**实 验 报 告**



**课程名称 信息安全**

**学 院 软件学院**

**专 业 软件工程**

**姓 名 黄鼎竣 符根**

**学 号 17302010015**

**开 课 时 间 2019 至 2020 学年第 二 学期**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| |  |  |  |  | | --- | --- | --- | --- | | 实验项目  名 称 | **一个简单的区块链钱包** | 成绩 |  |   **一、实验目的**  1) 了解区块链。  2) 实现一个简单的区块链钱包。  3) 验证区块链交易的有效性。  **二、实验内容**  1) 实现区块链钱包的功能，要能生成公私钥对，钱包地址，查询余额。  2) 根据钱包中生成的公私钥，创建新的交易，验证每笔交易的有效性并可以 生成新区块。  **三、实验步骤**   1. Block的实现   Block中，hash为整个交易字段的hash， previousHash代表上一block的hash，merkleRoot代表梅克尔树根的data，transactions代表所有交易， timeStamp为时间戳，nonce为工作量证明。  Block实现的功能如下  calculateHash 计算本区块的hash。  minBlock 挖矿，用于寻找工作量证明。  addTransaction 添加交易记录。  2.Blockchain的实现  Blockchain中维护一个区块链，并且会在运行时模拟2个用户进行交易  Blockchain中实现的方法如下：  isChainValid 检查区块链的完整性  addBlock 在区块链中添加一个新区块  3、Transaction的实现    Transection实现的功能如下  processTransaction 处理交易  getInputsValue 获得交易输入  generateSignature 创建签名  verifySignature 验证签名  getOutputsValue 获得交易输出  calulateHash 计算交易类的hash值  4. Wallet的实现    Wallet中具有公钥私钥对，钱包地址，UTXO池维护交易记录。  Wallet实现的功能如下  generateKeyPair 创建公私钥对  getBalance 查询余额  sendFunds 进行转账  getPrivateKey 获取私钥  generateAddress 创建地址  getAddress 获取地址  5.工具类的使用  Base58Util 进行base58编码和解码  StringUtil 进行SHA256加密、ECDSA签名和验证、根据交易记录返回梅克尔树的根  **四、实验结果及分析**      设置difficulty为3和6的两次运行情况。  **五、实验总结**  通过本次实验，我们对区块链技术有了更加深刻的认识。   1. 区块链实现了一个去中心化的分布式账本，每个节点都是信息或资源的管理者，一个节点出错不会影响其他节点。 2. 了解了非对称加密算法在区块链中的应用。 3. 区块链解决了交易中的对于第三方的信任的问题。区块链交易中不存在这样的第三方，通过智能合约的形式完成交易。对代码的安全性要求比较高，出现漏洞会造成严重的损失。 4. 在规模比较大的情况下，区块链的安全性是比较好的，51%攻击在现实上难以实现。 5. 区块链通过枚举nonce计算hash的方式产生新的区块（挖矿），运行效率很低，difficulty为3时完成一次交易只要1秒，difficulty为5时完成一次交易需要半分钟，difficulty为6时完成一次交易需要约2分钟。可见随着difficulty的增加区块链的运行效率将越来越低。 |
|  |