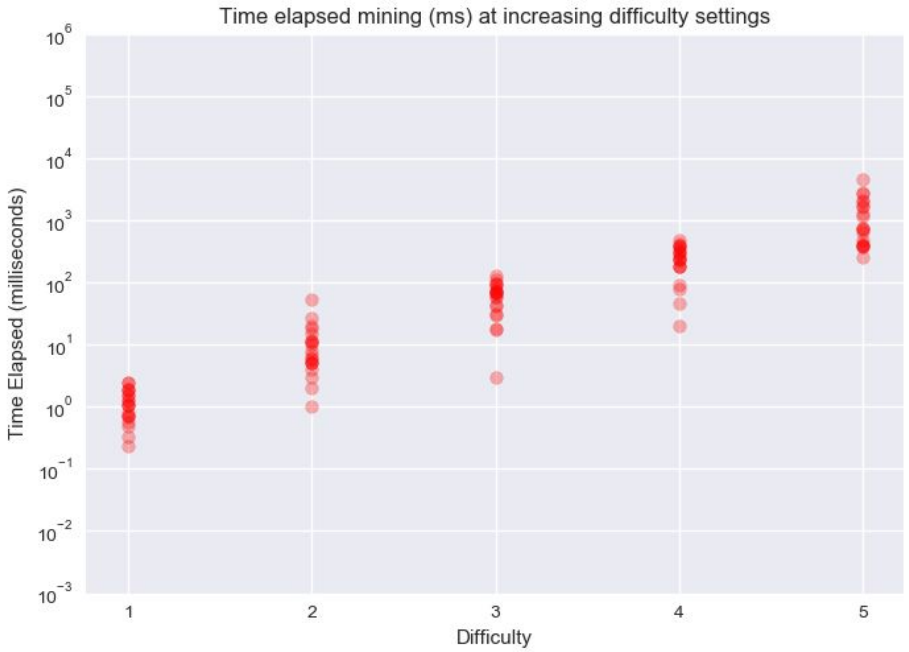
What is a Sybil attack?

Does the cryptocurrency prevent Sybil attacks?



Results

Time elapsed mining relative to mining difficulty setting



Results

Blockchain security

Tests showed the project successfully recognised any changes to the blockchain.

```
---------TESTING------------
Value: 10.0, Inputsum: 0.0, Overpay: 0.0, ID: test3
Block Mined: 00fc8325eb96d0578b4b81b2e61eed8067578ce3887b5f627279c93decad0c5c
Time elapsed mining: 446
Value: 6.0, Inputsum: 100.0, Overpay: 94.0, ID: caba88ed9698dc6f95e651103e428ed5804f1223d48be3e647b89e54eb6f099a
BLOCKCHAIN FAILURE: Hash of a block has been changed since inception!
Invalid blockchain: Aborting block mining...
Switching Blockchain...
```

Conclusion

What this project create?

Did this satisfy the project title?

Future work