UM–SJTU Joint Institute

Introduction to Cryptography
(VE475)

# Project Report

## Group 1

### bitcoin


Name: Liu Niyiqiu ID: 516370910118
Name: Xiang Zhiyuan ID: 516370910118
Name: S ID: 516370910118


Date: 26 July 2019

# Contents

# 1 Mining

## 1.1 Definition of Mining

The bitcoin is a decentralized cryptocurrent. No authorities are present to authenticate each transaction. Thus the burden of verifying transactions and gathering valid transactions lies to the miners. The ultimate goal of a miner is to constitute a block by solving a mathematical problem, which will be described in the next section. To compensate the computational power spent by the miner, some bitcoins are given to the first miner that create a new block. Also, the payer in a transaction may specify a transaction fee that will be given to the miner.

## 1.2 Mathematics of Mining

### 1.2.1 Proof of Work

The cost function is define as

$$\begin{aligned} \mathcal{F} : \mathcal{S} \times \mathbb{N}^* \times \mathbb{N}^* &\longrightarrow \{\text{True, False}\} \\ (s, D, x) &\longmapsto \mathcal{F}(s, D, x) \end{aligned}$$

The set $\mathcal{S}$ is the set of strings. $D \in \mathbb{N}^*$ is the difficulty level of this problem and $x$ is called a nonce. $\mathcal{F}(s, D, x)$ returns true if and only if $\text{Hash}(A|D|x)$ starts with $D$ zeros.

In the case of bitcoin, the hash function SHA-256 is used. In practice, $s$ and $D$ is fixed, the process of proof of work is to find a nonce $x$ such that $\mathcal{F}(s, D, x)$ returns true. An example of proof of work is shown in Fig. 1. In this process the nonce $x$ is chosen in the order of the natural numbers.

```
"Hello, world!0" => 1312af178c253f84028d480a6adc1e25e81caa44c749ec81976192e2ec934c64
"Hello, world!1" => e9afc424b79e4f6ab42d99c81156d3a17228d6e1eef4139be78e948a9332a7d8
"Hello, world!2" => ae37343a357a8297591625e7134cbea22f5928be8ca2a32aa475cf05fd4266b7
...
"Hello, world!4248" => 6e110d98b388e77e9c6f042ac6b497cec46660deef75a55ebc7cfdf65cc0b965
"Hello, world!4249" => c004190b822f1669cac8dc37e761cb73652e7832fb814565702245cf26ebb9e6
"Hello, world!4250" => 0000c3af42fc31103f1fdc0151fa747ff87349a4714df7cc52ea464e12dcd4e9
```

Figure 1: Example of a proof of work (from bitwiki).

### 1.2.2 Mining a New Block

The mining process is to solve the problem given by proof of work. At a given time, a node would gather transactions and form a block. To add this

block to the block chain, the node has to solve the following problem:

Looking for a nonce $x$ such that: $Hash(s|x) <$ target
$s = s_1|s_2|s_3|s_4|s_5$
$s_1 =$ version
$s_2 =$ hash of previous block
$s_3 =$ hash of merkle root
$s_4 =$ timestamp
$s_5 =$ target

A block is composed of a block header and a block body. The block header is defined as $s|x$. Once a suitable nonce $x$ is found, the miner is can publish this block and add it to the block chain.

## 1.3 General Procedure of Mining

1. Alice gathers the transactions and put them in a block (a block can contain approximately 4,000 transactions)
2. Alice tries to solve the proof of work by finding a suitable nonce $x$
3. If Alice is the first one to mine a new block, she may announce the block to the public and add it to the block chain
4. If in the process of mining, a new block is mined by Bob. Alice abandons her block and restart step 1.

## 1.4 The Byzantine Generals' Problem

A number of Byzantine Generals each has his own computer. They communicate through Internet to devise a plan to attack king's army. Only with a joint forces between the generals can they beat the king's army. However, several generals are spies deplored by the king. They would try to sabotage the proposed good plans. In this situation, the Byzantine General's Problem is given by how to agree upon a feasible plan to attack the king's army, given the condition that most of the generals (more than half in the case of bitcoin) are honest.

In the set up of bicoin, the Byzantine Generals' Problem is solved by the mining process at the cost of computational power (electricity). With the hard "inverse hash" step in the proof of work, the bitcoin system guarantees that no malicious user can double spend their bitcoins of forge a transaction, as will be shown in the next section.

### 1.5 Double Spending and Forgery

Now Eve has ten bitcoins and she proposes transactions to both Bob and Alice to give them ten bitcoins each. In the meantime, there are two miners Charlie and Manuel.

1. Eve announces a 10-bitcoin-transaction to both Bob and Alice. (She only has 10 bitcoins left)

2. Charlie first receives Eve's transaction to Alice, so he ignores Eve's transaction request to Bob.

3. Due to delay of the Internet, Manuel first receives Eves transaction to Bob. So he ignores Eve's transaction request to Alice.

4. Charlie and Manuel gather some transactions and both start to mine a block.

5. Without lose of generality, let's assume Manuel beats Charlie and solve the proof of work problem. Manuel happily add this new block to block chain.

6. Then Charlie would abandon his block. While gathering transactions for a new block, he would ignore Eve's transaction request because Eve's has already gave her remaining 10 bitcoins to Bob in the previous block mined by Manuel.

## 2 References


1. The Mathematics Behind Bitcoin, Cyril Grunspan, `https://webusers.imj-prg.fr/~ricardo.perez-marco/blockchain/BitcoinP7.pdf`

2. `https://en.bitcoinwiki.org/wiki`