红亚科技
HONGYAATECH

区块链技术深度剖析

红亚太学链系列课程

红亚科技
HONGYAATECH

第1章 区块链概述

讲师：王宝成

马云说过：对于新兴事物，绝大多数人第一看不见，第二看不起，第三看不懂，第四来不及。

如果你对比特币等数字货币还处于“看不懂”阶段，不想等到“来不及”阶段，红亚太学链系列课程之《区块链技术深度剖析》将深入浅出地介绍数字货币和区块链技术的运行原理，让你对挖矿、钱包、签名、密钥这些技术不再陌生。

目 录

CONTENTS

现实问题

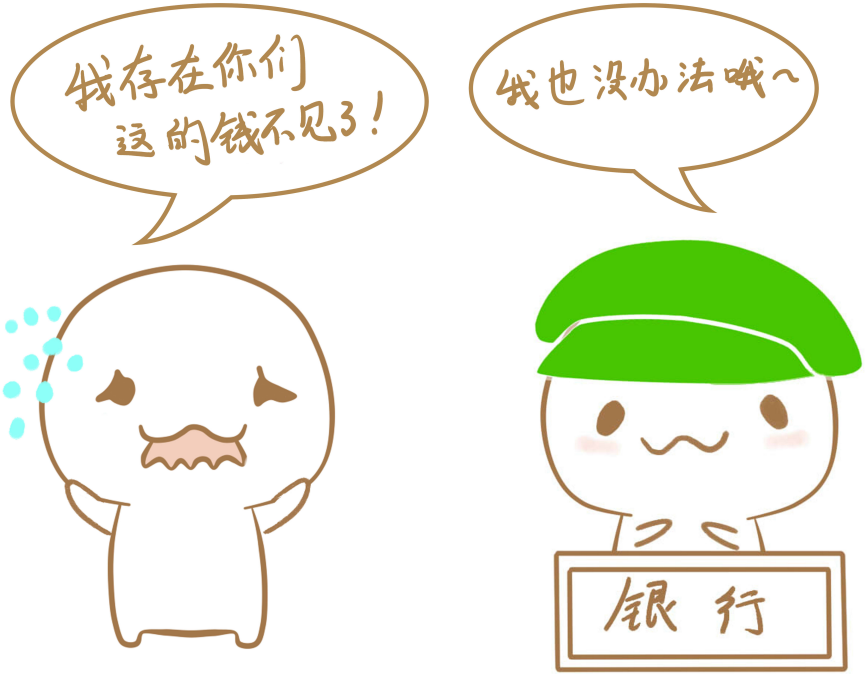
构建诚信社会

比特币运行机制

区块链与密码学

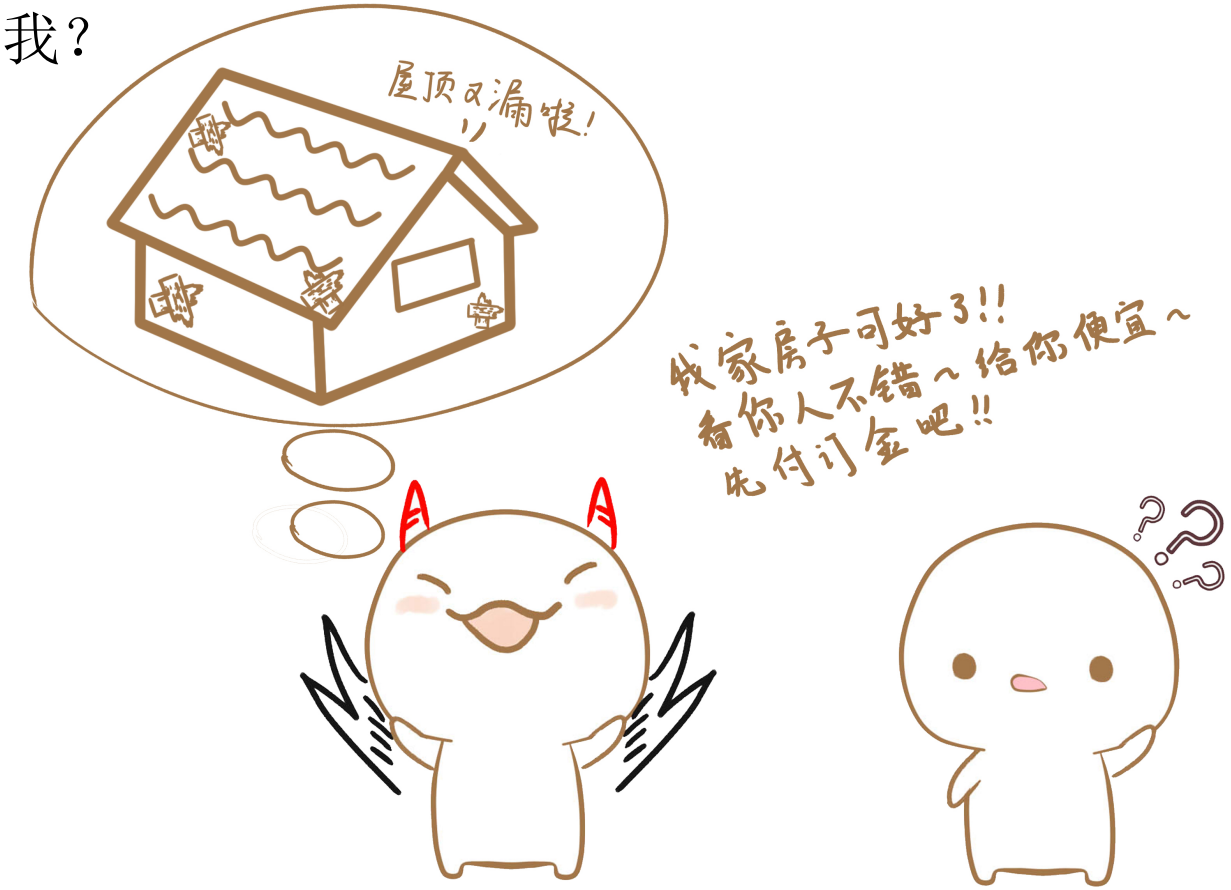
问题1 - 银行存款凭空消失，能找回吗？谁来负责？

2015年，我国多地频频出现银行储户存款“失踪”案件：浙江杭州42位银行储户发现，自己的数百万元存款仅剩少许甚至被“清零”；泸州老窖等知名企业存款也出现“异常”，甚至还出现3个月内农业银行、工商银行的5亿元不知去向。



问题2 - 陌生人之间如何实现相互信任？

北京的小赵想租个房子，房东告诉小赵他的房子不但新，而且各种设施完善，家具出了问题他都可以免费更换，租金还便宜。这么好的事，小赵肯定要掂量掂量：这房东是不是在唬我？



问题2续 - 陌生人之间如何实现相互信任？

同样的，小赵还想买辆二手车，但是卖家会有动机虚报自己的里程数，甚至谎称自己的车子没有经历过事故和维修，小赵该如何判断呢？

问题3 - 已发生的交易记录如何不被篡改？

玛丽安娜女士居住在洪都拉斯，她住在自家房子三十多年了。某天，玛丽安娜遭到法院传讯。A向法院申请驱逐令，原来国家产权局登记的是A的名字，而后房屋被拆毁。但后来经过法院查证，房子其实就是玛丽安娜女士的，但不动产已经毁了，玛丽安娜女士只能默默流泪……

这类扯皮的事情在全球都很普遍，房屋所有权保障的缺失也是不公正的源头。

问题4 - 该怎么证明我妈是我妈？如何实现自证？

北京市民陈先生一家三口准备出境旅游，需要明确一位亲人为紧急联络人，于是他想到了自己的母亲。可问题来了，需要书面证明他和他母亲是母子关系。可陈先生在北京的户口簿，只显示自己和老婆孩子的信息，而父母在江西老家的户口簿，早就没有了陈先生的信息。

那么，陈先生如何证明“我妈是我妈”呢？

问题4续 - 该怎么证明我妈是我妈？如何实现自证？

陈先生的遭遇，并非孤例，很多人在办事过程中遇到过类似令人啼笑皆非的证明：要证明你没犯过罪，要证明你没结过婚，要证明你没有要过孩子，要证明你没买过房……这样那样的证明，有的听起来莫名其妙，办起来更让人东奔西跑还摸不着头脑。

当我们对一些证明感到不可理解，去问工作人员为什么要这个证明，得到回答往往是“就是这么规定的”。

红亚科技
HONGYAATECH

目 录

CONTENTS

现实问题√

构建诚信社会

比特币运行机制

区块链与密码学

曾经某一段时间，社会诚信缺失问题非常突出，各种假冒伪劣、坑蒙拐骗、弄虚作假、尔虞我诈现象，给我国经济社会生活带来了无法估量的信任危机。

诚信缺失已经成为制约当前我国市场经济高效快速发展和社会文明建设的一个重要因素。

因此，我们必须正视我国诚信缺失的现状，深刻认识其危害性，把握现代社会中诚信缺失的社会原因，寻找解决方案，为治理诚信缺失问题提供有效的策略。

现实社会中，人与人、人与公司、公司与公司之间的交易需要公信力提供支撑。

公信力是指社会生活中，公共权力面对时间差序、公共交往以及利益交换时，所表现出的一种公平、公正、公开、人道、民主与责任的信任力。公信力一般由政府、国家机关或政府授权的第三方组织提供。通俗来说，公信力就是使公众信任的力量。

银行存款“失踪”、e租宝诈骗、百度“魏则西事件”——利用公信力为高风险的互联网金融产品进行背书，是否会对政府以及媒体的公信力带来损害？

伴随着这个问题的出现，一种用技术解决公信力的方案开始变得引人瞩目，这就是“区块链”（blockchain）。

区块链技术的核心功能指在提升公信力。

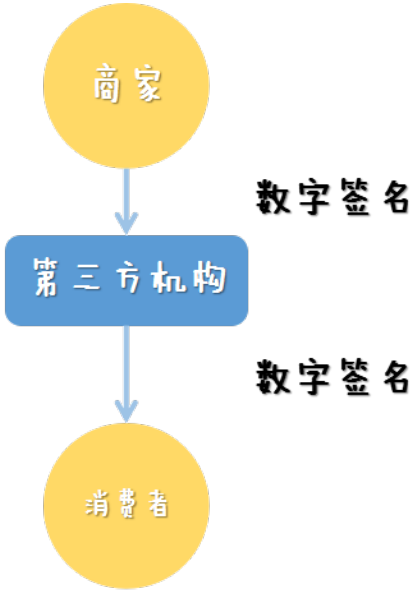
当前公信力模型中公信力仅由政府或政府所授权的第三方机构掌握，政府的自我监督能力未必能够被社会充分认可。

区块链技术可以很好地满足公信力需求，并把公信力抽象出来作为一个“去中心化”的存在，形成政府、大众、区块链与公信力互相监督的“公信新格局”。

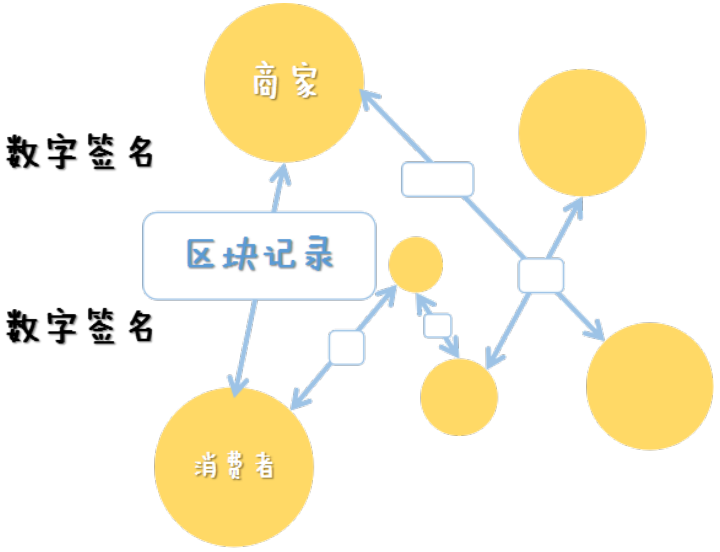
即信任是建立在区块链上的，而非由单个组织掌控，公信力可以被多方交叉验证与监督，得以实现和保障。

互联网上的贸易，几乎都需要借助可资信赖的第三方信用机构来处理电子支付信息。这类系统仍然内生性地受制于“基于信用的模式”。

区块链技术是构建比特币区块链网络与交易信息加密传输的基础技术。它基于密码学原理而不基于信用，可使得任何达成一致的双方直接支付，从而不需要第三方中介的参与。



传统支付系统



区块链支付系统

2016年1月，英国发表区块链白皮书，明确指出：区块链列入英国国家战略部署

2016年10月18日，工信部发布《中国区块链技术和应用发展白皮书》

2016年12月，国务院将区块链写入《“十三五”国家信息化规划》，与大数据、人工智能等成为国家战略前沿技术

2017年5月16日，工信部发布首个区块链标准《区块链参考架构》

国务院2017年10月13日印发《关于积极推进供应链创新与应用的指导意见》：提高质量安全追溯能力。

国际权威杂志《经济学人》、《哈佛商业周刊》、《福布斯杂志》等相继报道区块链技术将影响世界。

创业公司R3联合全球42家顶级银行成立区块链联盟，包括摩根大通、美国银行、汇丰银行、花旗银行、富国银行、三菱UFJ金融集团、高盛、德意志银行等。

百度加入Linux基金会领导的超级账本（Hyperledger）区块链联盟，成为该联盟最新成员。

金融区块链合作联盟深圳成立，腾讯、华为加入。

腾讯发布区块链方案白皮书……

1.5 该怎么证明我妈是我妈？如何实现自证？

2008年，区块链(blockchain)的概念浮出水面。

该技术将数据分区块存储，每一块包含一部分内容

每一个区块都会记录着前一区块的ID（唯一标识）

按时间顺序形成一个链状结构，并以密码学方式保证数据不可篡改，因而称为区块链技术。

想象一下：一个人从小学开始，每一年的成绩单，每一个学校的毕业证都可以在区块链上查到。

工作状况、婚姻状况、保险状况也都一一呈现在区块链之上。医生的每一次诊断都将写入区块不可修改。

数字仲裁可以直接从区块链上扣款，公益捐款的每一笔收和用途都记录在案。

我们生活的社会将不仅是一个数字化社会，而是区块链所带来的诚信社会。

未来已来，只是尚未流行，我辈仍需多努力……

目 录

CONTENTS

现实问题√

构建诚信社会√

比特币运行机制

区块链与密码学

2.0 比特币价格 - 疯狂的比特币 - 九年增长2800万倍

2010年5月22日，一名程序员用1万枚比特币购买了两个披萨。这被广泛认为是用比特币进行的首笔交易。

2016年年底一枚比特币6,000元左右

2017年年初一枚比特币7,000元左右

2017年年中一枚比特币30,000元左右

2017年年底一枚比特币130,000元左右

九年时间比特币从0.005RMB涨到了12万接近13万RMB,涨幅超过2800多万倍。

2018年开始一路暴跌—1月22日：10856美元……7000美元左右……

2.1 比特币是什么？

比特币是一种虚拟货币（数字货币）。

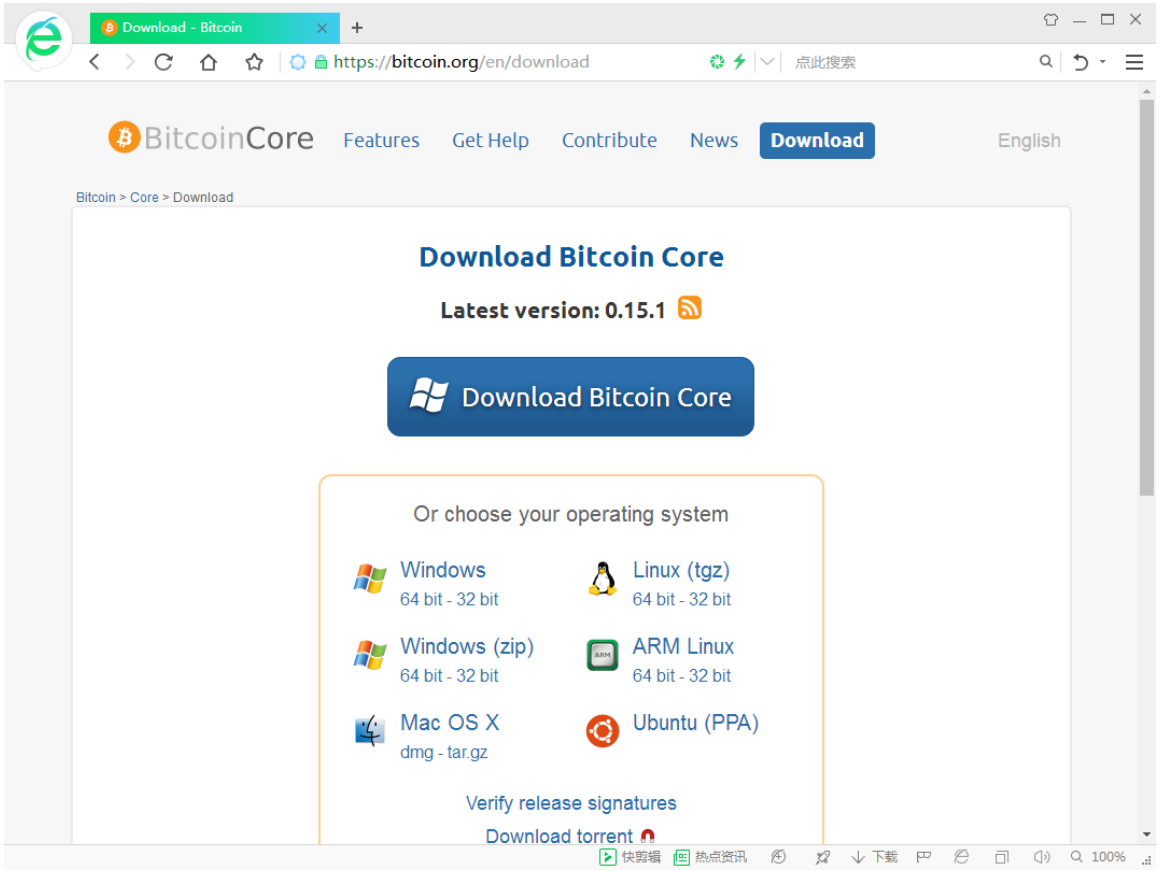
比特币基于一套密码编码、通过相关密码算法产生，这一规则不受任何第三方个人或组织干扰。

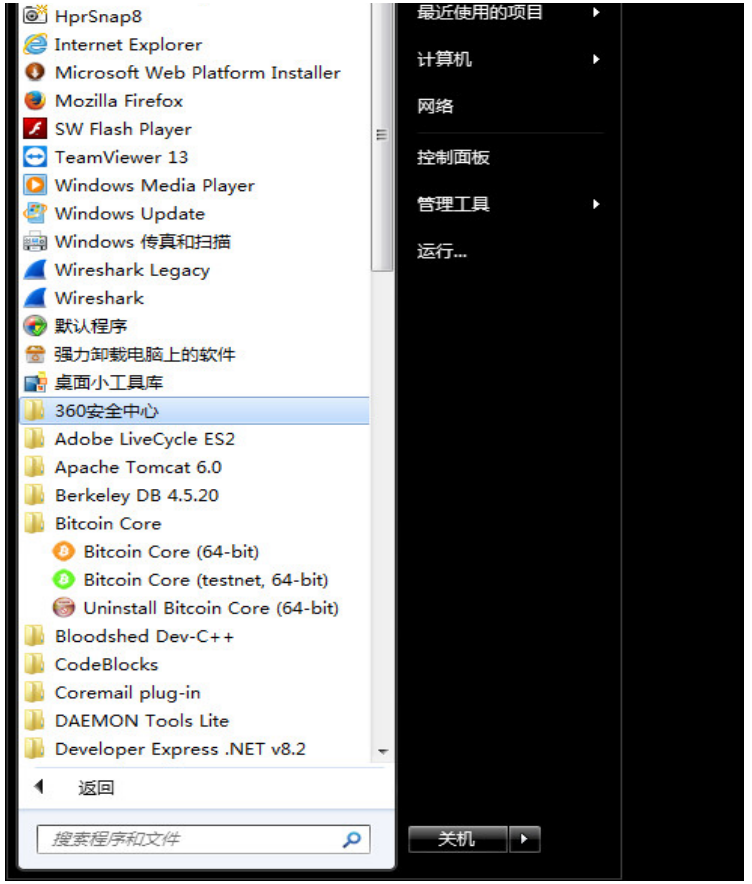
任何人都可以通过下载运行比特币客户端的方式参与比特币的制造与交易。

比特币利用数字签名的方式在P2P网络中流通。

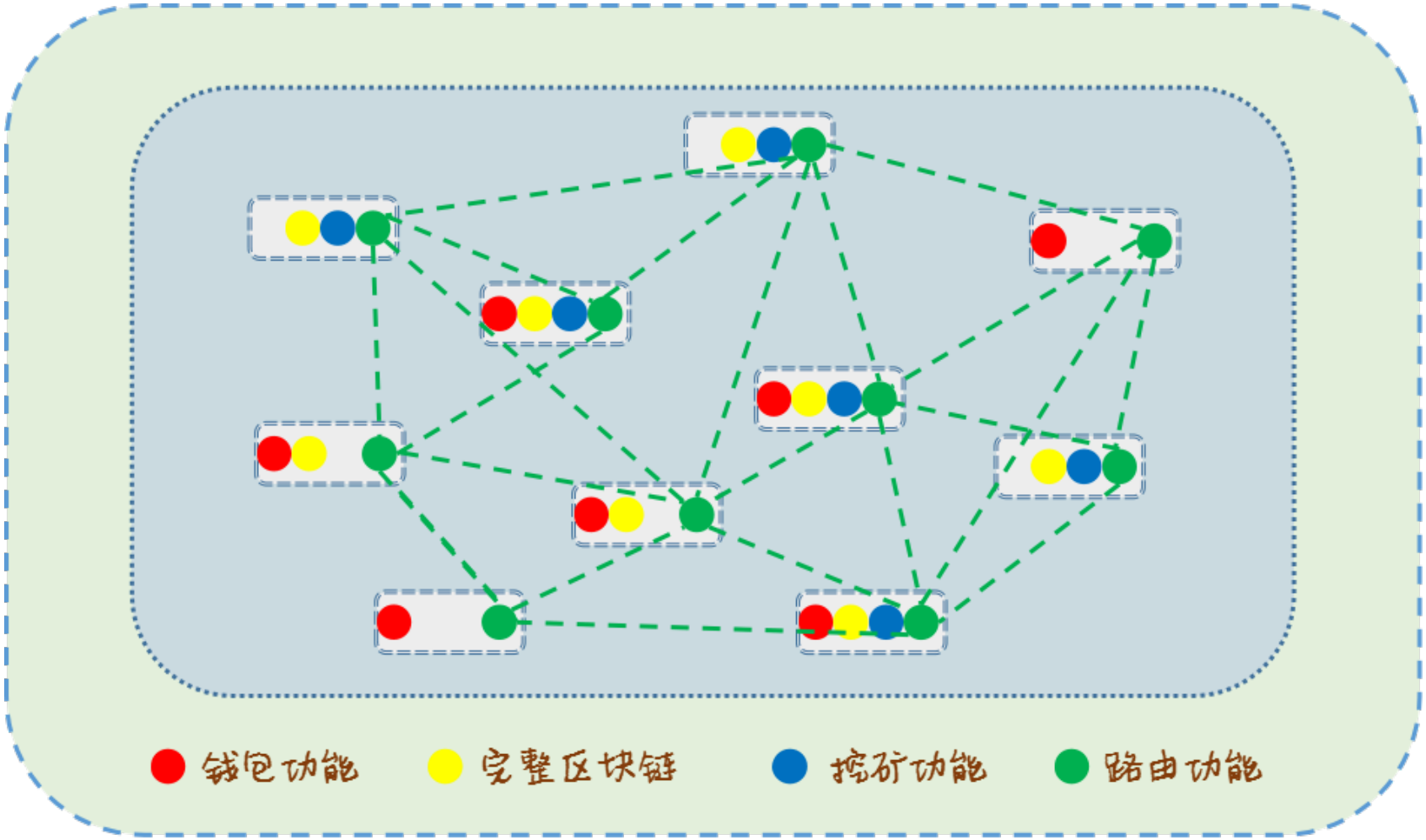
比特币的产生、交易都会通过P2P网络记录并向全网广播（避免伪造）。

2.1 比特币运行机制 - 核心客户端 - 中心化？？？





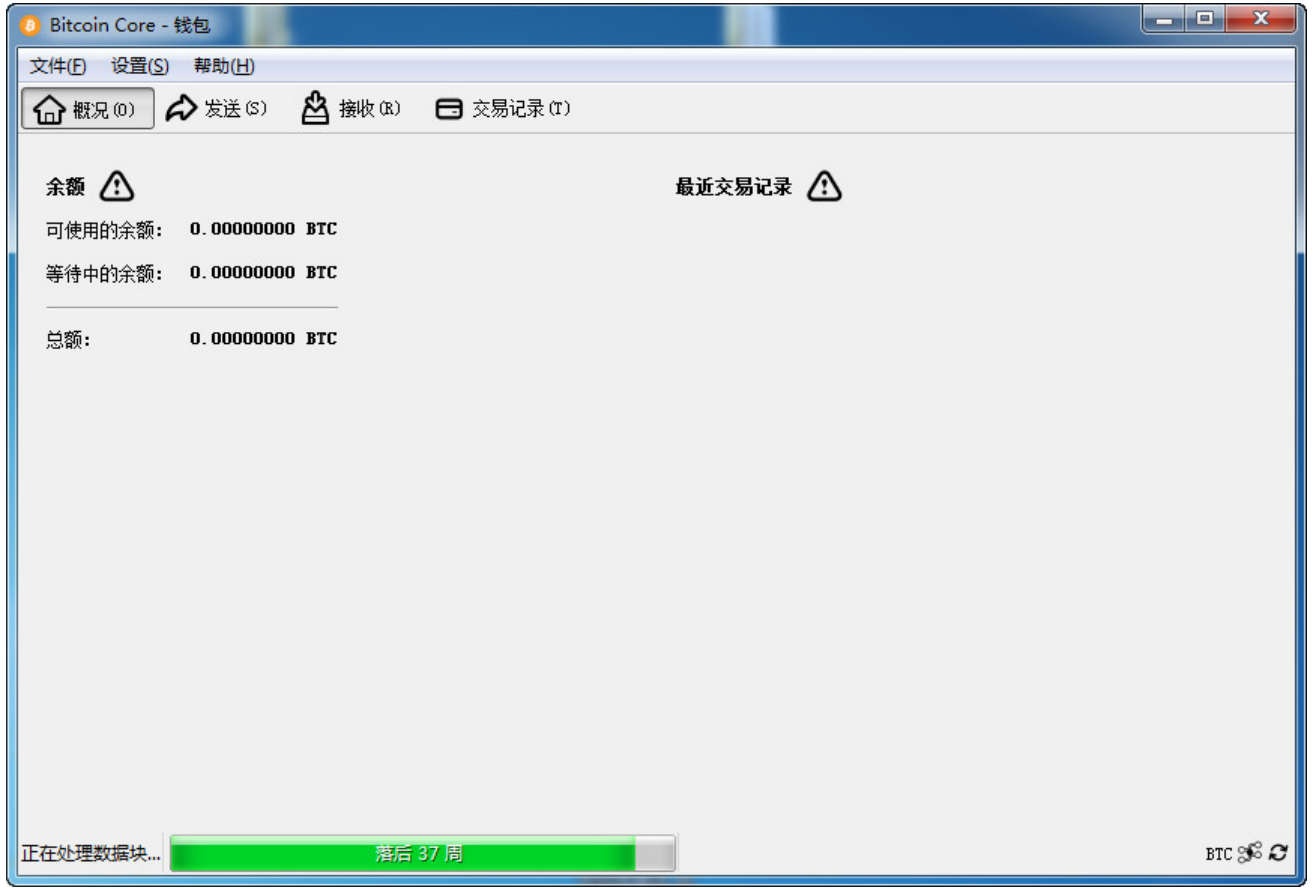
2.1 比特币运行机制 - 节点网络 - 去中心 - 去信任



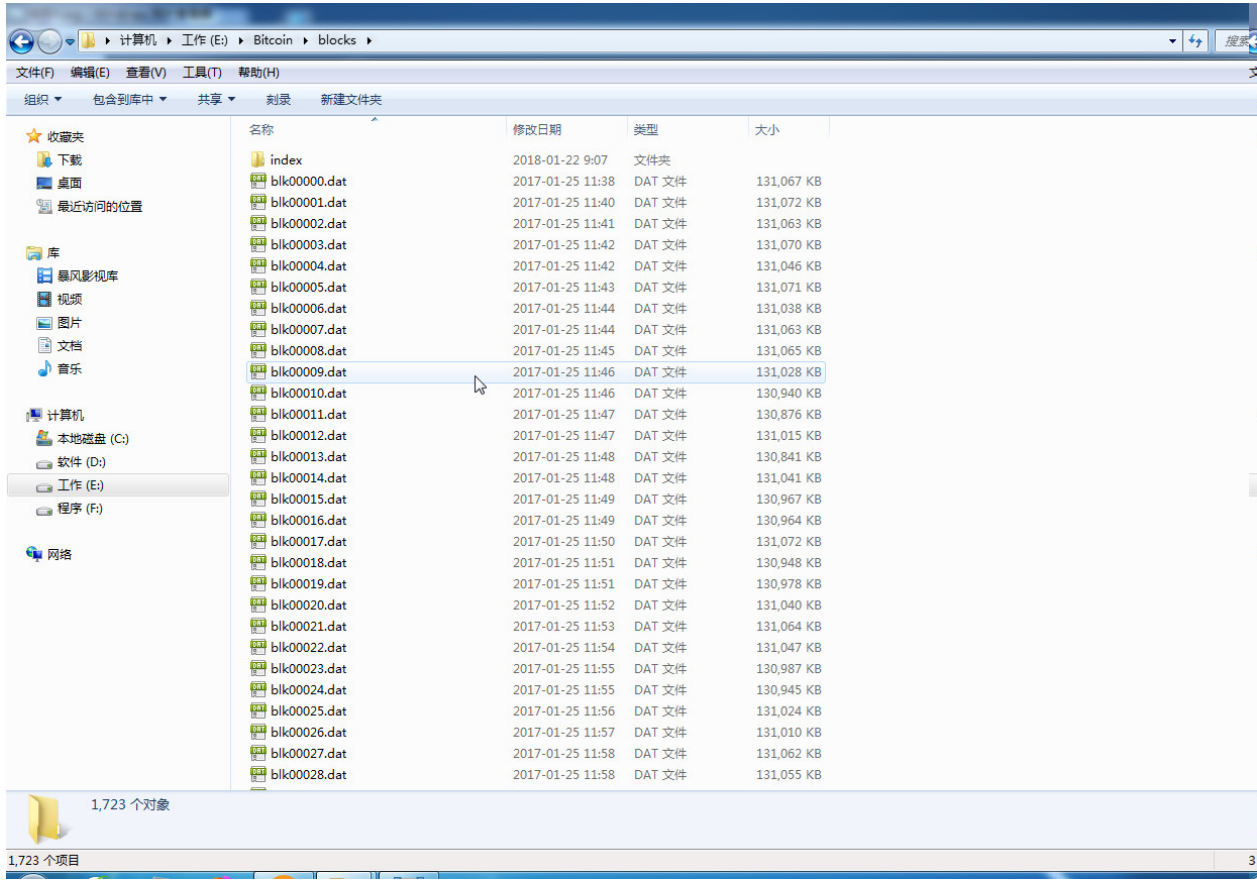
除了路由功能以外，其它的功能都不是必须的。

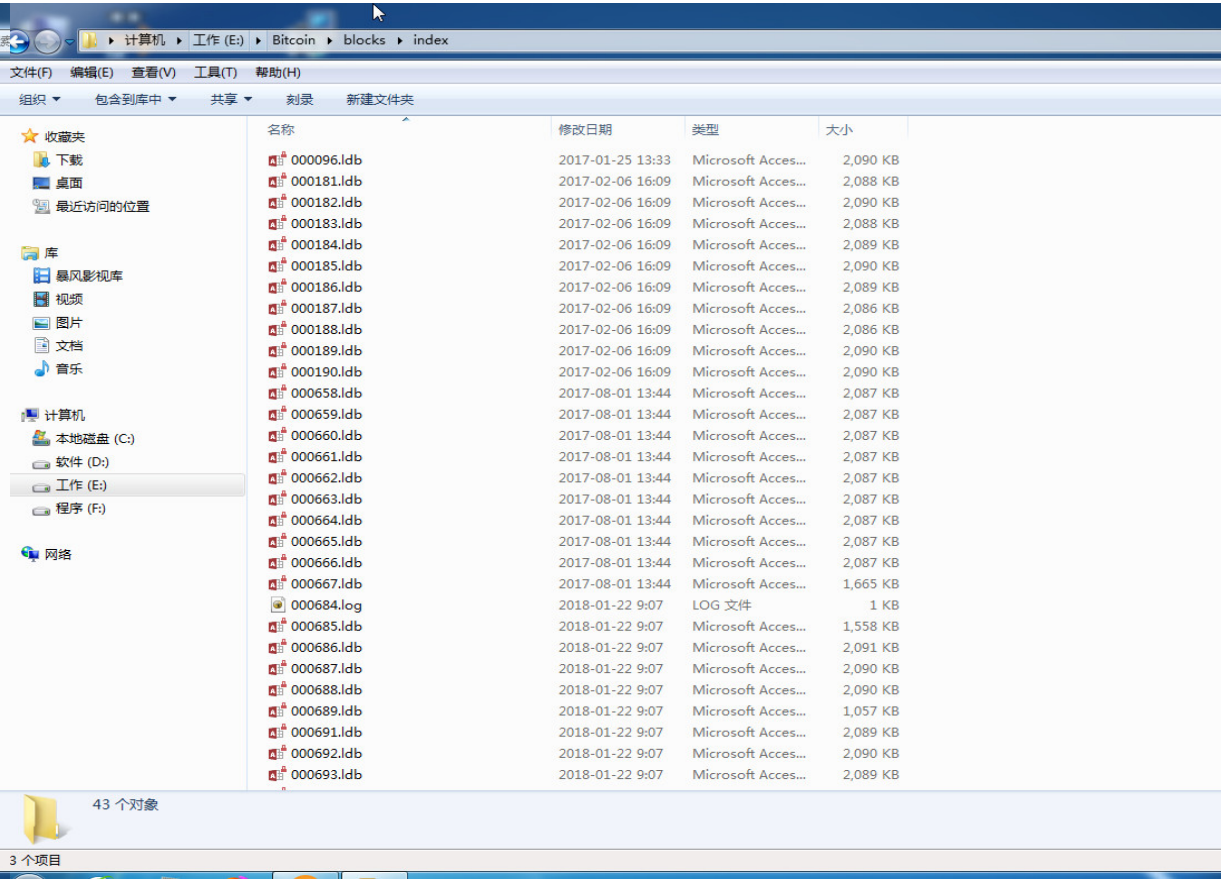
2.1 比特币运行机制 - 启动网络

2.1 比特币运行机制 - 加载数据

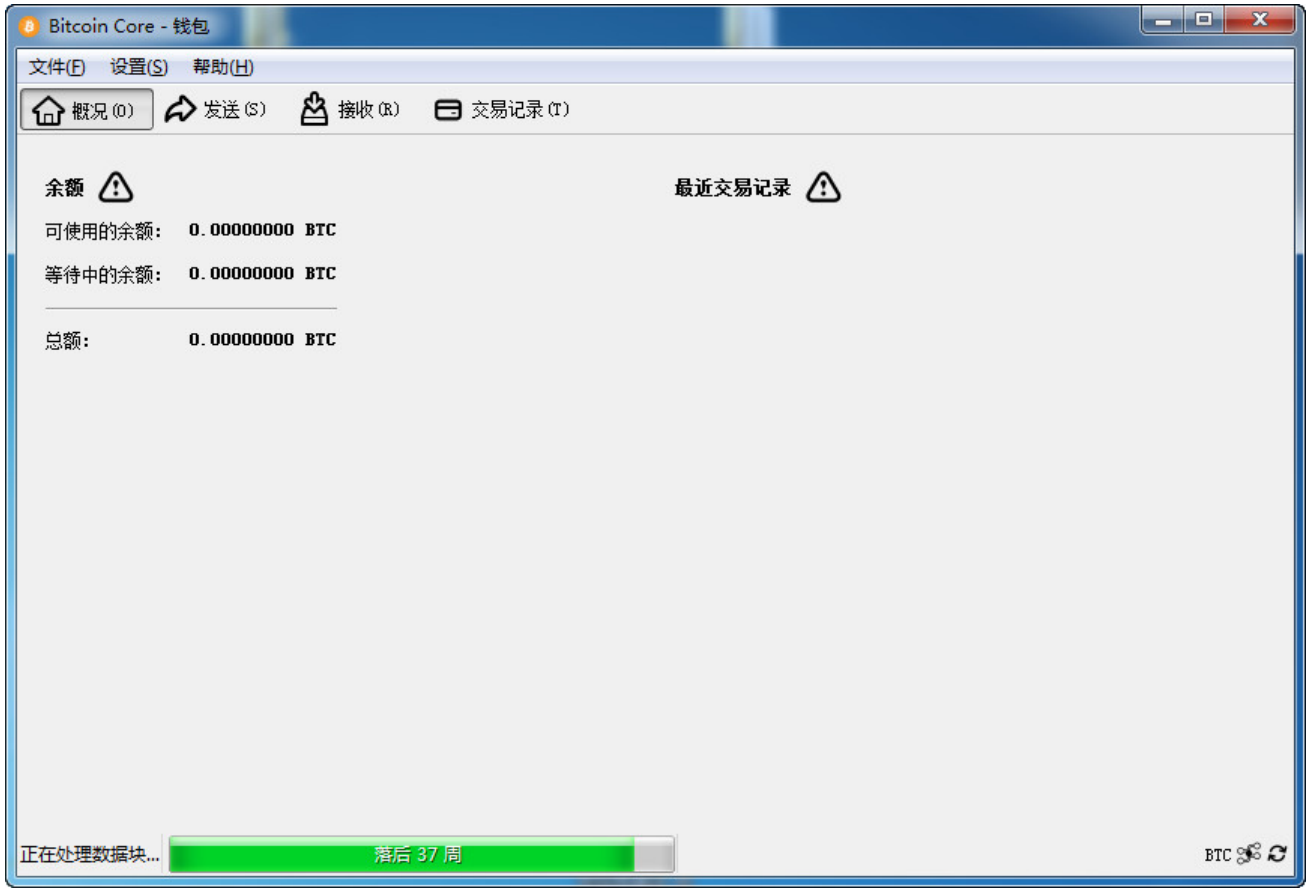


2.1 比特币运行机制 - 分布式账本 - 开放共识

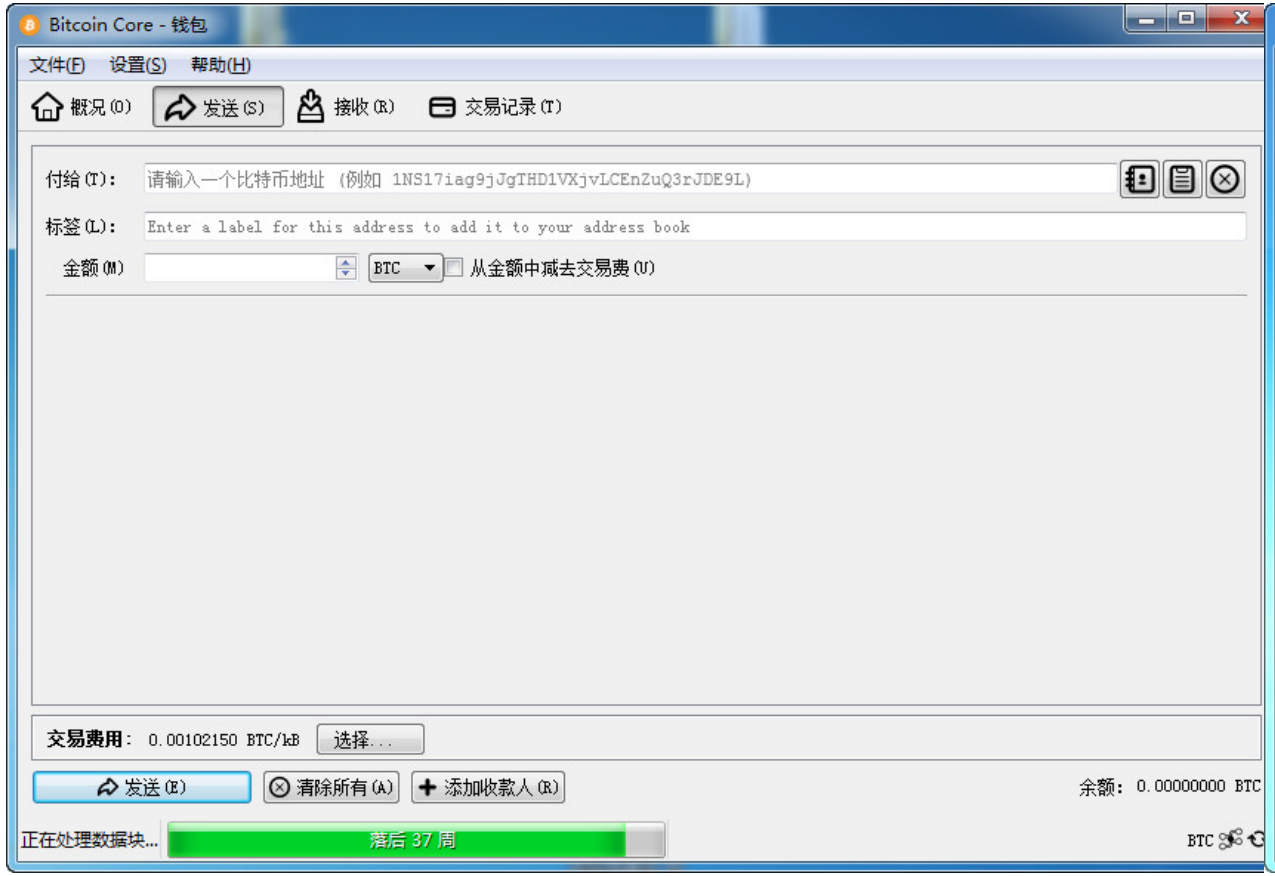


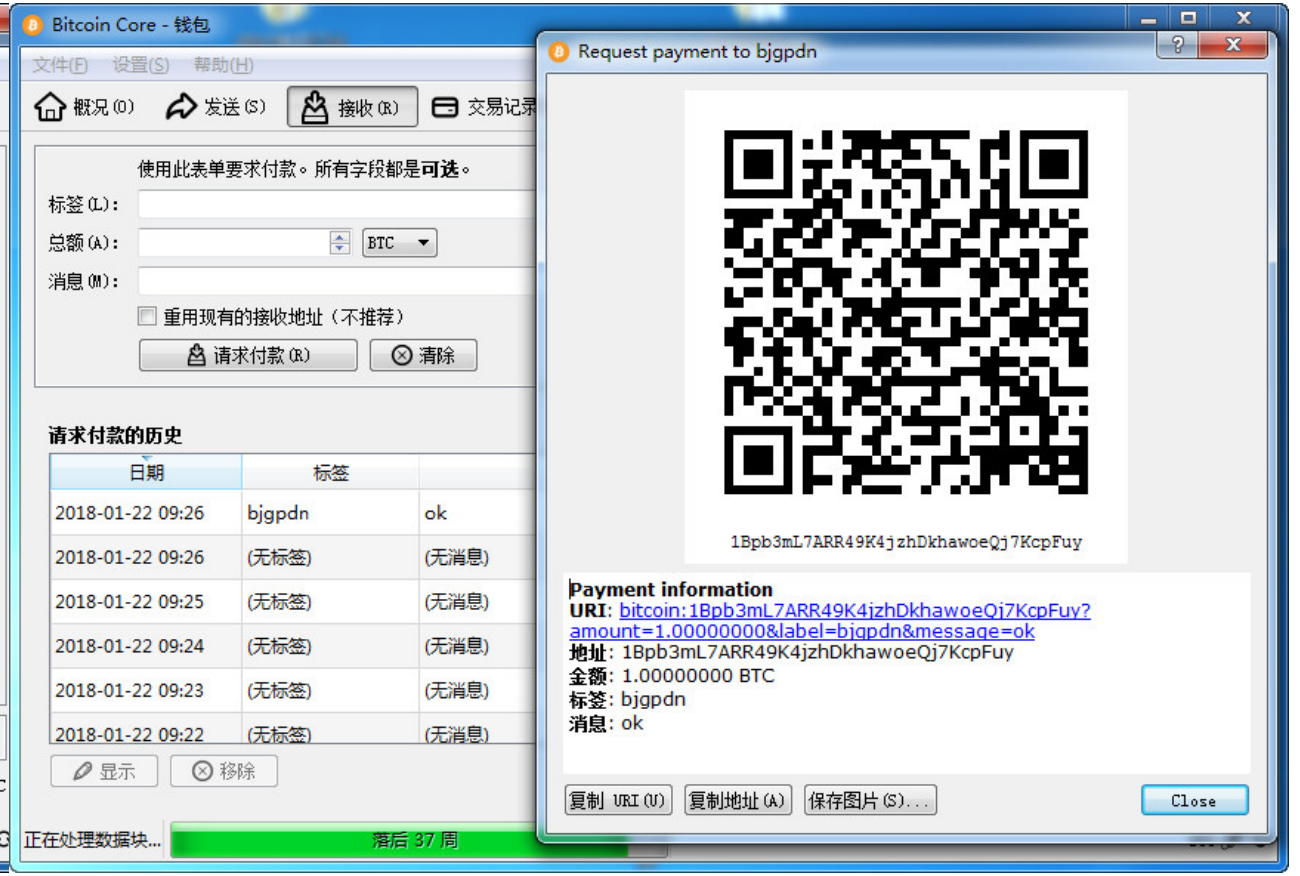


2.1 比特币运行机制 - 钱包 - 不可篡改 - 可追溯



2.1 比特币运行机制 - 交易透明 - 双方匿名



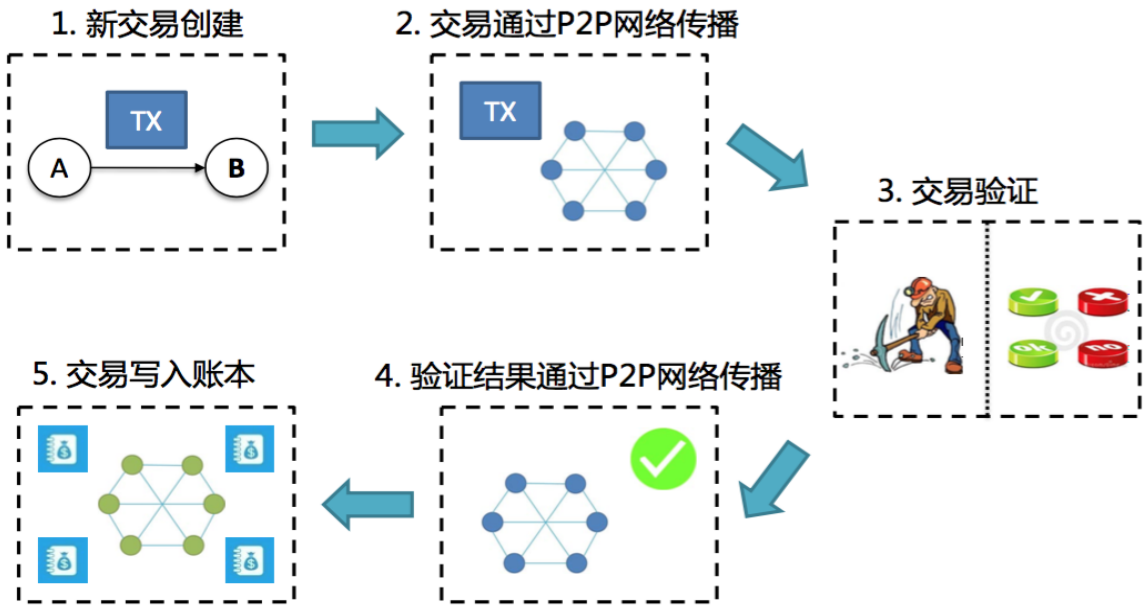


比特币不依靠特定货币机构发行，依据特定算法，通过大量的计算产生—“挖矿”。

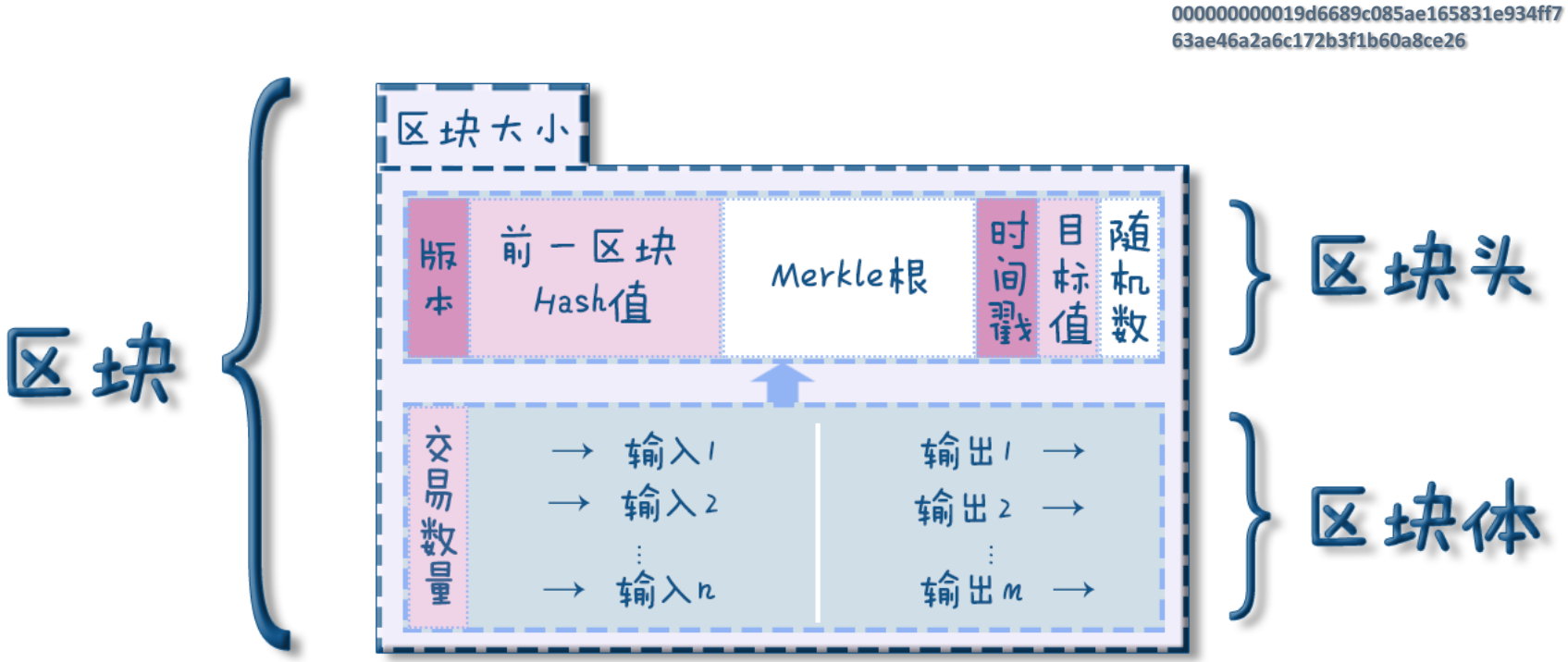
比特币系统使用整个P2P网络中众多节点构成的分布式数据库（区块链）来确认并记录所有的交易行为，并使用密码学的设计来确保货币流通各个环节安全性。

比特币与其他虚拟货币最大的不同，是其总数量非常有限，具有极强的稀缺性。一开始每个区块产生50个比特币,后来每4年减半,直到逼近为零，之后的总数量将被永久限制在2100万个。

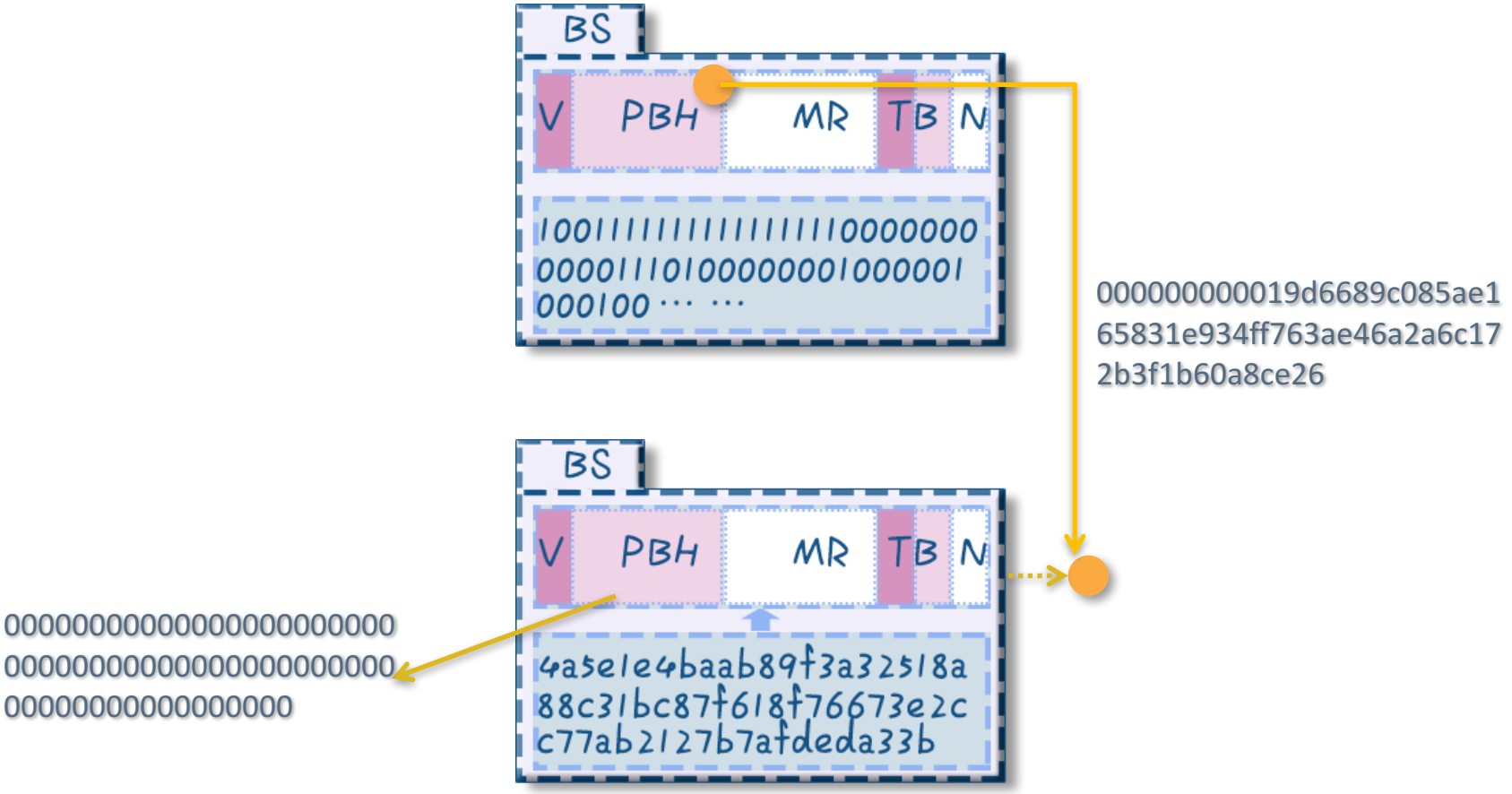
交易：填充订单的过程。


1. 新交易创建
TX
A
B
2. 交易通过P2P网络传播
TX
3. 交易验证
4. 验证结果通过P2P网络传播
5. 交易写入账本

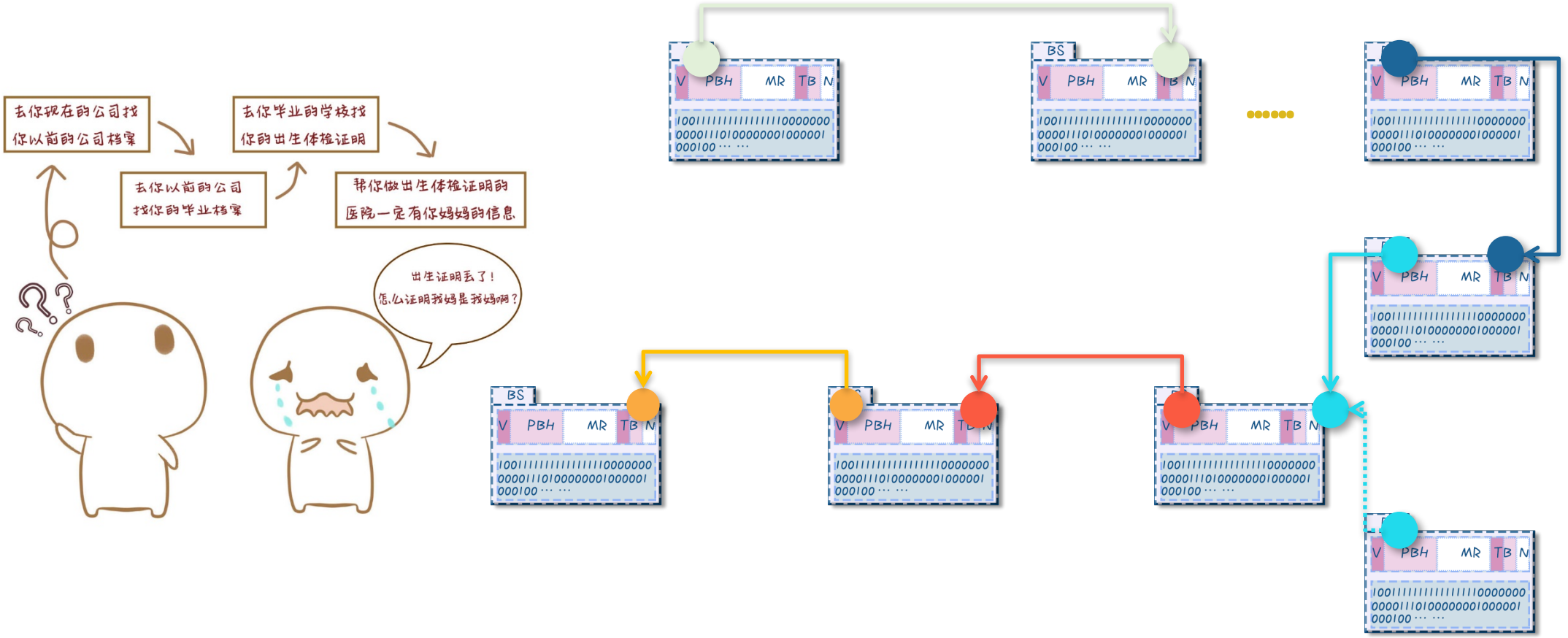
比特币系统存储的基本单元是区块，区块的标识是区块（头）的哈希值。



区块采用链式结构


BS
V
PBH
MR
TB
N
1001111111111111111110000000
00001110100000001000001
000100 … …
000000000019d6689c085ae1
65831e934ff763ae46a2a6c17
2b3f1b60a8ce26
BS
V
PBH
MR
TB
N
4a5e1e4baab89f3a32518a
88c31bc87f618f76673e2c
c77ab2127b7afdeda33b
0000000000000000000000
0000000000000000000000
00000000000000000

新增的区块都知道自己前一个区块（前一行记录）是什么，可以一直追溯到根。



新增交易的时根据前面的记录做校验，保证了区块的内容不容易被篡改。

2.2 比特币运行机制 - 区块数据结构

红亚科技
HONGYAATECH

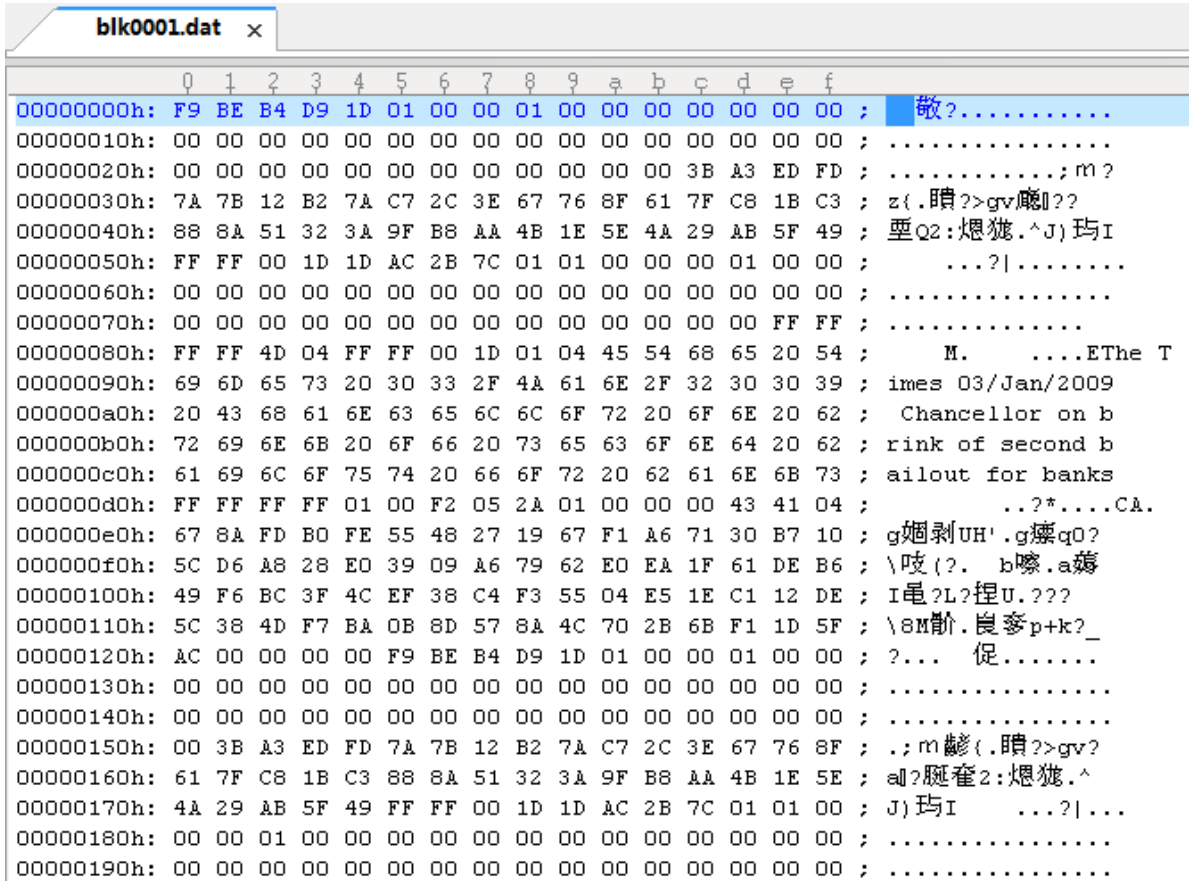
比特币区块数据结构表

比特币区块数据结构思维导图（图片）

比特币区块链数据结构E-R图

用UltraEdit查看创世区块数据

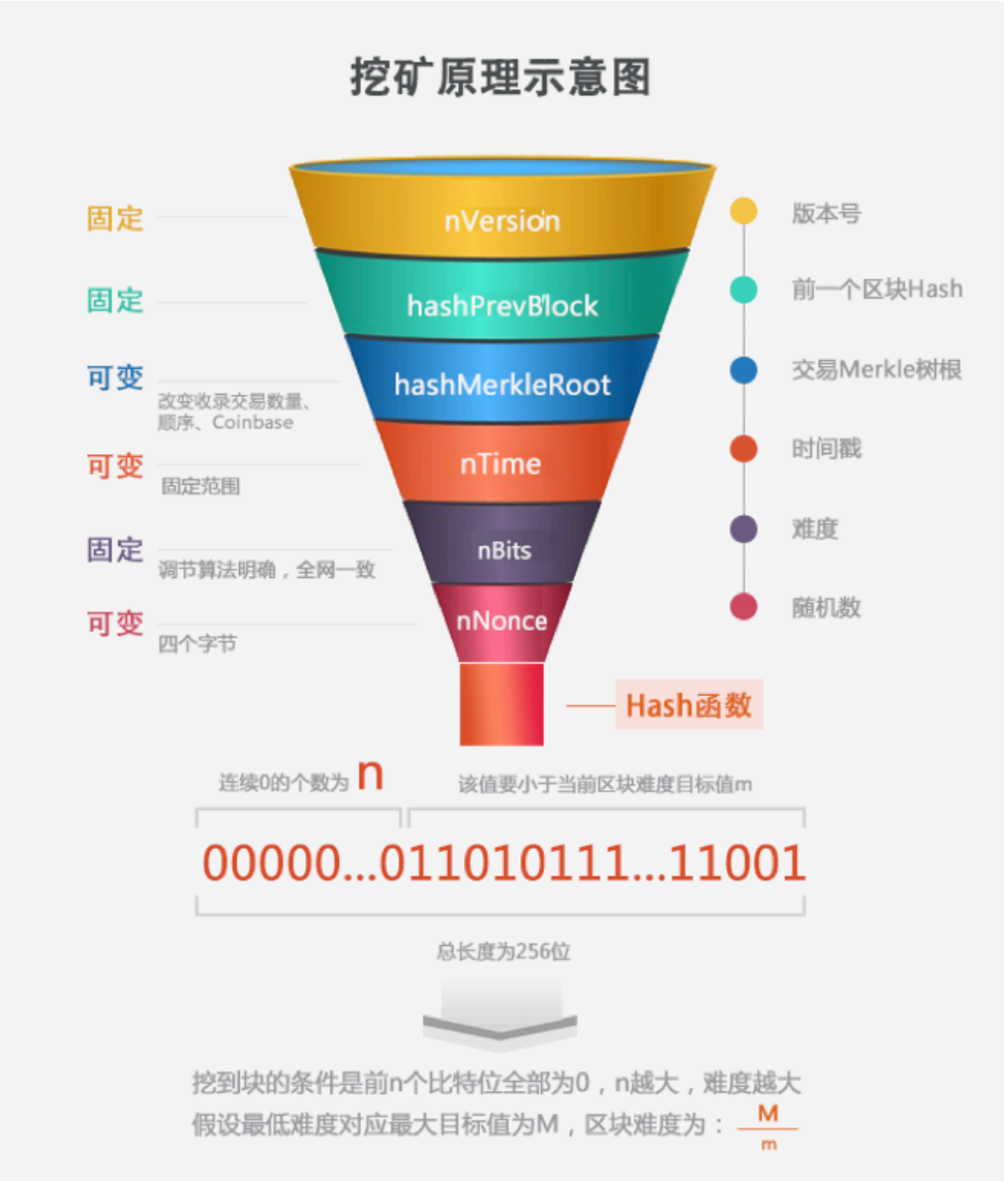
比特币0.1.5源码及UML图



2.2 比特币运行机制 - 挖矿

CPU挖矿 → 显卡挖矿 → 专用芯片矿机 → 矿池

2.2 比特币运行机制 - 挖矿



目 录

CONTENTS

现实问题√

构建诚信社会√

比特币运行机制√

区块链与密码学

区块链：一座类似“94年互联网”的金矿，方兴未艾

国内外金融巨头投身区块链技术的应用和研发

IBM、微软等主流技术公司也全面介入

区块链领域的投资更是呈现出爆发式增长

2016:“区块链元年”；2017:“区块链战略元年”

尴尬现状——概念上大火，实践仍停留在起步阶段

繁华落尽， 2017，将洗尽铅华，从浮躁中抬起头来

区块链技术是金融科技的核心，还被认为是继PC、互联网、社交网络、智能手机之后，人类的第五次计算革命，是下一代价值互联网的基石，为人类社会进入透明、可靠的信用社会打开了大门。

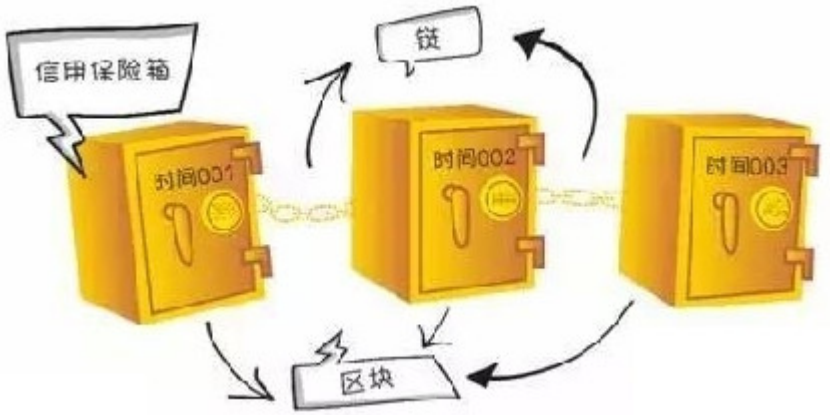
马云曾经说过：“很多人还没有搞清楚什么是PC互联网，移动互联网来了，我们还没有搞清楚移动互联的时候，大数据时代又来了”。

人们还没搞清楚大数据是什么，区块链又来了……

区块链技术将改变世界！我们正站在风口上……

区块链是比特币的底层技术，可应用于其它不同领域

区块链创造了一个“信任机制”，部署在点对点网络中，以密码学为基础，以共识机制为纲要，用一种链式结构存放数据。



在比特币网络中，数据以文件的形式被永久记录，这些记录称之为区块。

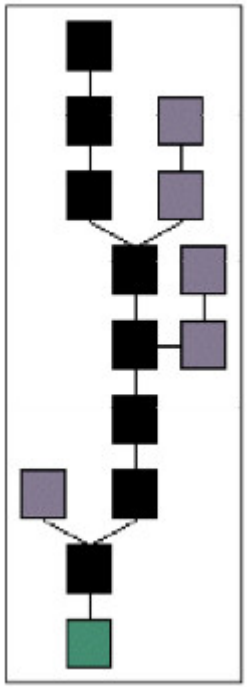
特点：分布式（去中心化）、匿名性（无需信任）、开放性（高度透明）、加密安全性（不可篡改）。

区块链是由一串使用密码学方法产生的、从后向前按时间有序链接起来的数据区块（包含若干交易信息）组成的数据结构。

每个区块都包含了前一区块（父区块）的哈希值(hash)；

区块通过“父区块哈希值”字段引用（指向）父区块；

把每个区块链接到各自父区块的哈希值序列就创建了一条一直可以追溯到第一个区块（创世区块）的链条。



密码学是用来保证信息安全的一种必要的手段。

没有密码就没有信息安全，密码学是信息安全的核心。

什么是信息安全？

信息安全、网络安全、信息与网络安全、网络与信息安全、计算机信息安全、数据安全……，统称：信息安全

属性：机密性、完整性、认证性、不可否认性和可用性

习近平指出：没有网络安全就没有国家安全！

2015.6.11“网络空间安全”国家一级学科获批……

区块链就是用信息安全的技术保障区块链网络、区块链数据的安全。

为了保证存储于区块链中的信息的安全与完整，区块及区块链的定义和构造中使用了包含哈希函数和椭圆曲线公钥密码技术在内的大量现代密码学技术。

同时这些密码学技术也被应用于设计基于工作量证明的共识算法并识别用户。

区块链代表了密码学与安全领域数十年来研究与突破的巅峰！来源于信息安全、反哺信息安全……

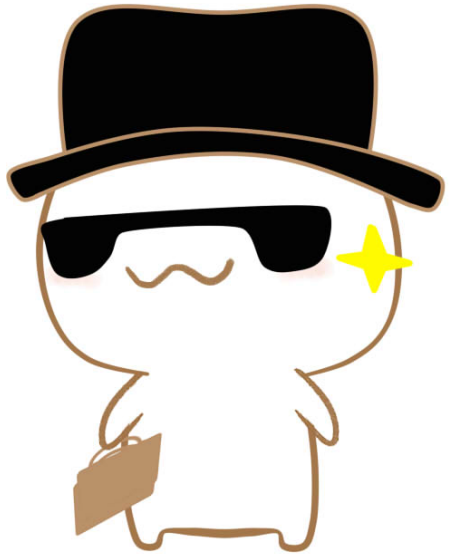
「在区块链的江湖中，每个人都是骗子」

- 江湖多风波，舟楫恐失坠
- 人在江湖飘，哪能不挨刀

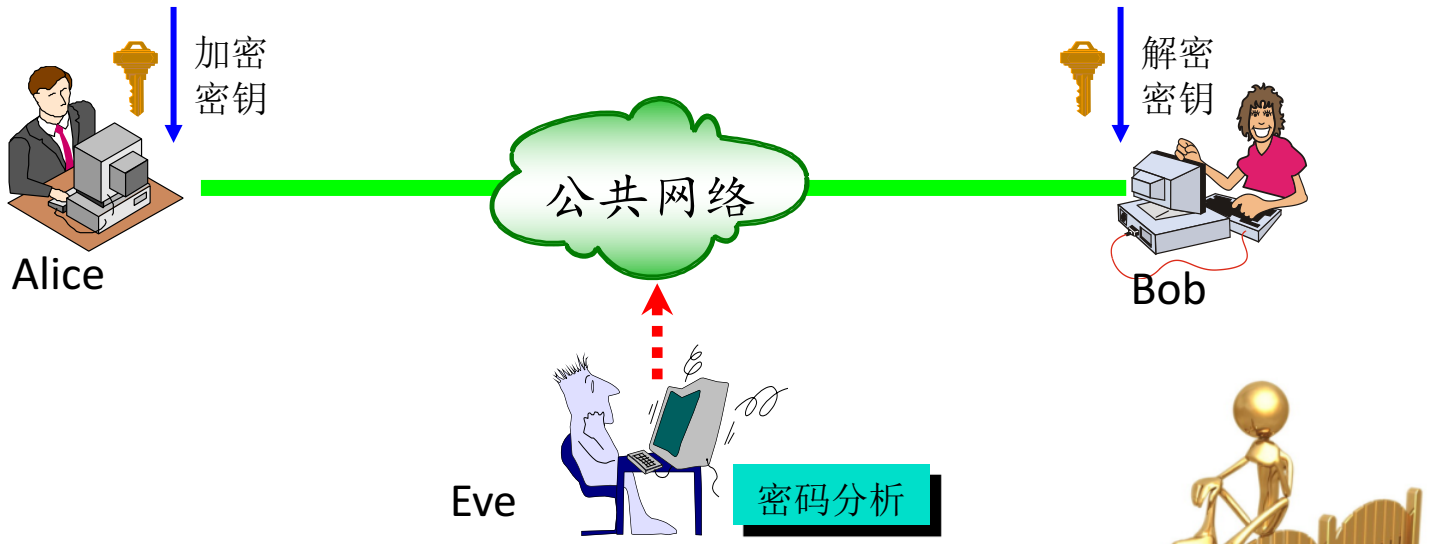
一个人，一口箱子。

一个沉默平凡的人，提着一口陈旧平凡的箱子，在满天夕阳下，默然地走入了长安古城。

——古龙《英雄无泪》



3.3 江湖多风波 - 互联网 + 江湖的攻击 - 窃听

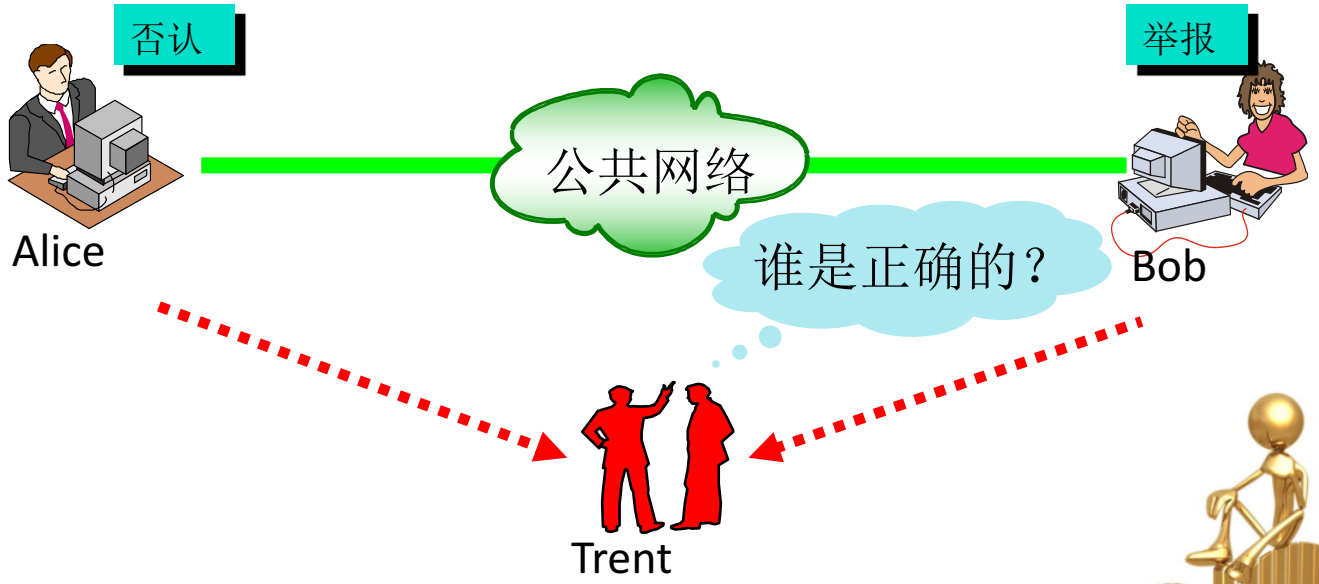


- 受威胁的属性：机密性
- 可应对的技术：加密

3.3 江湖多风波 - 互联网 + 江湖的攻击 - 篡改

- 受威胁的属性：完整性
- 可应对的技术：哈希函数

- 受威胁的属性：认证性
- 可应对的技术：消息认证（哈希函数）



- 受威胁的属性：不可否认性
- 可应对的技术：数字签名

对称密码

哈希函数（单向散列函数）

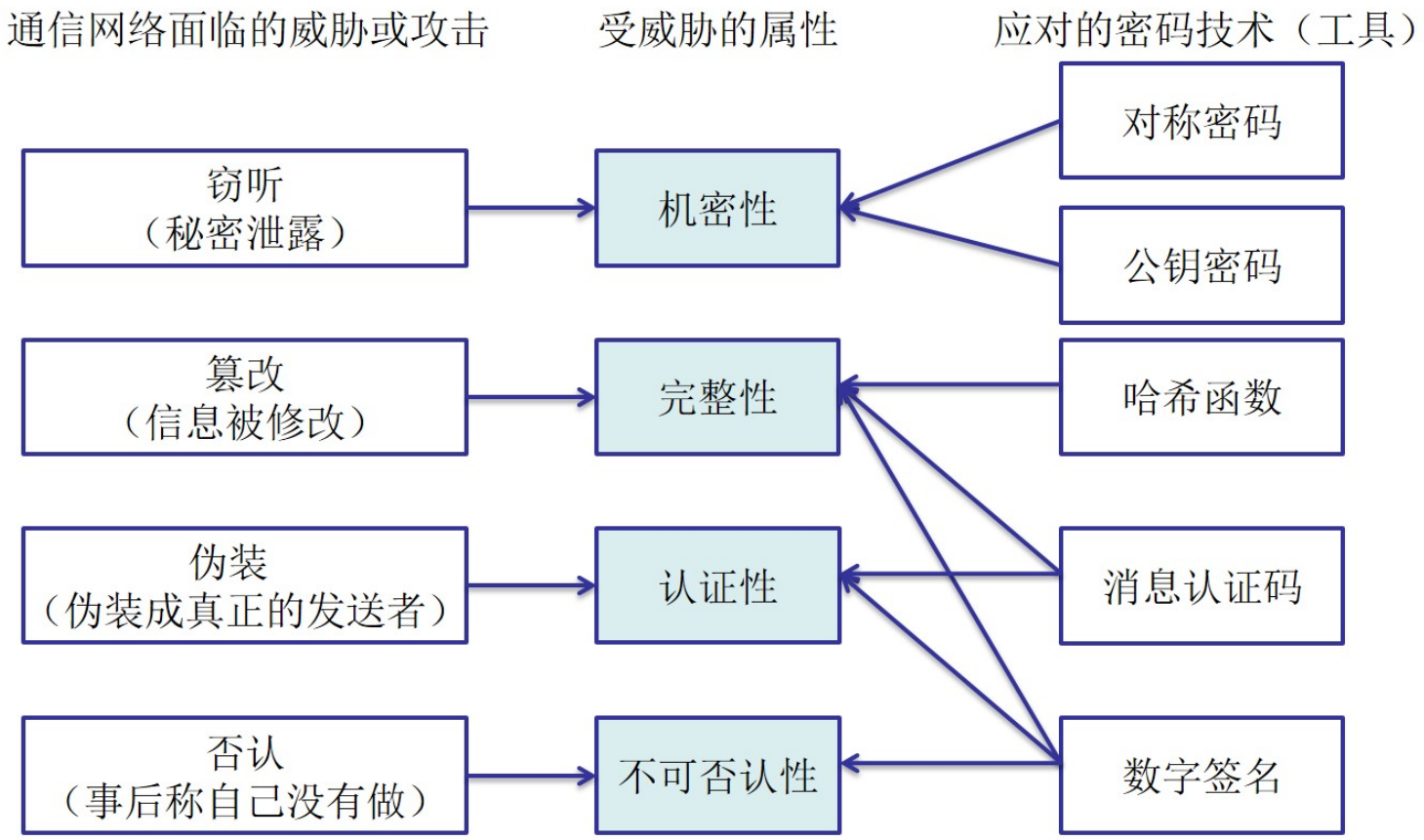
消息认证码

公钥密码

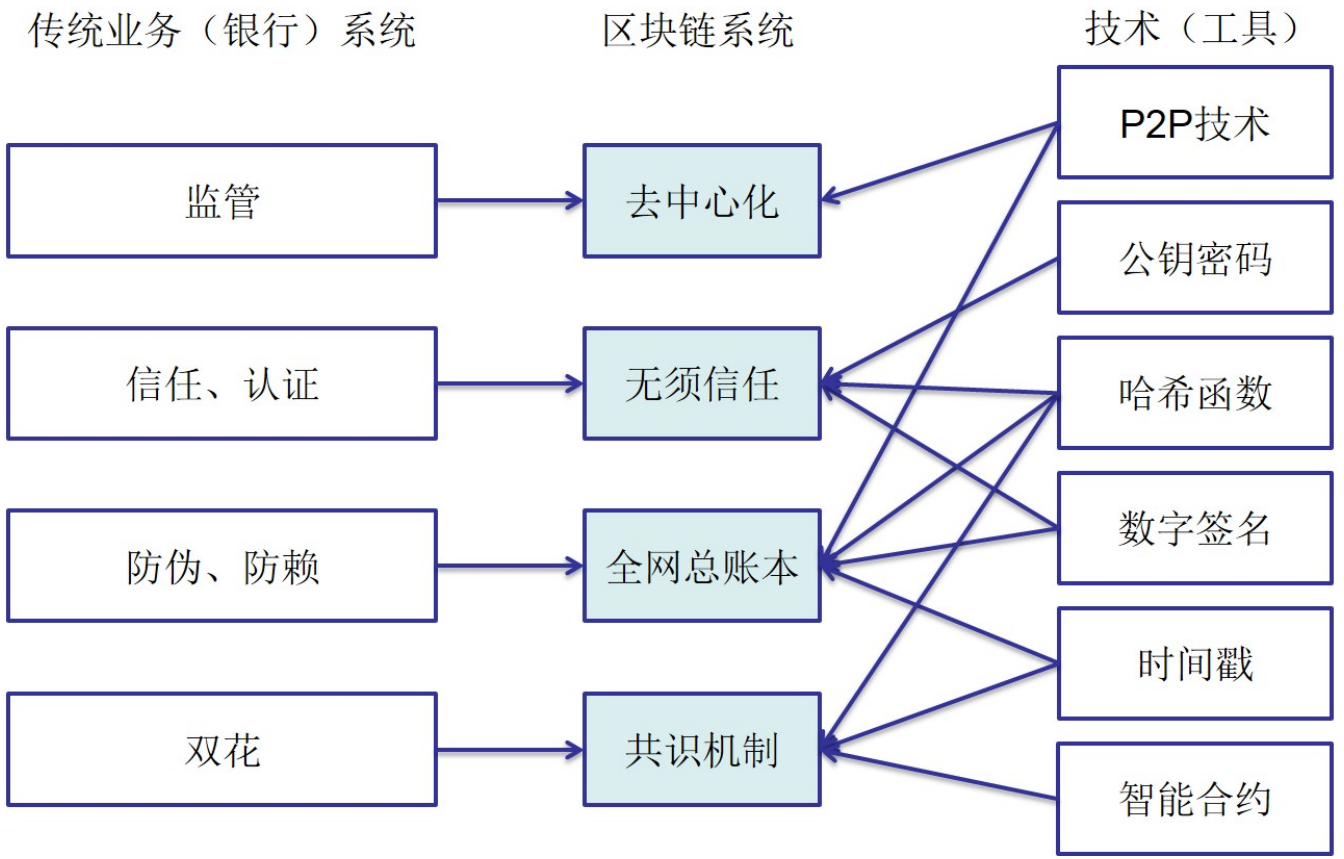
数字签名

伪随机数生成器

3.3 江湖多风波 - 密码学家的工具箱



3.3 江湖多风波 - 区块链江湖 - 安全工具箱



区块链和分布式账本技术是一种在对等网络环境下，通过透明和可信规则

构建不可伪造、不可篡改和可追溯的块链式数据结构，从而实现和管理可信数据的产生、存取和使用的技术。

与基于单一信用背书实体的传统信任机制不同，区块链的信任机制是多个参与方对透明和可信规则的共同信任、对客观信息技术的信任。

为了增加信任与充分透明，减少甚至完全剔除人的干预，大部分区块链技术平台皆以开源社区的形式存在。

红亚科技
HONGYAATECH

北京红亚华宇科技有限公司（简称：红亚科技），是一家专注于高校信息技术实训教育平台研发的创新型科技公司，公司旗下的信息安全教学平台包括四大安全实训教学系统：网络攻防实训及演练系统、网络攻防靶场实战系统、工控安全实训教学系统，区块链实训教学系统，目前公司的信息安全实训教学系统在国内已经有400多所高校用户，是国内著名的信息安全实训教育科技公司，2016年开始研究区块链，2018年1月率先推出 “红亚太学链”区块链实训教学系统，区块链实训系统涵盖“区块”及“链”的可视化分析与展示、创世区块的生成、P2P网络、交易与脚本、智能合约、“挖矿”等模块，共计100多个实训任务。

网络攻防

网络靶场

工控安全

区块链

红亚科技
HONGYAATECH

THANK YOU VERY MUCH

感谢聆听