Chapter7 区块链

苏玉萌

2017.11.17

主要内容

- 区块结构
- 区块头
  - 区块头结构剖析
  - Target & difficult
  - Target计算方法及动态调整算法
- 区块标识符
- 特殊区块
  - 创世块
  - 软分叉
- Merkle Tree

区块链

- 区块链是一种按照时间顺序将数据区块以顺序相连的方式组合成的一 种链式数据结构， 并以密码学方式保证的不可篡改和不可伪造的分布式账本。区块链首次从技术上解决了基于信任的中心化模型带来的安全问题
- 每个区块只有一个Parent，但可以暂时有多个Child
- 链的增长，是对之前区块的可信程度的一个增强，保证了老区块的不可变性

区块结构

字节	字段	说明
4	区块大小	用字节表示的该字段之后的区块大小
80	区块头	组成区块头的几个字段
1-9	交易计数器	该区块包含的交易数量，包含coinbase交易
不定	交易	记录在区块里的交易信息，使用原生的交易信息格式，并且交易在数据流中的位置必须与Merkle树的叶子节点顺序一致

比特币的区块大小目前被严格限制在1MB以内。4字节的区块大小字段不包含在此内。

区块大小并不存储在区块内

Block:170（16进制)

区块头：80字节

交易计数器：1-9字节，本区块共有两笔交易

- 0100000055bd840a78798ad0da853f68974f3d183e2bd1db6a842c1feecf222a000
  00000ff104ccb05421ab93e63f8c3ce5c2c2e9dbb37de2764b3a3175c8166562cac
  7d51b96a49fff001d283e9e702010000000100000000000000000000000000000
  0000000000000000000000000000000000ffffffff0704ffff001d0102ffffffff0100f
  2052a01000000434104d46c4968bde02899d2aa0963367c7a6ce34eec332b32e42
  e5f3407e052d64ac625da6f0718e7b302140434bd725706957c092db53805b821a
  85b23a7ac61725bac00000000100000001c997a5e56e104102fa209c6a852dd90
  660a20b2d9c352423edce25857fcd37040000000048473044022204e45e16932b8a
  f514961a1d3a1a25fdf3f4f7732e9d624c6c61548ab5fb8cd410220181522ec8eca0
  7de4860a4acdd12909d831cc56cbbac4622082221a8768d1d0901ffffffff0200ca9a
  3b00000000434104ae1a62fe09c5f51b13905f07f06b99a2f7159b2225f374cd378
  d71302fa28414e7aab37397f554a7df5f142c21c1b7303b8a0626f1baded5c72a70
  4f7e6cd84cac00286bee0000000043410411db93e1dcdb8a016b49840f8c53bc1e
  b68a382e97b1482ecad7b148a6909a5cb2e0eaddfb84ccf9744464f82e160bfa9b8
  b64f9d4c03f999b8643f656b412a3ac00000000

交易

交易1：Coinbase交易

交易2：普通交易

区块头结构（小端存储，80字节）

Bytes	Name	DataType	Description
4	version	int32_t	区块版本号，表示本区块遵循的验证规则
32	Previous block header hash	char[32]	前一区块的哈希值，采用SHA256(SHA256(父区块头)) 计算
32	Merkle root hash	char[32]	本区块中交易的merkle根哈希值，同样采用两次SHA256计算
4	Time	uint32_t	精确到秒的UNIX时间戳，是该区块产生的近似时间（矿工开始对头部进行hash计算的时间，是矿工可调整的）。必须严格大于前11个区块时戳的中位值，全节点会拒绝超出自己时钟2个小时的区块。
4	nBits	uint32_t	使用特定编码格式的该区块工作量证明算法的难度目标（target），本区块哈希值需要小于等于target
4	Nonce	uint32_t	为了找到满足难度目标所设定的随机数，为了解决32位随机数在算力飞升的情况下不够用的问题，规定时间戳和coinbase交易信息均可更改，以扩展nonce的位数

Block:170 区块头（小端存储、共80字节）

版本：4字节
0x 0000 0001

父区块头哈希值：32字节

0100000055bd840a78798ad0da853f68974f3d18

3e2bd1db6a842c1feecf222a00000000ff104ccb05

421ab93e63f8c3ce5c2c2e9dbb37de2764b3a317

难度目标：4字节
0x1d00ffff = 486604799

5c8166562cac7d**51b96a49**ffff001d283e9e70

Merkle根：32字节

时间戳4字节
自1970年1月1日0时0分以来的秒数，2009-01-12 03:30:25，共计1231731025秒，转为16进制为0x496AB951 小端格式存储即为 51b96a49

Nonce：4字节
0x709e3e28 = 1889418792

Target

- 初始target:0x1d00ffff

0x00000000ffff0000000000000000000000000000000000000000000000000000

- 每2016块调整target:

过去的2016个区块，出块平均时间小于10分钟，target变小，难度变高

过去的2016个区块，出块平均时间大于10分钟，target变大，难度变低

Target 调整方法

- 根据第1个区块和第2016区块的时间戳字段，计算这2016个区块产生的时间->actual timespan
- actual timespan会调整至多为预期时间（两周）的4倍或至少为预期时间的1/4（避免时间大幅度的起伏）
- $\mathrm{Target}_{\mathrm{new}} = \frac{\mathrm{Target}_{old2016} * ActualTimeSpan}{14*24*60*60}$

- Target 不能超过 00000000ffffffffffffffffffffffffffffffffffffffffffffffffffffffff 这个最大值

```cpp
unsigned int CalculateNextWorkRequired(const CBlockIndex* pindexLast, int64_t nFirstBlockTime, const Consensus::Params& params)
{
    if (params.fPowNoRetargeting)
        return pindexLast->nBits;

    // Limit adjustment step
    int64_t nActualTimespan = pindexLast->GetBlockTime() - nFirstBlockTime;
    if (nActualTimespan < params.nPowTargetTimespan/4)
        nActualTimespan = params.nPowTargetTimespan/4;
    if (nActualTimespan > params.nPowTargetTimespan*4)
        nActualTimespan = params.nPowTargetTimespan*4;

    // Retarget
    const arith_uint256 bnPowLimit = UintToArith256(params.powLimit);
    arith_uint256 bnNew;
    bnNew.SetCompact(pindexLast->nBits);
    bnNew *= nActualTimespan;
    bnNew /= params.nPowTargetTimespan;

    if (bnNew > bnPowLimit)
        bnNew = bnPowLimit;

    return bnNew.GetCompact();
}
```

```
consensus.powLimit = uint256S("00000000ffffffffffffffffffffffffffffffffffffffffffffffffffffffff");
consensus.nPowTargetTimespan = 14 * 24 * 60 * 60; // two weeks
consensus.nPowTargetSpacing = 10 * 60;
```

Difficulty

- 衡量找到一个小于、等于给定hash值（即target）的困难程度
- **Difficulty = original_target / current_target**

  original_target = 0x1d00ffff

  current_target = 0x1800d0f6
- difficulty = 0x00000000ffff0000000000000000000000000000000000000000 / 0x0000000000000000d0f60000000000000000000000000000000000
- =13470014305558.57
- 现在产生一个区块的难度是产生创世块难度的1,347,001,430,558.6倍。

Target nBits

Target nBits

Edit | History | Report Issue | Discuss

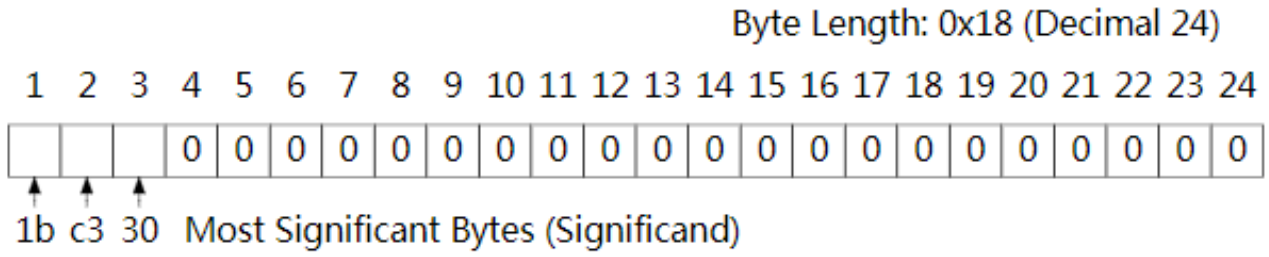
The target threshold is a 256-bit unsigned integer which a header hash must be equal to or below in order for that header to be a valid part of the block chain. However, the header field *nBits* provides only 32 bits of space, so the target number uses a less precise format called "compact" which works like a base-256 version of scientific notation:

0x181bc330 →	0x1bc330	*	256	^	(0x18	-	3)
nBits In Big-Endian Order	Significand (Mantissa)		Base		Exponent		Bytes In Significand

Result: 0x1bc330000000000000000000000000000000000000000000

Converting nBits Into A Target Threshold

As a base-256 number, nBits can be quickly parsed as bytes the same way you might parse a decimal number in base-10 scientific notation:



Quickly Converting nBits 0x181bc330 Into The Target Threshold 0x1bc330000000000000000000000000000000

由nBits算出Target

- Target： 256 Unsigned integer（32字节， 64个16进制字符)

- Target可由当前的挖矿难度（nBits或Difficulty）计算得出，以Block240203为例其nBits为0x1a011337,则其Target为

- 0x011337*2^(8*(0x1a-3))=

0x0000000000011337000000000000000000000000000000000000

Target共32个字节
前面补6字节的0
12位字符

Target threshold :共0x1a（26字节），52位16进制

区块标识符 识别区块的方式

- 区块头哈希值，唯一、明确的标识一个区块，任何节点通过简单的对区块头进行哈希计算都可以独立的获取该区块哈希值。

- 区块高度（不是唯一的标识符）

Summary	
Number Of Transactions	2234
Output Total	3,888.36058652 BTC
Estimated Transaction Volume	657.01080455 BTC
Transaction Fees	0.59985817 BTC
Height	495410 (Main Chain)
Timestamp	2017-11-21 12:18:24
Received Time	2017-11-21 12:18:24
Relayed By	SlushPool
Difficulty	1,364,422,081,125.15
Bits	402705995
Size	1075.799 kB
Weight	3992.456 kWU
Version	0x20000000
Nonce	3472078235
Block Reward	12.5 BTC

Hashes	
Hash	00000000000000000ba6fef2a5f0a0f2d0407e9d982b3b9568e70e7f400cf23
Previous Block	00000000000000000004f5c1c9882ddd657d91de81eabd5ab35c489efb3825e96
Next Block(s)	00000000000000000006934001b3f571be9e24ae579ef4181a9bd7bf4fd6f1133
Merkle Root	7e8545c4aa9ac2258ae34ec5be105b8238787dfba3bd52788e14350be1efe2a6

标致性的区块

- 创世块
- 版本变迁
  - Version 1 :2009年1月（从创世块开始）
  - Version 2 :2012年9月 （BIP34）
  - Version 3 : 2015年2月激活（BIP66）
  - Version 4 : 2015年12月激活（BIP65）
  - Version 0x20000000
  - Version 0x20000001 (csv 已激活)
  - Version 0x20000002（segwit ）
  - Version 0x20000010 （segwit2x BIP91）
  - Version 0x20000012 (segwit2x && segwit)

创世区块

Summary	
Number Of Transactions	1
Output Total	50 BTC
Estimated Transaction Volume	0 BTC
Transaction Fees	0 BTC
Height	0 (Main Chain)
Timestamp	2009-01-03 18:15:05
Received Time	2009-01-03 18:15:05
Relayed By	Unknown
Difficulty	1
Bits	486604799
Size	0.285 kB
Weight	0.896 kWU
Version	1
Nonce	2083236893
Block Reward	50 BTC

Hashes	
Hash	000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f
Previous Block	0000000000000000000000000000000000000000000000000000000000000000
Next Block(s)	00000000839a8e6886ab5951d76f411475428afc90947ee320161bbf18eb6048
Merkle Root	4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b

创世区块 交易

Transaction View information about a bitcoin transaction

4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b

No Inputs (Newly Generated Coins) → 1A1zP1eP5QGefi... (Genesis of Bitcoin) - (Unspent) 50 BTC

50 BTC

Summary	
Size	204 (bytes)
Weight	816
Received Time	2009-01-03 18:15:05
Reward From Block	0
Scripts	Hide scripts & coinbase
Visualize	View Tree Chart

CoinBase

04ffff001d0104455468652054696d65732030332f4a616e2f32303039204368616e63656c6c6f72206f6e206272696e6b206f66207365636f6e64206261696c6f757420666f722062616e6b73

(decoded) ┘��┌EThe Times 03/Jan/2009 Chancellor on brink of second bailout for banks

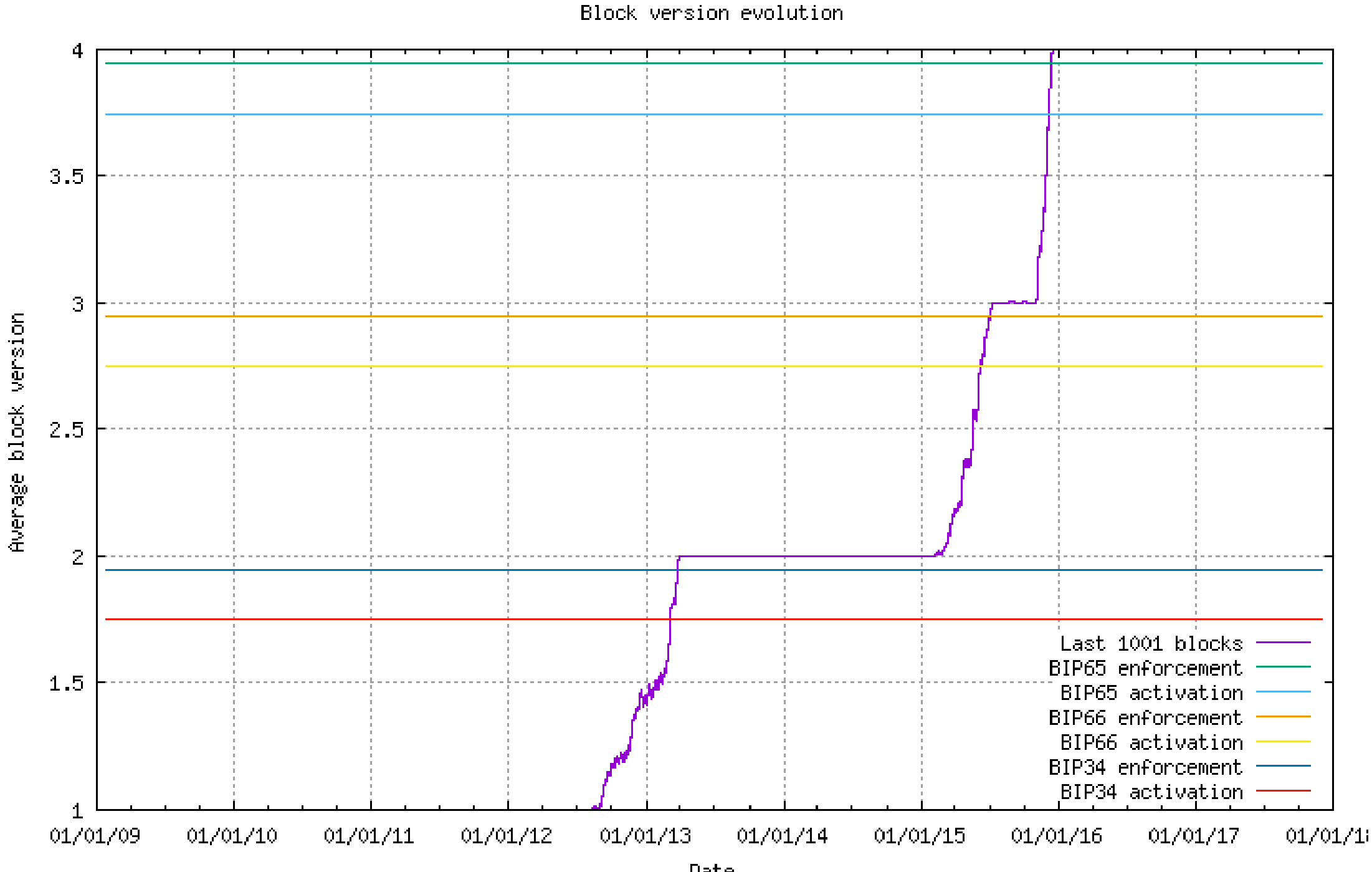
Output Scripts

区块版本变化

- BIP34 、66、 65
- Csv 、 segwit 、 segwit2X

BIP

- 比特币改进协议
- 主要为全网带来新的功能或信息。由于比特币的开源本质以及其系统中不存在中央机构，比特币软件鼓励开发者使用BIP作为一种交流意见、互换信息的主要方式。


Block version evolution
Average block version
4
3.5
3
2.5
2
1.5
1
01/01/09
01/01/10
01/01/11
01/01/12
01/01/13
01/01/14
01/01/15
01/01/16
01/01/17
Last 1001 blocks
BIP65 enforcement
BIP65 activation
BIP66 enforcement
BIP66 activation
BIP34 enforcement
BIP34 activation

Version2(BIP-34)

- 2012年12月被引入Bitcoin core0.7.0
- 普通交易，版本号大于1的视为non-standard交易，官方的satoshi客户端不会转发、添加这笔交易进区块
- Coinbase 的ScriptSig部分，区块的height为第一个字段（小端存储）
- 区块版本号变为2 (0x00000002) 小端：20000000

- 从224412区块开始(2013年5月)，拒绝在coinbase里没有height字段的区块
- 从227930区块开始，拒绝区块版本号为1的区块

227835区块


```
{
  "hash": "00000000000001aa077d7aa84c532a4d69bdbff519609d1da0835261b7a74eb6",
  "ver": 1,
  "prev_block": "000000000000170edd741e5b1691d0bbad395f5f60db80acfe02a17ca39d121",
  "mrkl_root": "9412a507ab9e366362ecf282ec22146a7861e6e72216fe5bdf593e0ee54c0003",
  "time": 1364140153,
  "bits": 436371822,
  "nonce": 2640915267,
  "n_tx": 122,
  "size": 53899,
  "tx": [
    {
      "hash": "c4f406368ba5eb3070162af94eba1e3871dede9333545062a6a45b8a3a50eb01",
      "ver": 1,
      "vin_sz": 1,
      "vout_sz": 1,
      "lock_time": 0,
      "size": 110,
      "in": [
        {
          "prev_out": {
            "hash": "0000000000000000000000000000000000000000000000000000000000000000",
            "n": 4294967295
          },
          "coinbase": "0479204f51024f09062f503253482f"
        }
      ],
      "out": [
        {
          "value": "25.06050010",
          "scriptPubKey": "03ddcdae35e28aca364daa1397612d2dafd891ee136d2ca5ab83faff6bc12ed67e OP_CHECKSIG",
          "next_in": {
            "hash": "f0016023d3f27d74f6f8f5260207581d8675980800ab179bfb93a431bc30cada",
            "n": 0
          }
        }
      ],
      "nid": "44964f1fe5934142cafde212b7dcb052d2b7876740affe551e05013a9bddb327"
    },
    {
      "hash": "cfd9c35ce38c7744627005729fba99a8a95aacf9fd8c44200ca0d2e03ab57e57",
      "ver": 1,
      "vin_sz": 1,
```

227836区块

小端:02000000
0x00000002

0x 03=下面3个字节表示高度
0x 0379fc = 227836


```
{
  "hash": "00000000000000d0dfd4c9d588d325dce4f32c1b31b7c0064cba7025a9b9adcc",
  "ver": 2,
  "prev_block": "00000000000001aa077d7aa84c532a4d69bdbff519609d1da0835261b7a74eb6",
  "mrkl_root": "38a2518423d8ea76e716d1dc86d742b9e7f3febda7bf9a3e18bcd6c8ad55ff45",
  "time": 1364140204,
  "bits": 436371822,
  "nonce": 30275792,
  "n_tx": 100,
  "size": 39628,
  "tx": [
    {
      "hash": "0f3601a5da2f516fa9d3f80c9bf6e530f1afb0c90da73e8f8ad0630c5483afe5",
      "ver": 1,
      "vin_sz": 1,
      "vout_sz": 1,
      "lock_time": 0,
      "size": 124,
      "in": [
        {
          "prev_out": {
            "hash": "0000000000000000000000000000000000000000000000000000000000000000",
            "n": 4294967295
          },
          "coinbase": "03fc7903062f503253482f04ac204f510858029a11000003550d3363646164312f736c7573682f",
          "sequence": 0
        }
      ],
      "out": [
        {
          "value": "25.06260000",
          "scriptPubKey": "OP_DUP OP_HASH160 e285a29e0704004d4e95dbb7c57a98563d9fb2eb OP_EQUALVERIFY OP_CHECKSIG",
          "address": "1MejoVXRvsmwyDpTpkw3VJ82NsjjT8SyEw",
          "next_in": {
            "hash": "2c144c8d17d64258b9bfaf37a330561af69b69f85e2287ef8924e9f4fe2a215c",
            "n": 0
          }
        }
      ],
      "nid": "d5188aad5d0d07ac75ca3d10bd0f7e443c9db3a50018641c20028a04ed58dbf2"
    },
    {
      "hash": "263b1f316ed3a8080871ddedb12cbed139596ca99e3e1468c3cc72f37ee6acef",
```

Version3(BIP-66)

- 2015年2月以软分叉的形式被添加进Bitcoin core 0.10.0，2015年7月正式生效
- 主要改变了比特币交易的验证规则，采用严格DER编码，修复原本采用Openssl带来的bug
- 区块版本从2升级至3

区块360000

Summary	
Number Of Transactions	1223
Output Total	14,371.18783222 BTC
Estimated Transaction Volume	2,563.78382692 BTC
Transaction Fees	0.21340477 BTC
Height	360000 (Main Chain)
Timestamp	2015-06-08 14:08:27
Received Time	2015-06-08 14:08:27
Relayed By	F2Pool
Difficulty	47,589,591,153.63
Bits	404167307
Size	778.316 kB
Weight	3113.012 kWU
Version	3
Nonce	2568655490
Block Reward	25 BTC

Hashes	
Hash	00000000000000000ca6e07cf681390ff888b7f96790286a440da0f2b87c8ea6
Previous Block	00000000000000000fb0dbaa535fe89556b5da5810f0af84e16eeb87b4a274ec
Next Block(s)	000000000000000000144eda4e110a9389cb8e6a301366445ffee980862faff5bc
Merkle Root	01c3f82b19ec7b09b3c5af91a23aa67c930cecae01da9e1a0da8ab7e4c4ab2f1

Version 4 (BIP65)

- 以软分叉的形式被引入Bitcoin Core 0.11.2(2015年11月)，2015年12月被激活
- 给比特币脚本系统新增一个操作符OP_CHECKLOCKTIMEVERIFY，允许交易输出在某未来区块高度后或者某未来时间后才可以被消费，在这笔交易输出还被锁定时，让交易输出不可被花费

- <now + 3 months> CHECKLOCKTIMEVERIFY DROP DUP HASH160 <Bob's Public Key Hash> EQUALVERIFY CHECKSIG

区块:398363

小端：04000000

0x00000004

版本为4

BIP65

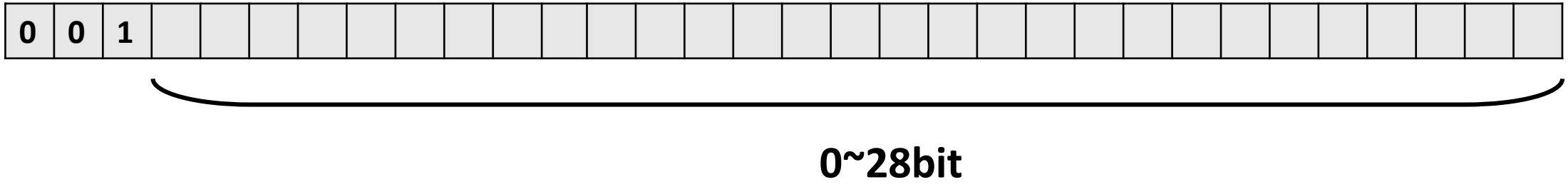
对比特币脚本添加了一个新的操作符OP_CHECKLOCKTIMEVERIFY，允许在未来某个区块高度后，或者未来某个时间节点后，这笔交易的输出才可以被使用

版本为4


```
{
  "hash": "00000000000000001bc56cb394d527409e748c1cd2f90d8058b42ca89737eaf",
  "ver": 4,
  "prev_block": "00000000000000037adb44f99678020538dbd9ed7ea8a368cb66ced02f1b89",
  "mrkl_root": "c427b92144c12bfee64c86bc3881c4ab9dafc58b7e187da1bb1ae572b55c29e4",
  "time": 1455439407,
  "bits": 403153172,
  "nonce": 1114021389,
  "n_tx": 1361,
  "size": 820449,
  "tx": [
    {
      "hash": "e70c7a9ad17a09f43981d2b04842837ddd94774218f08391213eaa4ff6660756",
      "ver": 1,
      "vin_sz": 1,
      "vout_sz": 1,
      "lock_time": 0,
      "size": 123,
      "in": [
        {
          "prev_out": {
            "hash": "0000000000000000000000000000000000000000000000000000000000000000",
            "n": 4294967295
          },
          "coinbase": "031b1406192f416e74506f6f6c2f7363322f384d2f2a1ea0cb2056c03e2fdf010000837e0600"
        }
      ],
      "out": [
        {
          "value": "25.23269864",
          "scriptPubKey": "OP_DUP OP_HASH160 35df7e6daa60393b0ed2474a21713a845a2212dd OP_EQUALVERIFY OP_CHECKSIG",
          "address": "15urYnyeJe3gwbGJ74wcX89Tz7ZtsFDVew",
          "next_in": {
            "hash": "a788cc778e1a3c5bde5535b967af500a41e71daaab8fb523f4e9e9b2c057691f",
            "n": 19
          }
        }
      ],
      "nid": "5618c826f7abe04399e383ff931d4ad6c9499265cb23aec3e163c41cf8d65ebf"
    },
    {
      "hash": "fb3af015d52402997fd25c4a03fd76178690f66640c1a0d7b9438bfa820dce3c",
      "ver": 1,
      "vin_sz": 45
```

BIP-9

- 定义了区块头部Version字段的修改规则，以允许同时部署多个软分叉，将version字段看做bit vector，每一位代表一个独立的提案，每次调整target（约两周）时，会统计支持这个软分叉的区块数目，一旦软分叉成功或者超时，会将占用的这个位撤销，以便于后续的软分叉使用这个bit
- 规定必须以001开头 （Version： 0x20000000~0x3FFFFFFF）
- 0x20000000代表none，不支持任何一个软分叉提案



按BIP-9规则部署的

Name	Bit	Mainnet Start	Mainnet Expire	Mainnet State	Testnet Start	Testnet Expire	Testnet State	BIPs
csv	0	2016-05-01 00:00:00	2017-05-01 00:00:00	active since #419328	2016-03-01 00:00:00	2017-05-01 00:00:00	active since #770112	68, 112, 113
segwit	1	2016-11-15 00:00:00	2017-11-15 00:00:00	-	2016-05-01 00:00:00	2017-05-01 00:00:00	active since #834624	141, 143, 147

CSV

- Version 0x20000001
- 在2016-05-01至激活前代表的是支持csv这个软分叉，在这之后，第0 bit和csv这个部署没有关系，csv从第419328区块开始被彻底激活（2016-07-04 23:16:01）
- 李康师兄有讲

CSV 从419328开始激活，第0位不被使用了

Summary	
Number Of Transactions	2200
Output Total	25,042.65794994 BTC
Estimated Transaction Volume	3,763.542803 BTC
Transaction Fees	0.57949039 BTC
Height	419327 (Main Chain)
Timestamp	2016-07-04 23:06:15
Received Time	2016-07-04 23:06:15
Relayed By	BTCC Pool
Difficulty	209,453,158,595.38
Bits	402997206
Size	997.962 kB
Weight	3991.596 kWU
Version	0x20000001
Nonce	2431550324
Block Reward	25 BTC

Summary	
Number Of Transactions	1667
Output Total	19,531.68424104 BTC
Estimated Transaction Volume	2,832.08600971 BTC
Transaction Fees	0.55670839 BTC
Height	419328 (Main Chain)
Timestamp	2016-07-04 23:16:01
Received Time	2016-07-04 23:16:01
Relayed By	KanoPool
Difficulty	213,398,925,331.32
Bits	402990845
Size	988.066 kB
Weight	3952.012 kWU
Version	0x20000000
Nonce	1353150910
Block Reward	25 BTC

Segwit

- Segwit Bip141:提出“witness”结构，将验证交易有效性的签名从交易结构中分离出来，只有需要验证交易时才需要传输Witness，普通使用者关注的是交易本身是否存在
- Bip 148:取代矿工决定是否进行升级更改比特币网络，转向由比特币经济主体（包括用户，交易所，钱包和支付处理商）来决定。通过用户激活软分叉的形式，去激活BIP141
- Bip91：拒绝没有Bit1隔离见证信号的区块，这样BIP141就会被兼容。BIP91会拒绝非隔离见证区块。使用bit4发出，这样纽约共识(segwit2X)就可以激活（80%算力用bit4发信号），同时激活现有的隔离见证方案。如果在8月1日前激活，BIP91将取代BIP 148，BIP 148是一个可能会引起网络分裂风险的提案

segwit

Summary	
Number Of Transactions	2072
Output Total	13,611.6666383 BTC
Estimated Transaction Volume	2,278.79572281 BTC
Transaction Fees	0.81275107 BTC
Height	444444 (Main Chain)
Timestamp	2016-12-21 15:55:40
Received Time	2016-12-21 15:55:40
Relayed By	BTCC Pool
Difficulty	310,153,855,703.43
Bits	402885509
Size	998.037 kB
Weight	3991.896 kWU
Version	0x20000002
Nonce	3260623471
Block Reward	12.5 BTC

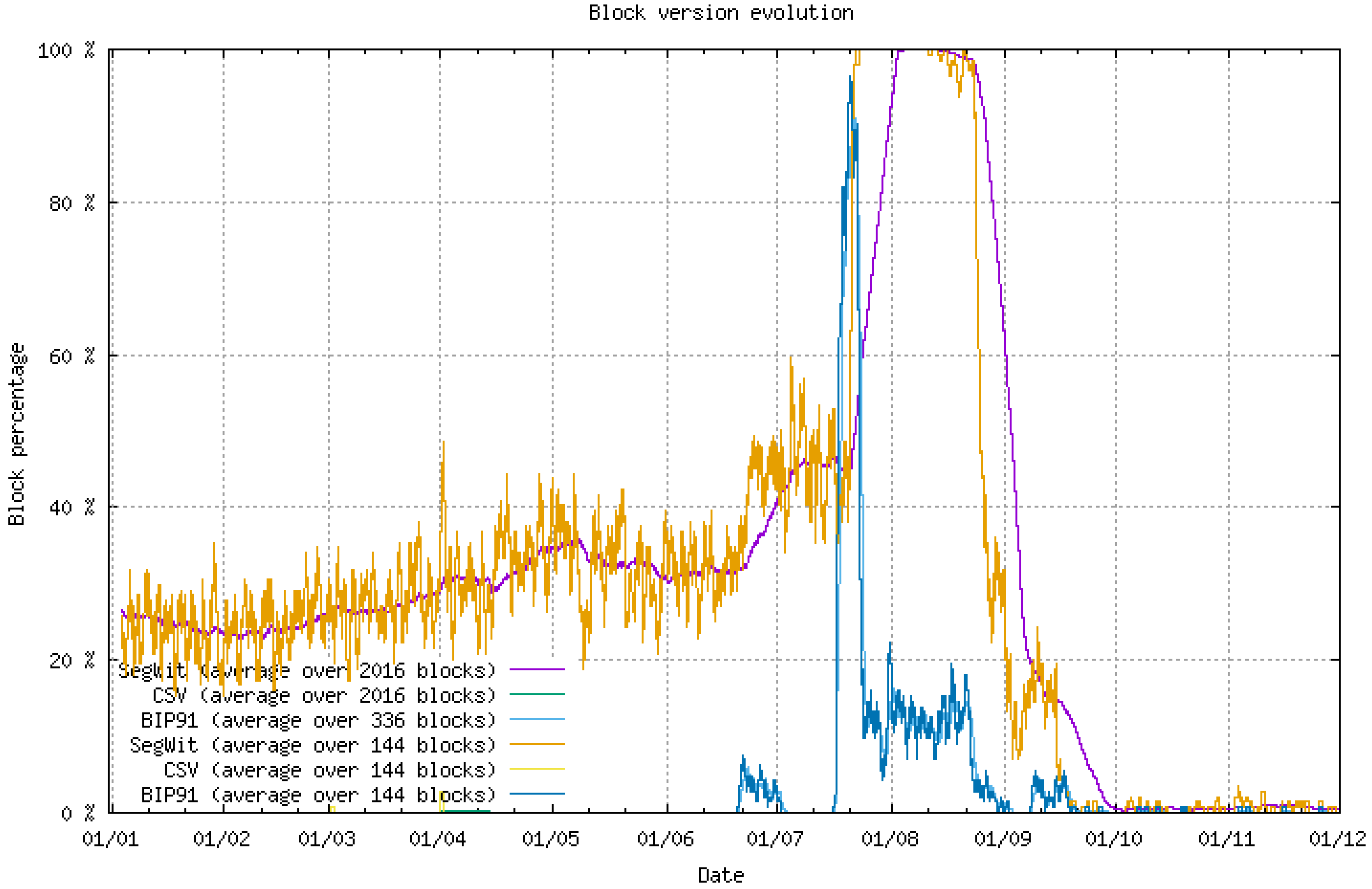
Summary	
Number Of Transactions	2117
Output Total	9,287.65464833 BTC
Estimated Transaction Volume	2,057.83469993 BTC
Transaction Fees	1.47458013 BTC
Height	480000 (Main Chain)
Timestamp	2017-08-10 23:25:59
Difficulty	923,233,068,448.91
Bits	402731232
Size	998.076 kB
Weight	3992.052 kWU
Version	0x20000002
Nonce	2733825927
Block Reward	12.5 BTC

BIP91
segwit2X

Summary	
Number Of Transactions	1
Output Total	12.5 BTC
Estimated Transaction Volume	0 BTC
Transaction Fees	0 BTC
Height	476754 (Main Chain)
Timestamp	2017-07-20 21:13:01
Difficulty	804,525,194,568.13
Bits	402742748
Size	0.261 kB
Weight	0.8 kWU
Version	0x20000010
Nonce	1414126950
Block Reward	12.5 BTC

Segwit &&segwit2x

Summary	
Number Of Transactions	1
Output Total	12.5 BTC
Estimated Transaction Volume	0 BTC
Transaction Fees	0 BTC
Height	493230 (Main Chain)
Timestamp	2017-11-05 19:55:38
Received Time	2017-11-05 19:55:38
Relayed By	BTC.TOP
Difficulty	1,452,839,779,145.92
Bits	402702781
Size	0.263 kB
Weight	0.808 kWU
Version	0x20000012
Nonce	3979754801
Block Reward	12.5 BTC


Block version evolution
100 %
80 %
60 %
40 %
20 %
0 %
Block percentage
01/01
01/02
01/03
01/04
01/05
01/06
01/07
01/08
01/09
01/10
01/11
01/12
Date
SegWit (average over 2016 blocks)
CSV (average over 2016 blocks)
BIP91 (average over 336 blocks)
SegWit (average over 144 blocks)
CSV (average over 144 blocks)
BIP91 (average over 144 blocks)

区块的连接

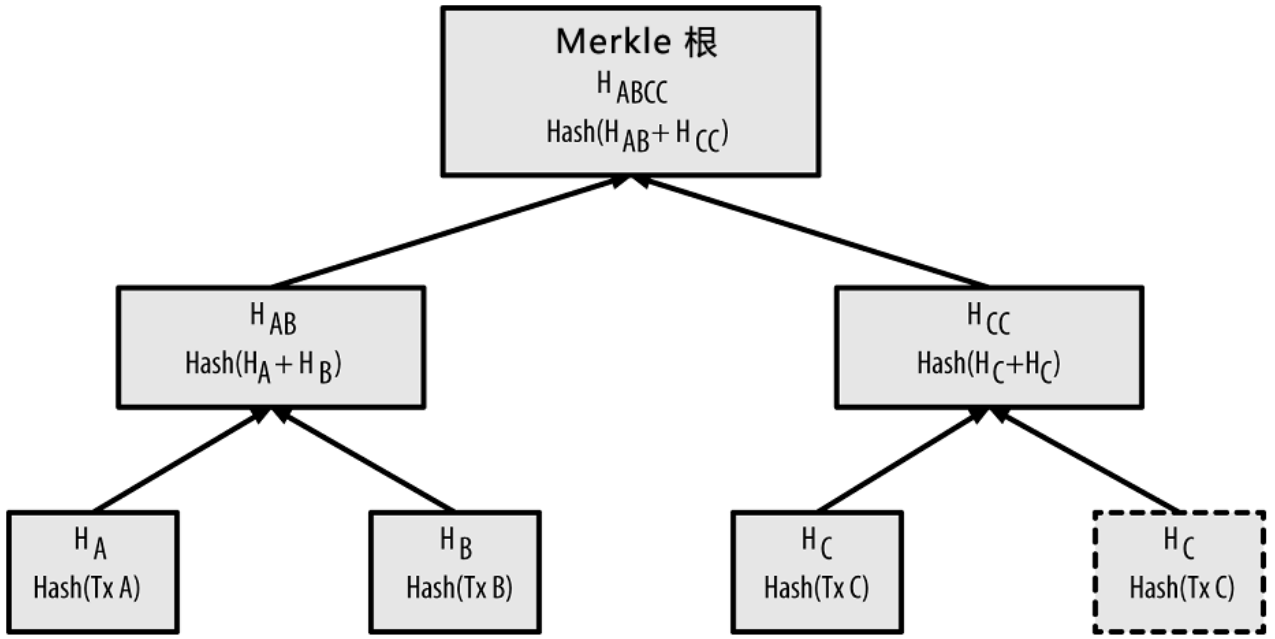

块高度 277316
头哈希值：
0000000000000001b6b9a13b095e96db
41c4a928b97ef2d944a9b31b2cc7bdc4
上一区块头哈希值：
0000000000000002a7bbd25a417c0374
cc55261021e8a9ca74442b01284f0569
时间戳：2013-12-27 23:11:54
难度：118093195.26
Nonce：924591752
Merkle 根：
c91c008c26e50763e9f548bb8b2
fc323735f73577effbc55502c51eb4cc7cf2e
交易
块高度
块高度 277315
头哈希值：
0000000000000002a7bbd25a417c0374
cc55261021e8a9ca74442b01284f0569
上一区块头哈希值：
0000000000000027e7ba6fe7bad39fa
f3b5a83daed765f05f7d1b71a1632249
时间戳：2013-12-27 22:57:18
难度：118093195.26
Nonce：421546901
Merkle 根：
5e049f4030e0ab2debb92378f5
3c0a6e09548aea083f3ab25e1d94ea1155e29d
交易

Merkle Tree

- 生成Merkle Tree
- 证明交易包含在merkle树中

Merkle Tree

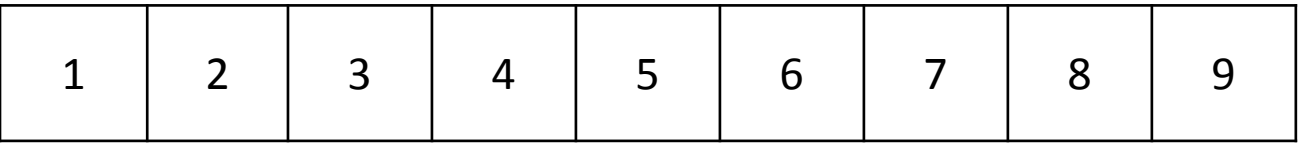
- 定义：Merkle树是一种**哈希二叉树**，它是一种用作快速归纳和校验大规模数据完整性的数据结构。这种二叉树包含加密哈希值
- 至多计算2*log2(N)次就能检查出数据元素是否在该树中



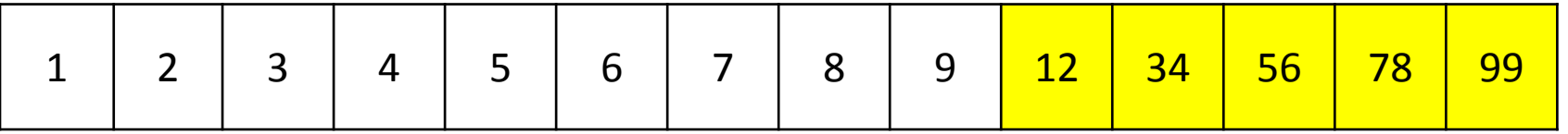
构建Merkle Tree

```
uint256 BuildMerkleTree() const
{
    vMerkleTree.clear();
    foreach(const CTransaction& tx, vtx)
        vMerkleTree.push_back(tx.GetHash());
    int j = 0;
    for (int nSize = vtx.size(); nSize > 1; nSize = (nSize + 1) / 2)
    {
        for (int i = 0; i < nSize; i += 2)
        {
            int i2 = min(i+1, nSize-1);
            vMerkleTree.push_back(Hash(BEGIN(vMerkleTree[j+i]),  END(vMerkleTree[j+i]),
                                       BEGIN(vMerkleTree[j+i2]), END(vMerkleTree[j+i2])));
        }
        j += nSize;
    }
    return (vMerkleTree.empty() ? 0 : vMerkleTree.back());
}
```

构建Merkle Tree实例

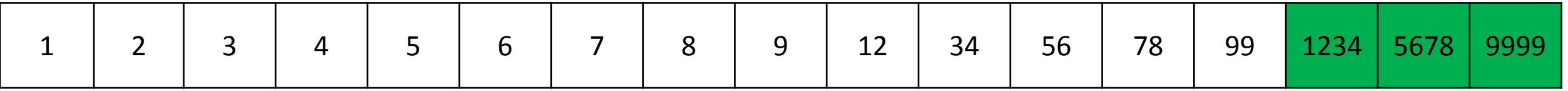


MerkleTree将交易哈希全部push

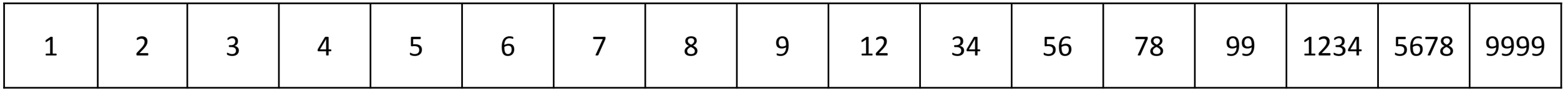


nSize = 9

nSize = 5

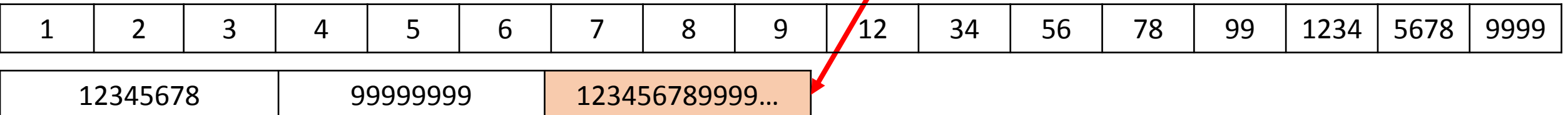


nSize = 3

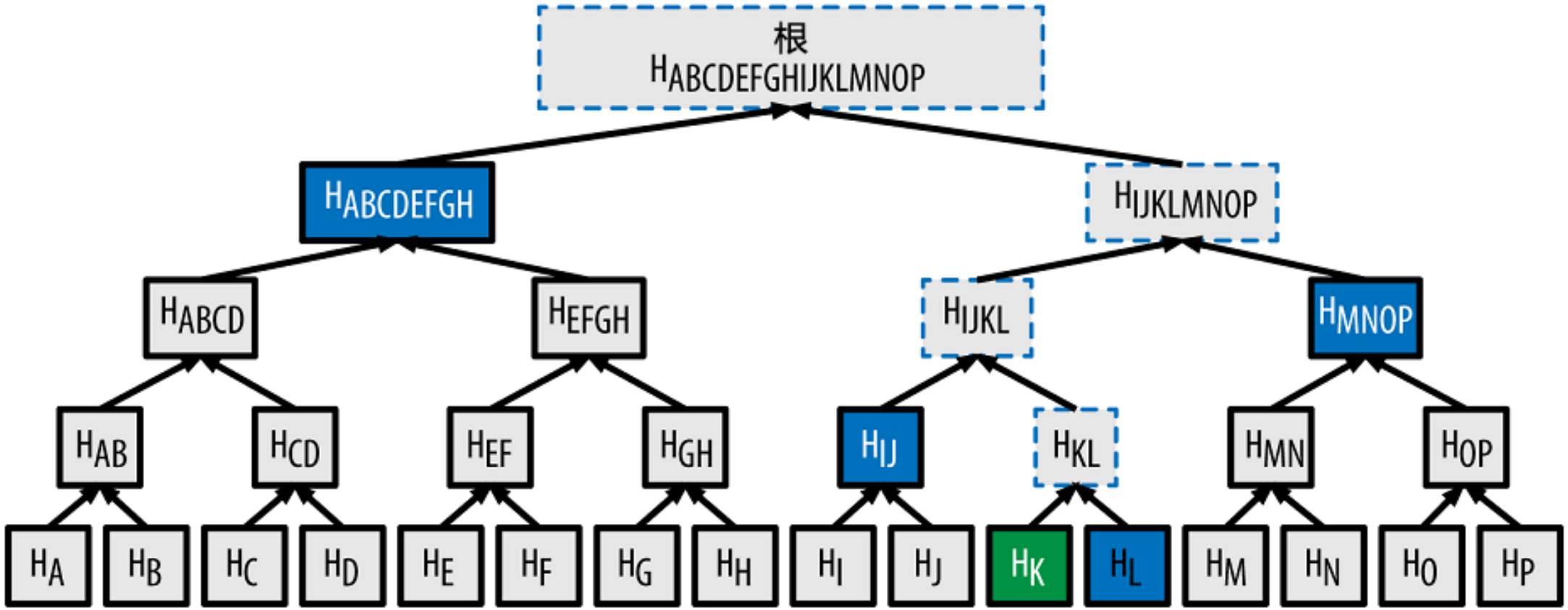


nSize = 2

MerkleRoot



证明交易Hk包含在merkle树中



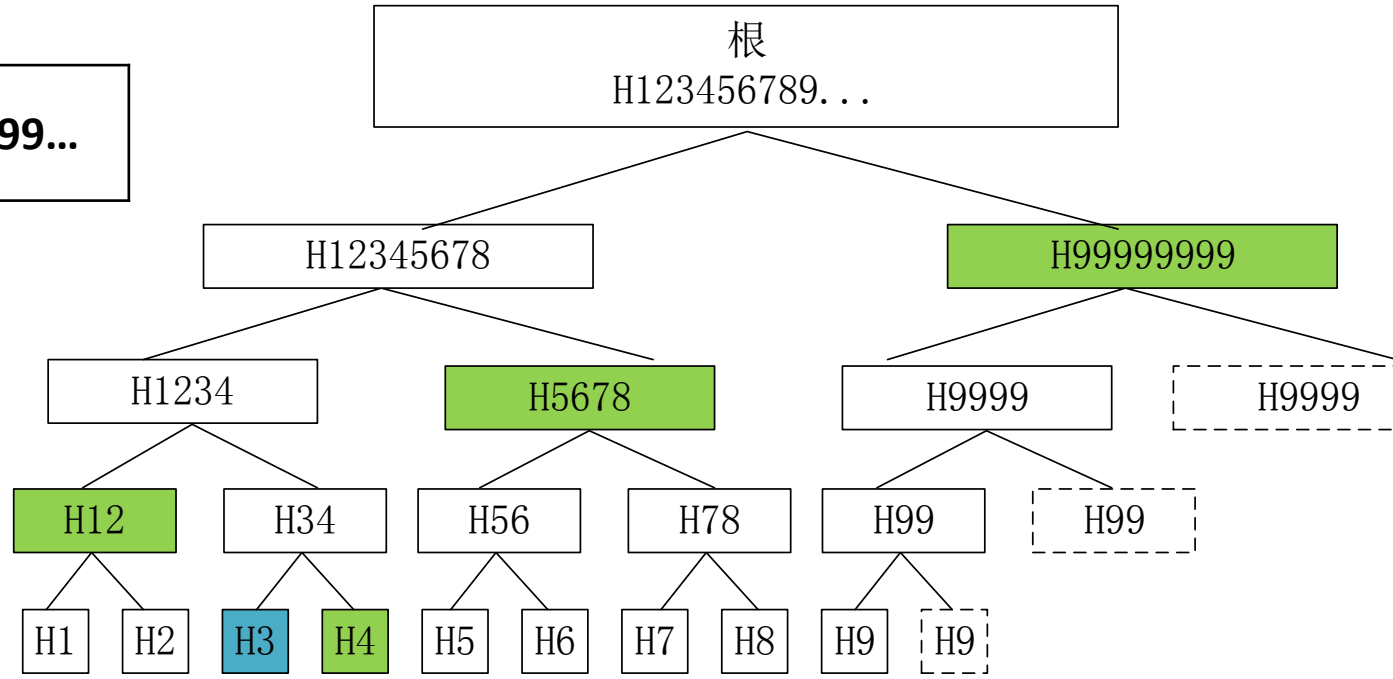
构建Merkle Path

```
vector<uint256> GetMerkleBranch(int nIndex) const
{
    if (vMerkleTree.empty())
        BuildMerkleTree();
    vector<uint256> vMerkleBranch;
    int j = 0;
    for (int nSize = vtx.size(); nSize > 1; nSize = (nSize + 1) / 2)
    {
        int i = min(nIndex^1, nSize-1);
        vMerkleBranch.push_back(vMerkleTree[j+i]);
        nIndex >>= 1;
        j += nSize;
    }
    return vMerkleBranch;
}
```

Merkle Path构建实例

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	2	3	4	5	6	7	8	9	12	34	56	78	99	1234	5678	9999

17	18	19
12345678	99999999	123456789999...



- nIndex = 2
- 确认交易id=3的这笔交易是否包含在这个merkle树中，会返回绿色标识的这几个hash值，即为所谓的path。
- 可以根据交易id=3与这几个点的hash值经过计算得到merkle root的值，与交易头部存储的merkle root值相比较，一致则证明了交易3确实存在于本区块交易中

END