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, a reward of 12.5 bitcoins is given to the first miner that create a new block. Also, the two parties between a transaction may specify a transaction fee that will be given to the miner.

1.2 Mathematics of Mining

1.3 The Byzantine Generals' Problem

2 References

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