

比特币介绍

技术篇

2 December 2017

沉风

内容

1.1.1

- 基础
- 地址
- 交易
- PoW共识
- DLT
- P2P
- 安全
- 钱包
- 扩展性
- 问题
- 总结

基础

- SHA
- RIPEMD-160

DSA

- RSA
- ECDSA

SHA

- Secure Hash Algorithm
- 对称加密技术
- SHA Family(SHA-1, SHA-2, SHA-3)

RIPEMD-160

- 同SHA256比起来生成地址更小
- 算法很好保证唯一性，减少hash冲突

RSA

- 非对称加密算法的始祖(公钥与私钥)
- 公钥负责加密, 私钥负责解密
- 私钥负责签名, 公钥负责验证
- 私钥可以得出公钥, 公钥不能反推私钥
- 数学原理与证明
- 加解密效率低
- 安全强度有限, 占用空间大

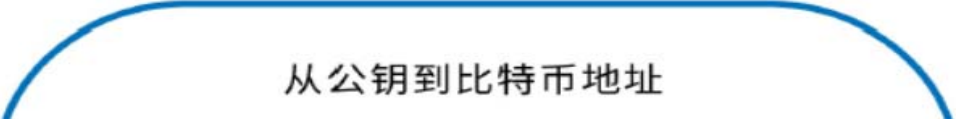
ECDSA

- 加解密效率高
- 相同安全强度, 占用空间小

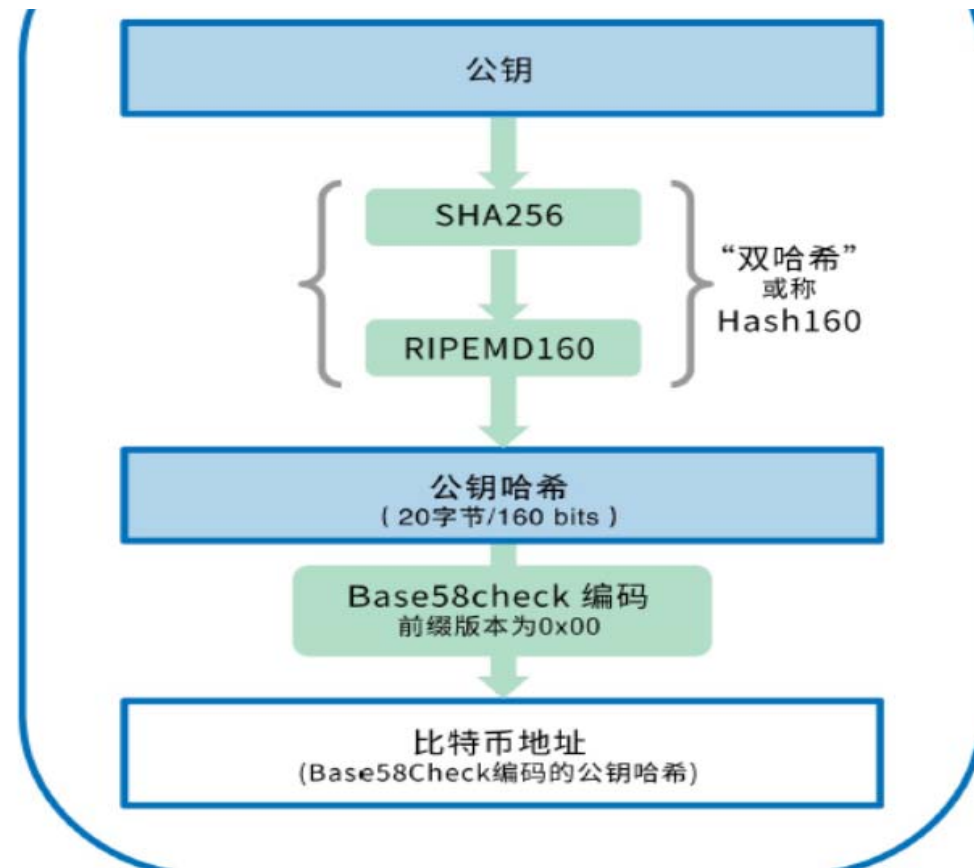
地址

- 创建钱包，就是创建地址
- 地址即帐户
- 谁拥有私钥，谁就是地址的主人

生成地址



从公钥到比特币地址



交易

- UTXO
- 交易类型
- 交易状态
- 交易脚本
- 交易示例

- 交易费用
- 避免双花

UTXO

- 谁可以使用UTXO

动用 UTXO 的时候，所有者必须使用私钥对交易进行签名，把交易 + 签名 + 公钥发送给全网网络，比特币节点就会对交易进行验证

交易类型

- P2PKH (Pay-to-Public-Key_Hash)
- P2PK (Pay-to-Public-Key)
- P2SH (Pay-to-Script-Hash)

交易状态

- 创建成功
- 锁定
- 广播成功/失败
- 丢弃
- Pending 阻塞
- 确认中
- 交易成功（6个确认认为成功）

交易时序

- 交易时间

交易费用

- 矿工决定
- 不公平性
- 维护系统运行

避免双花

- 公开帐本
- 多份帐本备份
- 验证
- 竞争记帐
- 如何发现双花
- 双花处理

PoW共识

- 拜占庭问题
- 难度
- 提高了作恶成本
- 牺牲能源

DLT

- block
- block chain

block

- 块内容
- 块大小

块内容

```
01000000 - version
0000000000000000000000000000000000000000000000000000000000000000 - prev block
3B43FBD0747B12B274C72C3F67768F617FC81BC3888A51323A9FB8444B1F5F4A - merkle root
```

110110-1000

110110-1000

块大小

- BTC 1M
- BCH 8M

block chain

- 最长链原则
- 硬分叉
- 软分叉

最长链原则

- 在最长链添加新区块

硬分叉

- 共识修改
- 新旧共识不能兼容（向后兼容）
- 所有的客户端升级或者分叉产生一条新链
- 例子：BCH

软分叉

- 共识修改
- 新旧共识兼容（向前兼容也向后兼容）
- 旧共识的客户端不需要升级
- 例子：P2SH

P2P

- 节点发现
- 节点通信

节点发现

- Address database (peers.dat)
- User-specified (-addnode and -connect)
- DNS seeding
- Hard-coded seeds
- From other peers ("getaddr" and "addr" messages)

节点通信

- 相互连接
- 策略

钱包

- 功能
- 技术本质
- 类型

功能

- 数字货币价值确权
- 数字货币价值存储
- 数字货币价值IO

技术本质

- 拥有私钥就代表拥有钱包
- 私钥存储
- 私钥控制价值IO

重要的事情说三遍：私钥，私钥，私钥

类型

- HD钱包
- 多签名钱包

安全

- 比特币网络
- 个人钱包
- 交易安全

比特币网络

- 51%攻击
- 自私挖矿Selfish mining
- P2P网络安全

51%攻击

- 矿场垄断算力
- 量子计算机

自私挖矿 Selfish mining

- 定义
- 检查

定义

- 矿工不广播自己最新挖出的区块

检查

- 块特征 (孤立)
- 时间特征

• 如何防止

P2P网络安全

- sybil attack

个人钱包

- 理论安全，在实践中会出现很多问题
- backup, backup, backup
- 私钥，私钥，私钥
- 重放攻击
- 认识，意识，学习

交易安全

- 中心化交易所 安全事故常有发生
- 去中心化交易 也并不安全

扩展性

- 闪电网络
- 隔离验证
- 区块扩容

闪电网络

- 交易与结算分离

隔离验证

- 大表拆小表

区块扩容

- BCH
- 大道到简
- 问题，并没有真没有解决问题

问题

1. 有了密码验证，为什么需要PoW？
2. 为什么一个交易需要6次确认？确认是如何进行？如何进行确认计数的？
3. 矿工如何验证交易？
4. 比特币交易性能问题的原因？
5. 为什么提高区块大小可以提高比特币的交易速度？是不是越大越快呢？

总结

- 比特币技术(P2P+BlockChain+PoW+Cryptography)
- 区块链技术的始祖

参考

- 《精通比特币》

比特币白皮书 (<https://bitcoin.org/bitcoin.pdf>)

深度解读比特币白皮书 (<https://www.btctrade.com/bitcoin/2066.html>)

Thank you

沉风

myself659@163.com (mailto:myself659@163.com)

<https://blog.ipds.top>

