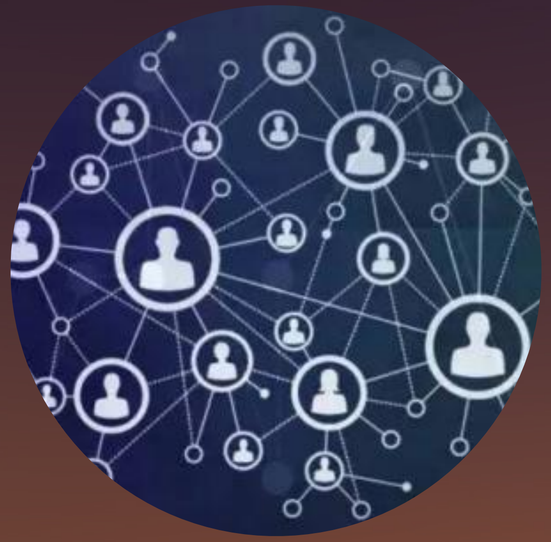
BITCOIN

zhu linfeng

1. 货币由中央银行发行
2. 防伪技术，不易复制
3. 交易双方信息保密

1. 与纸币属于同一货币系统
2. 银行清算，三方机构担保
3. 交易信息不保密

1. 货币由比特币网络发行
2. 区块链共识杜绝无效交易
3. 交易双方信息保密



去中心化

拒绝双重支付

匿名性

比特币发展历史

是目前市场总值最高的加密货币

2008 10 “中本聪”发表比特币白皮书，提出比特币

2009 01 比特币运行，每分钟诞生 50 BTC

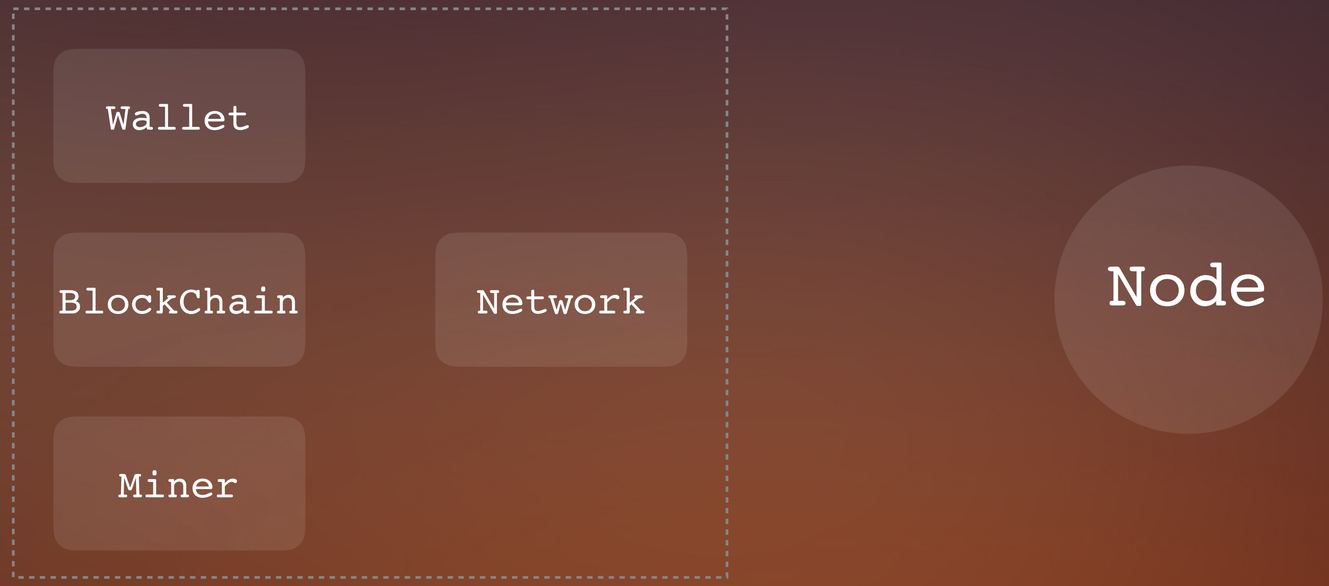
2010 05 佛罗里达州程序员使用 10000 BTC 购买两张披萨

2012 10 比特币挖矿奖励减半

2013 03 BlockChain 出现分叉

2014 02 第一台 BTC 的 ATM 在加拿大出现

2017 11 BTC 首次突破 10000$


Wallet
BlockChain
Network
Miner
Node

Wallet

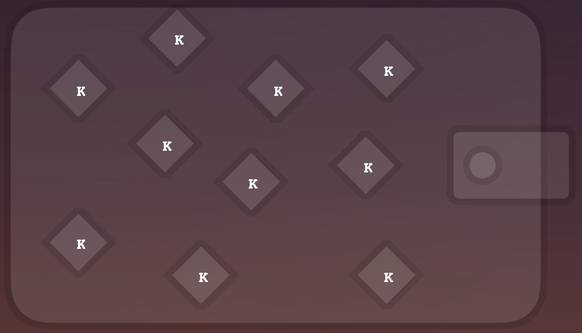
1. 一个钱包会包含多个地址，基本不设限
2. 地址是公钥或者由公钥生成
3. 私钥需要由口令解锁
4. 一般一个地址使用一次随即丢弃

Example : 1thMirt546nngXqyPEz532S8fLwbozud8

Multi-Sig Addresses : hash(address1 + address2 + . . .)

Vanity Addresses : 1yunjingitnngXqyPEz532S8fLwbozud8

Paper Addresses

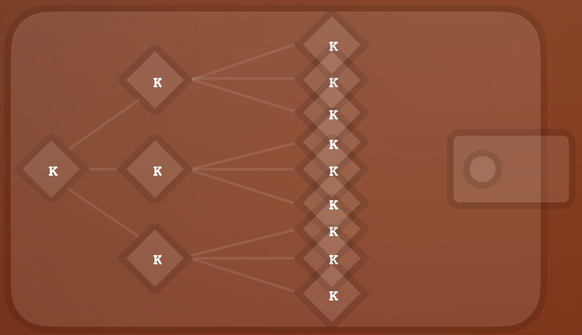


Non-Deterministic (Random) Wallets

随机生成密钥，每对密钥只使用一次
需要频繁备份，地址容易丢失，地址太多太杂
不便于管理、备份和导入

Deterministic Wallets

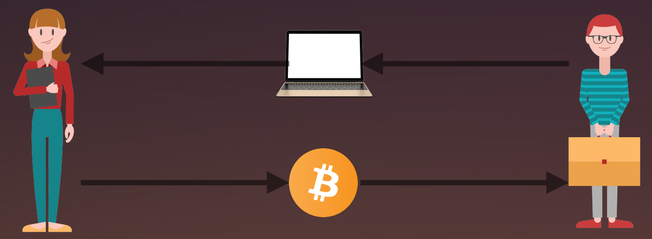
所有密钥由一个种子生成
便于管理、便于备份



Hierarchical Deterministic Wallets

所有密钥由一个种子生成
密钥组织成树形结构
便于组织机构使用管理

Transaction



ebadfaa92f1fd29e2fe296eda702c48bd11ffd52313e986e99ddad9084062167	8000000	0.08
6596fd070679de96e405d52b51b8e1d644029108ec4cbfe451454486796a1ecf	16050000	0.1605
b2affea89ff82557c60d635a2a3137b8f88f12ecec85082f7d0a1f82ee203ac4	10000000	0.1
7dbc497969c7475e45d952c4a872e213fb15d45e5cd3473c386a71a1b0c136a1	25000000	0.25
55ea01bd7e9afd3d3ab9790199e777d62a0709cf0725e80a7350fdb22d7b8ec6	54800000	0.548
12b6a7934c1df821945ee9ee3b3326d07ca7a65fd6416ea44ce8c3db0c078c64	10000000	0.1
7f42eda67921ee92eae5f79bd37c68c9cb859b899ce70dba68c48338857b7818	16100000	0.16

```
version: 1
input_counter: 4
vin: [
        {
            txid: 55ea01bd7e9afd3d3ab9790199e777d62a0709cf0725e80a7350fdb22d7b8ec6,
            tx_intput_n: 1,
            scriptSize: 856,
            scriptSig: . . .,
            sequence: 4294967295
        },
        {
            txid: 7dbc497969c7475e45d952c4a872e213fb15d45e5cd3473c386a71a1b0c136a1,
            tx_intput_n: 2,
            scriptSize: 793,
            scriptSig: . . .,
            sequence: 4294967295
        },
        {
            txid: 7f42eda67921ee92eae5f79bd37c68c9cb859b899ce70dba68c48338857b7818,
            tx_intput_n: 1,
            scriptSize: 456,
            scriptSig: . . .,
            sequence: 4294967295
        },
        {
            txid: b2affea89ff82557c60d635a2a3137b8f88f12ecec85082f7d0a1f82ee203ac4,
            tx_intput_n: 1,
            scriptSize: 856,
            scriptSig: . . .,
            sequence: 4294967295
        },
    ]
```

```
output_counter: 2
vout: [
        {
            amount: 10000000,
            scriptSize: 32,
            script: 1Bobirt546nngXqyPEz532S8fLwbozud8 ,
        },
        {
            amount: 5700000,
            scriptSize: 32,
            script: 1Alicet546nngXqyPEz532S8fLwbozud8 ,
        }
    ]
locktime: 1405559628
```

inputs = outputs + fee

1.058 = 1 + 0.057 + 0.01

1 BTC = 100000000 satoshi

minimal fee = 10000 satoshi

Transaction

create → broadcast → propagate → blockchain → consume

unlockScript + lockScript = Reverse Polish Notation

2 3 + 8 6 - x = 5 <==> (2 + 3) x (8 - 6) = 5

2 3 OP_ADD 5 OP_EQUAL

<Bob Signature> <Bob Public Key> OP_DUP OP_HASH160 <Bob Public Key Hash> OP_EQUAL OP_CHECKSIG

1. 脚本使交易验证十分灵活
2. 脚本很简单，不会引入漏洞

P2PK

pay to public key

lockScript 包含接收者公钥

P2PKH

pay to public key hash

lockScript 包含接收者钱包地址

Multi-Signature

pay to M addresses

need N sig to unlock

OP_RETURN

不包含交易信息，无法进行消费

交易输出最多携带 40 字节数据

验证结果永远为 invalid

P2SH

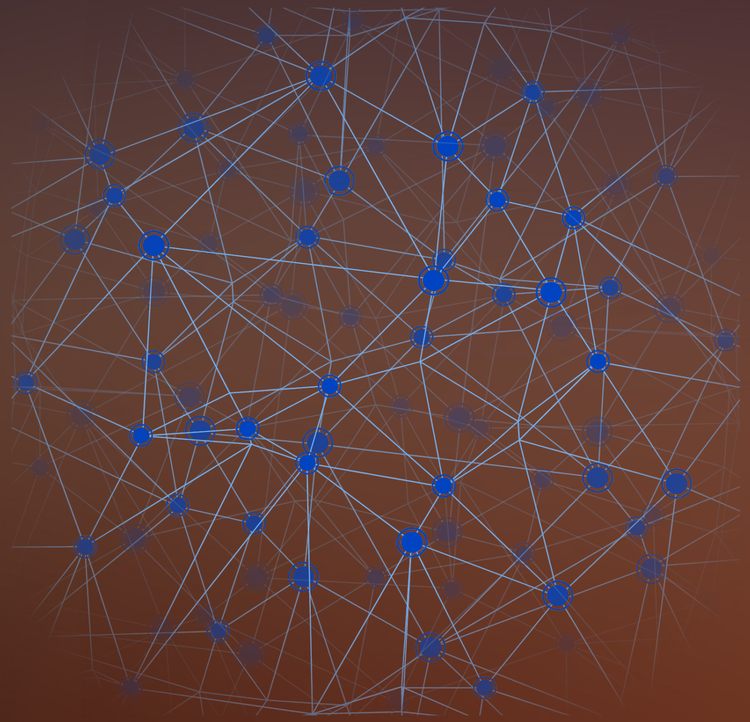
Pay to script hash

对 multi-signature 的简化

1. 一笔交易要等到加入到区块中后才被确认，等到 6 个区块后才被永久确认
2. 对于小额交易，不必要等待交易被加入区块即可认为交易成功，这样只需若干秒就能收到付款
3. 如果丢失钱包地址，那么其对应的交易将永久丢失，比特币存在流失现象

Network

1. 一个新启动的节点如何加入比特币网络?
2. 节点之间如何同步信息



1. 比特币网络有一些长期运行节点，称为种子节点，其记录着一些其他运行的节点
2. 新节点启动时，告知其某个种子节点的地址，从种子节点请求节点列表
3. 从节点列表中选择若干节点发起连接
4. 建立至少一个连接后，向邻居广播自身 IP 地址，以及从邻居获取 IP 地址列表，使互相认识
5. 节点启动后，会记住最近连接成功的邻居地址，在下次启动时直接连接该地址快速加入网络

同步交易信息

1. 同步所有尚未加入区块的交易
2. 交易信息保存于内存，是易失性的，节点重启后需要重新同步交易信息
3. 由于网络延迟，子交易会先于父交易到达节点，成为孤儿交易，临时保存于内存的孤儿交易池中

同步区块信息

1. 所有节点都内置了初始区块(中本聪挖出的第一个区块)
2. 节点维护区块链，区块链有高度，节点会尽量保持自身区块链高度与邻居的一致
3. 如果本节点区块链高度小于邻居(例如新启动的节点)，则从邻居同步所有缺失的区块并验证

SPV (Simplified Payment Verification)

1. 区块链全部数据超过 200G，同步耗时耗硬盘
2. 区块由区块头和交易信息组成，可以只同步区块头 (80 bytes)，使同步数据最多只需要几十兆
3. 只同步区块头也能完成对区块的验证
4. 当要验证交易时，则按需从网络获取相应的交易信息进行验证

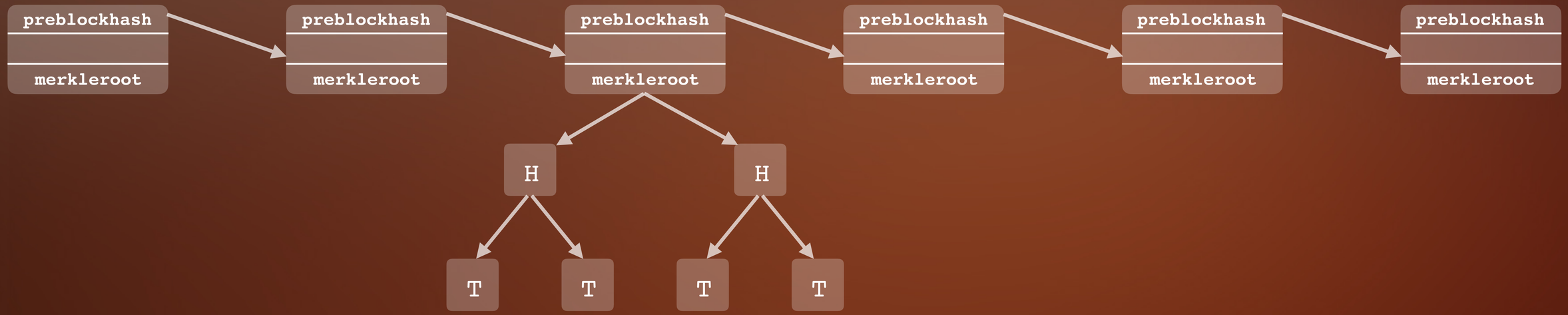
BlockChain

block structure

4 bytes	Block Size	The size of the block, in bytes, following this field
80 bytes	Block Header	Several fields form the block header (see below)
1-9 bytes (VarInt)	Transaction Counter	How many transactions follow
Variable	Transactions	The transactions recorded in this block

block header

4 bytes	Version	A version number to track software/protocol upgrades
32 bytes	Previous Block Hash	A reference to the hash of the previous (parent) block in the chain
32 bytes	Merkle Root	A hash of the root of the Merkle-Tree of this block's transactions
4 bytes	Timestamp	The approximate creation time of this block (seconds from Unix Epoch)
4 bytes	Difficulty Target	The proof-of-work algorithm difficulty target for this block
4 bytes	Nonce	A counter used for the proof-of-work algorithm



BlockChain


```
{
    "hash" : "000000000000001b6b9a13b095e96db41c4a928b97ef2d944a9b31b2cc7bdc4”,
    "confirmations" : 35561,
    "size" : 218629,
    "height" : 277316,
    "version" : 2,
    "merkleroot" : "c91c008c26e50763e9f548bb8b2fc323735f73577effbc55502c51eb4cc7cf2e”,
    "tx":[

        "d5ada064c6417ca25c4308bd158c34b77e1c0eca2a73cda16c737e7424afba2f",
        "b268b45c59b39d759614757718b9918caf0ba9d97c56f3b91956ff877c503fbe",

         ... 417 more transactions ...
    ],
    "time" : 1388185914,
    "nonce" : 924591752,
    "bits" : "1903a30c",
    "difficulty" : 1180923195.25802612,
    "chainwork" : "0000000000000000000000000000000000000000000000934695e92aaf53afa1a”,
    "previousblockhash" : "000000000000002a7bbd25a417c0374cc55261021e8a9ca74442b01284f0569”,
    "nextblockhash" : "000000000000000010236c269dd6ed714dd5db39d36b33959079d78dfd431ba7"
}
```

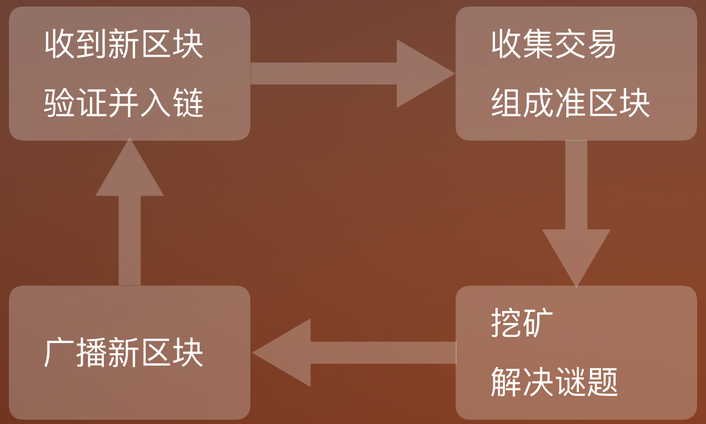

Genesis Block


```
 {
 "hash" : "000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f",

 "confirmations" : 308321,
 "size" : 285,
 "height" : 0,

 "version" : 1,
 "merkleroot" : "4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b",

 "tx":[

            "4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b"
 ],
 "time" : 1231006505,
 "nonce" : 2083236893,
 "bits" : "1d00ffff",
 "difficulty" : 1.00000000,
 "nextblockhash" : "00000000839a8e6886ab5951d76f411475428afc90947ee320161bbf18eb6048"

 }
```

Miner

1. 挖矿最重要的作用是产生信任 ： 信任 = 时间 + 计算量 + 电费

2. 为了鼓励节点挖矿，挖矿成功会有奖励 ： 奖励 = 新比特币 + 交易费



交易优先级

1. 区块第一个交易为 generation transaction, 是对矿工的奖励
2. 区块的前 50k 字节用于收纳高优先级交易。高优先级交易为 amout * age / bytes > 10^8 satoshis * 144 blocks / 250 bytes = 57600000
3. 区块剩余的空间收纳有服务费的交易，按 fee / bytes 排序
4. 若区块仍有剩余空间，则可能会收纳无服务费的交易（区块最大大小为: MAX_BLOCK_SIZE，目前为 1000000）

```
{
    version : 1,
    input_counter: 1,
    vin : [
        {
            coinbase : 03443b0403858402062f503253482f,    // set nonce by miner
            sequence : 4294967295
        }
    ],
    output_counter: 1,
    vout : [
        {
            value : 25.09094928,
            n : 0,
            scriptPubKey :
            {
                asm : 02aa970c592640d19de03ff6f329d6fd2eecb023263b9ba5d1b81c29b523da8b21\ OP_CHECKSIG,
                hex : 2102aa970c592640d19de03ff6f329d6fd2eecb023263b9ba5d1b81c29b523da8b21ac,
                reqSigs : 1,
                type : pubkey,
                addresses : [
                    1MxTkeEP2PmHSMze5tUZ1hAV3YTKu2Gh1N
                ]
            }
        }
    ],
    locktime : 1388185914,
}
```

1. 初始奖励为 50BTC
2. 每 210000 个区块(约 4 年)，奖励减半
3. 目前奖励为 12.5BTC
4. 到 2140 年，比特币总量将近 21000000

Miner

4 bytes	Version
32 bytes	Previous Block Hash
32 bytes	Merkle Root
4 bytes	Timestamp
4 bytes	Difficulty Target
4 bytes	Nonce

00000000000000004c296e6376db3a2412
71f43fd3f5de7ba18986e517a243baa7

Genesis Block bits: 1d00ffff

exponent: ld = 29

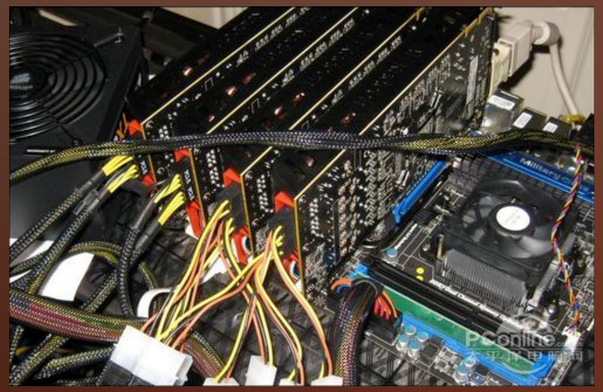
coefficient: 00ffff = 65535

target = coefficient * 2 ^ (8 * (exponent - 3)) =
26959535291011309493156476344723991336010898738574164086137773096960 =

00000000ffff0000000000000000000000000000000000000000000000000000

New Difficulty = Old Difficulty * (Actual Time of Last 2016 Blocks / 20160 minutes)

Miner



Consensus

- Independent verification of each transaction, by every full node, based on a comprehensive list of criteria
- Independent aggregation of those transactions into new blocks by mining nodes, coupled with demonstrated computation through a Proof-of-Work algorithm
- Independent verification of the new blocks by every node and assembly into a chain
- Independent selection, by every node, of the chain with the most cumulative computation demonstrated through Proof-of-Work

Verify Transaction

- The transaction’s syntax and data structure must be correct
- Neither lists of inputs or outputs are empty
- The transaction size in bytes is less than MAX_BLOCK_SIZE
- Each output value, as well as the total, must be within the allowed range of values (less than 21m coins, more than 0)
- None of the inputs have hash=0, N=-1 (coinbase transactions should not be relayed)
- nLockTime is less than or equal to INT_MAX
- The transaction size in bytes is greater than or equal to 100
- The number of signature operations contained in the transaction is less than the signature operation limit
- The unlocking script (scriptSig) can only push numbers on the stack, and the locking script (scriptPubkey) must match isStandard forms (this rejects “nonstandard” transactions)
- A matching transaction in the pool, or in a block in the main branch, must exist
- For each input, if the referenced output exists in any other transaction in the pool, reject this transaction
- For each input, look in the main branch and the transaction pool to find the referenced output transaction. If the output transaction is missing for any input, this will be an orphan transaction. Add to the orphan transactions pool, if a matching transaction is not already in the pool
- For each input, if the referenced output transaction is a coinbase output, it must have at least COINBASE_MATURITY (100) confirmations
- For each input, the referenced output must exist and cannot already be spent
- Using the referenced output transactions to get input values, check that each input value, as well as the sum, are in the allowed range of values (less than 21m coins, more than 0)
- Reject if the sum of input values < sum of output values
- Reject if transaction fee would be too low to get into an empty block
- The unlocking scripts for each input must validate against the corresponding output locking scripts

Verify Block

- The block data structure is syntactically valid
- The block header hash is less than the target difficulty (enforces the Proof-of-Work)
- The block timestamp is less than two hours in the future (allowing for time errors)
- The block size is within acceptable limits
- The first transaction (and only the first) is a coinbase generation transaction
- All transactions within the block are valid

THANKS