区块链基础技术

- 非对称加密
- 哈希函数，签名技术
- p2p网络，分布式数据库

区块链（比特币）关键问题

- 共识机制
- 拜占庭将军问题
- 双花问题
- 默克尔树

区块链（比特币）交易流程

- 角色分类 用户，旷工区别
- 转账流程
- 数据存储，UTXO(未花费的交易输出)
- 工作量证明
- 交易不可更改
- 余额查询

区块链（比特币）的不足

- 专业矿机的出现
- 电力浪费，专业挖矿组织，51%攻击的可能
- 通货紧缩系统，交易费过高，交易过慢

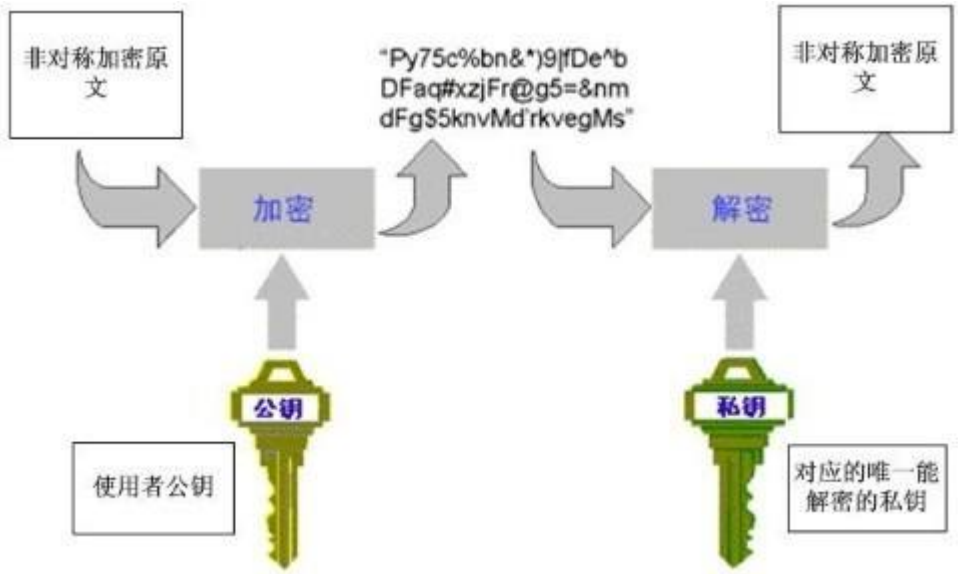
以太坊改进区块链2.0

- 避免专业矿机，但依旧是pow
- 总量未恒定
- 图灵完备，增加智能合约

私有链，公有链，联盟链

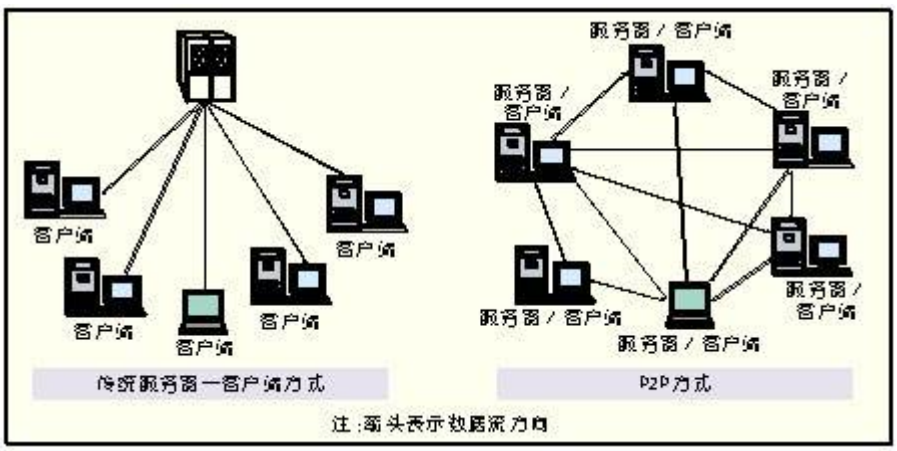
==========

非对称加密

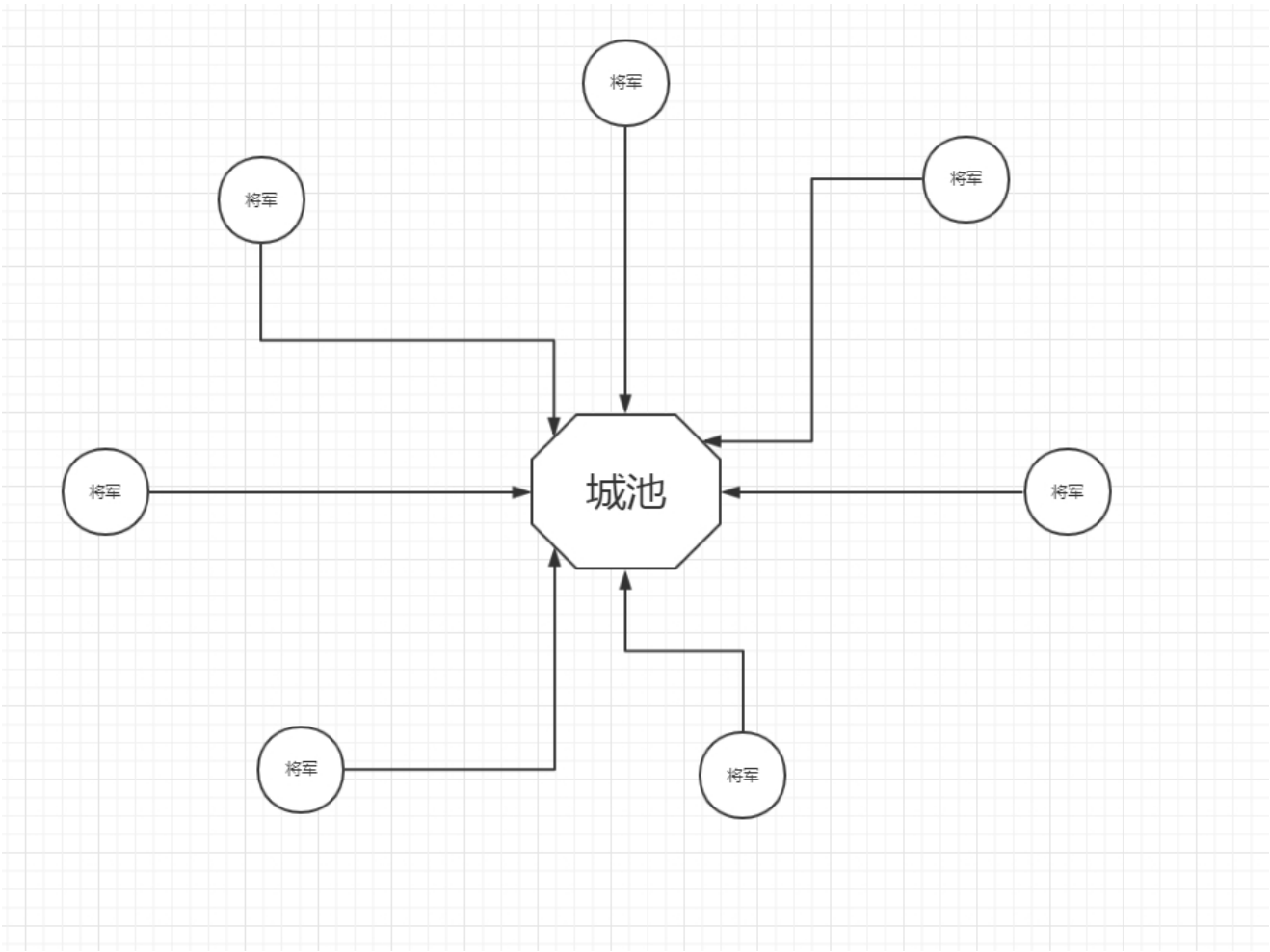


常用哈希（散列）函数 md5（128） sha1（160）

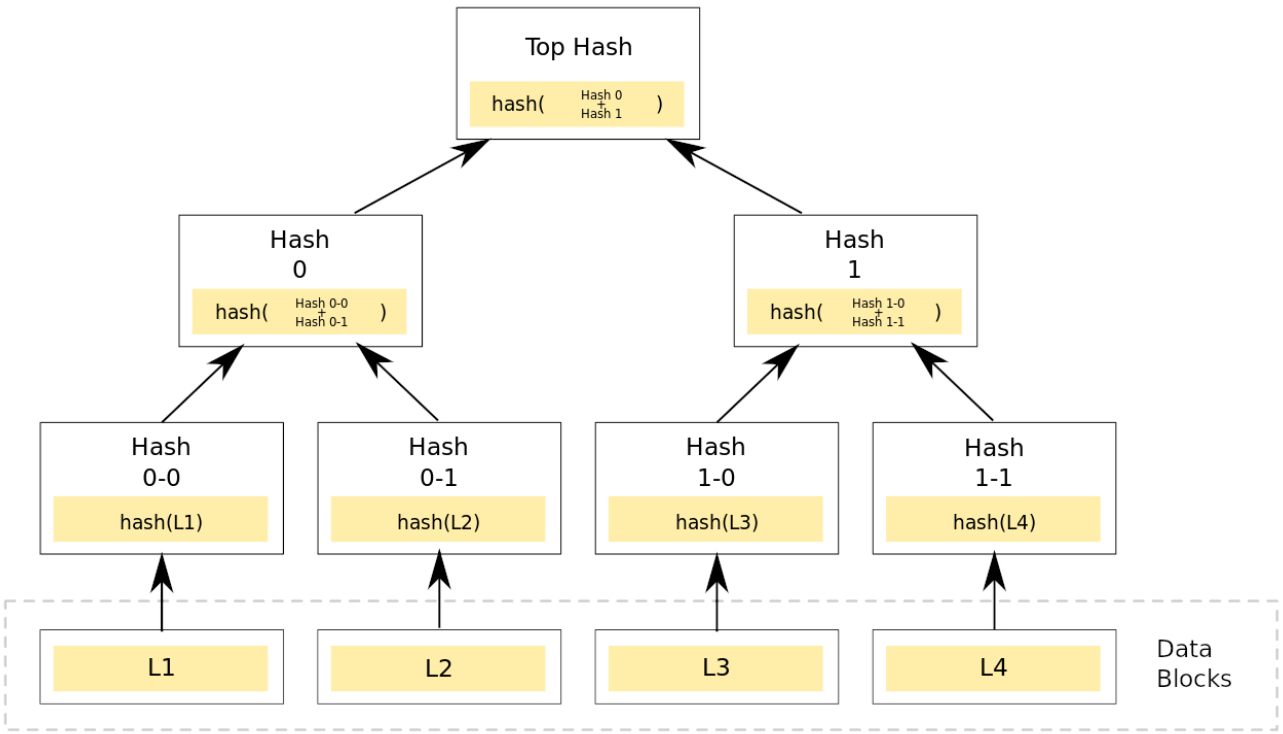
p2p网络(举例快播下载)



共识机制，拜占庭将军问题

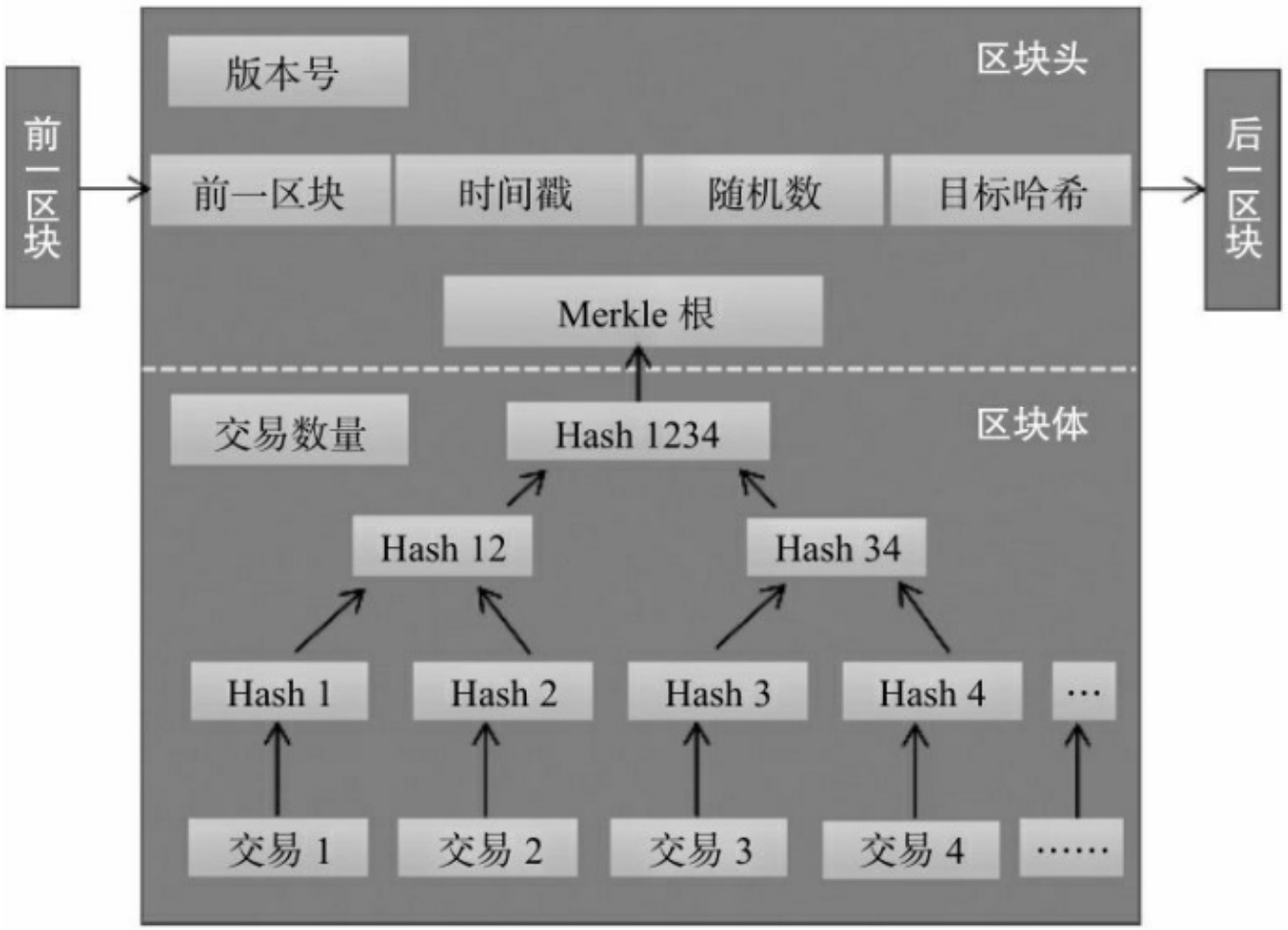


默克尔树



双花问题

比特币数据结构

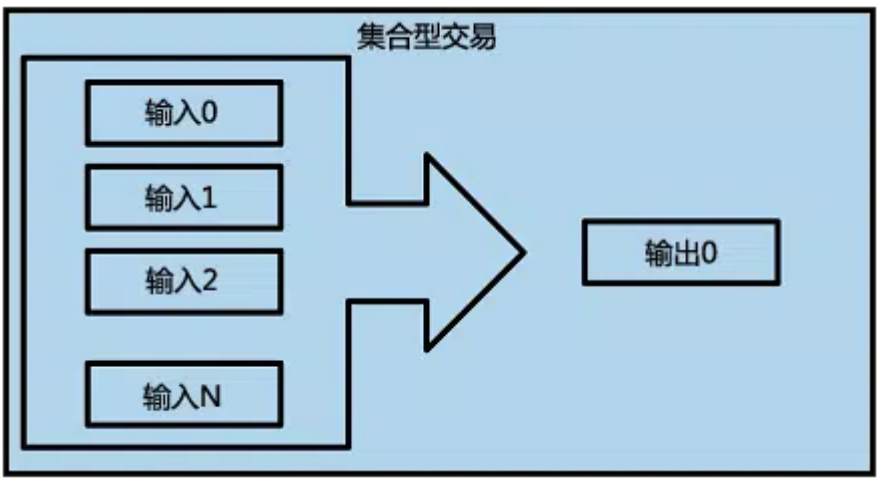


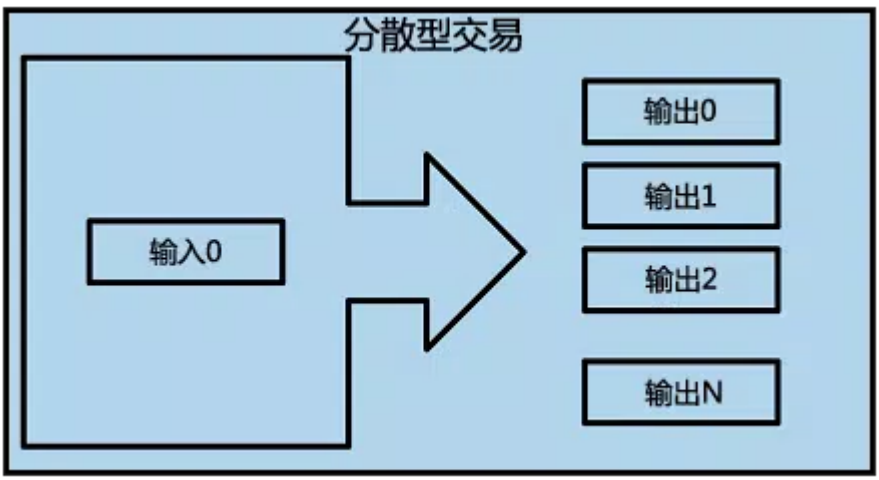
```
$ bitcoin-cli getblock 00000000000000051d2e759c63a26e247f185ecb7926ed7a6624b↵ c31c2a717b true
{
    "hash" : "00000000000000051d2e759c63a26e247f185ecb7926ed7a6624bc31c2a717
b",
    "confirmations" : 2,
    "size" : 248758,
    "height" : 286384,
    "version" : 2,
    "merkleroot" : "9891747e37903016c3b77c7a0ef10acf467c530de52d84735bd55538719f9916",
    "tx" : [
        "46e130ab3c67d31d2b2c7f8fbc1ca71604a72e6bc504c8a35f777286c6d89bf0",
        "2d5625725b66d6c1da88b80b41e8c07dc5179ae2553361c96b14bcf1ce2c3868",
        "923392fc41904894f32d7c127059bed27dbb3cfd550d87b9a2dc03824f249c80",
        "f983739510a0f75837a82bfd9c96cd72090b15fa3928efb9cce95f6884203214",
        "190e1b010d5a53161aa0733b953eb29ef1074070658aaa656f933ded1a177952",
        "ee791ec8161440262f6e9144d5702f0057cef7e5767bc043879b7c2ff3ff5277",
        "4c45449ff56582664abfadeb1907756d9bc90601d32387d9cfd4f1ef813b46be",
        "3b031ed886c6d5220b3e3a28e3261727f3b4f0b29de5f93bc2de3e97938a8a53",
        "14b533283751e34a8065952fd1cd2c954e3d37aaa69d4b183ac6483481e5497d",
        "57b28365adaff61aaf60462e917a7cc9931904258127685c18f136eeaebd5d35",
        "8c0cc19fff6b66980f90af39bee20294bc745baf32cd83199aa83a1f0cd6ca51",
        "1b408640d54a1409d66ddaf3915a9dc2e8a6227439e8d91d2f74e704ba1cdae2",
        "0568f4fad1fdeff4dc70b106b0f0ec7827642c05fe5d2295b9deba4f5c5f5168",
        "9194bfe5756c7ec04743341a3605da285752685b9c7eebb594c6ed9ec9145f86",
        "765038fc1d444c5d5db9163ba1cc74bba2b4f87dd87985342813bd24021b6faf",
        "bff1caa9c20fa4eef33877765ee0a7d599fd1962417871ca63a2486476637136",
        "d76aa89083f56fcce4d5bf7fcf20c0406abdac0375a2d3c62007f64aa80bed74",
        "e57a4c70f91c8d9ba0ff0a55987ea578affb92daaa59c76820125f31a9584dfc",
        "9ca8f969bd3ef5ec2a8685660fdbf7a8bd365524c2e1fc66c309acbae2c14ae3",

#[... many more transactions ...]

    ],
    "time" : 1392660808,
    "nonce" : 3888130470,
    "bits" : "19015f53",
    "difficulty" : 3129573174.52228737,
    "chainwork" : "0000000000000000000000000000000000000000000001931d1658fc04879e466",
    "previousblockhash" : "000000000000000177e61d5f6ba6b9450e0dade9f39c257b4d48b4941ac77e7",
    "nextblockhash" : "00000000000000001239d2c3bf7f4c68a4ca673e434702a57da8fe0d829a92eb6"
```

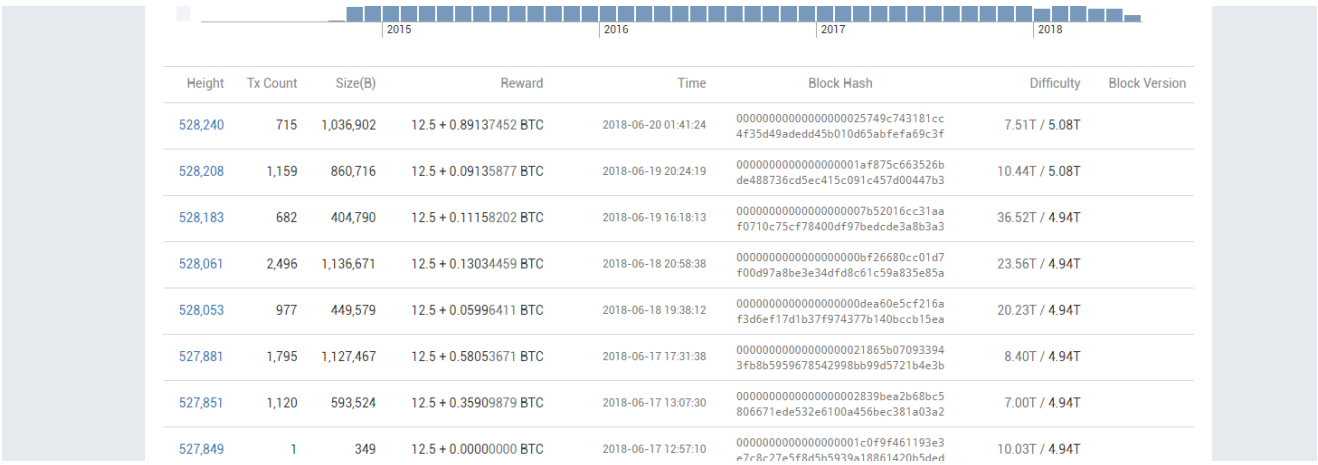
复式记账薄式交易

输入	值	输出	值
输入1	0.10 BTC	输出1	0.10 BTC
输入2	0.20 BTC	输出2	0.20 BTC
输入3	0.10 BTC	输出3	0.20 BTC
输入4	0.15 BTC		
总输入：	0.55 BTC	总输出：	0.50 BTC

	输入	*0.55 BTC*
-	*输出*	*0.50 BTC*
	差价	*0.05 BTC（隐含的交易费）*







Height	Tx Count	Size(B)	Reward	Time	Block Hash	Difficulty	Block Version
528,240	715	1,036,902	12.5 + 0.89137452 BTC	2018-06-20 01:41:24	00000000000000000025749c743181cc4f35d49adedd45b010d65abfefa69c3f	7.51T / 5.08T	
528,208	1,159	860,716	12.5 + 0.09135877 BTC	2018-06-19 20:24:19	00000000000000000001af875c663526bde488736cd5ec415c091c457d00447b3	10.44T / 5.08T	
528,183	682	404,790	12.5 + 0.11158202 BTC	2018-06-19 16:18:13	00000000000000000007b52016cc31aaf0710c75cf78400df97bedcde3a8b3a3	36.52T / 4.94T	
528,061	2,496	1,136,671	12.5 + 0.13034459 BTC	2018-06-18 20:58:38	00000000000000000000bf26680cc01d7f00d97a8be3e34dfd8c61c59a835e85a	23.56T / 4.94T	
528,053	977	449,579	12.5 + 0.05996411 BTC	2018-06-18 19:38:12	00000000000000000000dea60e5cf216af3d6ef17d1b37f974377b140bccb15ea	20.23T / 4.94T	
527,881	1,795	1,127,467	12.5 + 0.58053671 BTC	2018-06-17 17:31:38	00000000000000000021865b070933943fb8b5959678542998bb99d5721b4e3b	8.40T / 4.94T	
527,851	1,120	593,524	12.5 + 0.35909879 BTC	2018-06-17 13:07:30	00000000000000000002839bea2b68bc5806671ede532e6100a456bec381a03a2	7.00T / 4.94T	
527,849	1	349	12.5 + 0.00000000 BTC	2018-06-17 12:57:10	00000000000000000001c0f9f461193e3e7c8c27e5f8d5b5939a18861420b5ded	10.03T / 4.94T	

比特币钱包和交易所

Merkle树和简单支付验证（SPV）

布隆过滤器原理

SPV节点完全可以验证某个交易存在，但它不能验证某个交易（譬如同一个UTXO的双重支付）不存在，这是因为SPV节点没有一份关于所有交易的记录。