北京大学
PEKING UNIVERSITY

区块链课程

孙惠平
sunhp@ss.pku.edu.cn

北京大学 软件与微电子学院
School of Software and Microelectronics, Peking University

北京大学
PEKING UNIVERSITY

PART 第三章

比特币

凯恩斯在《货币论》上讲，货币可以承载债务，价格的一般等价物。货币的本质是等价物，它可以是任何东西，如：一张纸，一个数字，只要人们认可它的价值。人民币，美元等作为国家信用货币，其价值由国家主权背书。而数字货币是一种不依赖信用和实物的新型货币，它的价值由大家的共识决定。

比特币就是一种数字货币。

目录

CONTENTS

- 比特币简介
- 比特币地址
- 比特币钱包
- 比特币交易
- 比特币网络
- 比特币区块
- 比特币挖矿

第 一 节
比特币简介

01 比特币的由来
02 比特币的产生
03 比特币的定义
04 比特币的历史
05 比特币的生态

1.1 比特币的由来

货币的演化

物物交换
- 贝壳、羽毛、牲口等实物货币

金属货币
- 黄金、白银等贵金属

纸币
- 早期纸币、银票、廉价金属货币
- 纸币本位货币

中心化电子货币
- 在线支付
- 银行卡
- Q币等游戏币
- 电子现金

去中心化电子货币
- 比 特 币

商品货币时代

- 货币价值主要取决于贵金属的发现和冶炼

信用货币时代

- 货币本身没有价值而取决于对发行机构的信任

去中心货币时代

- 货币价值取决于人们对算法、系统的认可

1.2 比特币的产生

北京大学 PEKING UNIVERSITY

第一次以论文的形式提出（纽约时间2008.10.31）：

Bitcoin: A Peer-to-Peer Electronic Cash System

（比特币：一种点对点电子现金系统）

发明人
Satoshi Nakamoto
（中本聪）

论文解决了无监管网络世界里的两个实际问题

- 货币伪造问题
- 双重支付问题

Bitcoin P2P e-cash paper

Satoshi Nakamoto | Sat, 01 Nov 2008 16:16:33 -0700

I've been working on a new electronic cash system that's fully peer-to-peer, with no trusted third party.

The paper is available at:
http://www.bitcoin.org/bitcoin.pdf

The main properties:
Double-spending is prevented with a peer-to-peer network.
No mint or other trusted parties.
Participants can be anonymous.
New coins are made from Hashcash style proof-of-work.
The proof-of-work for new coin generation also powers the network to prevent double-spending.

Bitcoin: A Peer-to-Peer Electronic Cash System

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without the burdens of going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as honest nodes control the most CPU power on the network, they can generate the longest chain and outpace any attackers. The network itself requires minimal structure. Messages are broadcasted on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

Full paper at:
http://www.bitcoin.org/bitcoin.pdf

Satoshi Nakamoto

The Cryptography Mailing List
Unsubscribe by sending "unsubscribe cryptography" to

1.3 比特币的定义

1. 一个纯粹的点对点电子现金系统，使在线支付能够直接由一方发起并支付给另一人，中间不需要通过任何金融机构。

01

02

2. 不需要授信的第三方支持就能防止双重支付，点对点的网络环境是解决双重支付的一种方案。

03

3. 对全部交易加上时间戳，并将他们并入一个不断延展的基于哈希算法的工作量证明的链条作为交易记录。除非重新完成全部的工作量证明，形成的交易记录将不可更改。

04

4. 最长的链条不仅将作为被观察的事件序列的证明，而且被视为来自 CPU（中央处理器）的计算能力最大的池。只要大多数 CPU 的计算能力不被合作攻击的节点所控制，那么就会生成最长的、长度超过攻击者的链条。

05

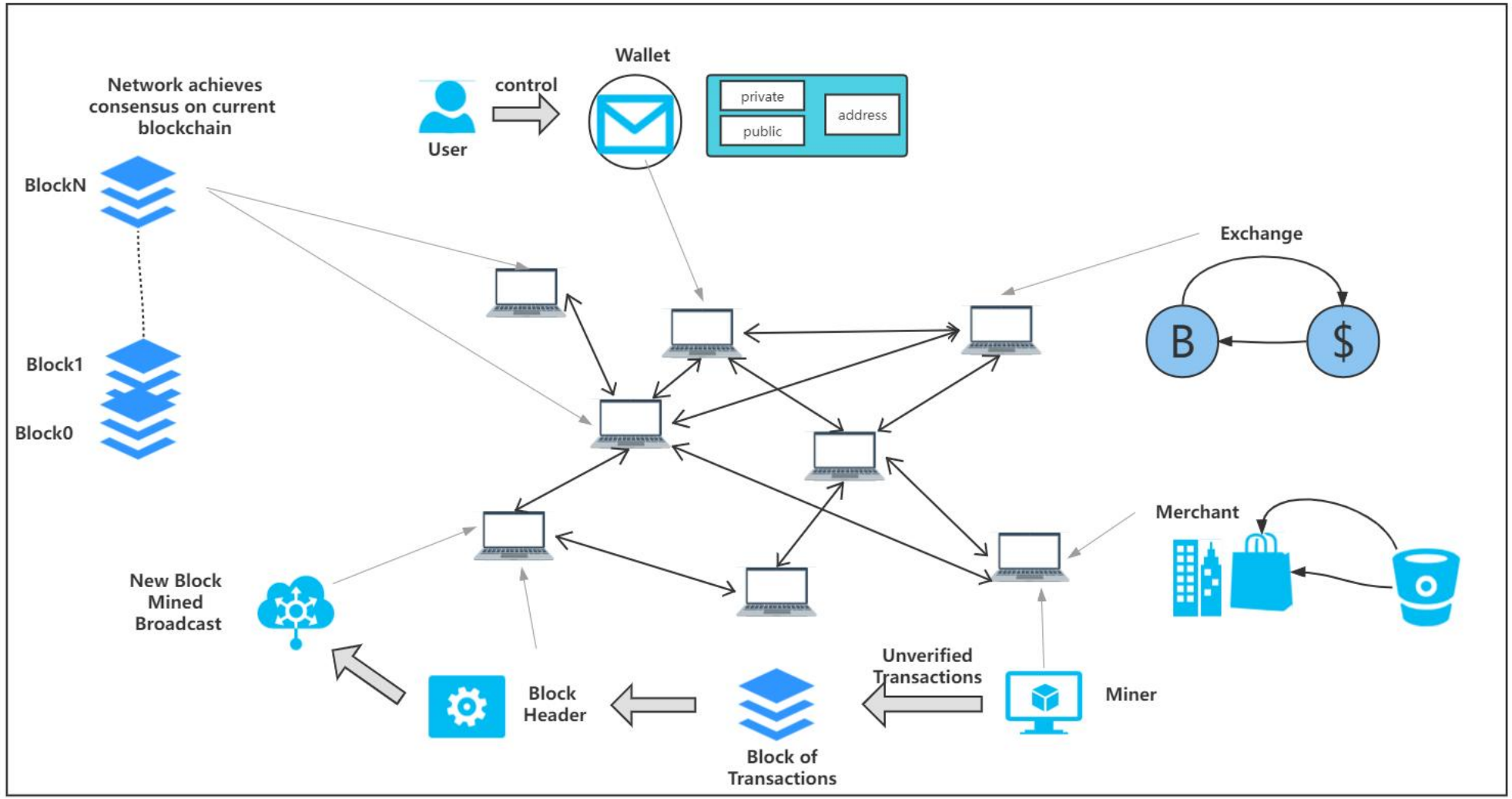
5. 这个系统本身需要的基础设施非常少，节点尽最大努力在全网传播信息即可，节点可以随时离开和重新加入网络，并将最长的工作量证明作为该节点离线期间发生的交易的证明。

1.4 比特币的历史

北京大学 PEKING UNIVERSITY

- 2008-10-31：中本聪发表论文《比特币：种点对点的电子现金系统》
- 2009-1-3：比特币创世区块（Genesis Block）诞生，第一批比特币被挖出
- 2010-5-22：比特币历史上第一笔交易：佛罗里达程序员LaszloHanyecz用1万个比特币购买了价值25美元的披萨
- 2011-6：比特币获得时代周刊和福布斯的关注，开始吸引主流媒体的目光
- 2012-11-28：比特币产量第一次减半
- 2013-8：德国联邦财政部承认比特币为“记账单位”，和外汇一样可具有结算功能，但不具备充当法定支付手段的功能。
- 2013-11：比特币交易平台火币网上比特币价格达到峰值8000元/个
- 2013-12：五部委联合发布《关于防范比特币风险的通知》，并禁止第三方支付参与比特币交易
- 2014-2：当时全球最大的比特币交易平台Mt.Gox 宣称85万个比特币被盗，随后破产
- 2014-6：美国加州最终通过AB-129法案，允许使用比特币等数字货币在加州进行消费
- 2014-7：戴尔、美国卫星电视巨头Dish Network、电子商务巨头新蛋网等接受比特币支付
- 2014-12：微软接受比特币支付，比尔盖茨认为令人兴奋
- 2015-1：Coinbase成为美国首家持牌比特币交易所
- 2015-6：纽约州金融服务局（NYDFS）宣布BitLicense许可证正式生效，纽约成为美国第一个正式推出定制比特币和数字货币监管的州
- 2015-10：欧盟法院裁定比特币交易免征增值税
- 2015-12：2015年度比特币上涨约120%，成为表现亮眼的投资品
- 2016-1：中国人民银行在京召开数字货币研讨会或推出央行数字货币
- 2016-5：日本首次批准数字货币监管法案，并定义比特币为财产
- 2016-7：比特币产量第二次减半

1.5 比特币的生态


Network achieves consensus on current blockchain
User
control
Wallet
private
public
address
BlockN
Block1
Block0
Exchange
B
$
Merchant
New Block Mined Broadcast
Block Header
Block of Transactions
Unverified Transactions
Miner

第 二 节

比特币地址

01 比特币的地址

02 公钥和私钥

03 地址转换

04 地址交易

2.1 比特币地址

日常生活中，如果我们想要开通一个账户，我们一般都会去银行等第三方中心化系统，办理开户手续。在第三方中心化系统中，账户开通依赖于第三方。

但去中心化的比特币系统中，没有类似银行这样的去中心化系统，很明显不能通过中心化的机构去“申请账户”。

那么，如果我们想在比特币系统中申请一个账户进行交易，我们应该怎么做呢？

2.2 公钥和私钥

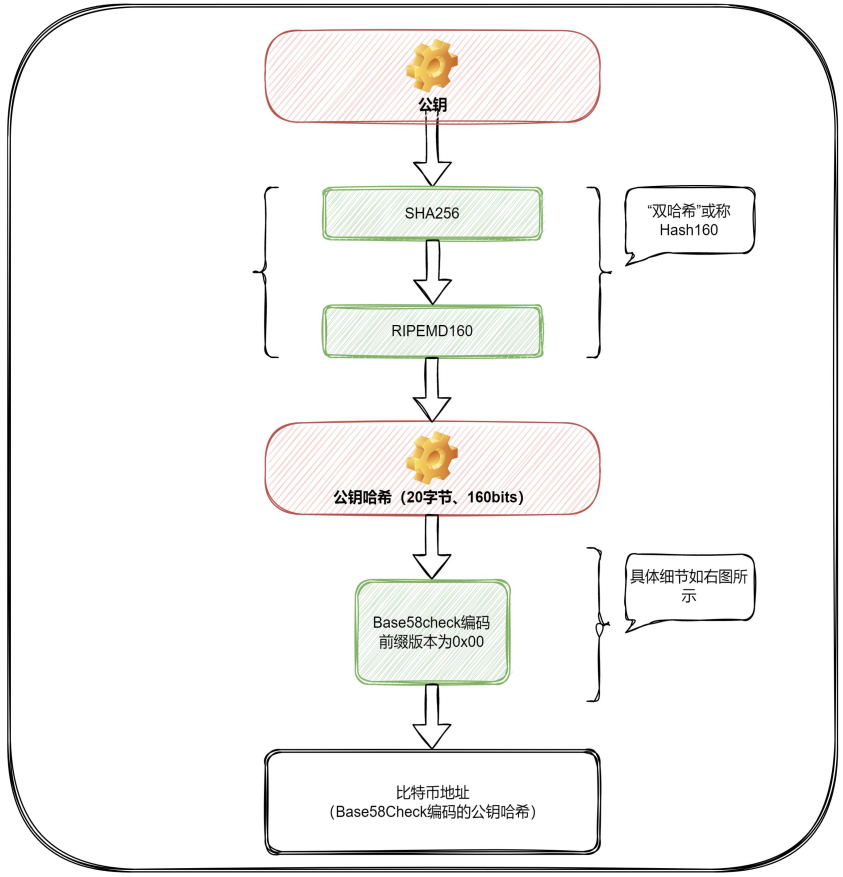
在比特币系统中，申请账户是用户自己来处理的，即自己创建一个公钥-私钥对。一对公私钥就是一个账户。

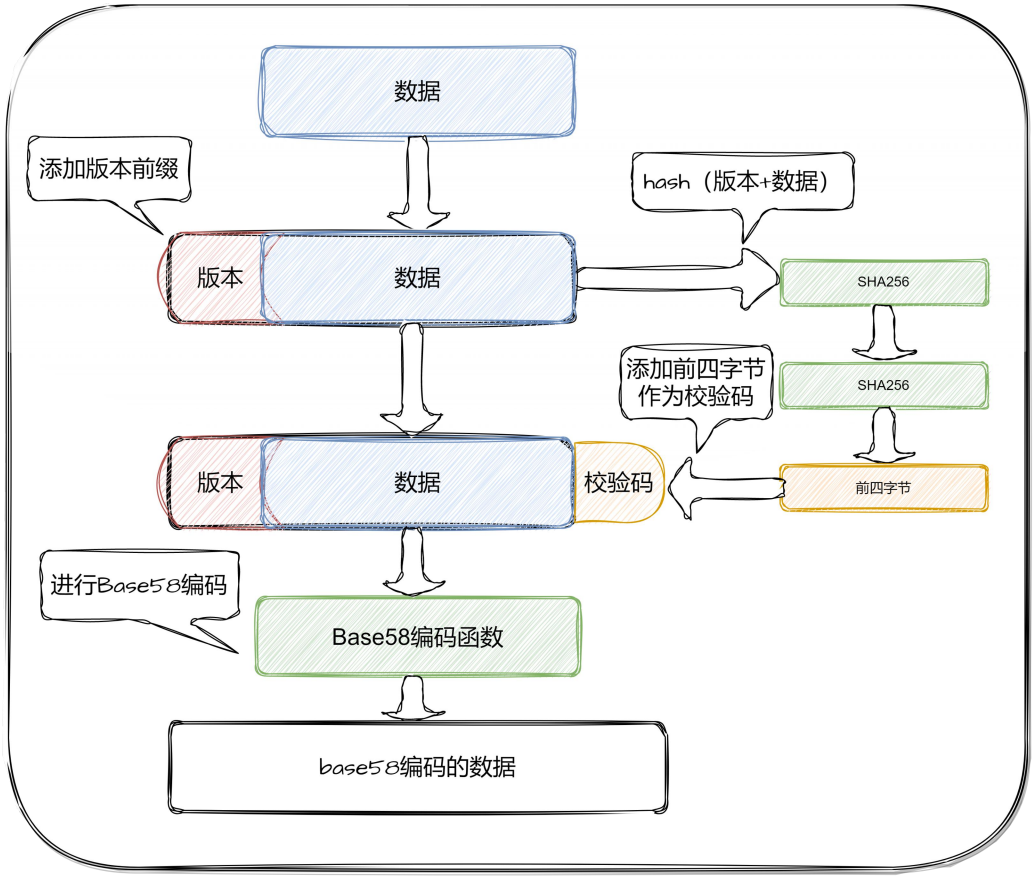
私钥是随机生成的一个数字。比特币中私钥使用椭圆曲线乘法这个单向加密的函数可以生成另一个数字，这个数字就是这个私钥所对应的公钥。

私钥格式案例	1E99423A4ED27608A15A2616A2B0E9E52CED330AC530EDCC32C8FFC6A526AEDD

私钥是用户对自己的比特币地址中的所有资金进行管理和花费必须的凭证，就像是传统银行卡的密码一样，因此私钥一旦泄露给了第三方，就相当于把该地址上的比特币交由他人控制了。此外， 用户最好对私钥进行备份，避免发生意外丢失的情况，因为私钥一旦丢失就无法恢复，该私钥所保护的相应地址上的比特币也就永远的丢失了。

2.3 地址转换

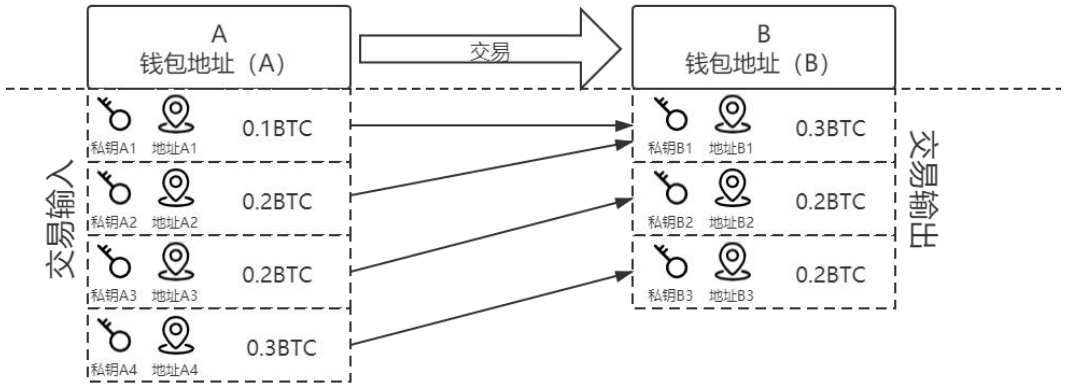




地址案例	16FQCgFD5gBoJvD8kauX9oVoRQhs1NTvb4

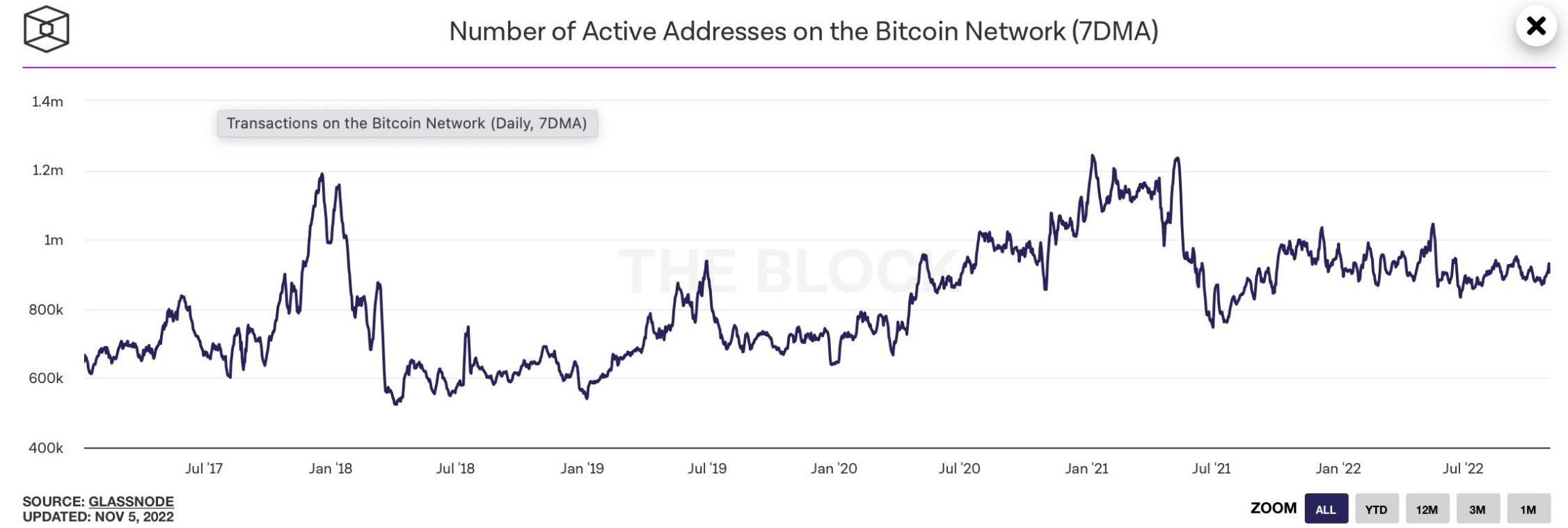
2.4 地址交易

比特币的交易过程中，每一笔交易都包含有一个或是多个的“输入”，同时也包含了一个或是多个的“输出”。并且输入和输出的总额并不一定持平，一般而言输出的总额要略小于输入，两者之间的差额代表了一笔默认的交易费用，交易费用会支付给将该交易计入账簿的矿工。



在目前的比特币系统中，为用户提供了“钱包”软件，为用户管理自己的多组私钥、多个比特币地址以及相应的比特币。通过使用“钱包”，用户可以生成大量的地址以及公私钥对，每个地址都可以存放比特币，只有持有该地址相应的私钥才能够使用存放其中的比特币进行转账、支付等操作。

2.4 地址交易



比特币网络中活跃的地址数量变化图

第 三 节

比特币钱包

01 钱包简介

02 钱包分类

03 钱包功能

04 钱包技术

05 钱包助记词

3.1 钱包简介

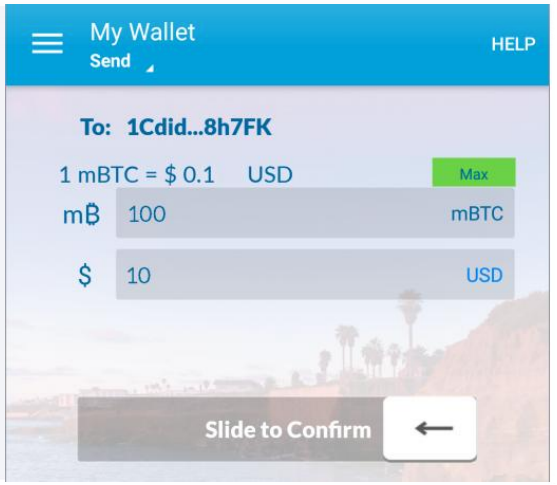
- **钱包**对多对公私钥进行管理，从而实现对地址的管理；
- 使用地址来标识身份更好地保护**隐私**，实现**匿名性**。

3.2 钱包分类

数字货币钱包大体可以分为两大类，冷钱包和热钱包。

冷钱包指不接触互联网，不能通过网络访问的钱包，被通过网络攻击盗取风险更低，但是丢失风险更高，易用性相对较低。如果钱包损坏，恢复会十分困难，因此需要注意钱包备份。

热钱包一般是通过互联网管理的在线钱包，例如用户使用一个账户密码，通过平台管理自己的若干密钥。热钱包使用更方便，但安全性较低。



3.2 钱包分类

基于钱包本身的属性，还可以进一步划分：

硬件钱包

安全硬件的一种应用。是一种为存储和管理比特币地址和私钥而设计的硬件，通过专门的硬件来存储私钥信息。

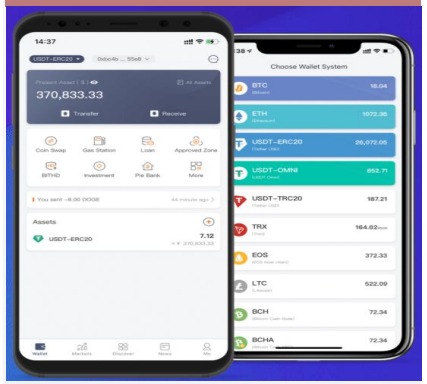
特点：硬件钱包的安全性较高，与网络隔绝，且在硬件本身层面也设置保护。
不过硬件钱包往往价格较高，而且易用性有限。

纸钱包

纸钱包也是一种离线冷钱包，其思路本质上就是“把私钥写在纸上“。

特点：纸钱包的离线性质使得其安全性较好。
纸钱包一般也用作对硬件或其它存储介质的一种备份，存储于保险柜中。

手机钱包



手机钱包是以手机app形式进行密钥管理的钱包。

特点：其与移动结合的特性使得易用性较强，支持面对面使用QR码的快速交易。手机钱包一般由用户名密码登录，并在app内管理私钥。

网络钱包

Web钱包将钱包实现为一种web服务。通过账号密码的方式在线访问和管理钱包，在服务器端备份密钥信息。

特点：因为它依赖于互联网，并且包含了对平台的信任。对服务器的攻击可能导致私钥被盗。因此，一般认为web钱包的安全性相对更低。

桌面钱包

桌面钱包将钱包实现为计算机桌面应用。桌面钱包的环境允许用户对自己的账户和资金有完整的掌握和控制，而不依赖在线服务商。

特点：一些桌面钱包的设计可以利用硬件支持，得到更高的安全性。并且桌面钱包软件一般还可以作为比特币全节点运行，参与挖矿过程等。

3.3 钱包功能

- 钱包的基本功能

存储公私钥

存储和保管用户的私钥，并且使用用户的私钥对交易记录进行签名，以确保交易记录的安全性和不可否认性。

生成地址

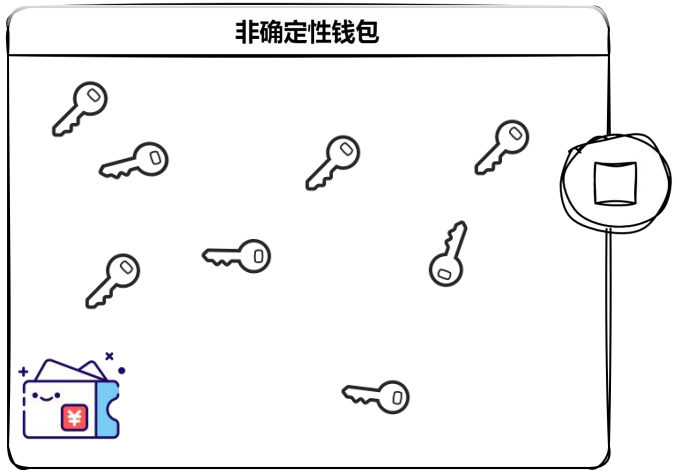
使用用户的私钥生成公钥，并且使用公钥生成用户的地址，利用这些地址来接收其它用户给钱包的比特币转账。

网络广播

将签名后的交易记录通过点对点网络广播给节点。

3.4 钱包技术

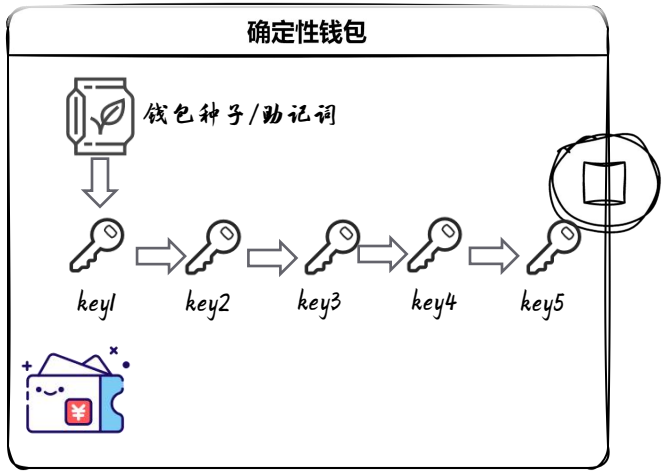
私钥管理是数字货币钱包的核心功能，根据私钥生成方式和私钥的关系，存在非确定性钱包、确定性钱包、分层确定性钱包三类钱包技术。



1、早期的比特币钱包模式，设计简单，难以备份，管理和导入

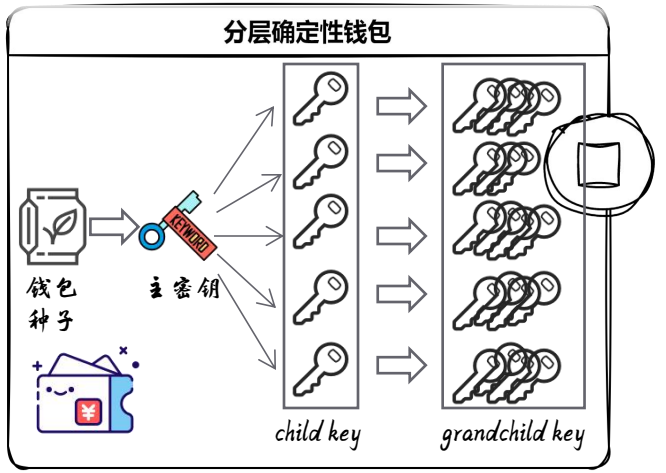
2、私钥是由没有逻辑关系的随机序列生成，因此私钥之间没有逻辑关系

3、多个无关联私钥的每一个都需要进行备份，产生了较大的管理开销



1、为了避免非确定性钱包备份开销问题，通过引入钱包种子（助记词）的方式，生成新的私钥序列。

2、只需要备份种子就可以保证恢复所有密钥，备份开销更小，恢复也十分便捷。



1、分层确定性钱包以树状的方式生成新的私钥。在备份和恢复的时候仍然只需要保存种子

2、具有主公钥属性，不仅可以用主私钥（种子直接生成）生成之后的所有私钥序列，还可以用对应的主公钥生成之后钱包中所有地址序列，并保证地址和生成的私钥对应。

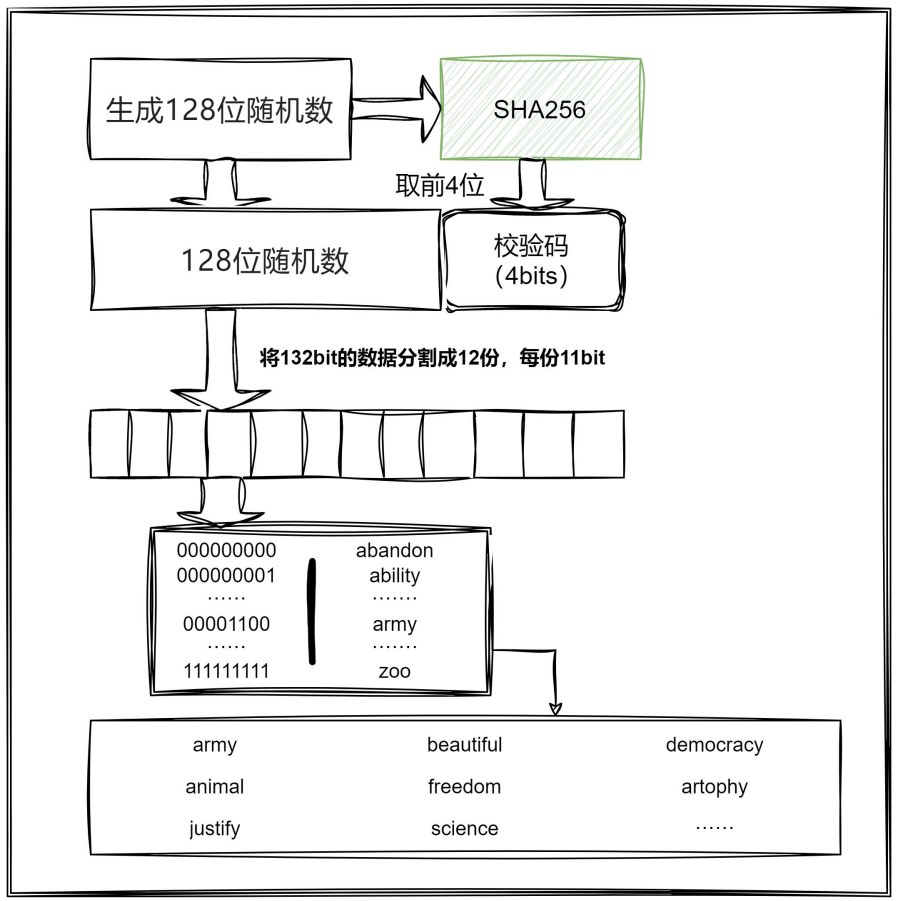
3.5 助记词

基于安全考虑，钱包私钥是一个64位的随机字符串，例如下面这串数字：

0fcdc0ad9a0ea09e839767d6e8d90fedbf8f32d7aebd349893695daa4f51599e

然而这样的种子/主密钥使用人脑记忆难度极大。此时就希望使用一些含有意义的词语组合来替代字符串，方便记忆和记录，这就是助记词。助记词的生成过程如右图所示

Lane 1	1、生成128位随机数（BIP29中称为熵、Entropy、ENT） 2、对随机数做SHA256，取前4位为校验码
Lane 2	3、将1、2步骤中得到的结果拼接成一个132位的字符 4、将132位的数按顺序平均分成12份，每份11个字符
Lane 3	5、将11位字符转化为十进制数字，并查询BIP39中单词表，按顺序找到对应的单词 6、这些查到的单词串就是一份助记词



3.5 助记词

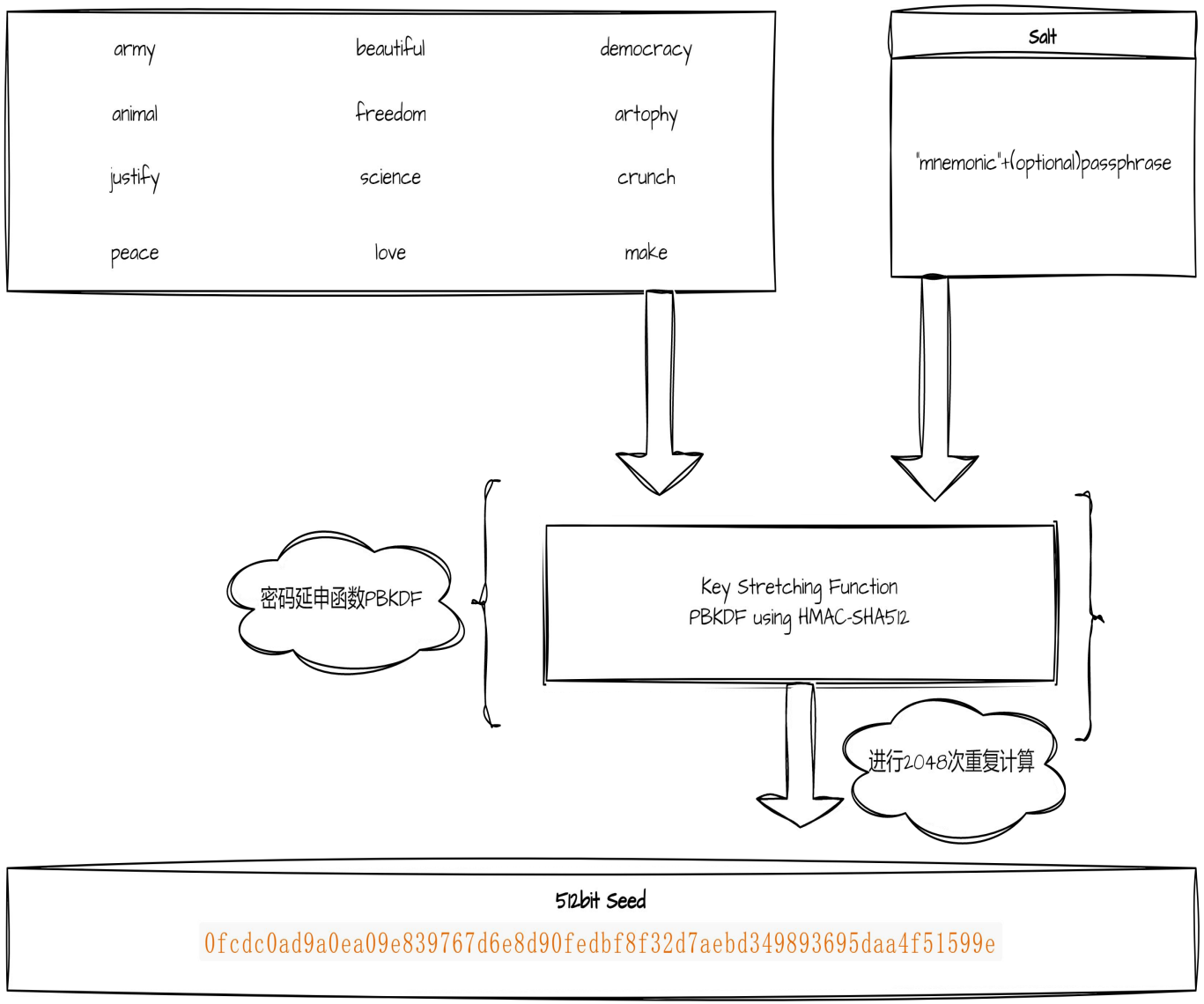
上图举例的是12词的助记词生成说明，我们在生成助记词时候，还支持15、18、21、24词的助记词，随机数、校验码及分割长度如下表格

助记词长度	熵	校验码	总长度	分割长度
12	128	4	132	11
15	160	5	165	11
18	192	6	198	11
21	224	7	231	11
24	256	8	264	11

3.5 助记词

助记词需要如何转换成钱包呢？这里种子成了关键的一环。为了安全性考虑，生成种子这一步可以设置一层密码，助记词+助记词密码进行拉升处理，得到一个512位（64字节）的种子。

Lane 1	1、助记词作为密码（Password） 2、"mnemonic" + 助记词密码 作为盐（Salt）
Lane 2	3、HMAC-SHA512 作为PBKDF2的随机函数（PBKDF2 Password-Based Key Derivation Function 2 是常用的拉伸函数算法中的一种）（HMAC） 4、进行2048次重复计算
Lane 3	5、生成一个512位（64字节）的种子（dkLen） 种子 DK = PBKDF2(HMAC, Password, Salt, c, dkLen)，如右图所示



3.5 助记词

北京大学 PEKING UNIVERSITY

Mnemonic

You can enter an existing BIP39 mnemonic, or generate a new random one. Typing your own twelve words will probably not work how you expect, since the words require a particular structure (the last word is a checksum)

For more info see the BIP39 spec

Generate a random 12 word mnemonic, or enter your own below.

BIP39 Mnemonic

army van defense carry jealous true garbage claim echo media make crunch

BIP39 Passphrase (optional)

BIP39 Seed

5b56c417303faa3fcba7e57400e120a0ca83ec5a4fc9ffba757fbe63fbd77a89a1a3be4c6719
6f57c39a88b76373733891bfaba16ed27a813ceed498804c0570

Coin

Bitcoin

BIP32 Root Key

xprv9s21ZrQH143K3t4UZrNgeA3w861fwjYLaGwmPtQyPMmzshV2owVpfBSd2Q7YsHZ9j6
i6ddYjb5PLtUdMZn8LhvuCVhGcQntq5rn7JVMqnie

第 四 节

比特币交易

01 交易描述

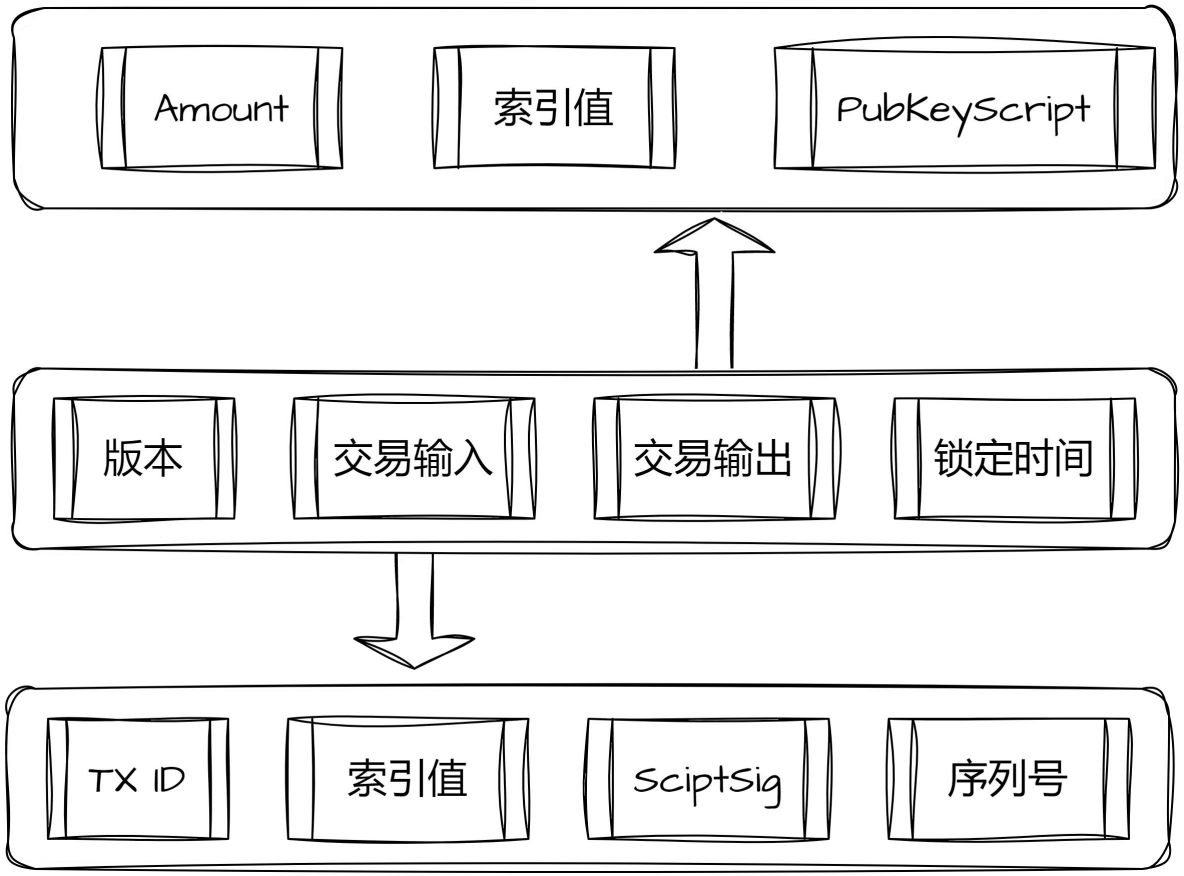
02 交易构成-UTXO

03 交易形式

04 交易过程示例

05 交易脚本

4.1 交易描述

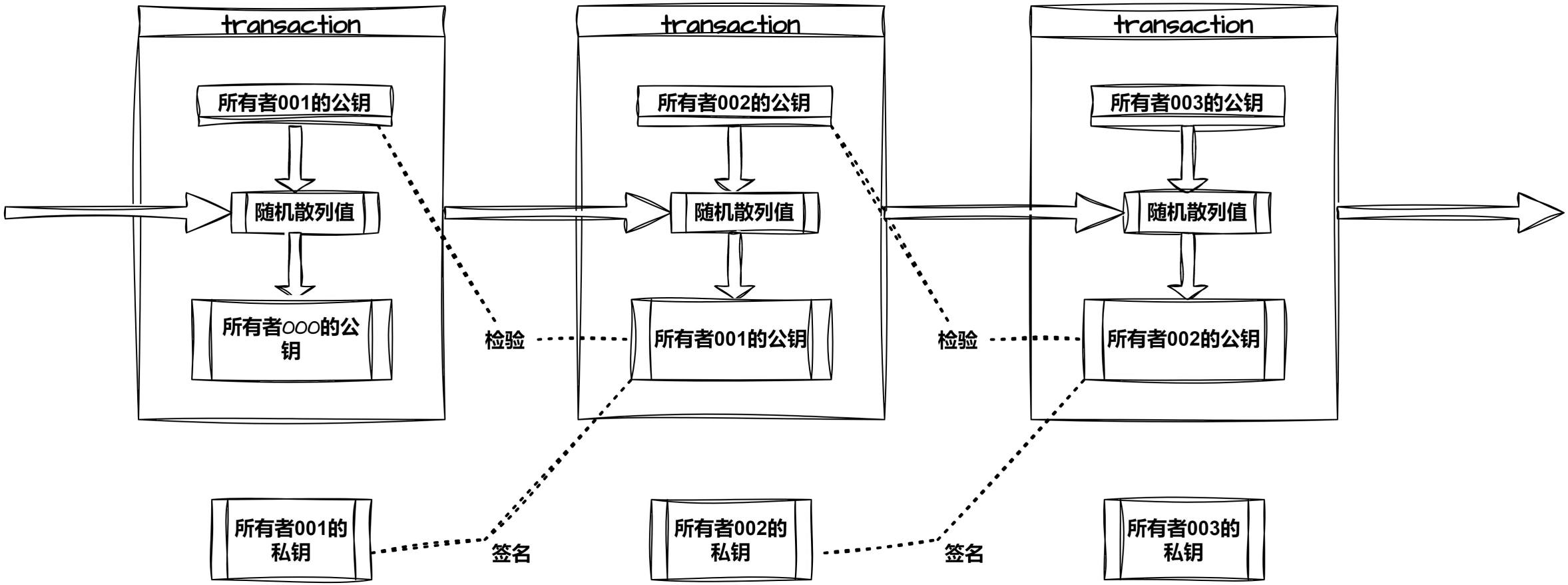


如图所示，比特币交易的主要构成部分，包括版本信息、交易输入、交易输出和锁定时间。

每一笔比特币交易中具有一个四字节的交易版本号，它告知比特币节点和矿工应该使用哪一套规则用来验证这笔交易，使得开发者在为未来的交易创建新的规则时可以不验证之前产生的交易；

每一笔交易中至少包含一个交易输入和一个交易输出，每个交易输入会花费上一个交易输出产生的比特币，每个交易输出都作为UTXO直到被作为交易输入花费掉。

4.1 交易描述



- 比特币中，存储的只有交易信息使用**收款人的公钥**对交易内容进行加密，这样就只有收款人才能解密

具体内容： 消息中包发送者的公钥，使用**发送者的私钥**进行签名，这样就能确认该交易是属于发送者的，并且该消息确实是发送者所发送的

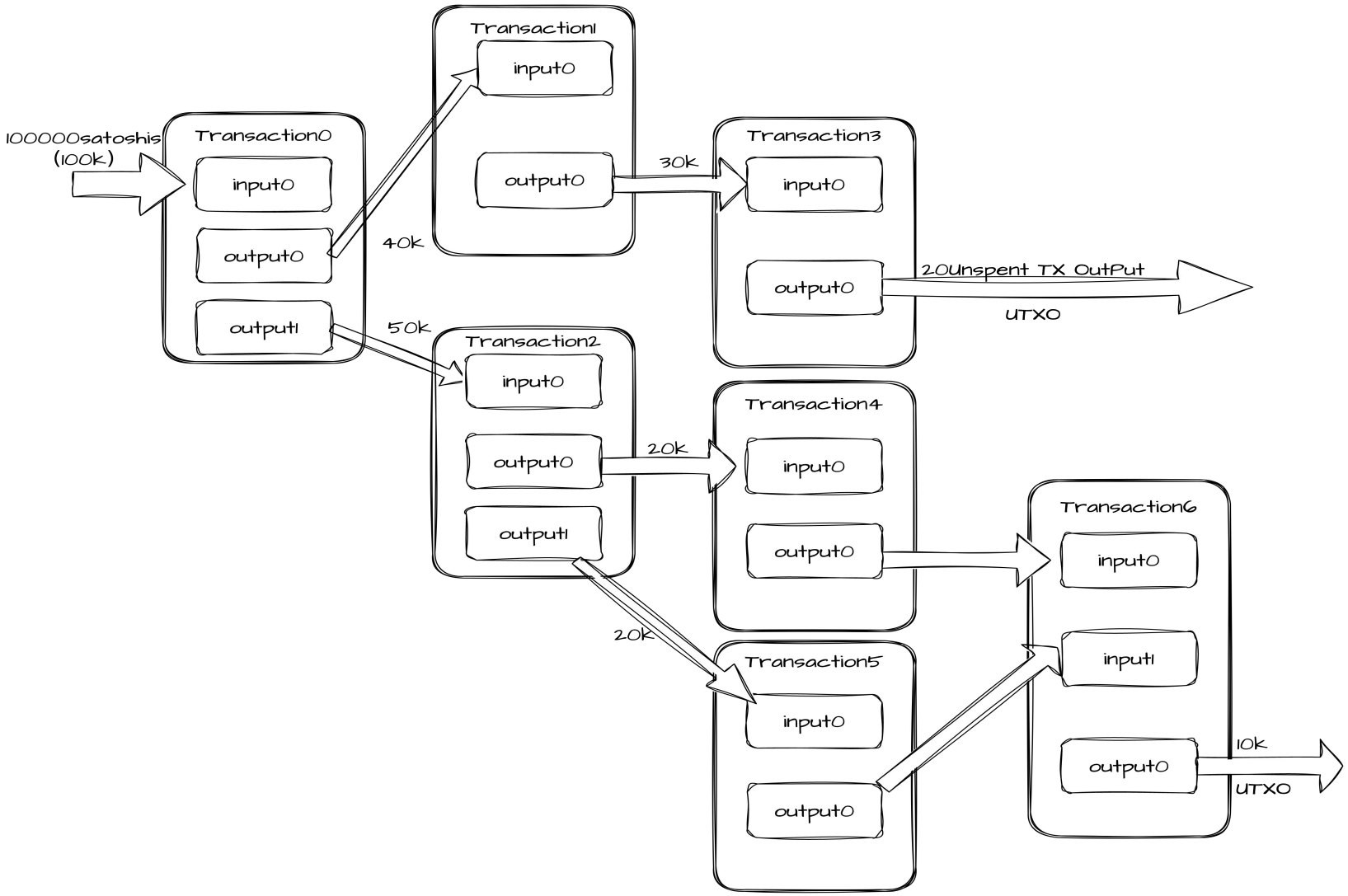
4.1 交易描述

组合和分隔

- 每次交易时，只能选择原来的交易，来源
- 每笔交易可以有**多个输入和输出**
- 中间的差值作为交易费，或者返回给发送者

Input和output

- Input中包含前一次交易的信息
- Output中包本次交易的接收者信息



Triple-Entry Bookkeeping (Transaction-to-transation) As used by Bitcoin

4.2 交易构成-UTXO

比特币交易的基本单位是未花费的交易输出，简称UTXO（Unspent Transaction Output）。比特币币值最小单位是聪，类似于人民币中的分，1聪为0.00000001个比特币，UTXO是一定数量的聪。

- 被交易消耗的UTXO称为交易输入。

尺寸	字段	说明
32个字节	交易	指向交易包含的被花费的UTXO的哈希指针
4个字节	输出索引	被花费的UTXO的索引号，第一个是0
1–9个字节（可变整数）	解锁脚本尺寸	用字节表示的后面的解锁脚本长度
变长	解锁脚本	一个达到UTXO锁定脚本中的条件的脚本
4个字节	序列号	目前未被使用的交易替换功能，设成0xFFFFFFFF

- 由交易创建的UTXO称为交易输出。

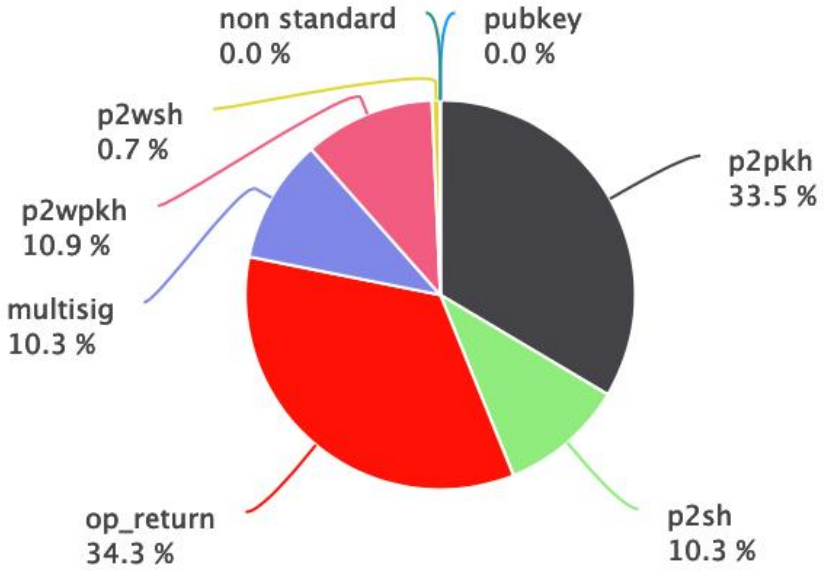
尺寸	字段	说明
8个字节	总量	用聪表示的比特币值（10-8比特币）
1–9个字节（可变整数）	锁定脚本尺寸	用字节表示的后面的锁定脚本长度
变长	锁定脚本	一个定义了支付输出所需条件的脚本

4.2 交易构成-UTXO

北京大学 PEKING UNIVERSITY

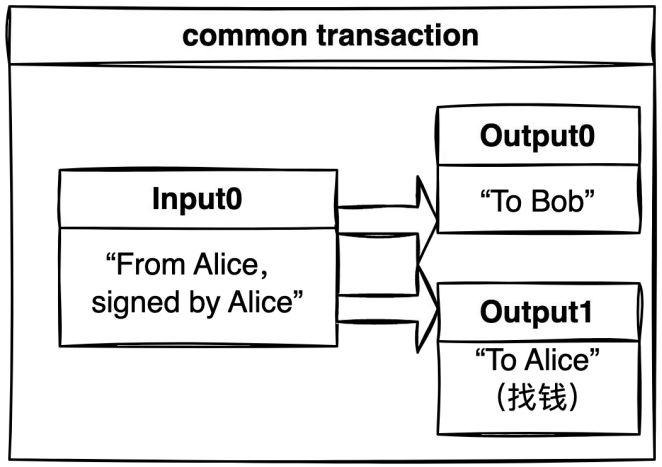
Transaction unspent outputs (UTXO)

PUBKEY	48 081
P2PKH	50 636 443
P2SH	15 598 968
MULTISIG	438 042
P2WPKH	16 395 243
P2WSH	1 007 057
NON STANDARD	9 149
OP_RETURN	51 768 629
OP_RETURN_NON_STANDARD	36 807
Total	136 121 606
Total spendable	84 316 170

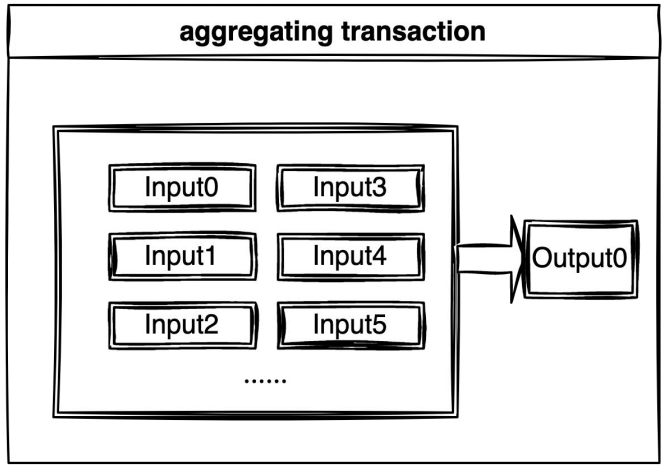


交易构成

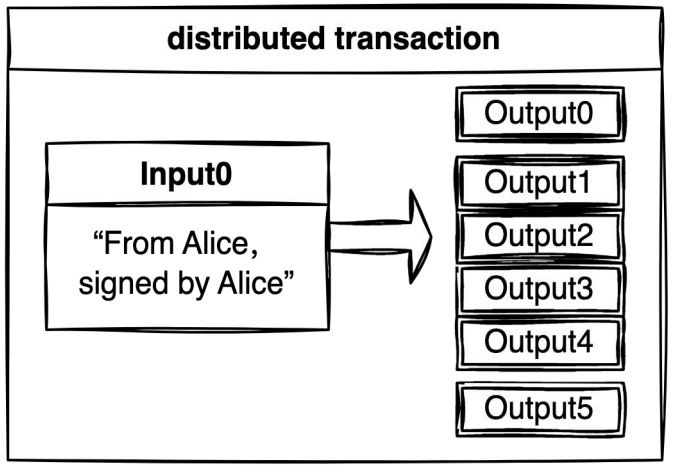
4.3 比特币交易-交易形式



最常见的交易形式是从一个地址到另一个地址的简单支付，这种交易也常常包含给支付者的“找零”。
一般交易有一个输入和两个输出



另一种常见的的交易形式是集合多个输入到一个输出的模式。
类似于我们现实生活中将很多硬币和纸币零钱兑换为一个等额大钞。
像这样的交易有时由钱包应用产生来清理许多在支付过程收到的小数额的找零



最后，另一种在比特币账簿中常见的交易形式是将一个输入分配给多个输出，即多个接收者的交易。
这类交易有时被商业实体分配资金

4.3 交易过程示例

- 宋同学最近想要学习区块链有关内容。于是他想买一本区块链相关书籍。首先去京东以及淘宝等互联网平台上看到了有关信息，然后又去校内二手书平台查看。书店店长老姜因为较为熟悉区块链，所以建议他使用比特币来向自己购买这本书。

宋同学还没有使用过比特币，他应该怎样完成这笔交易呢？

4.3 交易过程

宋同学首先在自己手机上下载一个比特币客户端，然后比特币客户端自动生成一个钱包，随机生成一个私钥和对应的比特币地址。同时，姜老板创建一个地址（生成公钥和私钥对）由于接收本次交易的比特币，并且把公钥给宋同学。

01

图4.3 宋同学在申请地址

宋同学给自己同学小刘借了1BTC，随后，宋同学利用他的私钥对前一次交易（比特币来源小刘）和下一位所有者姜老板的信息签署一个数字签名，并把这个签名附加在这枚货币的末尾，制作成交易

02

随后，宋同学将交易广播至全网，每个节点都将受到的交易信息纳入一个区块中

要点: 对于姜老板而言，该枚比特币会即时显示在比特币钱包中，但直到区块确认成功之后才可用。目前一笔比特币从支付到最终确认成功，需要6个区块确认之后才能真正确认到账。

03

4.3 交易过程

04

每个节点通过解一道数学难题，从而去获得创建新区块权利，并争取得到比特币的奖励（新比特币会在次过程中产生）

要点：节点反复尝试随机数，将该随机数、前一个区块的哈希值等信息，送入SHA256算法计算出散列值，该散列值需要满足一定的条件。答案并不唯一。

05

当一个节点找到解时，它就向全网广播该区块记录的所有盖时间戳交易，并由其它节点核对

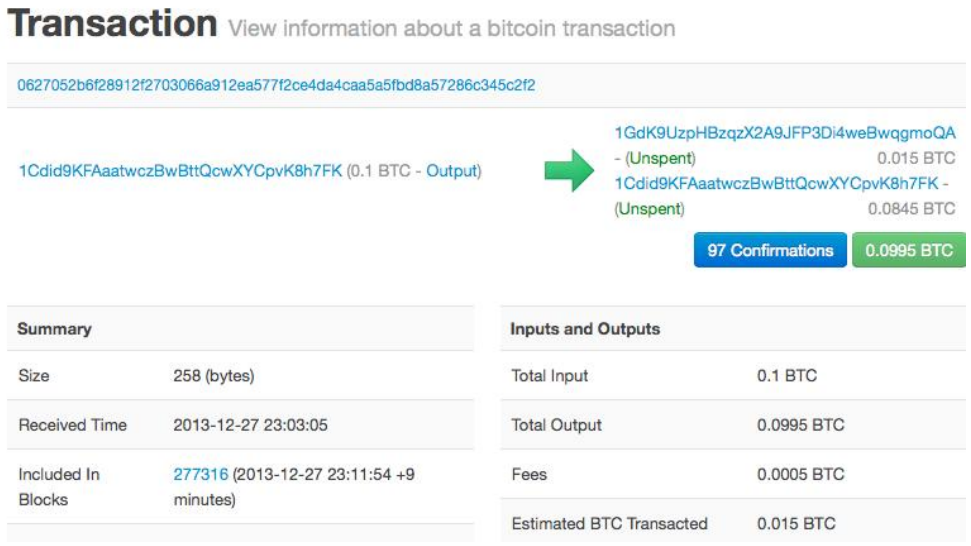
要点：时间戳用来证明特定区块必然于某个特定的时间是存在的。比特币网络采取从5个以上节点获取时间，然后取中间值的方式作为时间戳。

06

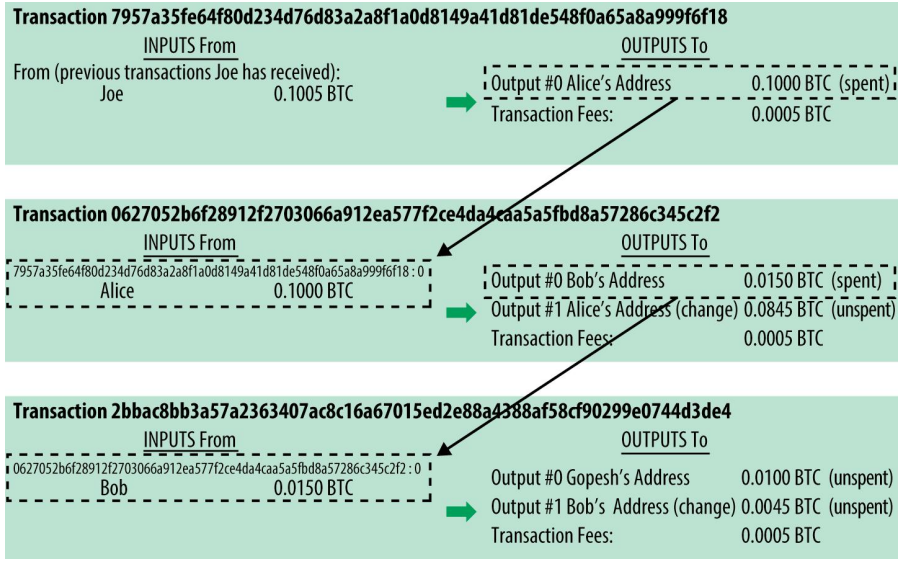
全网其它节点核对该区块记账的正确性，没有错误之后他们将在该合法区块之后竞争下一个区块，这样就形成了一个合法记账的区块。

要点：每个区块的创建时间大约在10分钟。根据全网算力，会自动调整每个区块的生成难度。

4.4 交易示例

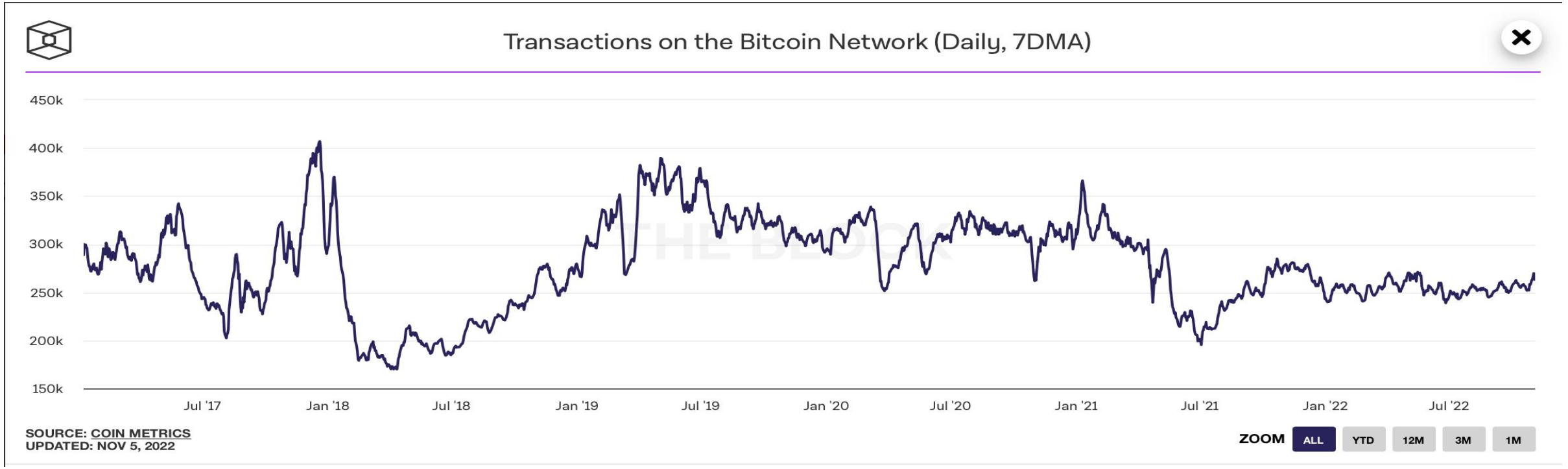


交易明细



交易上链

4.4 交易示例



比特币网络每日交易数量变化

4.5 交易脚本

脚本是保障交易完成，检查交易是否合法的核心机制，当所依附的交易发生时被触发，通过脚本机制而非固定的交易过程，比特币实现了一定的可扩展性。比特币脚本语言是一种非图灵完备的语言，类似Forth语言。

一般每个交易都会包括两个脚本：负责输入的（scriptSight）解锁脚本和负责输出的（scriptPubkey）锁定脚本。

解锁脚本-负责输入

输入脚本可以用来证明自己满足交易输出脚本的锁定条件，即对某个交易的输出的拥有权

锁定脚本-负责输出

输出脚本一般由付款方对交易设置锁定，用来对能动用这笔交易的输出的对象进行权限控制，例如限制必须是某个共钥的拥有者才能花费这笔交易。

4.5 交易脚本

输出脚本目前支持两种类型：

P2PKH（Pay-To-Public-Key-Hash）

允许用户将比特币发送到一个或多个典型的比特币地址上，前导字节一般为0x00

P2SH，Pay-To-Script-Hash

支付者创建一个输出脚本。里面包含另一个脚本（认领脚本）的哈希，一般用于需要多人签名的场景，前导字节一般为0x05

以 P2PKH 为例，输出脚本的格式为：

```
scriptPubKey: OP_DUP OP_HASH160 <pubKeyHash> OP_EQUALVERIFY OP_CHECKSIG
```

在P2PKH中，资金的转移条件为锁定脚本，是由付款方写到锁定脚本中的，如果要转移资金，需要持有者提供公钥和私钥签名，构成交易输入中的解锁脚本。在P2PKH方式下，资金转移的形式比较固定，缺乏灵活性，无法支持较为复杂的需求。

4.5 交易脚本-P2SH

P2SH(Pay-to-ScriptHash)，即向脚本哈希支付。

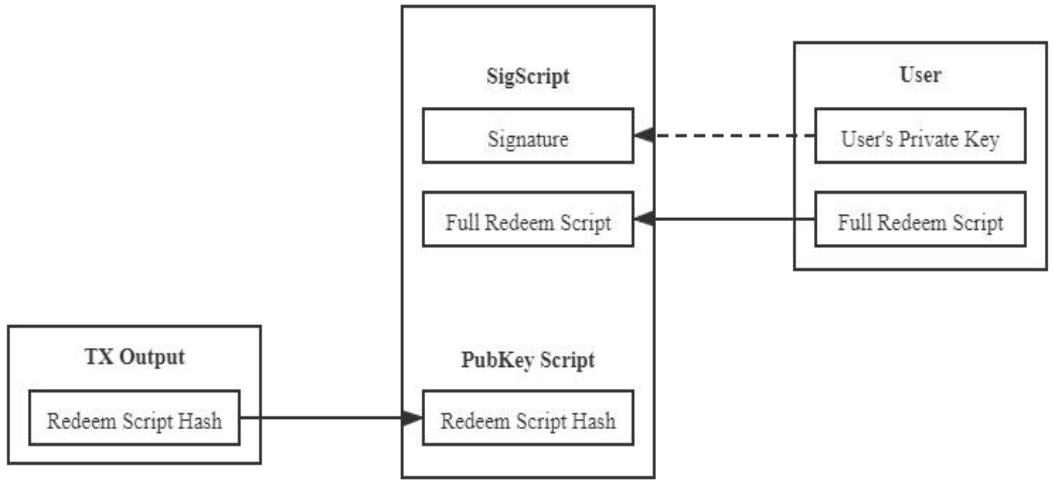
在P2SH中，资金的转移条件是一个赎回脚本(redeem script)。

P2SH交易过程如下所示：

1、收款方先构建一个赎回脚本，其中的内容即资金转移条件。

2、收款方计算赎回脚本的哈希值并把这个哈希值发送给付款方，此哈希值是一个P2SH类型的比特币地址。

3、付款方构建交易，但交易输出不再包含锁定脚本，而是被赎回脚本的哈希值所取代。付款方并不清楚也不关注具体的资金转移条件。



比特币P2SH

P2SH多用于N-M多重签名，即收款方可以赎回脚本中添加适当的转移条件，就可以把脚本哈希变成一个N重签名地址，在预定的N个公钥中，给出其中M个相应的签名就能通过验证并花费资金。

第 五 节
比特币网络

01 节点类型
02 网络类型
03 通信类型

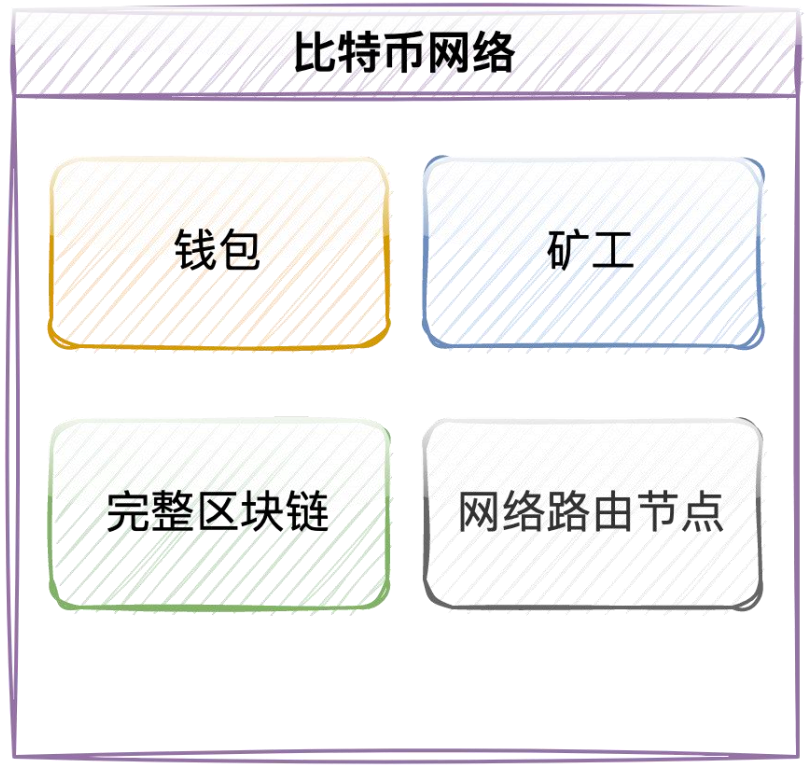
5.1 比特币网络- 节点类型

- 比特币是一种点对点的电子现金系统，这里的点对点实际上就是节点对节点。转账交易发生后，由转账的节点向外进行广播，最终扩散至全网络。尽管比特币P2P网络中的各个节点相互对等，但是根据所提供的功能不同，各节点可能具有不同的分工。每个比特币节点都是路由、区块链数据库、挖矿、钱包服务的功能集合。

节点类型

依照节点承载的功能类型进行划分

依照节点承载的功能类型进行划分：钱包、矿工、完整区块链、网络路由节点。



5.1 比特币网络- 节点类型

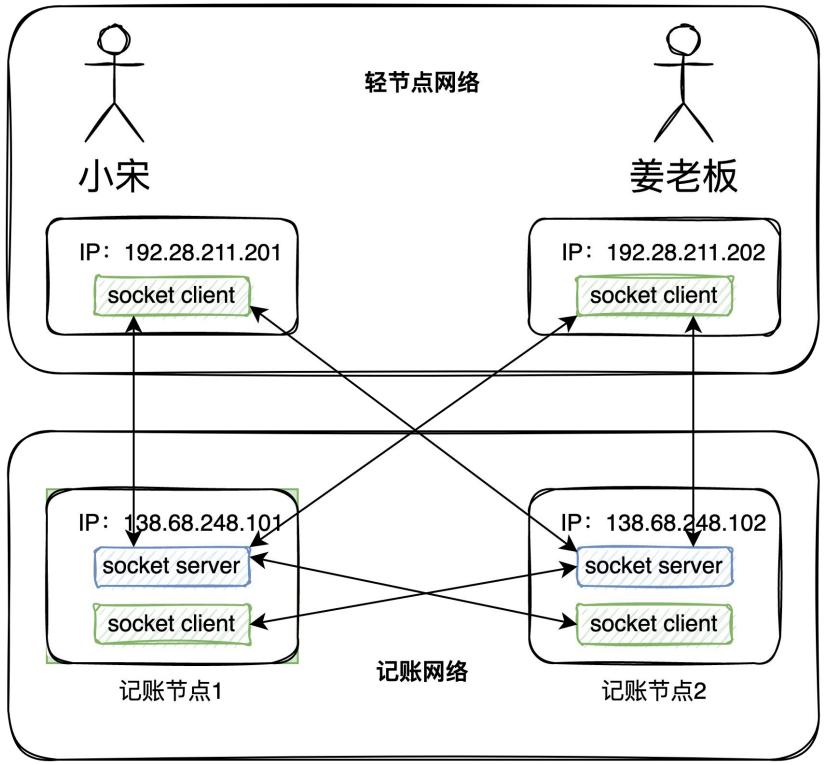
北京大学 PEKING UNIVERSITY

依照节点的功能进行划分

核心客户端节点	包含钱包、矿工、完整区块存储、网络路由四种功能。
全节点	拥有完整的区块链数据，具有网络路由功能
独立矿工节点	拥有完整区块链数据，具有路由功能和挖矿能力，能不依赖其他节点的算力单独进行挖矿
轻量级钱包(SPV)	包含钱包与路由转发功能

5.1 比特币网络- 节点类型

每个节点都参与验证并传播交易及区块信息，发现并维持与对等节点的连接。另外还有一些节点只保留了区块链的一部分，它们通过一种名为“简易支付验证（SPV）”的方式来完成交易验证。这样的节点被称为“SPV节点”，又叫“轻量级节点”。



因此，节点又可以分为“全节点”和“轻节点”。全节点就是拥有全网所有交易数据的节点，轻节点就是只拥有和自己相关的交易数据节点。

5.1 比特币网络- 节点类型

依照节点保存区块数据内容和是否能独立完成交易验证划分

全节点的特征

•每个节点都有一个完整的账本副本，因此所有交易数据公开透明，系统中的人都可以看到。

•每个节点的权利是一样的，任意节点被摧毁，都不会影响到整个系统的安全，也不会造成数据丢失。

•每个节点的账本数据是完全一样的，也就意味着，单个节点的数据篡改是没有任何意义的。

轻节点的特征

•每个节点只保存区块链数据的部分信息（如：区块头）不能独立地进行区块和交易的验证。

•每个节点通过简易支付验证（Simplified Payment Verification，简称SPV）方式向其他节点请求数据来完成支付验证。

5.1 比特币网络- 节点类型

全节点	轻节点
一直在线	不是一直在线
在本地硬盘上维护完整区块链信息	不保存整个区块链，只需要保存每隔区块块头
在内存中维护UTXO集合，以便于快速检验交易合法性	不保存全部交易，只保存和自己有关的交易
监听比特币网络中交易内容，验证每个交易合法性	无法验证大多数交易合法性，只能检验和自己相关的交易合法性
决定哪些交易会打包到区块中	无法检测网上发布的区块正确性
监听其他矿工挖出的区块，验证其合法性	可以验证挖矿难度
挖矿： 1. 决定沿着哪条链挖下去。 2. 当出现等长分叉，选择哪一个分叉	只能检测哪个是最长链，不知道哪个是最长合法链

5.1 比特币网络- 节点类型

比特币网络全球节点实时分布

5.2 比特币网络- 网络类型

比特币系统的P2P网络

比特币网络协议允许全节点（对等节点）协作地维护一个对等网络，用于路由区块和交易。对等网络是指位于同一网络中的每台计算机都彼此对等，各个节点共同提供网络服务，不存在任何“特殊”节点。每个网络节点以“扁平（flat）”的拓扑结构相互连通。在对等网络中不存在任何服务端、中央化的服务、以及层级结构。

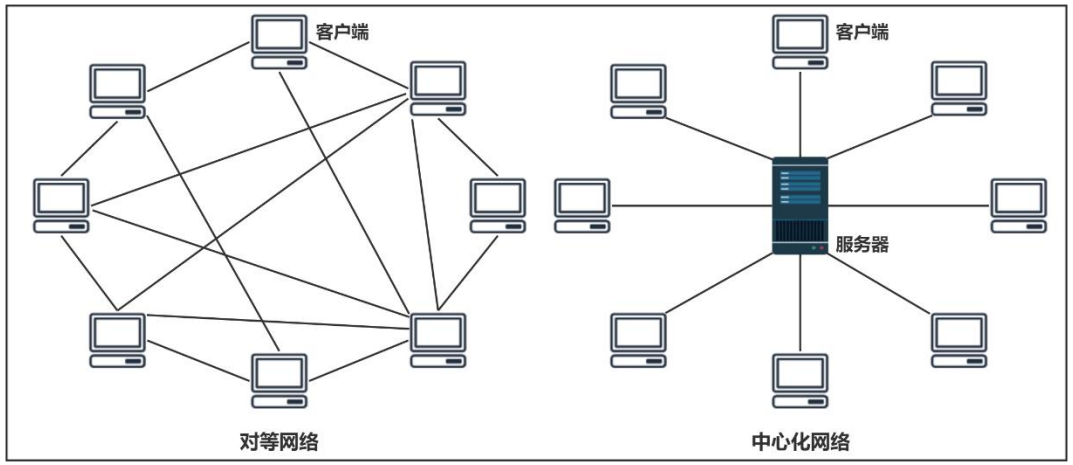


图5.2 对等网络和中心化网络

可拓展性	去中心化	容错性高	最终一致性
节点可以随意的添加和删除，新的节点可以随时接入网络中	对等网络中不会严格区分客户端和服务器，每个节点同时作为客户端和服务器，接入网络的节点都能与网络中的其他节点路由信息	整个网络的容错性高，不会因为其中任何节点的宕机而影响网络中的信息传播	在任意时刻加入对等网络，其都会达到与其他节点相同的数据状态，能够实现最终一致性

5.2 比特币网络- 网络类型

比特币网络一致性维持：gossip协议

- 新的交易向全网进行广播；
- **每一个节点都将收到的交易信息纳入一个区块中**；
- 每个节点都尝试在自己的区块中找到一个具有足够难度的工作量证明；
- 当一个节点找到了一个工作量证明，它就向全网进行广播；
- 当且仅当包含在该区块中的所有交易都是有效的且之前未存在过的，其他节点才认同该区块的有效性；
- 其他节点表示他们接受该区块，而表示接受的方法，则是在跟随该区块的末尾，制造新的区块以延长该链条，而将被接受区块的随机散列值视为先于新区快的随机散列值。

5.3 比特币网络- 通信类型

北京大学 PEKING UNIVERSITY

节点发现

当新的网络节点启动后，为了能够参与协同运作，它必须发现网络中的其他比特币节点。新的网络节点必须发现至少一 个网络中存在的节点并建立连接。

节点离开

退出节点,向确定接收其键值的邻居节点发送离开消息并接收所述邻居节点的确认消息;所述退出节点向所述邻居节点转移键值,并向其他节点发送离开消息;所述键值转移完成后,所述退出节点退出P2P网络。

5.3 比特币网络- 通信类型

北京大学 PEKING UNIVERSITY

传播交易

当前所有者将交易单广播至全网，每个节点会将数笔未验证的交易Hash值收集到区块中，每个区块可以包含数百笔或上千笔交易。最快完成POW的节点，会将自己的区块传播给其他节点。

传播区块

新发现的区块在网络中传播时，每个节点在将其继续发送到它的对等节点前，会进行一系列的测试工作，以验证其有效性。结果就是，只有有效的区块才会被传播到网络当中。独立验证也保证了诚实矿工挖出的新区块能被区块链接纳，并赢得奖励。

第六节
比特币区块

01 创世区块

02 区块链结构

03 高度和深度

04 区块链分叉

05 区块链压缩和剪裁

6.1 比特币区块-创世区块

北京时间2009年1月4日（当地时间1月3日），一个名为“中本聪”的极客在位于芬兰赫尔辛基的一个小型服务器上，亲手创建了第一个区块，即比特币创世区块，并获得了第一笔50枚比特币的奖励。就在这一天，第一枚比特币诞生了。当时，中本聪将当天泰晤士报的头版“总理已经濒临对银行第二次救助的边缘”记录在了创世区块之中。这不但清晰地展示着比特币的诞生时间，还表达着对旧体系的嘲讽。


THE TIMES

£1.50

Eat Out from £5

More than 900 great restaurants, including four Gordon Ramsay favourites from £15

Israel prepares to send tanks and troops into Gaza

Chancellor on brink of second bailout for banks

Billions may be needed as lending squeeze tightens

99p

Michael Sheen Frost, Nixon and me

Working mums So that's how she does it

Detox in style The best spas on the planet

Salmon Rushdie I Won't Marry Again

Giant Killing? Guide to the FA Cup Third Round

6.1 比特币区块-创世区块

北京大学 PEKING UNIVERSITY

Bitcoin block 0 mined by Anonymus

Time	2009-01-03 18:15:05
Transactions	1
Size	285 bytes
Stripped size	285 bytes
Weight	1 140
Block difficulty	2 536
Network difficulty	1
Version	0x01
Bits	0x1d00ffff
Nonce	0x7c2bac1d
Block reward	50.00000000 BTC
Fee reward	0 BTC

Coinbase message

EThe Times 03/Jan/2009 Chancellor on brink of second bailout for banks

Block	000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f
Previous block	0000000000000000000000000000000000000000000000000000000000000000
Next block	00000000839a8e6886ab5951d76f411475428afc90947ee320161bbf18eb6048
Merkle root	4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b

Coinbase hex

```
04ffff001d0104455468652054696d65732030332f4a616e2f32303039204368616e63656c6c6f72206f6e206272696e6b206f662
07365636f6e64206261696c6f757420666f722062616e6b73
```

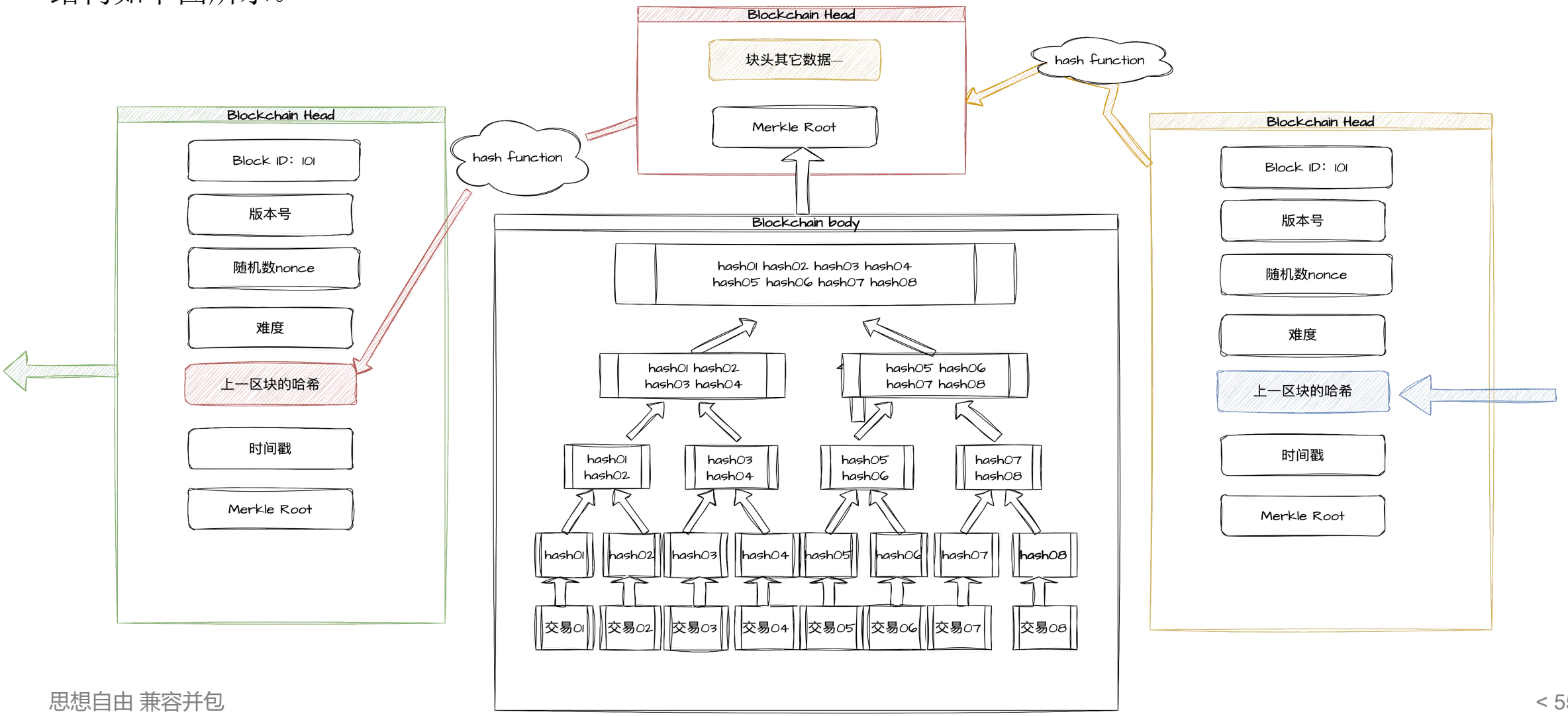
Header

```
010000000000000000000000000000000000000000000000000000000000000000000000
003ba3edfd7a7b12b27ac72c3e67768f617fc81bc3888a51323a9fb8aa4b1e5e4a29ab
5f49ffff001d1dac2b7c01
```

创世区块

6.2 比特币区块-区块链结构

比特币的区块由两部分构成：包含元数据的区块头和紧跟其后的包含一长串交易列表的区块体。区块的结构如下图所示。



6.2 比特币区块-区块链结构

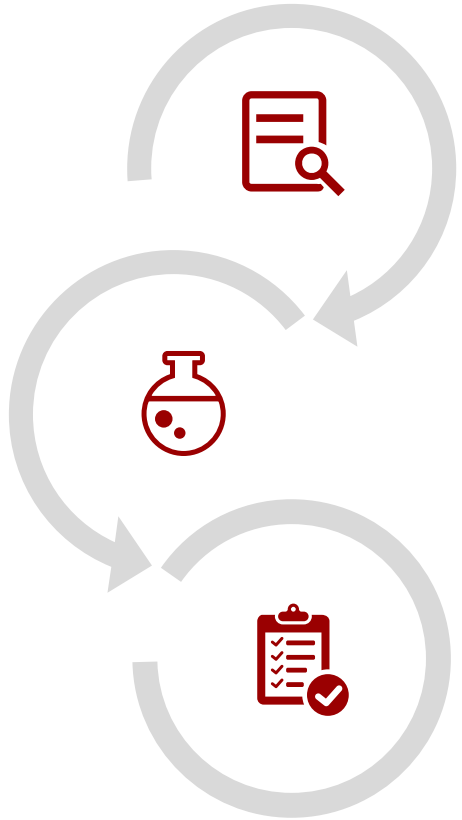
- 区块头由三组区块元数据组成。

父区块哈希

首先是一组引用父区块哈希值的数据，这组元数据用于将该区块与区块链中前一区块相连接。

元数据

第二组元数据，即难度、时间戳和nonce，与挖矿竞争相关。



Merkle树根

第三组元数据是Merkle树根。主要用来简化交易的结构。

6.3 比特币区块-区块高度和深度

区块的深度和高度不同，通常是指某个区块之后产生了多少个区块，即已经被多少个区块验证过。如**SPV**节点在验证交易时，如果包含一个交易的区块，已经被**6**个区块校验过，即可认为不会被篡改和在该块之前产生分叉，从而判断交易是有效的。

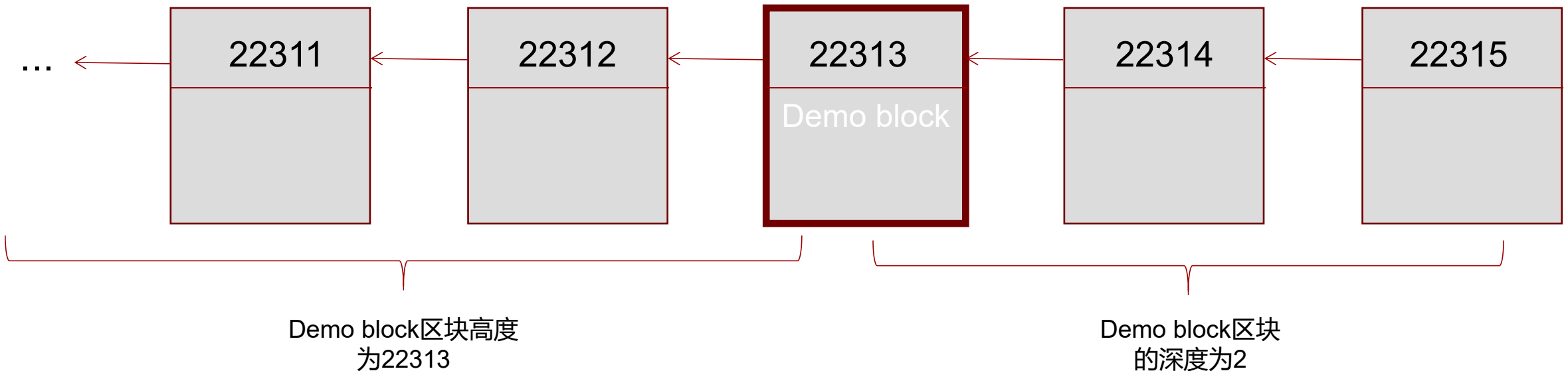


图6.3.2 区块的高度和深度示例

6.3 区块一致性

为了保证比特币区块链数据的一致性，我们需要满足两个条件：

1、创世区块数据的一致性

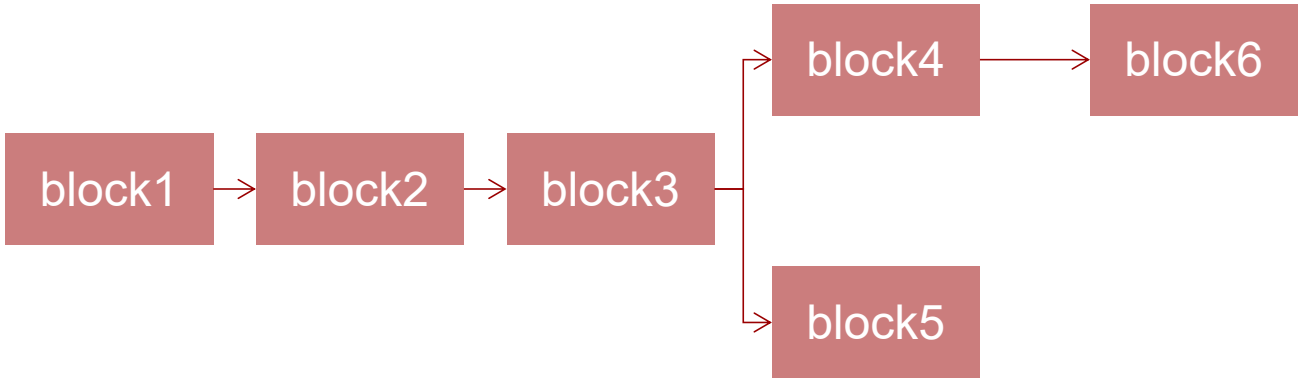
2、新区块数据的一致性

由数学归纳法可知，如果能满足这两个条件，即可满足所有区块链数据的一致性。而前者我们可以依靠代码对创世区块的统一记录来完成，后者则需要设计一套协议，使得在新交易不断出现的场景下也能保证新区块数据的一致性。

6.4 区块链分叉

在比特币中，通过调整难度大约每10分钟就产生一个新区块。一旦某个区块计算出下一个合法的区块，便会将该区块向全网广播，其他矿工会放弃当前的区块，在新区块之后重新尝试计算下一个区块。区块的高度随着每生产一个区块而增长。

然而，尽管现在比特币系统计算下一个区块需要花费巨额的算力，但仍然存在两个节点同时或者在相近时间计算出合法区块。当这种情况发生时，区块链就会发生分叉。



此时，比特币协议对节点选择某个区块并无要求，仅需要在自己最早听到的区块后计算下一个区块即可。一旦某个分支率先计算出下一个区块，所有节点应当放弃较短的分支，到较长分支后进行新区块计算。这也就是比特币的“最长链法则”。

6.4 区块链分叉

除了上一节中区块可能会因为在同时同一高度上产生从而分叉外，因为共识规则的变更或者新功能的升级也可能会产生分叉。为了保持共识，所有完整节点都使用相同的共识规则来验证块。但是，有时会更改共识规则以引入新功能。当实施新规则时，未升级的节点将遵循旧规则，而升级后的节点将遵循新规则，这可能会在一段时间内产生分叉，因为节点的更新需要时间，可能会产生两种情况：

遵循新共识规则的块将被升级的节点接受，但未升级的节点将拒绝接受该块

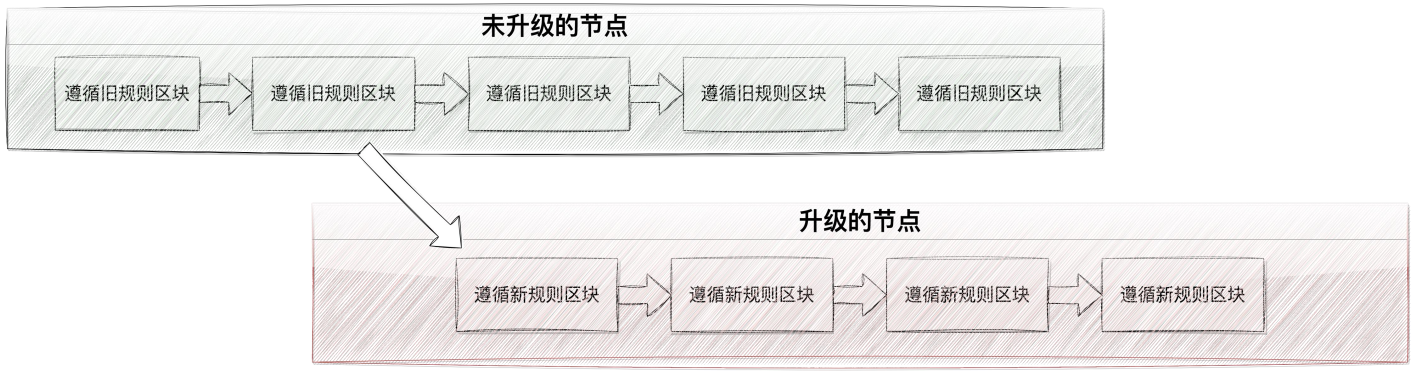
例如，在一个块中使用了新的交易功能：升级后的节点理解并接受该功能，但未升级的节点则拒绝该功能，因为它违反了旧规则。

遵循新共识规则和旧共识规则的块都会被升级节点接受，但新规则的块会被未升级节点拒绝。

例如，在一个块中使用了新的功能：升级的节点会接受它，而未升级的节点则拒绝了它。

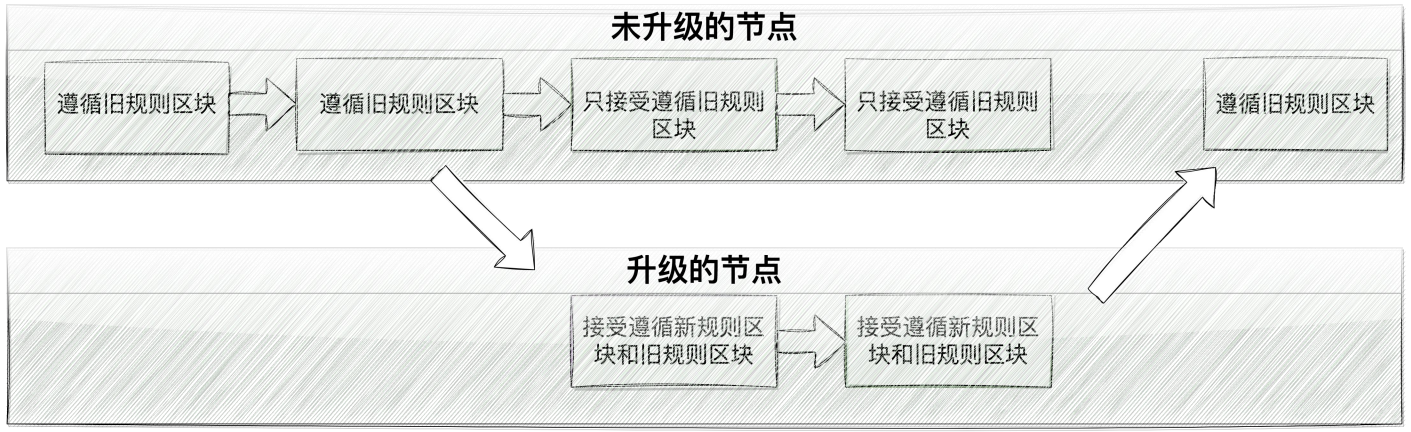
6.4 区块链分叉

在第一种情况下，发生的分叉叫硬分叉，其分叉过程如下图所示



在硬分叉的情况下，因为那些未升级的节点会拒绝接受新规则的块，从而未升级节点产生的区块会在未升级节点构成的链上被接受。升级节点产生的块会在升级节点构成的链上被接受，从而产生了两个独立的链，产生了永久的分叉。

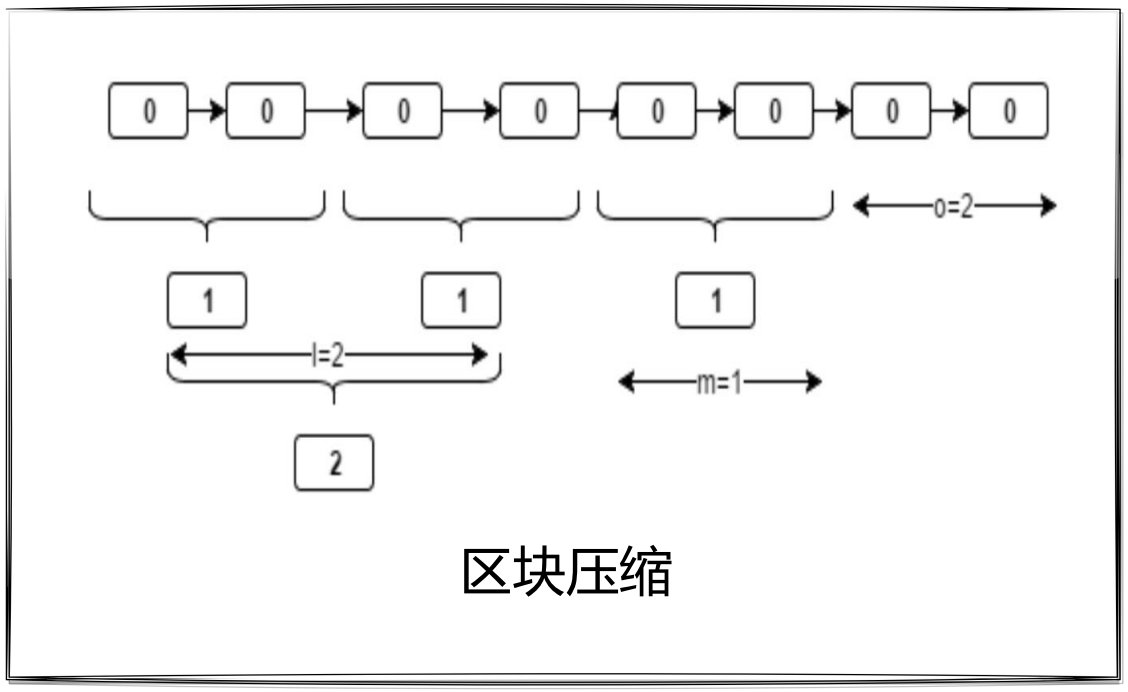
第二种情况下，发生的分叉叫软分叉，其分叉过程如下图所示



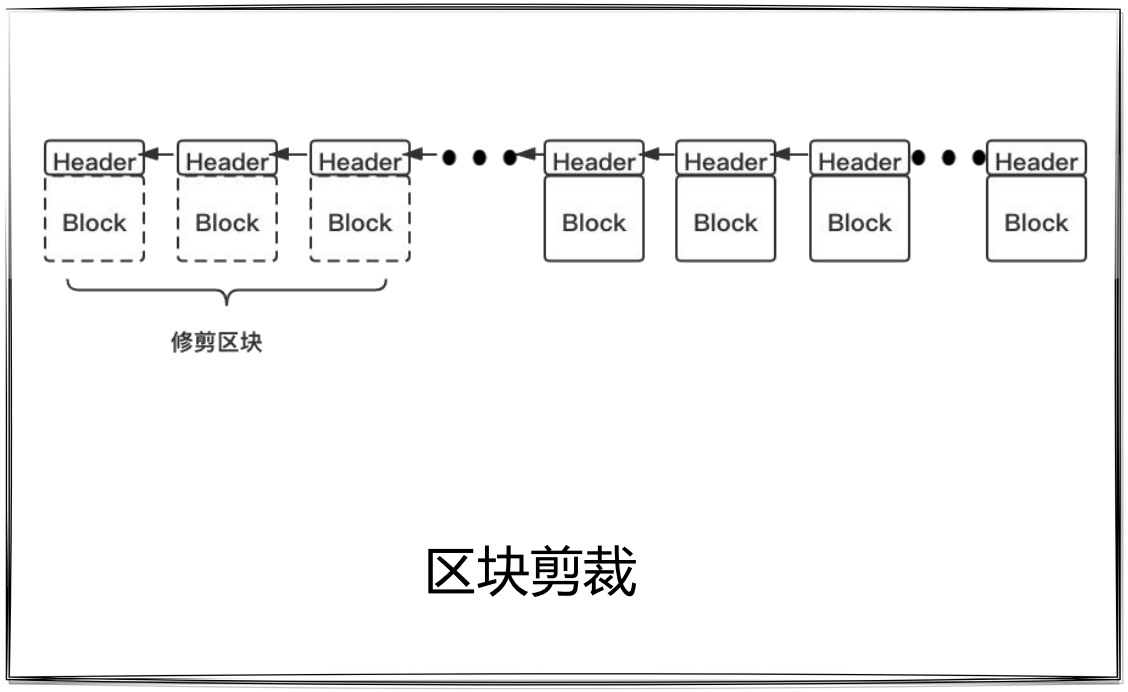
在软分叉的情况下，如果升级的节点掌握了大多数的算力，则可以防产生永久的分叉，因为这些升级的节点占有大多数算力，可以构造最长有效链，最终未升级的节点将接受其作为最长有效链。

6.4 区块的压缩和剪裁

在比特币的设计中，区块随着时间不断的增长，因为去中心化和安全性的设计，每个完整节点都会保存一个完整的区块链的历史账本。这也就意味着对节点存储有着很高的要求。截止到2021年，区块链的规模已经接近300G，且还在维持着接近150M/天的增长率增长。这种规模和严重影响到了整个网络的可拓展性，对带宽的需求和新节点同步时间的增长也成为了需要考虑的问题。为了面对区块链的这种膨胀的问题，一些方法也被提出来减少当前比特币区块链的大小，常见有压缩和剪裁两种方式。



区块压缩



区块剪裁

第 七 节

比特币挖矿

01 挖矿过程

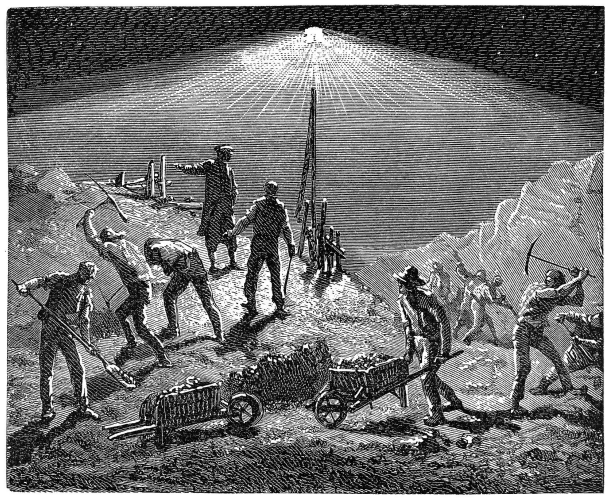
02 挖矿难度

03 挖矿激励

04 挖矿难度

05 矿池

7.1 比特币挖矿-矿工



比特币需要矿工

- 存储和广播区块
- 验证交易有效性
- 对区块进行共识投票

但是，节点为什么要成为一名矿工呢?

7.1 比特币挖矿-矿工

矿工节点的工作

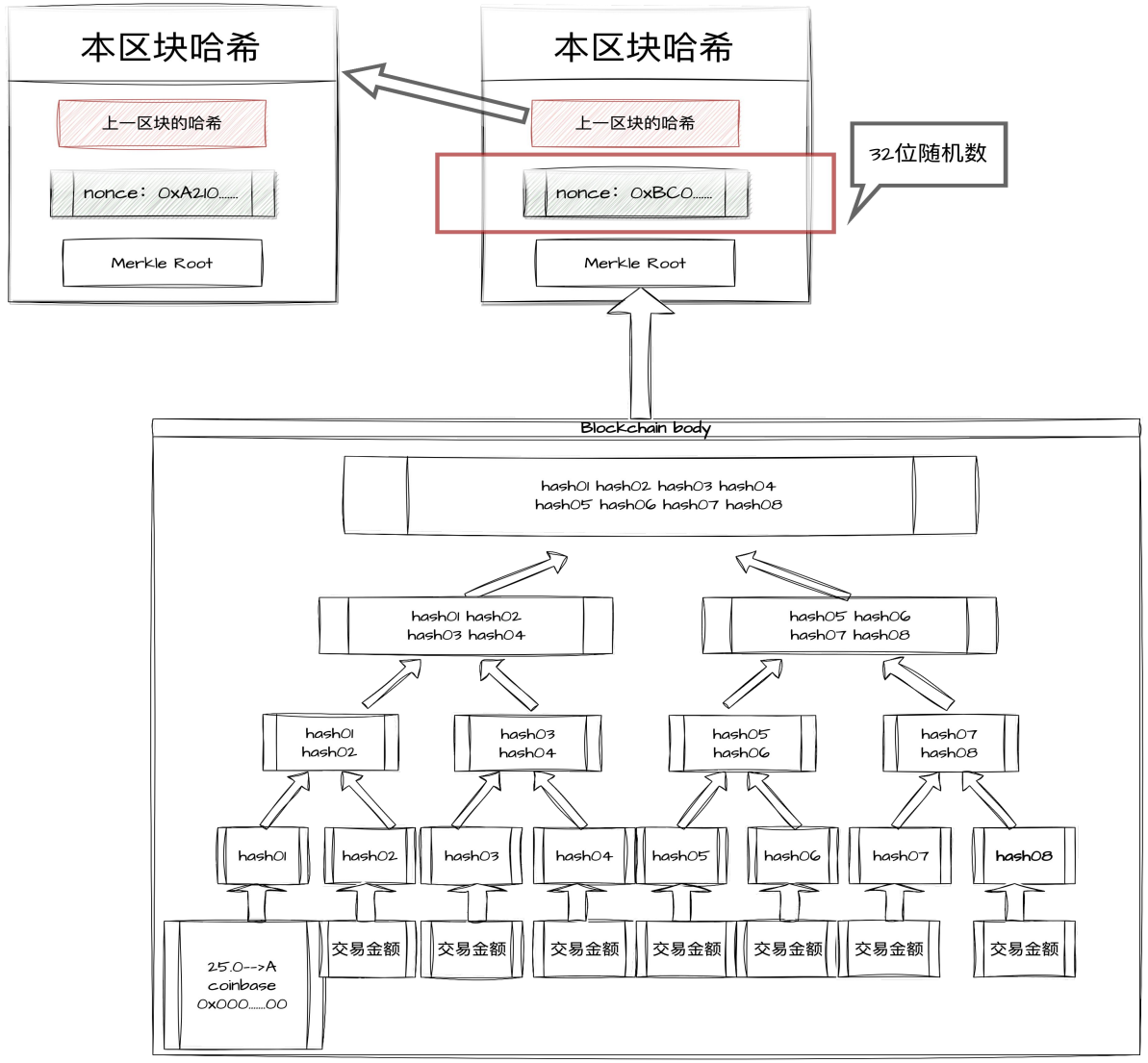
监听交易广播

- 维护区块链网络和监听新的区块
- 组装一个备选区块
- 找到一个让你的区块有效的随机数
- 希望你的区块被全网接受
- 利润

7.2 比特币挖矿-挖矿过程

挖矿是通过不断修改一个随机数，重复计算区块头的哈希，直到找到一个与目标值匹配的哈希的过程。由于哈希函数的输出是无法预测的，因此为了找到一个符合预期的目标值需要不断修改随机数生成不同的哈希，直到碰巧得到希望的结果。

在挖矿过程中，矿工先创建一个填满交易的候选区块。接着，矿工计算区块头的哈希，看其是否小于当前的目标值。如果哈希不小于目标值，矿工就修改随机数（通常就是对随机数加1）并进行计算。在比特币网络中，矿工需要进行上亿次计算才有可能找到一个随机数，得到的哈希值足够小。



7.2 挖矿难度

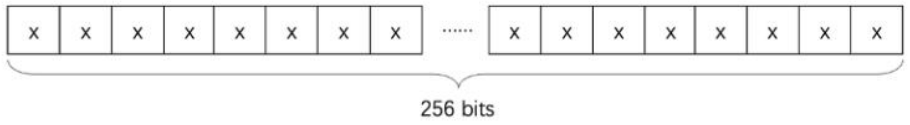
如下图所示，挖矿难度的调节是一个动态调节过程。

比特币区块平均每10分钟生成一个，这是系统运行和交易处理速度的基础。保持这个恒定的速率不仅是短期目标，也需要长期维持。随着时间的推移，加入到系统的节点数越来越多，算力越来越强，产生区块的时间会变短。

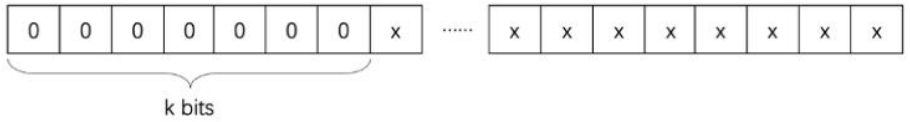
为了维护区块频率的稳定性，需要对挖矿难度进行调节。

每经过2016个区块，所有节点都会调整工作量证明的难度。难度调整算法会计算出最后2016个区块的产生时间，并与预期时间20160分钟进行比较，如果实际产生时间大于20160，那么会降低挖矿难度，否则就会上调挖矿难度。

- 哈希函数SHA-256，输出为256bits，每个bit等概率为0/1且相互独立



- 结果前 k 位都为 0 的概率为 $1/2^k$，期望上计算2^k可以得到一个这样的哈希值



$$T_{new} = T_{old} \cdot \frac{Time\ of\ the\ last\ 2016\ blocks}{2016 \cdot 10\ minutes}.$$

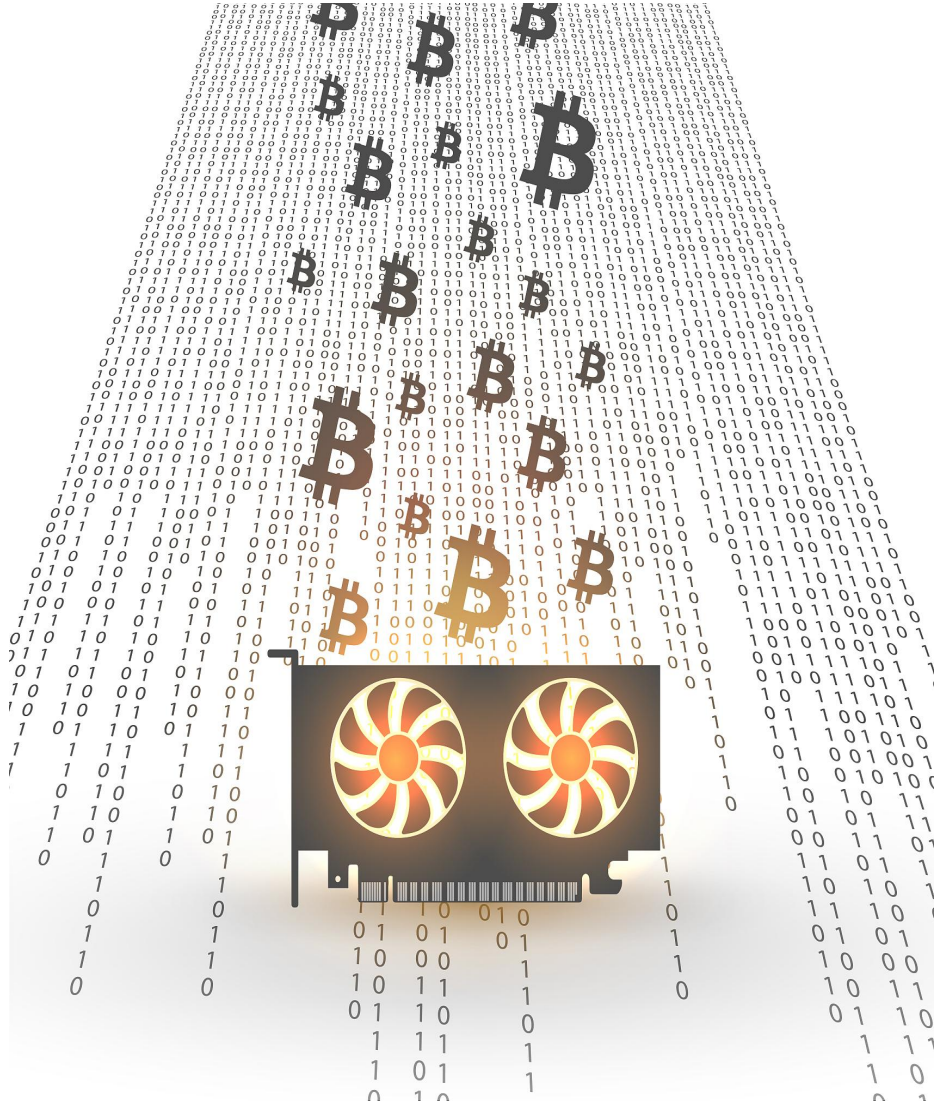
7.2 挖矿难度

早期的比特币矿工采用 CPU 挖矿，此时矿工算力为10MH/s~30MH/s。

2010年第一次 出现了 GPU 挖矿，优化后的GPU算力可达60MH/s。由于CPU和GPU容易获得，普通矿工也可以获取到，因此矿工之间的算力并没有数量级的差异。

2011年6月出现了FPGA矿机，矿机的芯片经过了优化，提高了对哈希函数的运算能力。该矿机算力达到了10G/s。2014 年出现的第三代矿机算力达到了 1T/s。

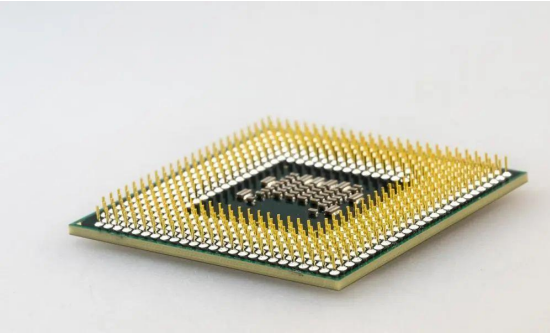
2018 年比特大陆推出的矿机算力达到了10T/s。专业矿机的算力与普通 CPU、GPU 的算力差达到了两个数量级。目前使用最广泛的设备是ASIC，该设备运算能力已经达到了TH/s。



7.2 挖矿难度

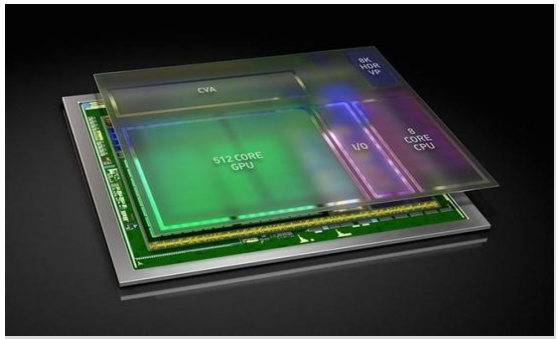
如上图所示，可以看出在2010年至2016年，难度值位于非常低的范围。但是从2016年开始至今，难度值开始大幅度提高，这与挖矿设备算力有着密切关系。

7.3 挖矿设备发展历史



CPU：数据中心里的主要计算单元。对于大部分数据中心来说，它们的各种软硬件基础设施都是围绕CPU设计建设的。所以CPU在数据中心的部署、扩展、运维，包括生态其实都已经非常成熟。

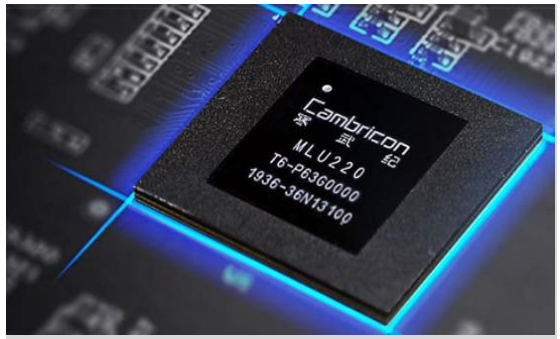
优点：灵活性，同构性。
缺点：算力有限，功耗较高
对海量的数据进行处理，基于传统CPU的计算结构很难满足需求



GPU：图形处理器，又称显示核心、视觉处理器、显示芯片，是一种专门在个人电脑、工作站、游戏机和一些移动设备（如平板电脑、智能手机等）上做图像和图形相关运算工作的微处理器。

优点：提供了多核并行计算的基础结构，且核心数非常多，可以支撑大量数据的并行计算，拥有更高的浮点运算能力。
缺点：管理控制能力（最弱），功耗（最高）。

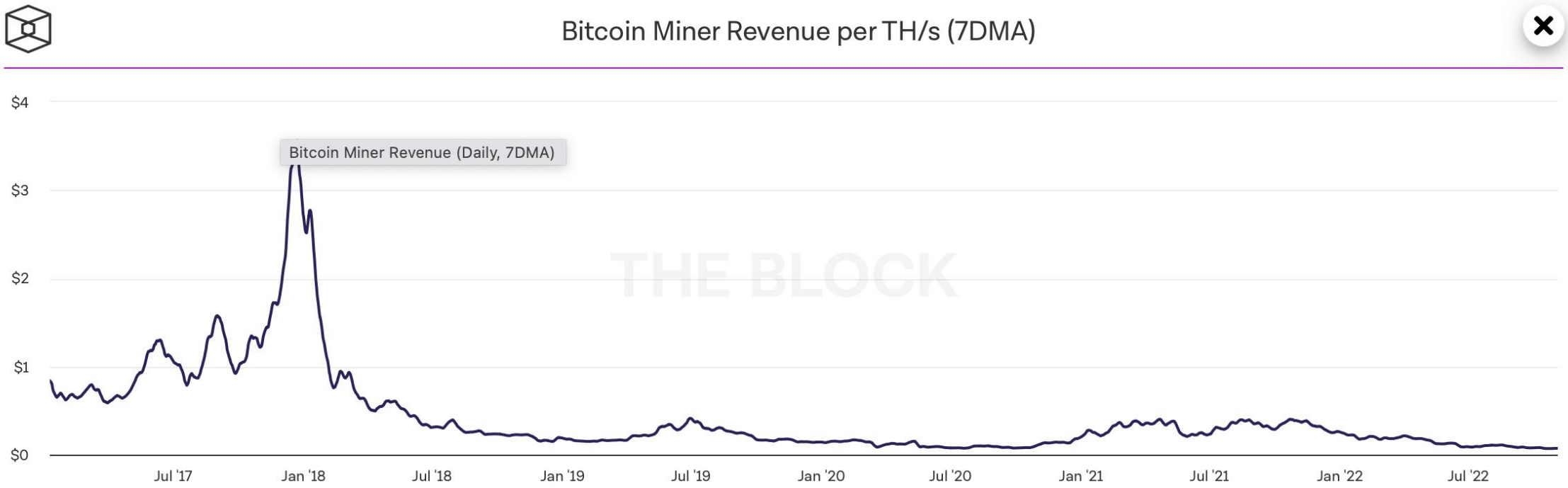
FPGA是在PAL、GAL等可编程器件的基础上进一步发展的产物。它是作为专用集成电路（ASIC）领域中的一种半定制电路而出现的，既解决了定制电路的不足，又克服了原有可编程器件门电路数有限的缺点。
优点：可以无限次编程，延时性比较低，同时拥有流水线并行和数据并行（GPU只有数据并行）、实时性最强、灵活性最高
缺点：开发难度大、只适合定点运算、价格比较昂贵



ASIC,即专用集成电路，ASIC就是所谓的人工智能专用芯片。研发这样的芯片有着极高的成本和风险。与软件开发不同，芯片开发全程都需要大量的人力物力投入，开发周期往往长达数年，而且失败的风险极大

优点：有着极高的性能和极低的功耗，和GPU相比，它的性能可能会高十倍，功耗会低100倍
缺点：灵活性不够，成本比FPGA贵

7.4 挖矿激励



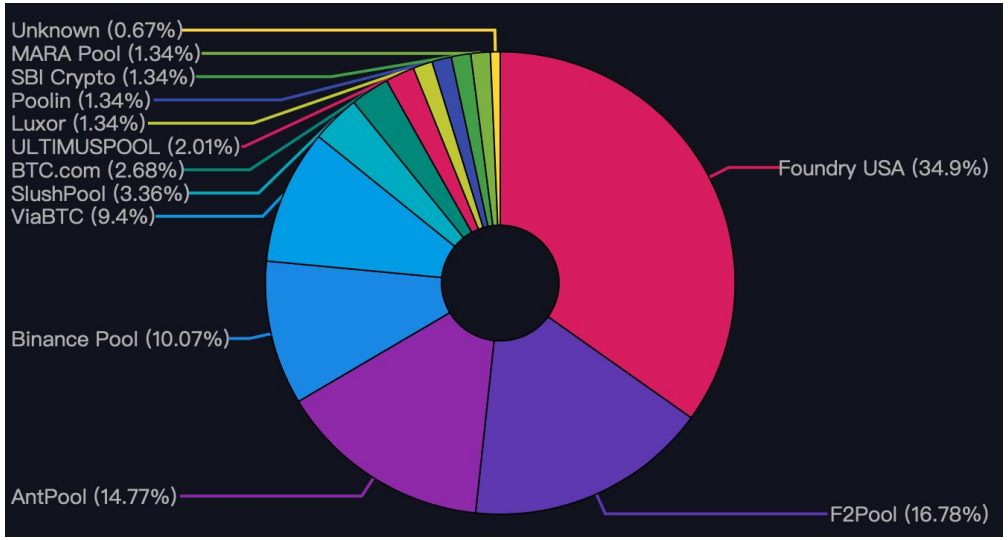
为了保证所有节点按照比特币协议进行，比特币系统设计了如下的经济激励手段。当矿工挖到一个区块时，将得到相当可观的奖励（当前为30万美元一个区块）。矿工正常生成区块可以获得区块奖励加上该区块中所有交易的手续费，区块奖励每 4 年减半，保障了比特币总数2100万个，避免通货膨胀。

7.5 比特币挖矿-矿池

比特币系统中，当矿工挖到一个区块时，将得到相当可观的奖励。然而，单个矿工能挖到区块的概率却极低（平均需要数年时间）。面对这一耗时费力的任务，近年来出现了基于“风险共担”思想的集中式矿池（Mining Pool）。一个矿池中会有许多矿工。当矿池中的某个矿工挖到了新的区块，矿池会根据每个矿工的算力贡献大小，进行奖励分配。

#blocks find in one year	Probability（Pission dist）
0	42.4%
1	36.4%
2	15.6%
3+	5.6%

矿池每年挖到区块数量及其概率



矿池实时占比排行

7.5 比特币挖矿-矿池

北京大学 PEKING UNIVERSITY

区块

区块高度	矿池	时间戳	已出块	奖励	费用	交易	大小
761990	Binance Pool	2022-11-06 22:27	8分钟之前	6.49 BTC	0.24 BTC	3,364	1.54 MB
761989	ViaBTC	2022-11-06 21:48	46分钟之前	6.35 BTC	0.10 BTC	2,008	1.12 MB
761988	SlushPool	2022-11-06 21:37	58分钟之前	6.27 BTC	0.02 BTC	634	276.24 kB
761987	Foundry USA	2022-11-06 21:33	1小时之前	6.32 BTC	0.07 BTC	1,623	1.11 MB
761986	Foundry USA	2022-11-06 21:26	1小时之前	6.30 BTC	0.05 BTC	1,405	1.47 MB
761985	Foundry USA	2022-11-06 21:22	1小时之前	6.36 BTC	0.11 BTC	2,280	1.57 MB
761984	Poolin	2022-11-06 21:12	1小时之前	6.44 BTC	0.19 BTC	3,046	1.47 MB
761983	AntPool	2022-11-06 20:46	1小时之前	6.40 BTC	0.15 BTC	2,747	1.51 MB
761982	F2Pool	2022-11-06 20:27	2小时之前	6.27 BTC	0.02 BTC	250	628.73 kB
761981	Foundry USA	2022-11-06 20:26	2小时之前	6.38 BTC	0.13 BTC	2,654	1.62 MB
761980	Foundry USA	2022-11-06 20:09	2小时之前	6.40 BTC	0.15 BTC	1,654	1.26 MB
761979	F2Pool	2022-11-06 19:59	2小时之前	6.30 BTC	0.05 BTC	1,159	591.34 kB

矿池实时挖矿信息

7.5 比特币挖矿-矿池

北京大学 PEKING UNIVERSITY

矿机型号	算力	功耗	单位功耗	日产出	电费	电费占比	日净利润	关机币价
蚂蚁矿机 S19 XP	140 T	3010 W	21.50 W/T	¥ 73.92	¥ 23.83	32.23%	¥ 50.09	¥ 49194.88
锦鲤矿机 C16 Max	113 T	3400 W	30.08 W/T	¥ 59.67	¥ 26.92	45.11%	¥ 32.75	¥ 68854.38
蚂蚁矿机 S19 Pro	110 T	3250 W	29.54 W/T	¥ 58.08	¥ 25.74	44.31%	¥ 32.34	¥ 67631.83
神马矿机 M30S++	112 T	3472 W	31.00 W/T	¥ 59.14	¥ 27.49	46.48%	¥ 31.65	¥ 70940.10
锦鲤矿机 C16 Pro	98 T	3200 W	32.65 W/T	¥ 51.75	¥ 25.34	48.96%	¥ 26.41	¥ 74731.62
神马矿机 M30S+	100 T	3400 W	34.00 W/T	¥ 52.80	¥ 26.92	50.98%	¥ 25.88	¥ 77803.46
蚂蚁矿机S19	95 T	3250 W	34.21 W/T	¥ 50.16	¥ 25.74	51.31%	¥ 24.42	¥ 78308.48

矿机收益排行榜

本章小结

本章主要围绕比特币展开

第一节对比特币进行了简单介绍，主要从货币发展历史，比特币的产生，比特币定义，比特币的生态这几个方面展开介绍

第二节介绍比特币的地址。首先是公钥和私钥的原理，其次是地址如何进行转换，以及如何进行地址交易。

第三节介绍了比特币的钱包，首先对钱包进行简介，然后对钱包的类型，钱包功能，钱包技术等展开了介绍。

第四节介绍了比特币的交易，首先对比特币中的交易进行了描述，然后对构成交易的UTXO进行了详解，之后通过小宋去姜老板的书店买书的例子详细解释了交易的过程。

第五节介绍了比特币的网络，从节点类型，网络类型和通信类型对比特币网络进行了展开介绍。

第六节介绍了比特币的区块，首先为大家展示了创世区块的结构，之后从区块数据结构，区块链式结构，区块高度深度和区块压缩剪裁等几个方面对比特币区块进行了详细讲解，

第七节介绍了比特币挖矿，从挖矿原因，矿工职能，挖矿难度，挖矿激励，矿池对比特币挖矿进行了讲解。

北京大学
PEKING UNIVERSITY

感谢观看