优权天成
YQTC TECH

比特币，从入门到精通（放弃）

主讲： 韦忠汕

目录

优权天成 YQTC TECH

优权天成 YQTC TECH

1.1 什么是比特币?

噢，是勒索种病毒，前段时间爆发过

是传销工具吧，国家在打击这东西

NONONO，正确的姿势应该是：**比特币是一种去中心化的数字货币**，其发行不由任何一个组织控制，数量上限为2100万，并且在任何有网络的地方都能够流通。

1.2 货币的本质

1.价值尺度　发行数量上限为2100万，本身具有价值，可以作为衡量价值的标准

2.流通手段　通过网络进行流通，非常便捷

3.存储手段　以数据形式存储在硬盘，存储零成本

4.支付手段　可以用来进行支付

5.世界货币　全世界通用，有网即可使用

1.3 分布式账本

A		B		C	
奖励A: 5	X	奖励A: 5	X	奖励A: 5	X
A->B : 5	X	A->B : 5	X	A->B : 5	X
B->C : 2	X	B->C : 2	X	B->C : 2	X
B->B : 3		B->B : 3		B->B : 3	
C->A : 2		C->A : 2		C->A : 2	

A的5个币从何而来?

余额: A : 2 B : 3 C : 0

好处: 1.可追溯 2.去中心化 3.不可篡改

2.1 基本名词介绍

公钥

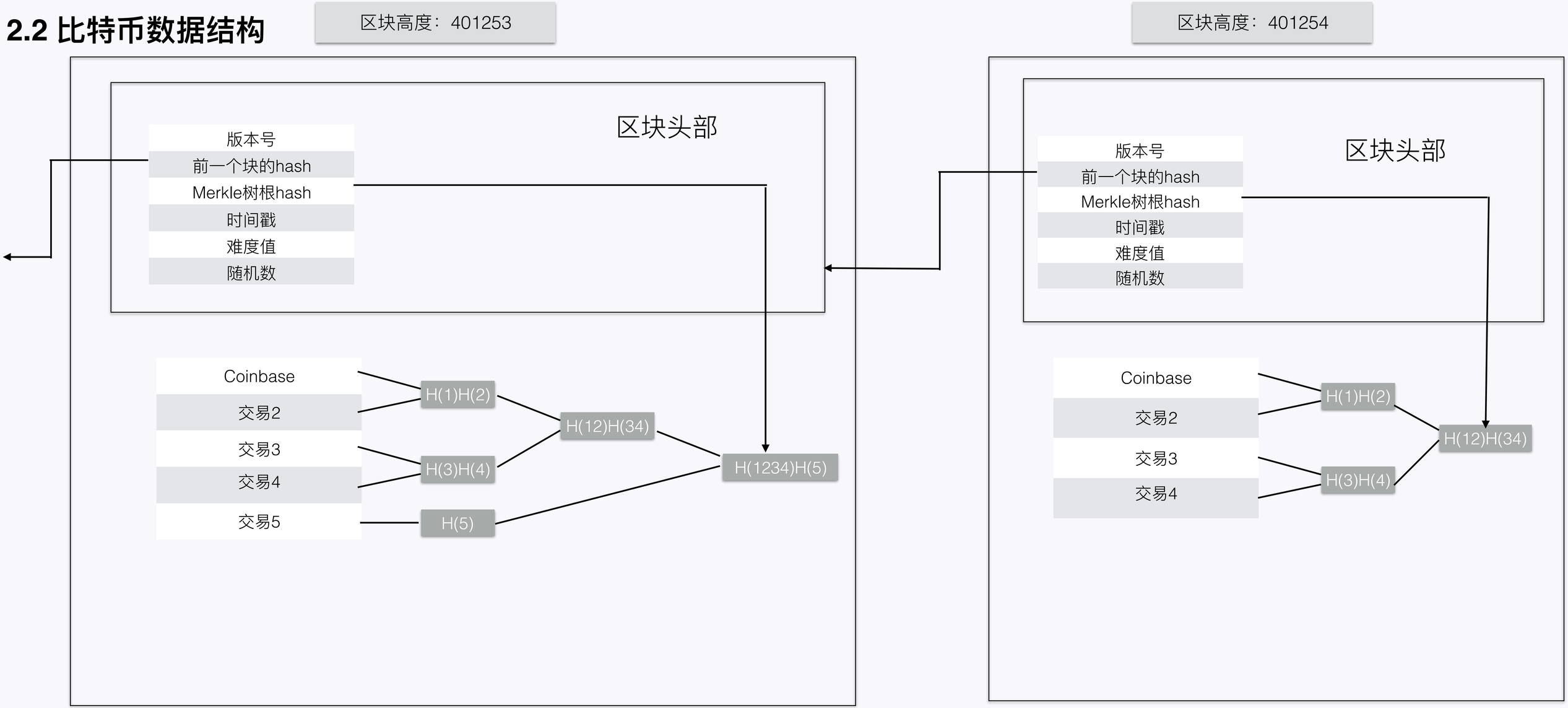
私钥

签名

哈希

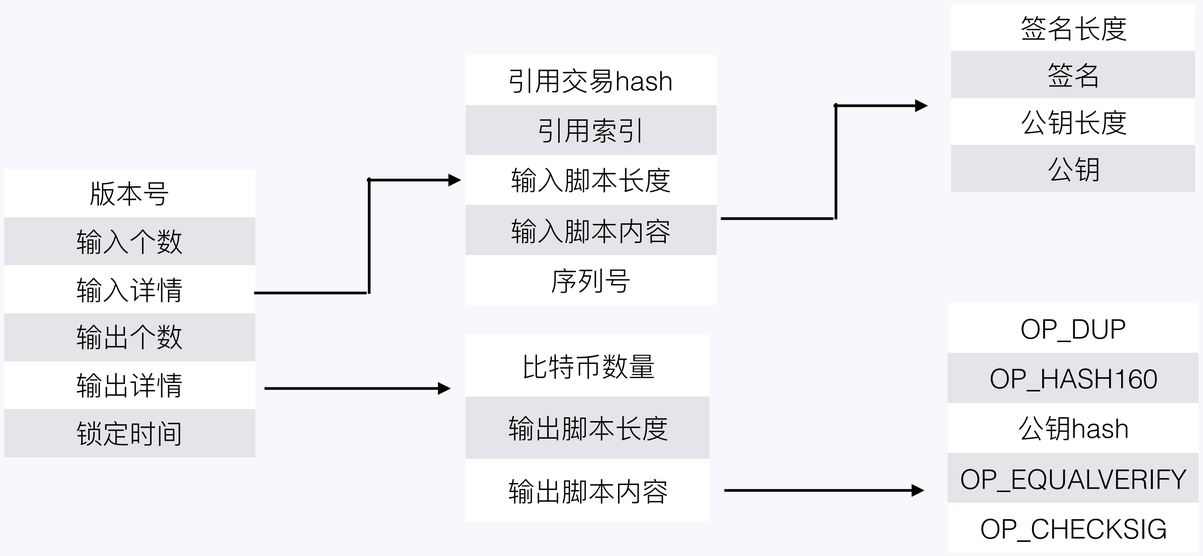
哈希碰撞

2.2 比特币数据结构


区块高度：401253
区块头部
版本号
前一个块的hash
Merkle树根hash
时间戳
难度值
随机数
Coinbase
交易2
交易3
交易4
交易5
H(1)H(2)
H(3)H(4)
H(5)
H(12)H(34)
H(1234)H(5)
区块高度：401254
区块头部
版本号
前一个块的hash
Merkle树根hash
时间戳
难度值
随机数
Coinbase
交易2
交易3
交易4
H(1)H(2)
H(3)H(4)
H(12)H(34)

2.2 比特币数据结构

每笔交易具体内容（标准交易类型）：



交易类型：

1.P2PKH

2.P2PK

3.P2SH

签名类型：

1.SIGHASH_ALL

2.SIGHASH_NONE

3.SIGHASH_SINGLE

2.3 交易生成、发送、验证

2.3.1 查找UTXO

$ bitcoin-cli listunspent


```
[
  {
    "txid" : "9ca8f969bd3ef5ec2a8685660fdbf7a8bd365524c2e1fc66c309acbae2c14ae3",
    "vout" : 0,
    "address" : "1hvzSofGwT8cjb8JU7nBsCSfEVQX5u9CL",
    "account" : "",
    "scriptPubKey" : "76a91407bdb518fa2e6089fd810235cf1100c9c13d1fd288ac",
    "amount" : 0.05000000,
    "confirmations" : 7
  }
]
```

优权天成 YQTC TECH

2.3 交易生成、发送、验证

2.3.2 创建一笔交易

```
$ bitcoin-cli createrawtransaction
‘[{"txid":"9ca8f969bd3ef5ec2a8685660fdbf7a8bd365524c2e1fc66c309acbae2c14ae3","vout":0}]‘
‘{“1LnfTndy3qzXGN19Jwscj1T8LR3MVe3JDb”:0.025, “1hvzSofGwT8cjb8JU7nBsCSfEVQX5u9CL”:
0.0245}’
```


```
{
  "txid" : "0793299cb26246a8d24e468ec285a9520a1c30fcb5b6125a102e3fc05d4f3cba",
  "version" : 1,
  "locktime" : 0,
  "vin" : [
    {
      "txid" : "9ca8f969bd3ef5ec2a8685660fdbf7a8bd365524c2e1fc66c309acbae2c14ae3",
      "vout" : 0,
      "scriptSig" : {
        "asm" : "",
        "hex" : ""
      },
      "sequence" : 4294967295
    }
  ],
  "vout" : [
    {
      "value" : 0.02500000,
      "n" : 0,
      "scriptPubKey" : {
        "asm" : "OP_DUP OP_HASH160 d90d36e98f62968d2bc9bbd68107564a156a9bcf OP_EQUALVERIFY OP_CHECKSIG",
        "hex" : "76a914d90d36e98f62968d2bc9bbd68107564a156a9bcf88ac",
        "reqSigs" : 1,
        "type" : "pubkeyhash",
        "addresses" : [
          "1LnfTndy3qzXGN19Jwscj1T8LR3MVe3JDb"
        ]
      }
    },
    {
      "value" : 0.02450000,
      "n" : 1,
      "scriptPubKey" : {
        "asm" : "OP_DUP OP_HASH160 07bdb518fa2e6089fd810235cf1100c9c13d1fd2 OP_EQUALVERIFY OP_CHECKSIG",
        "hex" : "76a91407bdb518fa2e6089fd810235cf1100c9c13d1fd288ac",
        "reqSigs" : 1,
        "type" : "pubkeyhash",
        "addresses" : [
          "1hvzSofGwT8cjb8JU7nBsCSfEVQX5u9CL"
        ]
      }
    }
  ]
}
```

2.3 交易生成、发送、验证

2.3.3 交易签名

```
$ bitcoin-cli signrawtransaction
0100000001e34ac1e2baac09c366fce1c2245536bda8f7db0f6685862aecf53ebd69f9a89c0000000000ffffffff02a0
2526000000000001976a914d90d36e98f62968d2bc9bbd68107564a156a9bcf88ac506225000000000001976a914
07bdb518fa2e6089fd810235cf1100c9c13d1fd288ac00000000
```


```
{
  "txid" : "ae74538baa914f3799081ba78429d5d84f36a0127438e9f721dff584ac17b346",
  "version" : 1,
  "locktime" : 0,
  "vin" : [
    {
      "txid" : "9ca8f969bd3ef5ec2a8685660fdbf7a8bd365524c2e1fc66c309acbae2c14ae3",
      "vout" : 0,
      "scriptSig" : {
        "asm" : "304402203e8a16522da80cef66bacfbc0c800c6d52c4a26d1d86a54e0a1b76d661f020c9022010397f00149f2a8fb2bc5bca52f2d7a7f87e3897a273c71dc5127",
        "hex" : "47304402203e8a16522da80cef66bacfbc0c800c6d52c4a26d1d86a54e0a54b277e4af52051a06012103a8fb2bc5bca52f2d7a7f87e3897a273c7197a2"
      },
      "sequence" : 4294967295
    }
  ],
  "vout" : [
    {
      "value" : 0.02500000,
      "n" : 0,
      "scriptPubKey" : {
        "asm" : "OP_DUP OP_HASH160 d90d36e98f62968d2bc9bbd68107564a156a9bcf OP_EQUALVERIFY OP_CHECKSIG",
        "hex" : "76a914d90d36e98f62968d2bc9bbd68107564a156a9bcf88ac",
        "reqSigs" : 1,
        "type" : "pubkeyhash",
        "addresses" : [
          "1LnfTndy3qzXGN19Jwscj1T8LR3MVe3JDb"
        ]
      }
    },
    {
      "value" : 0.02450000,
      "n" : 1,
      "scriptPubKey" : {
        "asm" : "OP_DUP OP_HASH160 07bdb518fa2e6089fd810235cf1100c9c13d1fd2 OP_EQUALVERIFY OP_CHECKSIG",
        "hex" : "76a91407bdb518fa2e6089fd810235cf1100c9c13d1fd288ac",
        "reqSigs" : 1,
        "type" : "pubkeyhash",
        "addresses" : [
          "1hvzSofGwT8cjb8JU7nBsCSfEVQX5u9CL"
        ]
      }
    }
  ]
}
```

优权天成 YQTC TECH

2.3 交易生成、发送、验证

2.3.4 发送交易

$ bitcoin-cli sendrawtransaction
0100000001e34ac1e2baac09c366fce1c2245536bda8f7db0f6685862aecf53ebd69f9a89c0000000000ffffffff02a0
2526000000000001976a914d90d36e98f62968d2bc9bbd68107564a156a9bcf88ac5062250000000000001976a914
07bdb518fa2e6089fd810235cf1100c9c13d1fd288ac00000000

2.3.5 验证交易

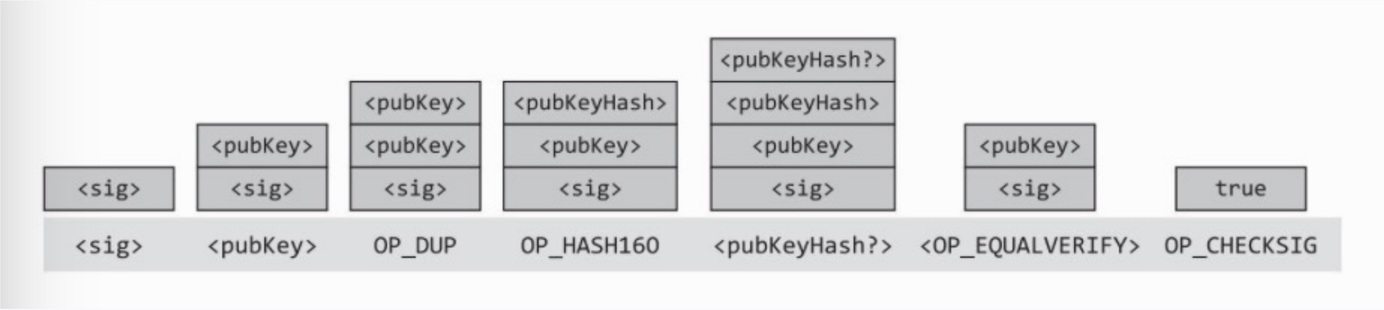
1. 检查前一个块的hash是否相同

2. 检查当前区块hash是否满足难度值

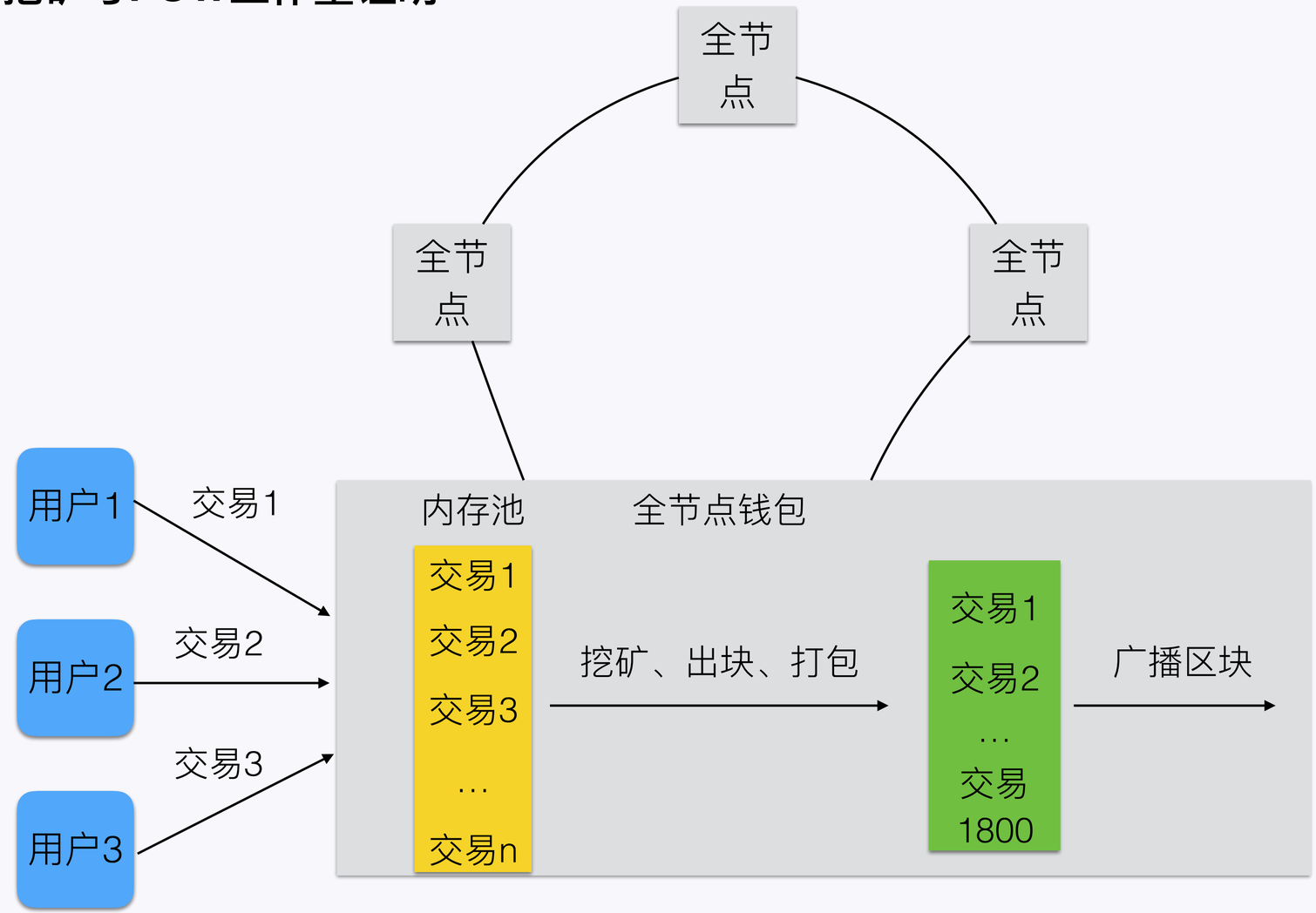
3. 校验签名

输入脚本签名：<sig> <pubkey>

待花费的输出脚本：OP_DUP OP_HASH160 <pubkeyHash> OP_EQUALVERIFY OP_CHECKSIG



2.4 挖矿与POW工作量证明



挖矿：

找到一个随机数使得 区块的hash < 难度值

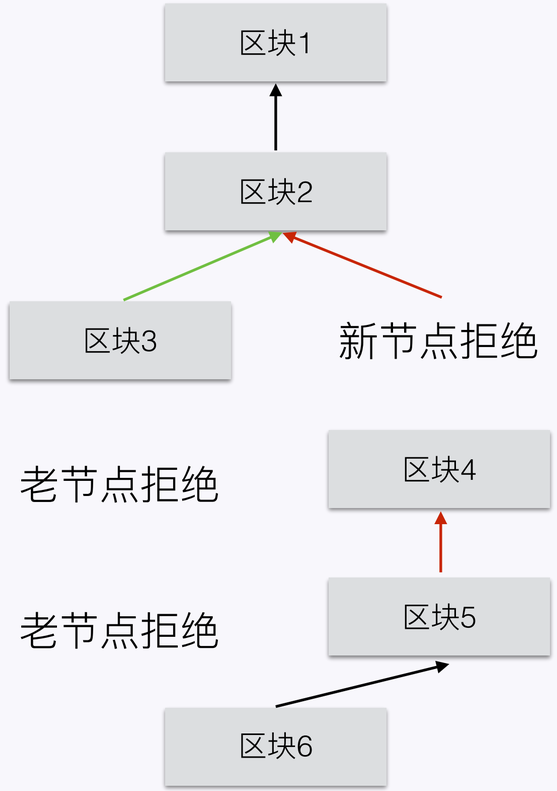
POW工作量证明：

寻找随机数不断试错的过程

2.5 软分叉与硬分叉

2.5.1 隔离见证与软分叉

什么是软分叉？　当新共识规则发布后，没有升级的节点会因为不知道新共识规则下，而生产不合法的区块，就会产生临时性分叉。



老节点发现非法的区块3

新节点拒绝

新节点发现合法的区块4

老节点拒绝

新节点发现合法的区块5

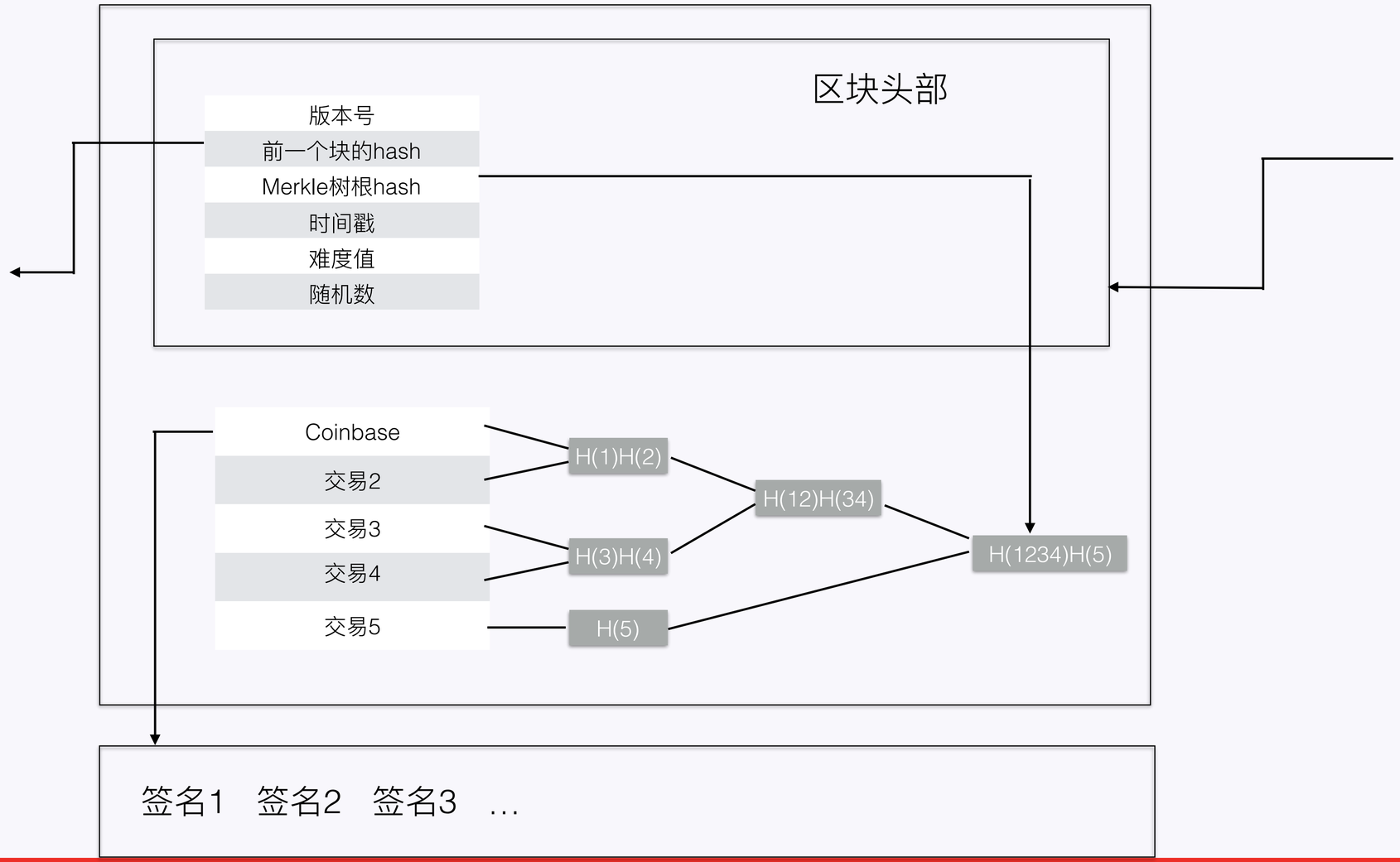
老节点拒绝

最长链原则红链胜出

软分叉需要全网绝大部分算力支持才能完成

2.5 软分叉与硬分叉

什么是隔离见证？　简单的说，隔离见证是将签名信息从区块中剥离，放到另外地方进行存储，也称分离见证。

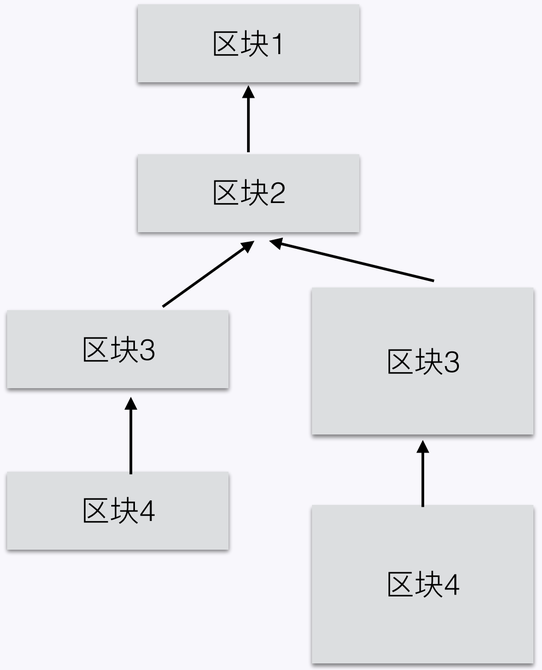


2.5 软分叉与硬分叉

2.5.1 BCC与硬分叉

什么是硬分叉？　当区块链发生永久性分歧，在新共识规则发布后，部分没有升级的节点无法验证已经升级的节点生产的区块，通常硬分叉就会发生。

BCC将区块大小强行改为8M，导致新旧节点不兼容，最终分叉成为两条链



硬分叉需要矿工强行站队

2.6 常见的攻击手段

1. 51%攻击（双花、DDoS）

2. 粉尘交易攻击

3. 交易延展性攻击

4. 重放攻击

优权天成 YQTC TECH

3.1 扩容之争

satoshi
Founder
Sr. Member
Activity: 364
Ignore

Re: [PATCH] increase block size limit
October 04, 2010, 07:48:40 PM
#9

It can be phased in, like:

```
if (blocknumber > 115000)
  maxblocksize = largerlimit
```

It can start being in versions way ahead, so by the time it reaches that block number and goes into effect, the older versions that don't have it are already obsolete.

When we're near the cutoff block number, I can put an alert to old versions to make sure they know they have to upgrade.

2015.5

加文提出扩大区块至20M

2015.12

提出隔离见证

2016.1 九二共识

执行classc方案区块扩容至2M

2016.2 香港共识

部署SW，区块扩容至2M

2016.4 core背叛香港共识

社区分裂

2017.5 纽约共识

在SW下，区块扩容至2M

3.2 排队硬分叉

bcc: 2017年8月1日分叉。8M区块，不支持SW

btg: 2017年10月25日分叉。显卡挖矿，支持SW

b2x: 2017年8月1日分叉。2M区块，支持SW，不设重放保护

bcd: 2017年11月24日分叉。总量2.1亿，出块速度2分钟，加密交易金额

sbtc: 预计2017年12月14日分叉。8M区块，智能合约，零知识验证

ub: 预计2017年12月16日分叉。8M区块，支持SW，智能合约型POW，扩展侧链

lbtc: 预计2017年12月23日分叉。2M区块，智能合约、DPos共识、出块速度3秒

此外还有bta btp bum god bcp bts …

四、思考和展望

优权天成 YQTC TECH

1. BTC or BCC

稳定性

去中心化性

技术可行性

2. POW or POS

商业化

安全性

经济性

3. ICO or IFO

政策风险

知名度

生态闭环

4. 参考文献

1. <区块链技术驱动金融>

2. http://www.8btc.com/tan90d144

3. http://8btc.com/article-1914-1.html


THANK YOU
优权天成
YQTC TECH