泡沫与价值并存

区块链及其应用

- 王华强
- UCAS 基科(雾)

Contents

1. 区块链简介

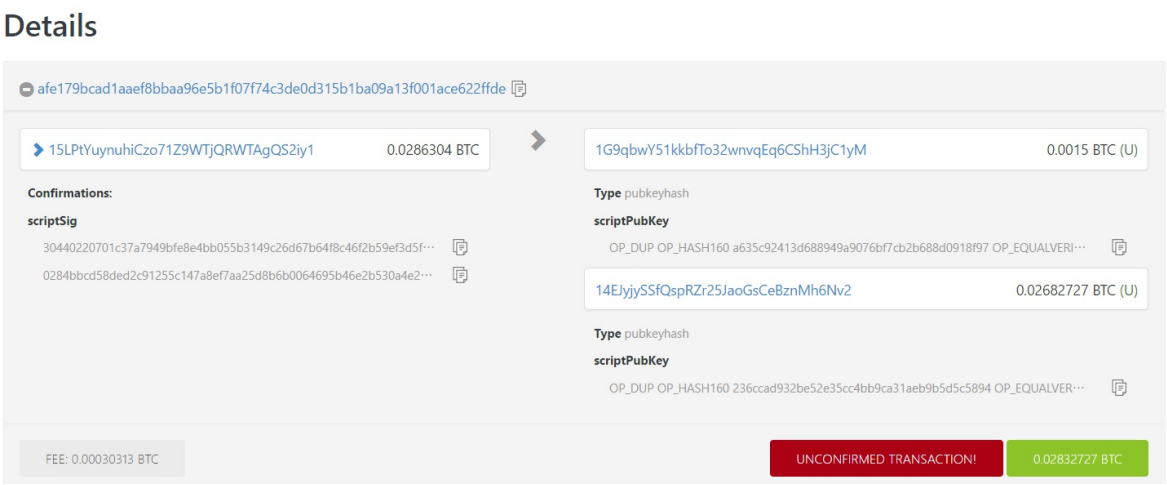
(PublicBlockChains Only, 以Bitcoins为例)

ref: http://news.at.zhihu.com/story/9666826

- 中心化与去中心化
- 区块链是一个去中心化的系统
- 交易记录, 区块, , 挖矿, 区块链

1.1 交易记录

实例: 一条转账记录



实时实例:https://blockexplorer.com/

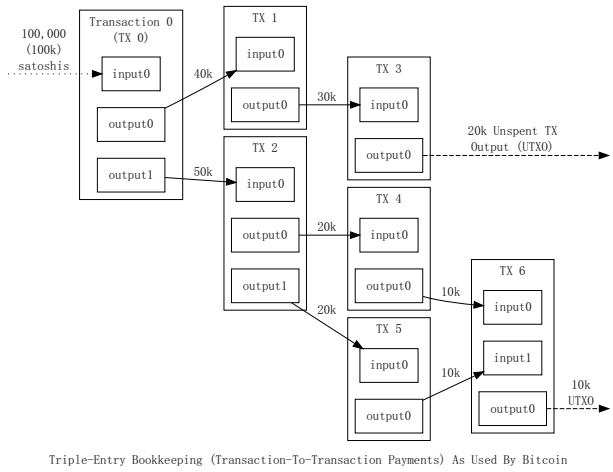
小纸条模型

一次转账的过程:

```
graph TD
图1.一次转账的过程

A-->一次转账记录_A转给B1Bitcoin
A-->公钥
A-->私钥
```

```
一次转账记录_A转给B1Bitcoin-->明文转账记录
明文转账记录-->定长字符串1
hash函数-->定长字符串1
定长字符串1-->数字签名
私钥-->数字签名
数字签名--分发-->B
公钥--分发-->B
明文转账记录--分发-->B

B-->由数字签名和公钥解码出的定长字符串2
B-->由明文和哈希函数计算出的定长字符串3
hash函数-->由明文和哈希函数计算出的定长字符串3
由数字签名和公钥解码出的定长字符串2-->比较
由明文和哈希函数计算出的定长字符串3-->比较

比较--一致-->承认交易
比较--不一致-->不承认交易
```

转账的简单模型:



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

---

拥有数字货币的本质是拥有交易记录

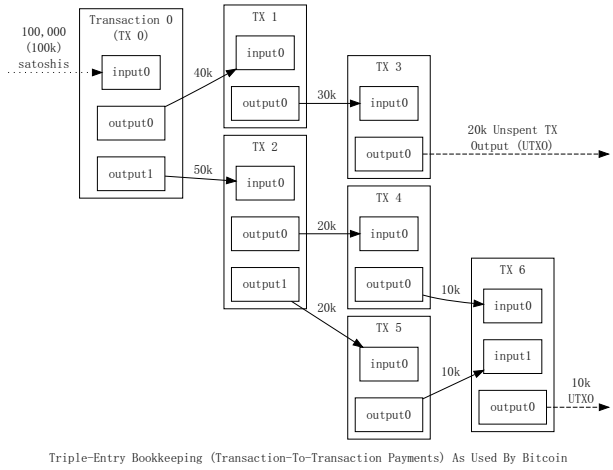
交易记录有以下几种状态:

- 有效
- 无效
- 未确认

1.2 区块

实例: https://blockexplorer.com/

转账的简单模型:



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

ref: https://bitcoin.org/en/developer-guide#block-chain-overview

---

1.3 挖矿

区块头实例:

```
An example header in hex:

02000000 ........................... Block version: 2

b6ff0b1b1680a2862a30ca44d346d9e8
910d334beb48ca0c0000000000000000 ... Hash of previous block's header
9d10aa52ee949386ca9385695f04ede2
70dda20810decd12bc9b048aaab31471 ... Merkle root

24d95a54 ........................... Unix time: 1415239972
30c31b18 ........................... Target: 0x1bc330 * 256**(0x18-3)
fe9f0864 ........................... Nonce
```

挖矿的收益:

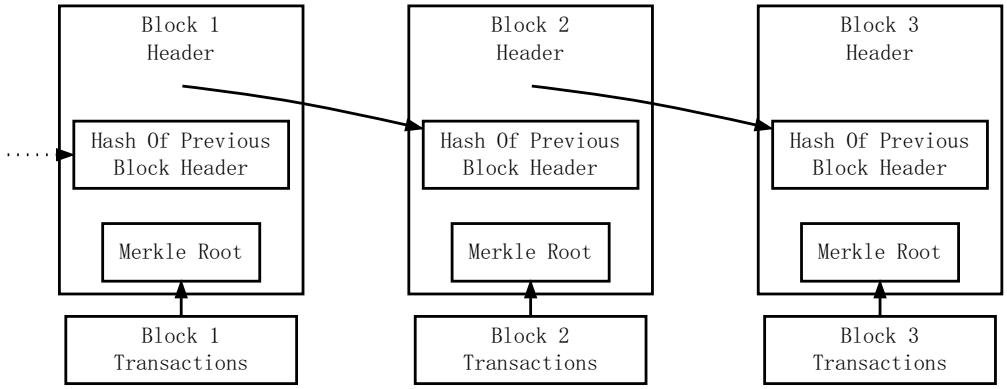
- 新的区块
- 矿工收益

1.4 区块的特性

> - 产生,挖掘,校验速度大致相等
> - 全网会尽力控制在一个周期内只有一个节点能够成功挖出区块，但是不能够完全避免多个节点同时挖出区块的可能性
> - 全网并不是产生唯一的一个区块等待挖掘；每个节点事实上都在周期性的创造区块和挖出区块；只是在某一个节点的视野里，它不能感知到另外一个节点上区块的产生

1.5 区块链

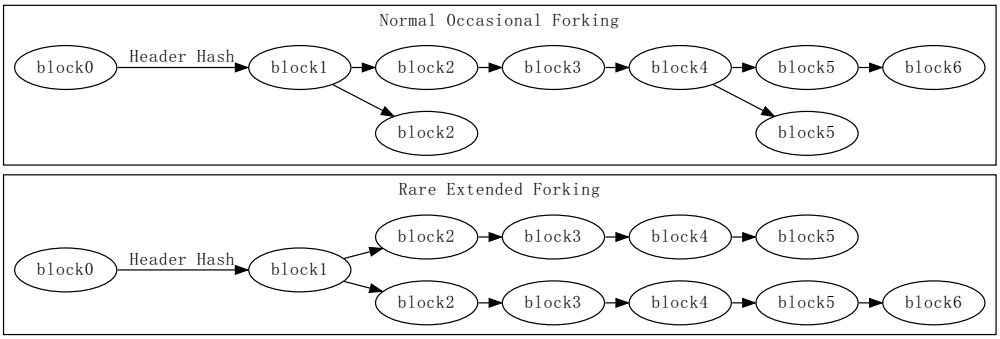
区块链的简单模型:



Simplified Bitcoin Block Chain

补充: 分叉, 双重支付, 51%攻击, 延迟

分叉:



延迟

1.5 回顾

- 交易记录
- 区块, 挖矿
- 区块链

ref: https://www.zhihu.com/question/20792042

---

2. 区块链应用: Bitcoin

在其他数字货币ICO时, Bitcoin作为一个重要的中转.

ref: https://zh-cn.bitcoin.it/wiki/%E7%AE%80%E4%BB%8B

2.1 实例: 比特币交易的实时情况

实时的区块变动及转账情况:

https://blockexplorer.com/

国内的数字货币交易平台:

https://www.huobipro.com/zh-cn/btc_usdt/exchange/

---

3. 区块链应用: Ethereum

智能合约与去信任化交易.

- Gas
- Ether

- ref:
- https://github.com/ethereum
- https://www.ethereum.org/
- http://ethfans.org/

3.1 CryptoKitties

https://www.cryptokitties.co/

---

4. ICO: 泡沫之下

4.1 何为ICO

> ICO（是Initial Coin Offering缩写），首次币发行，源自股票市场的首次公开发行（IPO）概念，是区块链项目首次发行代币，募集比特币、以太坊等通用数字货币的行为.

4.2 ICO现状

关于防范代币发行融资风险的公告:

http://www.csrc.gov.cn/pub/newsite/zjhxwfb/xwdd/201709/t20170904_323047.html

> 本公告发布之日起，各类代币发行融资活动应当立即停止。已完成代币发行融资的组织和个人应当做出清退等安排，合理保护投资者权益，妥善处置风险。有关部门将依法严肃查处拒不停止的代币发行融资活动以及已完成的代币发行融资项目中的违法违规行为。

---

5. 结语

泡沫与价值并存