



区块链与密码学

何德彪 & 罗敏

武汉大学
国家网络安全学院



1、课程内容

- ① 区块链基本原理；
- ② 区块链系统常用密码算法；
- ③ 区块链系统开发技术

2、教学方式和目的

方式：课堂教学为主

目的：了解和掌握区块链原理、关键密码算法、会设计并实现简单的区块链系统。

3、课程考核

口头报告 + 区块链系统设计

4、成绩计算

口头报告 * 30% + 区块链系统设计 * 70%

5、教材和参考书目

- ① 区块链技术及应用；清华大学出版社出版；华为区块链技术开发团队 著
- ② 区块链技术进阶与实战；人民邮电出版社；蔡亮，李启雷，梁秀波 著
- ③ 可证明安全算法与协议；科学出版社；张华，温巧燕，金正平 著
- ④ 密码学引论（第二版）；武汉大学出版社；张焕国，王张宜 著



第一章、比特币及其原理

何德彪

武汉大学
国家网络安全学院



目 录

- 1.0. 引言
- 1.1. 比特币的诞生
- 1.2. 疯狂的比特币
- 1.3. 比特币的通俗故事
- 1.4. 比特币的交易
- 1.5. 比特币的挖矿
- 1.6. 比特币的分叉
- 1.7. 其它密码货币

目 录

1.0. 引言

1.1. 比特币的诞生

1.2. 疯狂的比特币

1.3. 比特币的通俗故事

1.4. 比特币的交易

1.5. 比特币的挖矿

1.6. 比特币的分叉

1.7. 其它密码货币

1.0 引言

从前，我要付给小明2块钱。



帅气的我



小明

我掏出钞票甩给小明，
并在自己的小本本上记下：
“我给了小明两块钱。”



帅气的我



小明

小明拿到钱，
在自己的小本本上记下：
“小帅给了我一块钱，还欠我一块！”



帅气的我



小明

我去！！账对不上了！
听谁的？？谁在撒谎？？？



你TM在逗我

帅气的我



小明

1.0 引言

银行出场!



第三方支付：或者找我也行哦!

既然你们都信任我，这帐就由我来记吧！
保证账目不会偏袒不会出错



帅气的我



小明

1.0 引言

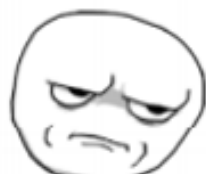
不过这手续费可不能不交



而且万一发生储户存款丢失、
票据变报纸这种事情，人家也
不想的啦



手续费我可以少收，不过要
用你们的大数据变现嘿嘿嘿



你TM在逗我
帅气的我



小明

1.0 引言

去中介！踢开银行、第三方支付



真是个好办法



我们按照区块链的规则，
约法三章



帅气的我



小明

①每次交易，咱俩中间只能有一个人记账；具体谁来记，咱们石头剪刀布（工作量证明）

如果一笔交易两个人都记账，很容易记岔掉；
如果每次都是一个人记账，这个人权力太大，容易腐化堕落；
石头剪刀布最好啦，每次记账人都是随机的，公平！



帅气的我



小明

*实际区块链运转机制中用的当然不是石头剪刀布，而是让全网节点比赛，看谁先算出一个前x位都是0的随机数。谁就获得记账权。这也太难了！举个例子，整个比特币网络要10分钟才能找出一个前10位都是0的随机数。所以，可以确保同时只有一个节点记账。

②甭管谁记账，另一个人必须原封不动照抄一遍，放进自己的账本（全网同步备份）

把我们形成共识的记录在全网每一个角落备份，一方面可以保证数据不会遗失，另一方面也可以对抗篡改



帅气的我



小明

*说是照抄一遍，其实交易内容是可以加密的。虽然密文全网同步备份，没有对应的私钥还是看不到内容——确保数据私密性和安全性。

③记完账后，在字迹上盖个印章，这样只要印章完好无损，就说明后来字迹没有被篡改过（Merkel根）

这样一来，一旦账本记好，就不能编辑了，避免了被人篡改



帅气的我



小明

*这个“印章”是比喻区块正文的对应hash（叫做Merkel根），只要正文被篡改哪怕一丁点儿，hash就会变得完全不一样，“大家”也就知道正文被篡改了。于是这种篡改内容就会被整个区块链系统无情地抛弃。

1.0 引言

利用对等网络和密码技术实现的密码货币系统，
交易账单**不可逆**，**不可伪造**，**不可否认**，**可验证**。



1.0 引言



图1.0. 区块链应用范围示意图, 消息来源: 百度图库

目 录

- 1.0. 引言
- 1.1. 比特币的诞生
- 1.2. 疯狂的比特币
- 1.3. 比特币的通俗故事
- 1.4. 比特币的交易
- 1.5. 比特币的挖矿
- 1.6. 比特币的分叉
- 1.7. 其它密码货币

1.1 比特币的诞生

2008年11月,一位化名为中本聪(Satoshi Nakamoto)的人,在密码学论坛 metzdowd.com 发表的一篇名为 *Bitcoin: A Peer-to-Peer Electronic Cash System*(《比特币:一种点对点的电子现金系统》)的论文中首先提出了比特币。2009年1月3日,中本聪发布了比特币系统并挖掘出

第一个区块,被称为“创世区块”,最初的50个比特币宣告问世。同时有趣的是,中本聪在创世区块中带上了一句话以证明这个区块挖出于2009年1月3日,这句话就是图 中的《泰晤士报》2009年1月3日的头版新闻标题——*Chancellor on brink of second bailout for banks*(《财政大臣正处于第二次救助银行之际》)。

1.1 比特币的诞生



图1.1. 2009年1月3日泰晤士报

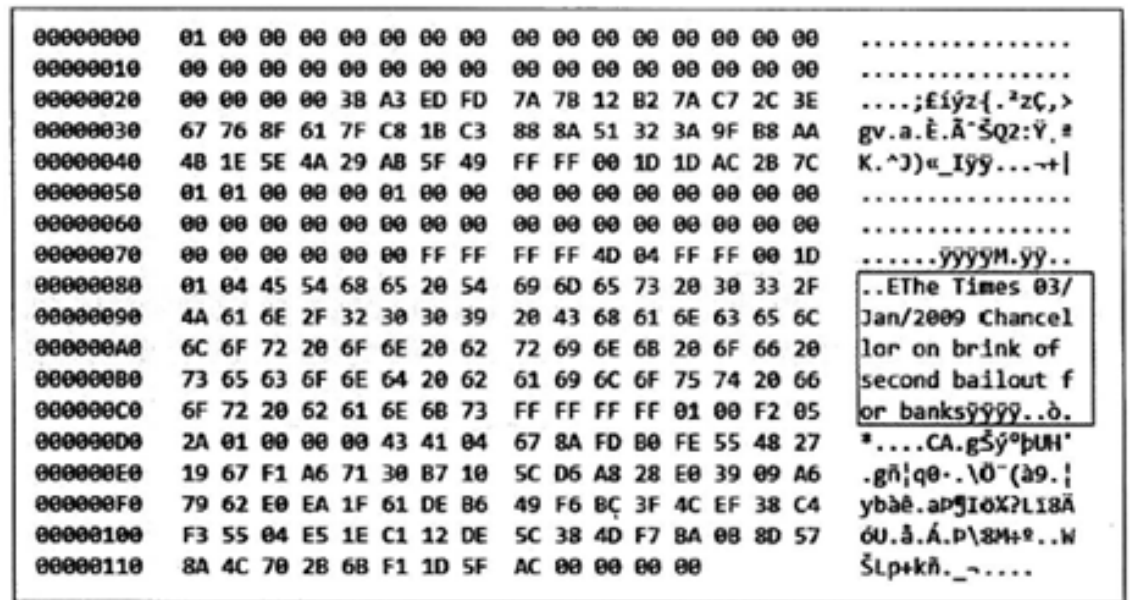


图1.2. 比特币的创始块

1.1 比特币的诞生

截至 2018 年,比特币系统已经运行了整整十年。比特币系统软件全部开源,系统本身分布在全球各地,无中央管理服务器,无任何负责的主体,无外部信用背书。在比特币运行期间,有大量黑客无数次尝试攻克比特币系统,然而神奇的是,这样一个“三无”系统,近十年来一直都在稳定运行,没有发生过重大事故。这一点无疑展示了比特币系统背后技术的完备性和可靠性。近年来,随着比特币的风靡全球,越来越多的人对其背后的区块链技术进行探索和发展,希望将这样一个去中心化的稳定系统应用到各类企业应用之中。

除了其背后的技术所具有的价值,比特币作为一种虚拟货币,也逐渐与现实世界的法币建立起了“兑换”关系,其本身有了狭义的“价格”。

1.1 比特币的诞生

2010年5月22日,美国佛罗里达州程序设计员拉斯洛·豪涅茨(Laszlo Hanyecz)用1万个比特币,换回了比萨零售店棒约翰(Papa Johns)的一个价值25美元的比萨。

比萨日: $10000 \text{ 个} * 69035 \text{ 元/个} = 690350000$ (六亿九千零三十五万) 元

备注: 价格取自2020年2月21日21:35

目 录

- 1.0. 引言
- 1.1. 比特币的诞生
- 1.2. 疯狂的比特币
- 1.3. 比特币的通俗故事
- 1.4. 比特币的交易
- 1.5. 比特币的挖矿
- 1.6. 比特币的分叉
- 1.7. 其它密码货币

1.2 疯狂的比特币

1.2.1. 疯狂的比特币价格

在 2011 年 1 月,1 个比特币还不值 30 美分,但在随后的几个月里,它的价格一路走高,突破了 1 美元,很快上升到 8 美元,然后是 20 美元。到 2011 年 6 月 9 日,1 个比特币的价格已经涨到了 29.55 美元,半年时间涨幅约为 100 倍。但是随后不久,比特币交易平台 Mt. Gox 由于其交易平台本身的漏洞被黑客攻击,使平台本身和其用户蒙受了较大的损失,比特币的安全性受到了投资者们的质疑。因为该事件,比特币价格持续走低,急剧回落,在仅仅半年时间后的 2011 年 11 月,比特币的价格已经低至 2 美元,相比 6 月份的最高价跌去了 90% 以上。

2012 年 12 月 6 日,世界首家比特币交易所在法国诞生,比特币单价重回巅峰期,单枚涨至 13.69 美元。

1.2 疯狂的比特币

1.2.1. 疯狂的比特币价格

2017 年是比特币发展史上十分重要的一年,全年整体涨幅高达 1 700%。2017 年一整年,比特币价格走势犹如一轮过山车,暴增暴跌让投资者为之疯狂。在 2017 年全年,比特币最低价格是 789 美元,对应日期为 1 月 11 日;最高价位为 19 142 美元,对应日期是 12 月 18 日。

9 月,我国发布《关于防范代币发行融资风险的公告》,国内市场热度渐渐消退,但在全球市场上,日本和韩国比特币投资者持续涌入,比特币价格一路高涨,12 月 18 日触及历史峰值。然而随后迅速开始暴跌,12 月 31 日封盘价跌破 11 000 美元。

1.2 疯狂的比特币

1.2.1. 疯狂的比特币价格

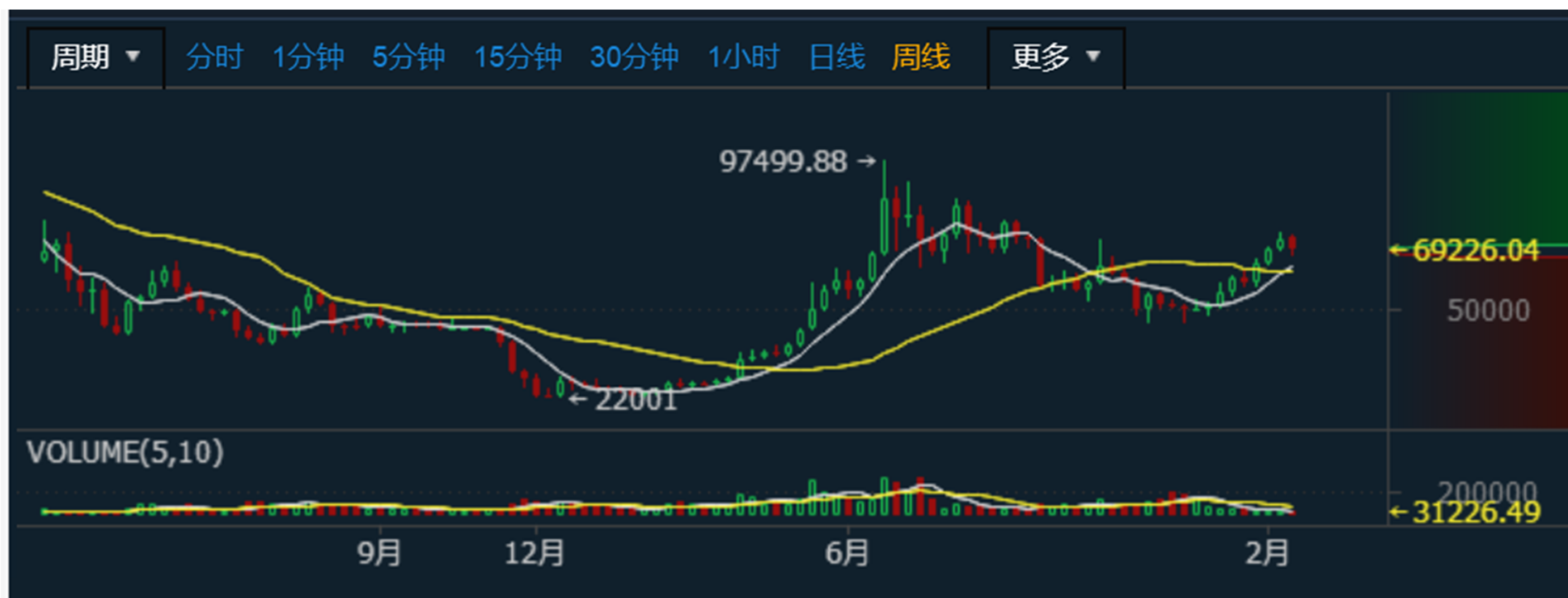


图1.3. 2019年3月7日到2020年2月15日比特币价格走势图
来源: https://www.zb.live/trade/kline/btc_qc

1.2 疯狂的比特币

1.2.2. 疯狂的矿机和芯片

在比特币疯狂的价格和犹如过山车般的价格波动吸引了越来越多投机者的同时,比特币矿机及芯片技术也取得了长足进展。**所谓比特币“矿机”,就是用于赚取比特币的计算机。**用户下载专用的比特币运算软件,在矿机上运行相应的软件,参与记账并获取对应的记账奖励。

从比特币诞生以来,比特币挖矿经历了CPU挖矿-GPU挖矿-专业矿机挖矿几个阶段:

➤ **第一阶段（挖矿初期）——主要依靠CPU**

在比特币发展初期的挖矿难度较小,因此大部分个人PC直接挖矿的收益都大于功耗。



图1.4. CPU图片

1.2 疯狂的比特币

1.2.2. 疯狂的矿机和芯片

➤ 第二阶段（挖矿中期）——主要依靠GPU

随着全网挖矿难度的不断增加，另外，随着比特币价格的疯涨，于是较高端的显卡组装的挖矿设备就诞生了.在其中的一段时间，比特币5天之内从0.008美元涨到了0.08美元，到2010年10月的时候，比特币的价格已经涨到了0.15美元.GPU挖矿时代从此开始了.

- ✓ 2010年7月18日，一个名叫ArtForz的矿工，第一个实现了用个人的 OpenCL GPU 挖矿.
- ✓ 2010年12月，Marek Palatinus创建了第一个矿池slusHPOOL，史称“泥潭”.
- ✓ 2011年1月3日：比特币两周年之际，GPU的算力达到了120MH/S，矿池的算力则达到10GH/S.



图1.5. GPU图片

1.2 疯狂的比特币

1.2.2. 疯狂的矿机和芯片

➤ 第三阶段（挖矿后期）——主要依靠专业矿机(FPGA、ASIC)

2013年年初，南瓜张研发了第一台FPGA矿机——南瓜机，开启了FPGA挖矿的新纪元.ASIC芯片也开始不断迭代，从110nm到55nm，从55nm到28nm，从28nm到16nm，再到7nm.出现了烤猫、阿瓦隆、鸽子、比特大陆等矿机公司.

- ✓ 2013年6月，烤猫推出现货USB矿机.
- ✓ 2014年8月，烤猫推出Tube矿机，算力：850GH/S，功率：900W.
- ✓ 2016年6月，比特大陆推出蚂蚁矿机S9，算力14TH/S.
- ✓ 2018年8月，嘉楠耘智宣布全球首个7纳米挖矿芯片成功量产，并应用于阿瓦隆A9系列矿机.
- ✓ 2019年11月21日晚，嘉楠耘智正式在纳斯达克上市，成为“全球区块链第一股”，是国内首家赴美上市的矿机企业.



图1.6. 专业矿机图片

1.2 疯狂的比特币

1.2.3. 疯狂的矿场和矿池

随着比特币价格的震荡式飙升,人们仿佛像美国西部刚刚发现金矿一样,纷纷投入“挖矿”的事业之中。由于比特币的产生速率基本保持稳定,但对于单个节点来说,其挖到某个比特币的概率与其算力占有所有参与挖矿竞争节点总算力的比例成正比,因此,随着参与到比特币挖矿竞争中的机器及算力大幅上升,单个节点或少量的算力能够成功挖到比特币的概率急剧下降,小规模挖矿参与者的收益难以得到保障,因此两种不同的组织相继登场,分别是矿场和矿池,它们的目的都是集中算力,提升挖矿概率,从而提升收益。

矿场是将挖矿产业化的产物。简单来说,矿场即为挖矿设备管理场所。早期的矿场非常简单,只有一些简单的机架供矿机的安置,同时仅提供简单的网络、电力等资源。

1.2 疯狂的比特币

1.2.3. 疯狂的矿场和矿池

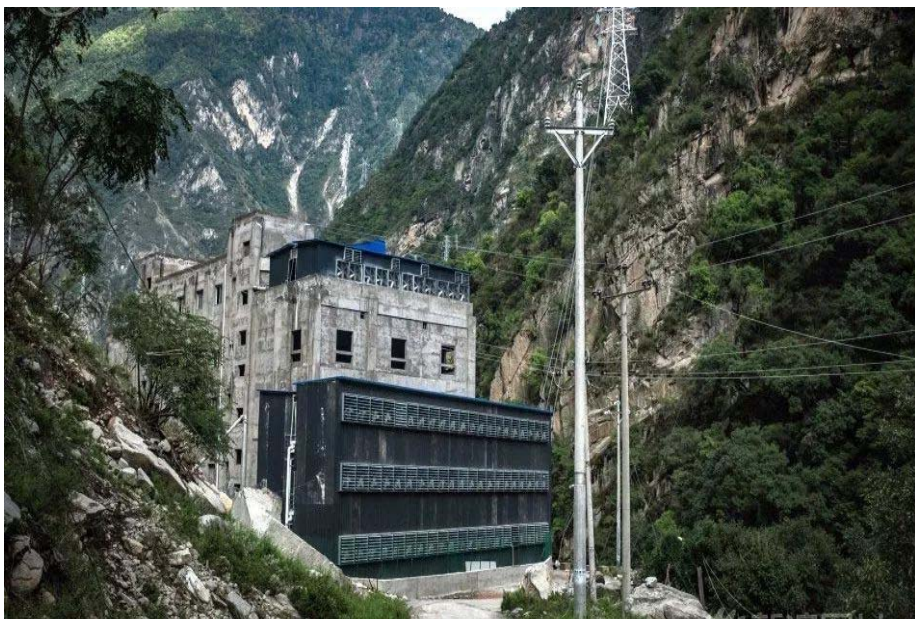


图1.7. 矿场外部图片



图1.8. 矿场内部图片

1.2 疯狂的比特币

1.2.3. 疯狂的矿场和矿池

除了矿场这种产业化的挖矿方式,还有一种将大量算力较低设备进行联合、共同运作挖矿的平台,即“矿池(Mining Pool)”,加入“矿池”的设备即被称作“矿工”。在“矿池”中,不论“矿工”所能提供的运算力的多寡,只要是通过加入矿池来参与挖矿活动,无论是否成功挖掘出有效区块,在该矿池挖矿成功后皆可经由对矿池的贡献(即投入的算力)来获得比特币奖励。亦即多人合作挖矿,获得的比特币奖励也由多人依照贡献度分享。这种组织方式实际上并没有提高单个矿工挖矿收益的期望值,但提升了单个矿工收益的稳定性。

截至2018年10月,根据BTC.com的分析,如图 所示,排名前六的比特币矿池占据整体比特币挖矿算力61.4%的份额,分别是BTC.com(占比17.4%)、蚂蚁矿池(antpool, 15.3%)、ViaBTC(12.6%)、SlushPool(11.9%)、BTC.TOP(10.6%)、F2Pool(9.6%)。世界上

1.2 疯狂的比特币

1.2.3. 疯狂的矿场和矿池

最大的比特币矿池是蚂蚁矿池,算力达到惊人的 2 500PH/s,如果将超级计算机“天河二号”每秒 33P FLOPS(Peta FLOPS)的计算能力换算成哈希计算的话,大约是蚂蚁矿池的千分之一

注: 1PH/s是每秒1 000 000 000 000 000次哈希运算

在 2012 年,矿池总算力之和已经接近比特币总算力的一半。近几年,矿池更是逐渐成为算力的主力,算力呈现集中化趋势。然而,这种集中化的趋势会带来一些弊端。由于在比特币世界中,算力高即代表着产生记账区块的概率高,即代表着“记账权”更强。如果矿池算力不断提升,单家矿池算力达到 50% 以上,即可以对比特币进行 51% 攻击,对比特币系统的开采权和记账权进行垄断。

1.2 疯狂的比特币

1.2.3. 疯狂的矿场和矿池

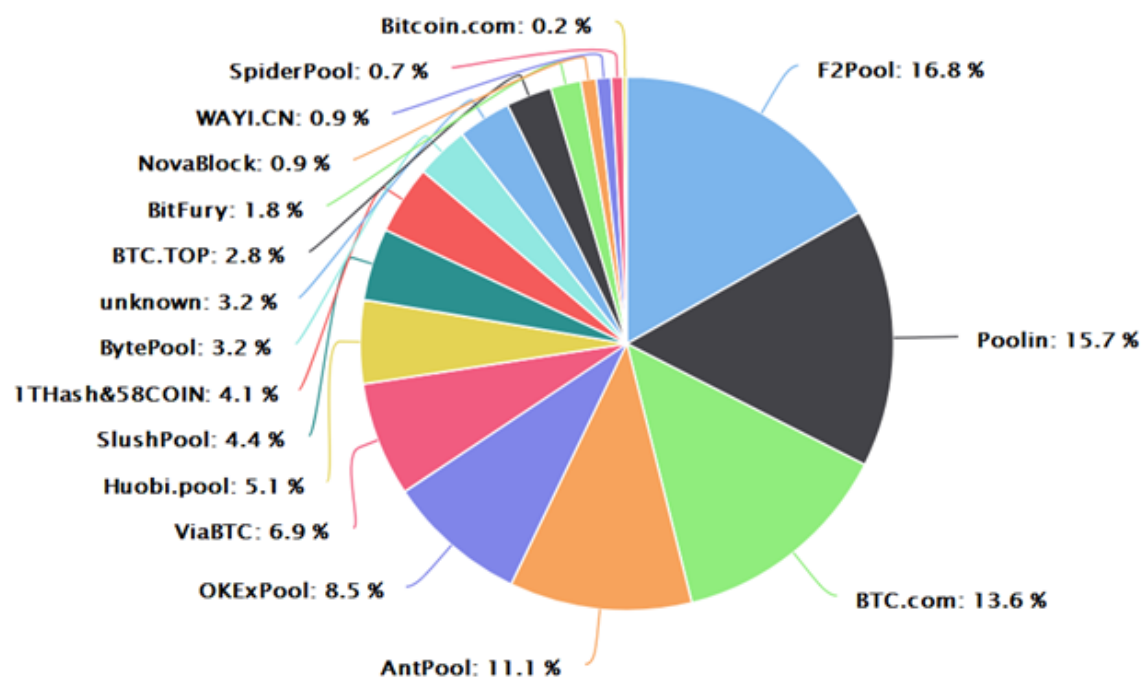


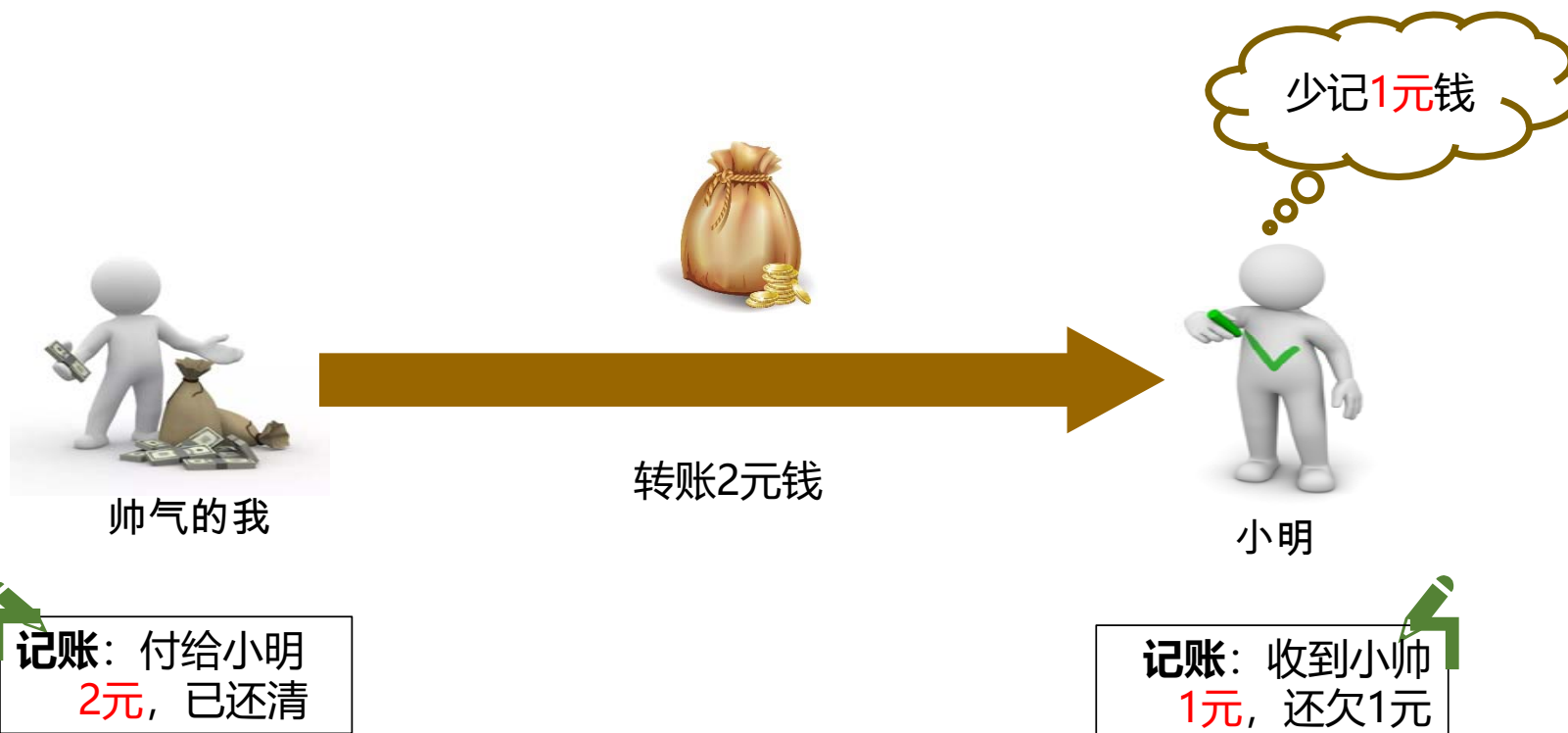
图1.9. 比特币矿池算力分布饼图 (2020年2月21日)

数据来源: <https://btc.com>

目 录

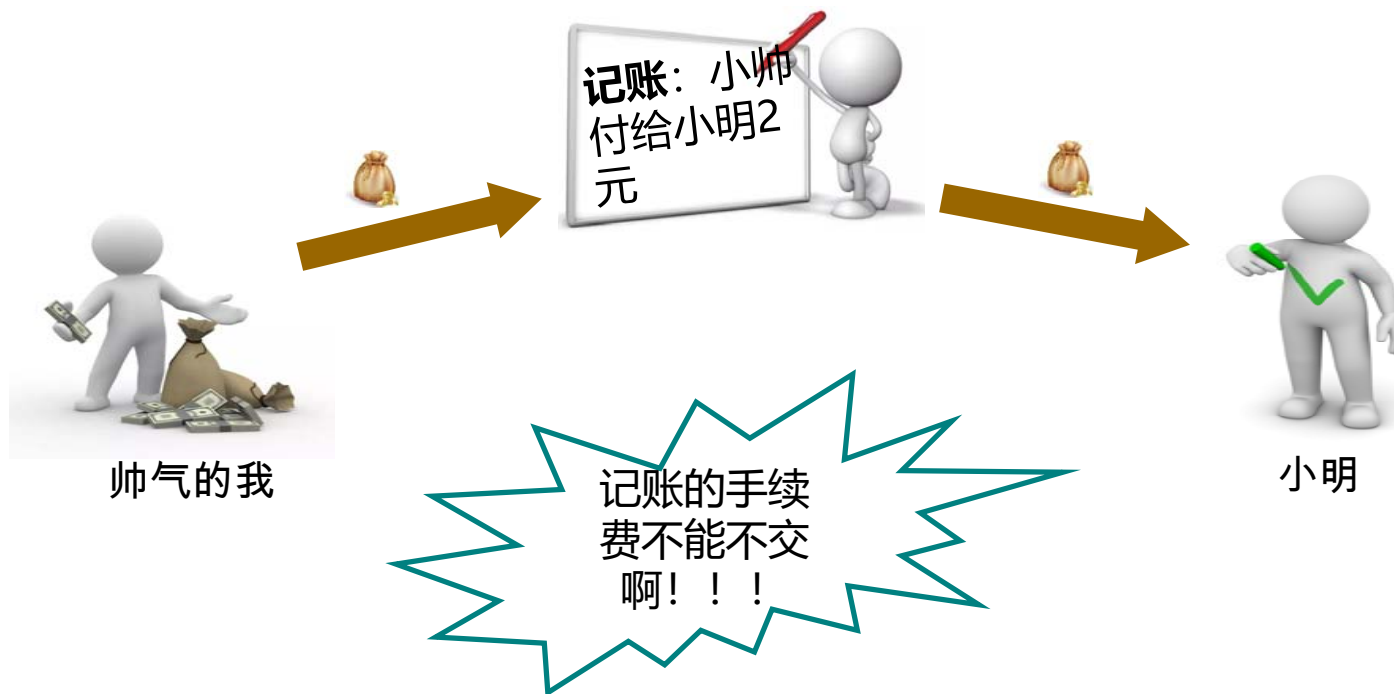
- 1.0. 引言
- 1.1. 比特币的诞生
- 1.2. 疯狂的比特币
- 1.3. 比特币的通俗故事
- 1.4. 比特币的交易
- 1.5. 比特币的挖矿
- 1.6. 比特币的分叉
- 1.7. 其它密码货币

1.3 比特币通俗的故事

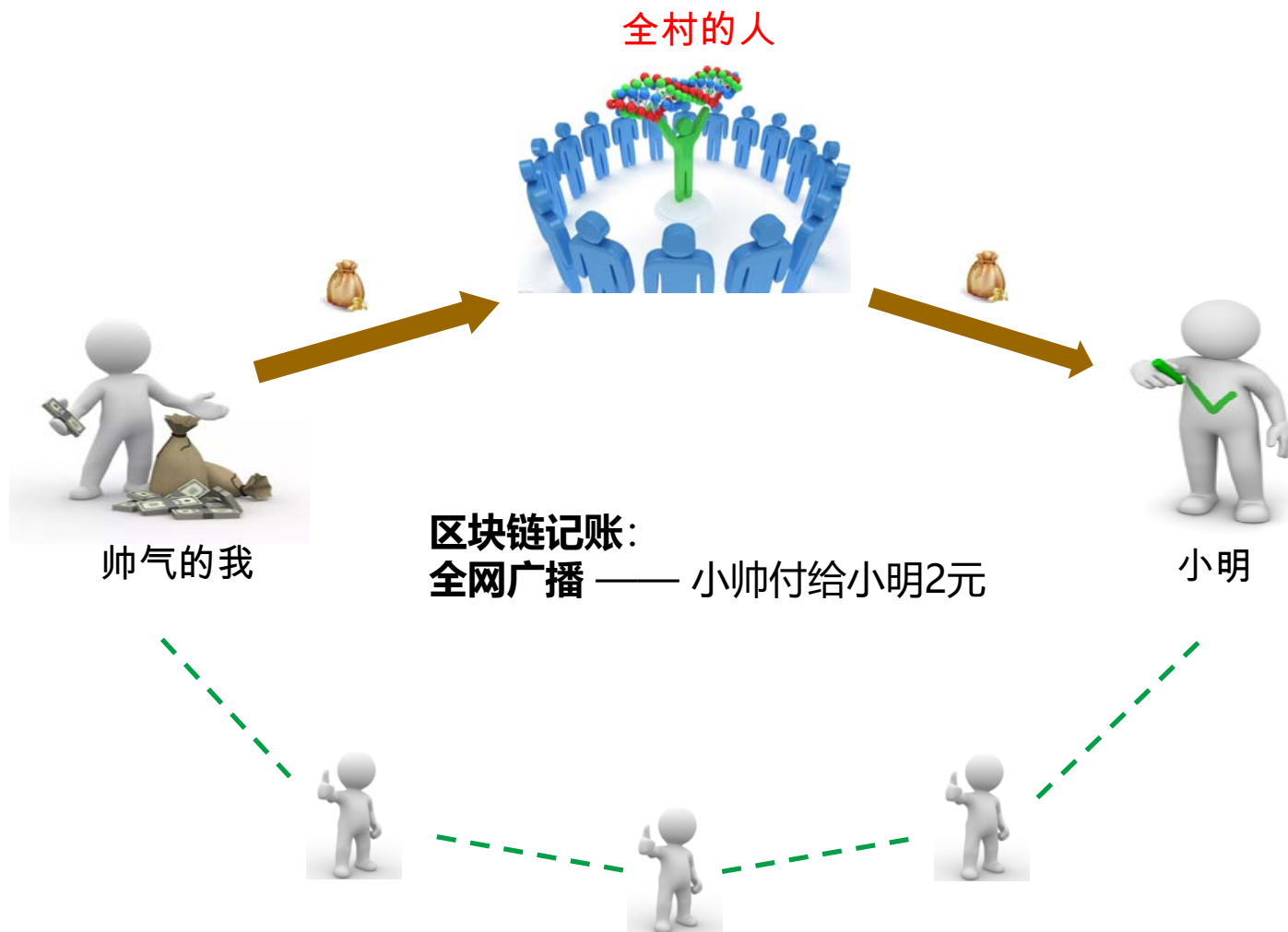


1.3 比特币通俗的故事

银行、微信、支付宝...



1.3 比特币通俗的故事



1.3 比特币通俗的故事

故事到此并未结束,由此引出了三个值得思考的问题。

(1) 记的账在后面会不会被篡改?

(2) 村民有什么动力帮别人记账?

(3) 这么多人记账,万一记的不一致岂不是坏了,以谁记的为准?

比特币系统巧妙地解决了这三个问题。

第一,比特币采用两种策略保证账本不可篡改:①人人记账。人人手上都维护一本账本,这样即使某个人改了自己的账本,他也无权修改其他村民手上的账本,修改自己的账本相当于“掩耳盗铃”,别人是不会认可的。②采用“区块+链”的特殊账本结构。在这种账本结构中,每一个区块保存着某段时间内所发生的交易,这些区块通过链式结构连接在一起,形成了一个记录全部交易的完整账本。如果对区块内容进行了修改就会破坏整个区块链的链式结构,导致链条断了,从而很容易被检测到,这两个策略保证了从全局来看整个账本是不可篡改的。

1.3 比特币通俗的故事

第二,前面一条中提到了人人参与记账,大家肯定会问“凭啥要我帮别人记账呢”。这就涉及比特币系统中的激励机制。参与记账的村民,被称为“矿工”。这些矿工中,首个记账被认可的人:①将获得一笔奖励,这笔奖励就是若干个比特币,这也是比特币发行的唯一来源,这种奖励措施使众多矿工积极参加记账;②谁在某一块账本被认可,其他人都会分别拷贝这一块账本,从而保证所有人维护的账本是完全一致的。这两点保证了区块链的自动安全运行。

第三,既然有了激励,大家就会争抢着记账并努力让自己的记账被认可,怎么确定以谁记的为准呢?为了能够确定以谁记的账为准,村民们想到了一个公平的办法:对每一块账本(类比为我们现实账本上的一页),他们从题库中找了一道难题,让所有参与记账的“矿工”都去破解这道难题,谁若最先破解了,该页/块就以他记的账为准。这个破解难题的过程,就被称为“挖矿”,也即工作量证明的过程。这里需要说明的是,这个难题的解题过程需要不断地尝试,较为困难,但是找到答案发给别人后,别人是很容易验证的。

1.3 比特币通俗的故事

因此,比特币通过“区块+链”的分布式账本保障了交易的不可篡改,通过发放比特币的激励措施激励了“矿工”的参与,通过计算难题(矿工挖矿)解决了记账一致性的问题。这样,完美地形成了一个不依赖任何中间人即可完成记账的自动运行系统。

要对比特币交易进行介绍,我们首先要了解比特币地址的概念。要参与比特币系统中的交易过程,需要一个类似于现实世界中银行“账户”的实体。

比特币交易即为从一个比特币地址向另一个比特币地址进行转账的过程,每个交易可能会包含多笔转账。

目 录

- 1.0. 引言
- 1.1. 比特币的诞生
- 1.2. 疯狂的比特币
- 1.3. 比特币的通俗故事
- 1.4. 比特币的交易
- 1.5. 比特币的挖矿
- 1.6. 比特币的分叉
- 1.7. 其它密码货币

1.4 比特币的交易

比特币交易有两种类型,一种是 Coinbase 交易,也就是挖矿奖励的比特币,这种交易没有发送人。另一种就是我们常见的普通交易了,即普通地址之间的转账交易。

BLOCKCHAIN.COM				Products	Data	Explorer	Q	Login	Sign Up
Hash	2d315e81b8509d7ee75d45b569a35f9ed52b5564331bba2785bb9...								2020-02-22 12:52
	COINBASE (Newly Generated Coins)					➔	1MUz4VMYui5qY1mxUiG8BQ1Luv6tqkvail	12.51381406 BTC	
							OP_RETURN	0.00000000 BTC	
							OP_RETURN	0.00000000 BTC	
							OP_RETURN	0.00000000 BTC	
Fee	0.00000000 BTC (0.000 sat/B - 0.000 sat/WU - 362 bytes)								12.51381406 BTC
Hash	6dbbb87f307ab692c04796c400feff8c844516825d27f05ee8b4fa1...								2020-02-22 12:51
	12nZnwZNdqQxYPKaCMBWSWss6fvanhTqqC	3.99550499 BTC			➔	35eS86a7f7HYnRDazEVGncvwhwPNPpXfJh	0.00456552 BTC		
						19WvgcvFHyvE7t26yYskfwtRbZaDPWLj6g	3.99071447 BTC		
Fee	0.00022500 BTC (100.446 sat/B - 25.112 sat/WU - 224 bytes)								3.99527999 BTC

图1.10. 比特币的Coinbase交易和普通交易

信息来源: <https://www.blockchain.com/explorer>

1.4 比特币的交易

比特币使用了secp256k1椭圆曲线，其描述参数为：

$$E : y^2 \equiv x^3 + ax + b \pmod{p}$$

p : 代表有限域 F_p 的那个质数

a, b : 椭圆方程的参数

G : 椭圆曲线上的一个基点 $G = (x_G, y_G)$

n : G 在阶

$$p = \text{FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFE FFFFFFFC2F}$$

$$= 2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1$$

$$a = 0$$

$$b = 7$$

$$x_G = 79BE667E F9DCBBAC 55A06295 CE870B07 029BFCDB 2DCE28D9 59F2815B 16F81798$$

$$y_G = 483ADA77 26A3C465 5DA4FBFC 0E1108A8 FD17B448 A6855419 9C47D08F FB10D4B8$$

$$n = \text{FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFE BAAEDCE6 AF48A03B BFD25E8C D0364141}$$

比特币地址的产生过程如下：

1.4 比特币的交易

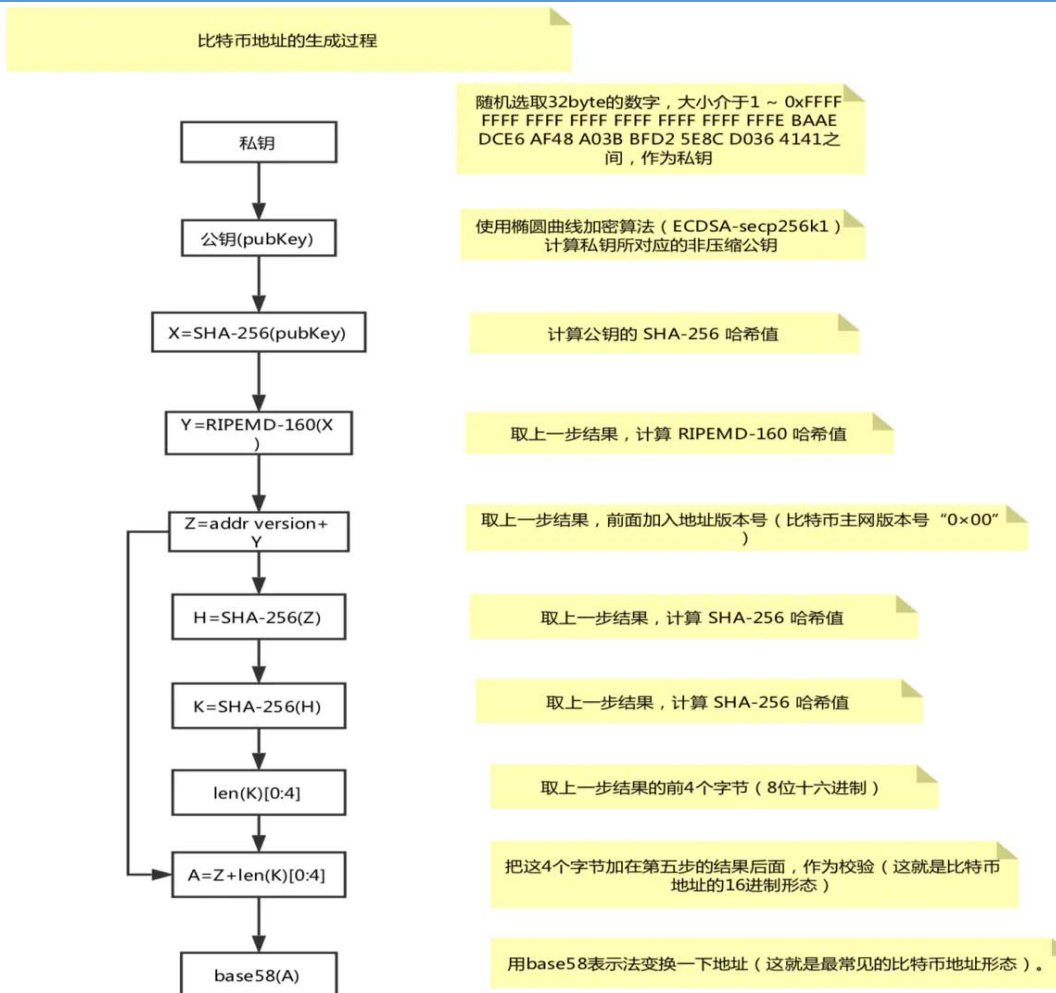


图1.11. 比特币地址产生过程

1.4 比特币的交易

- ① 随机选取一个**32字节的数作为私钥**(大小介于1~0xFFFF FFFF FFFF FFFF FFFF FFFF FFFF FFFF BAAE DCE6 AF48 A03B BFD2 5E8C D036 4141之间)：18e14a7b6a307f426a94f8114701e7c8e774e7f9a47e2c2035db29a206321725
- ② 计算私钥所对应的**非压缩公钥**：（共65字节，1字节0x04，32字节为x坐标，32字节为y坐标）
0450863AD64A87AE8A2FE83C1AF1A8403CB53F53E486D8511DAD8A04887E5B23522CD470243453A299FA9E77237716103ABC11
A1DF38855ED6F2EE187E9C582BA6
- ③ 计算公钥的**SHA-256**哈希值：600FFE422B4E00731A59557A5CCA46CC183944191006324A447BDB2D98D4B408
- ④ 计算上一步哈希值的**RIPEMD-160**哈希值：010966776006953D5567439E5E39F86A0D273BEE
- ⑤ 在上一步结果之间加入**地址版本号**：（如比特币主网版本号"0x00"）00010966776006953D5567439E5E39F86A0D273BEE
- ⑥ 计算上一步结果的**SHA-256**哈希值：445C7A8007A93D8733188288BB320A8FE2DEBD2AE1B47F0F50BC10BAE845C094
- ⑦ 再次计算上一步结果的**SHA-256**哈希值：D61967F63C7DD183914A4AE452C9F6AD5D462CE3D277798075B107615C1A8A30
- ⑧ 取上一步结果的**前4个字节**：（8位十六进制数）D61967F6，把这4个字节加在第五步结果的后面，作为校验（这就是比特币地址的16进制形态）00010966776006953D5567439E5E39F86A0D273BEED61967F6
- ⑨ 用**base58**表示法变换一下地址：（这就是最常见的比特币地址形态）16UwLL9Risc3QfPqBUvKofHmBQ7wMtjvM

目 录

- 1.0. 引言
- 1.1. 比特币的诞生
- 1.2. 疯狂的比特币
- 1.3. 比特币的通俗故事
- 1.4. 比特币的交易
- 1.5. 比特币的挖矿
- 1.6. 比特币的分叉
- 1.7. 其它密码货币

1.4 比特币的交易

比特币钱包是一个形象的概念,就是保存和管理比特币地址以及对应公私钥对的软件。根据终端类型的不同,比特币钱包可以分为桌面钱包、手机钱包、网页钱包和硬件钱包。按照私钥的存储方式,可以分为冷钱包、热钱包两种。

- ▶ **冷钱包是指互联网不能访问到私钥的钱包:** 冷钱包往往依靠“冷”设备确保比特币私钥的安全,比如不联网的电脑、手机、写着私钥地址的小本本等.冷钱包避免了被黑客盗取私钥的风险,但是可能面临物理安全风险,比如电脑丢失损坏等。
- ▶ **热钱包是指互联网能访问到私钥的钱包:** 热钱包往往是在线钱包的形式.使用热钱包时,最好在不同平台设置不同密码,且开启二次认证,以确保自己的资产安全。



图1.13. 比特币冷钱包



图1.12. 比特币热钱包

1.5 比特币的挖矿

“挖矿”成功即是该节点成功获得当前区块记账权,也就是说其他节点就“照抄”该挖矿成功的节点的当前区块。获得记账权的节点会获取一定数量的比特币奖励,以此激励比特币网络中的所有节点积极参与记账工作。该奖励包含系统奖励和交易手续费两部分,系统奖励则作为比特币发行的手段。最初每生产一个“交易记录区块”可以获得 50 比特币的系统奖励,为控制比特币发行数量,该奖励每 4 年就会减半,到 2140 年即会基本发放完毕,最终整个系统中最多只能有 2 100 万个比特币。

比特币系统大约每 10 分钟会记录一个数据块,这个数据块里包含了这 10 分钟内全网待确认的部分或全部交易。所谓的“挖矿”,就是争夺将这些交易打包成“交易记录区块”的权利。比特币系统会随机生成一道数学难题,后续会详细描述该数学难题,所有参与挖矿的节点一起参与计算这道数学难题,首先算出结果的节点将获得记账权。

1.5 比特币的挖矿

每个节点会将过去一段时间内发生的、尚未经过网络公认的交易信息进行收集、检验、确认,最后打包并加签名为一个无法被篡改的“交易记录区块”,并在获得记账权后将该区块进行广播,从而让这个区块被全部节点认可,让区块中的交易成为比特币网络上公认已经完成的交易记录,永久保存。

挖矿最主要的工作就是计算上文提到的数学难题,最先求出解的矿工即可获得该块的记账权。在介绍这个数学难题前,先简单介绍一下哈希算法。哈希算法的基本功能概括来说,就是把任意长度的输入值通过一定的计算,生成一个固定长度的字符串,输出的字符串即为该输入的哈希值。比特币系统中采用 SHA-256 算法,该算法最终输出的哈希值长度为 256bit。

1.5 比特币的挖矿

1.5.1. 挖矿的原理

Merkle树是一种树（数据结构中所说的树），通常称为Merkle Hash Tree，常用于高效汇总和验证大数据集的完整性.具有以下特点：

- ① 默克尔树常见的结构是二叉树，但它也可以是多叉树，它具有树结构的全部特点.
- ② 默克尔树的基础数据不是固定的，因为它只要数据经过哈希运算得到的hash值.
- ③ 默克尔树是从下往上逐层计算的，就是说每个中间节点是根据相邻的两个叶子节点组合计算得出的，而根节点是根据两个中间节点组合计算得出的，所以叶子节点是基础.

1.5 比特币的挖矿

1.5.1. 挖矿的原理

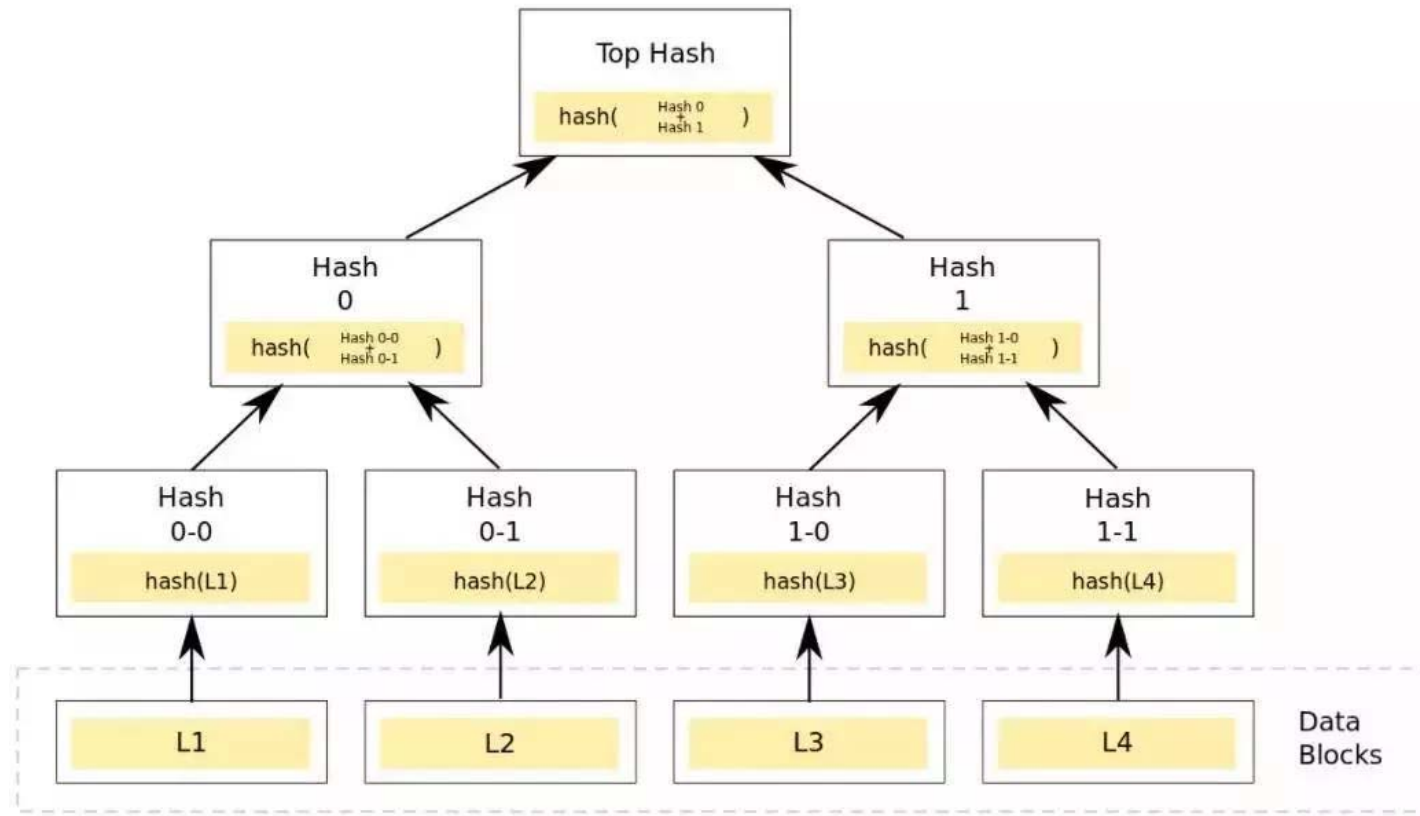


图1.14. Merkle示意图
信息来源：百度图片

1.5 比特币的挖矿

1.5.1. 挖矿的原理

比特币中每个区块生成时,需要把上一个区块的哈希值、本区块的交易信息的默克尔树根、一个未知的随机数(nonce)拼在一起计算一个新的哈希值。为了保证 10 分钟产生一个区块,该工作必须具有一定难度,即哈希值必须以若干个 0 开头。哈希算法中,输入信息的任何

微小改动即可引起哈希值的巨大变动,且这个变动不具有规律性。因为哈希值的位数是有限的,通过不断尝试随机数 nonce,总可以计算出一个符合要求的哈希值,且该随机数无法通过寻找规律计算出来。这意味着,该随机数只能通过暴力枚举的方式获得。挖矿中计算数学难题即为寻找该随机数的过程。

1.5 比特币的挖矿

1.5.1. 挖矿的原理

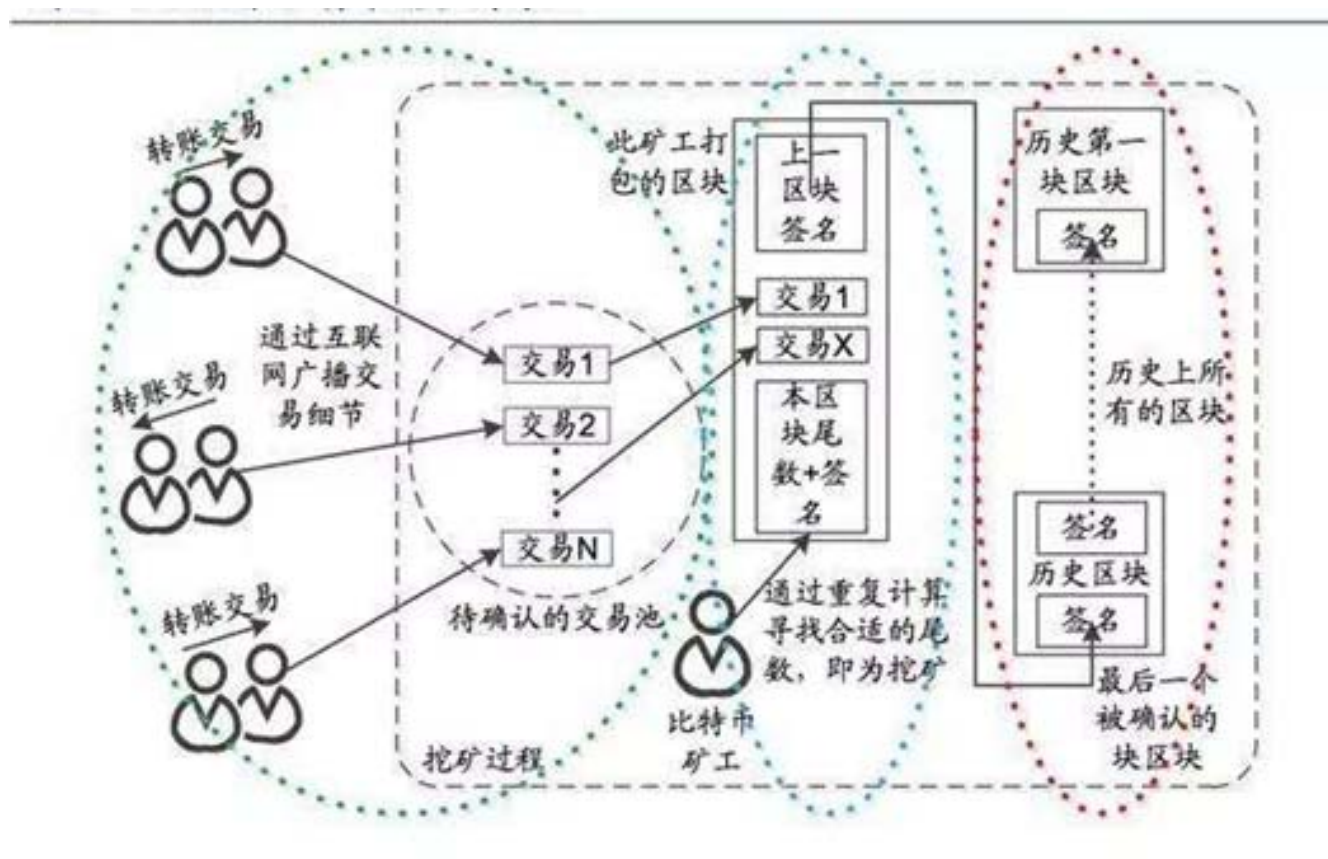


图1.15. 比特币挖矿示意图
信息来源：百度图片

1.5 比特币的挖矿

1.5.1. 挖矿的原理

哈希值由 16 进制数字表示,即每一位有 16 种可能。根据哈希算法的特性,出现任何一个数字的概率是均等的,即每一位为“0”的概率为 $1/16$ 。要求某一位为“0”平均需要 16 次哈希运算,要求前 n 位为“0”,则需要进行哈希计算的平均次数为 16 的 n 次方。矿工为了计算出该随机数,需要花费一定的时间进行大量的哈希运算。

某个矿工成功计算出该随机数后,则会进行区块打包并全网广播。其他节点收到广播后,只需对包含随机数的区块按照同样的方法进行一次哈希运算即可,若哈希值以“0”开头的个数满足要求,且通过其他合法性校验,则接受这个区块,并停止本地对当前区块随机数的寻找,开始下个区块随机数的计算。

随着技术的发展,进行一次哈希计算速度越来越快,同时随着矿工的逐渐增多,算出满足哈希值以一定数量“0”开头的随机数的时间越来越短。为保证比特币始终按照平均每 10 分钟一个区块的速度出块,必须不断调整计算出随机哈希计算的平均次数,即调整哈希值以“0”

1.5 比特币的挖矿

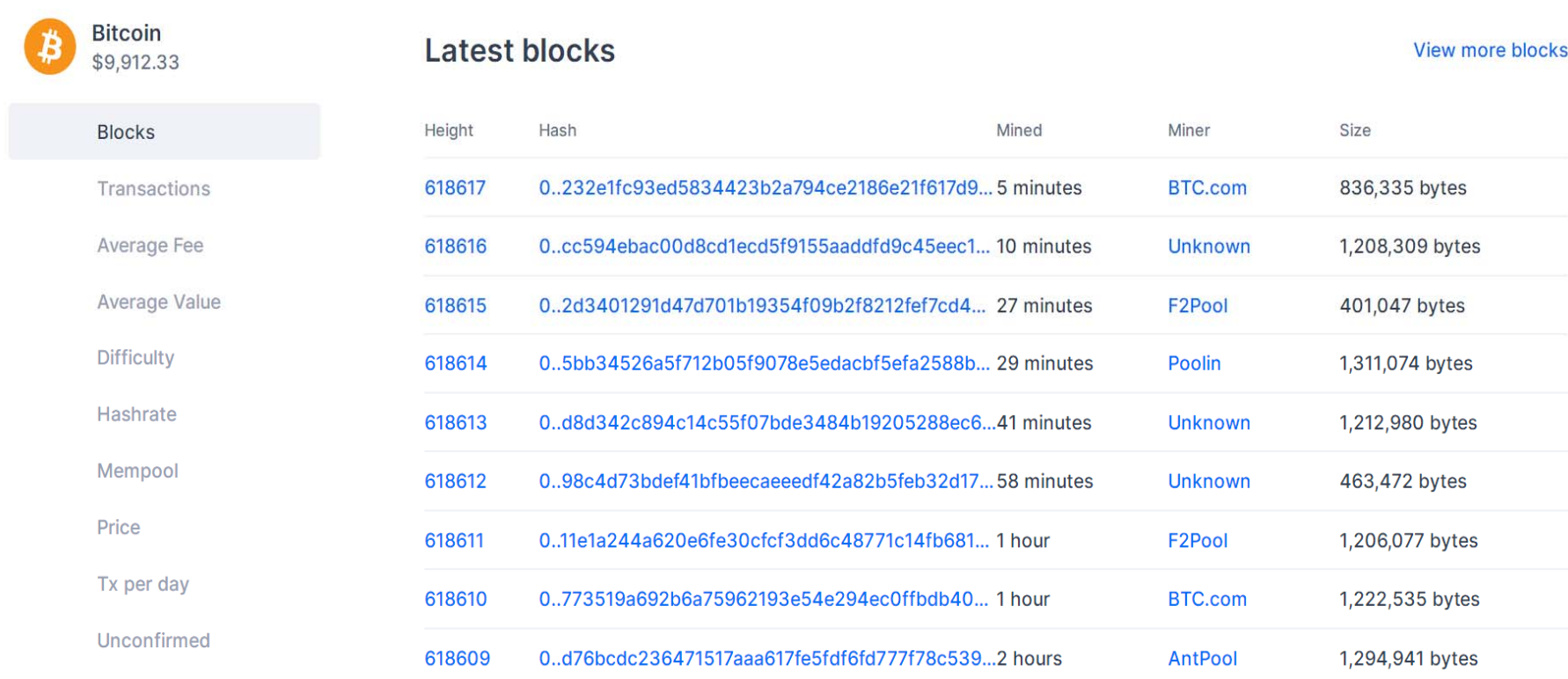
1.5.1. 挖矿的原理

开头的数量要求,以此调整难度。比特币中,每生成 2 016 个区块就会调整一次难度,即调整周期大约为两周($2\ 016 \times 10\text{min} = 14$ 天)。也就是说,对比生成最新 2 016 个区块花费的实际时间和按照每 10 分钟出一个块生成 2 016 个块的期望时间,若实际时间大于期望时间则降低难度,若实际时间小于期望时间则增加难度。

同时,为防止难度变化波动太大,每个周期调整幅度必须小于一个因子(当前为 4 倍)。若幅度大于 4 倍,则按照 4 倍调整。由于按照该幅度调整,出块速度仍然不满足预期,因此会在下一个周期继续调整。

1.5 比特币的挖矿

1.5.1. 挖矿的原理



Bitcoin		Latest blocks			View more blocks	
\$9,912.33		Height	Hash	Mined	Miner	Size
Blocks		618617	0..232e1fc93ed5834423b2a794ce2186e21f617d9...	5 minutes	BTC.com	836,335 bytes
Transactions		618616	0..cc594ebac00d8cd1ecd5f9155aaddfd9c45eec1...	10 minutes	Unknown	1,208,309 bytes
Average Fee		618615	0..2d3401291d47d701b19354f09b2f8212fef7cd4...	27 minutes	F2Pool	401,047 bytes
Average Value		618614	0..5bb34526a5f712b05f9078e5edacbf5efa2588b...	29 minutes	Poolin	1,311,074 bytes
Difficulty		618613	0..d8d342c894c14c55f07bde3484b19205288ec6...	41 minutes	Unknown	1,212,980 bytes
Hashrate		618612	0..98c4d73bdef41bfbeecaeedf42a82b5feb32d17...	58 minutes	Unknown	463,472 bytes
Mempool		618611	0..11e1a244a620e6fe30cfcf3dd6c48771c14fb681...	1 hour	F2Pool	1,206,077 bytes
Price		618610	0..773519a692b6a75962193e54e294ec0ffbdb40...	1 hour	BTC.com	1,222,535 bytes
Tx per day		618609	0..d76bcd3236471517aaa617fe5fdf6fd777f78c539...	2 hours	AntPool	1,294,941 bytes
Unconfirmed						

图1.16. 比特币区块生成时间

信息来源: <https://www.blockchain.com/explorer>

1.5 比特币的挖矿

1.5.2. 矿池的原理

随着区块链的日渐火爆,参与挖矿的人越来越多,按照比特币原本的设计模式,只有成功打包一个区块的人才能获取奖励。如果每个矿工都独立挖矿,在如此庞大的基数下,挖矿成功的概率几乎为0,只有一个幸运儿可以获取一大笔财富,其他矿工投入的算力、电力资源就会白白亏损。或许投入一台矿机,持续挖矿好几年甚至更久才能挖到一个区块。

为了降低这种不确定性,矿池应运而生。假如有10万矿工参与挖矿工作,这10万矿工的算力和占这个网络的10%,则这10万个矿工中的某个矿工成功挖到下个块的概率即为1/10。即平均每个矿工成功挖到下个区块的概率为1/1 000 000,即平均每个矿工要花费19年可以成功挖到一个区块,然后获得相应的比特币奖励。这种挖矿模式风险过大,几乎没人可以承受。但是假设这10万个矿工共同协作参与挖矿,则平均每100分钟即可成功挖到一个区块,然后按照每个矿工提供的算力分配该次收益。这10万个矿工的收益也会趋于稳定。

1.5 比特币的挖矿

1.5.2. 矿池的原理

协调矿工进行计算的思路也非常简单,矿池将打包区块需要的交易等信息验证完成后发送给矿工,然后降低矿工的挖矿难度。比如某个时段比特币系统需要哈希值“0”开头的个数大于50个,矿池可以将难度降低到40个“0”开头,矿工找到一个40个“0”开头哈希值的方案后,即可提交给矿池。矿池收到一个满足哈希值“0”开头个数大于50个的方案时,即可提交至比特币网络。当然,你也许会想:如果矿工计算得到一个“0”开头个数大于50的哈希值后,则直接提交给比特币网络,独享该区块的收益;如果计算得到一个“0”开头数在40到50之间的则提交到矿池,享受整个矿池分配的收益。该方案当然是行不通的,因为区块内容是由矿池发送给矿工的,即受益者地址已经包含在该区块中了,即使直接提交,最终受益的也是矿池。如果修改该地址,即意味着区块内容改变,则前面计算的哈希值也无效了。最后矿池按照矿工提交方案数量计算贡献的算力,最后根据算力分配收益。

当前的主流挖矿协议是stratum, 以前还有GBT(getblocktemplate)、getwork等几种协议, 它们都过时了. 可以用免费的Cpuminer软件把协议调通. 软件地址为:
<https://sourceforge.net/projects/cpuminer/files>

1.5 比特币的挖矿

1.5.2. 矿池的原理

1. 客户端首先向服务器发送subscribe指令

```
{"id": 1, "method": "mining.subscribe", "params": ["cpuminer/2.5.0"]}
```

参数中指明矿工软件的名称和版本号。

2. 服务器端返回信息

比特币挖矿实际上就是去寻找随机数nonce，有时所有的随机数都试遍了，仍无法满足目标，就需要用到extra nonce。

```
1  {
2      "id":1,
3      "result":
4      [
5          [
6              ["mining.set_difficulty","deadbeefcafebabe0100000000000000"], //后面是stratum session id
7              ["mining.notify","deadbeefcafebabe0100000000000000"]
8          ],
9          "7000000", // ExtraNonce1 十六进制
10         4 // ExtraNonce2_size 字节
11     ],
12     "error":null
13 }
```

1.5 比特币的挖矿

1.5.2. 矿池的原理

3. 客户端发送认证信息

用户名是钱包的地址，我这里使用的是比特币测试网络的地址，并没有以1开头.

```
1 {  
2   "id": 2,  
3   "method": "mining.authorize",  
4   "params": ["myAzQj4bH4mMF2GpoLSY2v4qVquASTpzR4", "x"]  
5 }
```

4. 服务器返回true，表示用户验证通过

```
{"id":2,"result":true,"error":null}
```

5. 服务器端发回难度设置消息

```
{"id":null,"method":"mining.set_difficulty","params":[8]}
```


1.5 比特币的挖矿

1.5.2. 矿池的原理

6. 服务器发送通知消息

矿工可能用到了多线程，所以需要job id来区分不同的线程，后面是一堆用于区块生成的信息。

```
1  {
2  "method":"mining.notify",
3  "params":[
4    "3d", // 作业ID
5    "af8cecebf98...4310000000", //previous block hash
6    "010000000100000...000000", //generation tx part1
7    "0d2f6e6f646.....5b36ec88ac00000000", //generation tx part2
8    ["6fb6....80cb","d4464...49a5a290", ... ,"68d803...4ec79d161"], // merkle branches 默克尔树分支
9    "20000000", // block version
10   "1a3fffc0", // nBits encoded network difficulty
11   "5a158226", //nTime, 时间戳
12   false // clean jobs, 如果是true, 则表示其它矿工爆块了, 开始新一轮计算
13 ]
14 }
```

1.5 比特币的挖矿

1.5.2. 矿池的原理

7. 客户端发现一个nonce，提交给服务器

```
1  {
2  "method": "mining.submit",
3  "params": [
4      "myAzQj4bH4mMF2GpoLSY2v4qVquASTpzR4", //worker name
5      "4c", //job id
6      "00000000", //extranonce2
7      "5a158557", //nTime
8      "6ae65681" //nonce
9  ],
10 "id":4
11 }
12
```

1.5 比特币的挖矿

1.5.2. 矿池的原理

8. 服务器返回结果

返回true表示服务器认可客户端的工作.

```
1 | {  
2 |   "id":4,  
3 |   "result":true,  
4 |   "error":null  
5 | }
```

目 录

- 1.0. 引言
- 1.1. 比特币的诞生
- 1.2. 疯狂的比特币
- 1.3. 比特币的通俗故事
- 1.4. 比特币的交易
- 1.5. 比特币的挖矿
- 1.6. 比特币的分叉
- 1.7. 其它密码货币

1.6 比特币的分叉

软件由于方案优化、BUG 修复等原因进行升级是一种非常常见的现象。如手机应用等传统软件,升级非常简单,只需厂商发布,用户接受升级即可。但是对于比特币这种去中心化的系统,升级是非常困难的,需要协调网络中每个参与者。软件升级意味着运行逻辑的改变,但是在比特币中,升级必然会导致不同节点在一定时间内运行不同的版本,于是就会产生分叉。

分叉主要包含软分叉和硬分叉两种。如果比特币升级后,新的代码逻辑向前兼容,即新规则产生的区块仍然会被旧节点接受,则为软分叉;如果新的代码逻辑无法向前兼容,即新产生的规则产生的区块无法被旧节点接受,则为硬分叉。

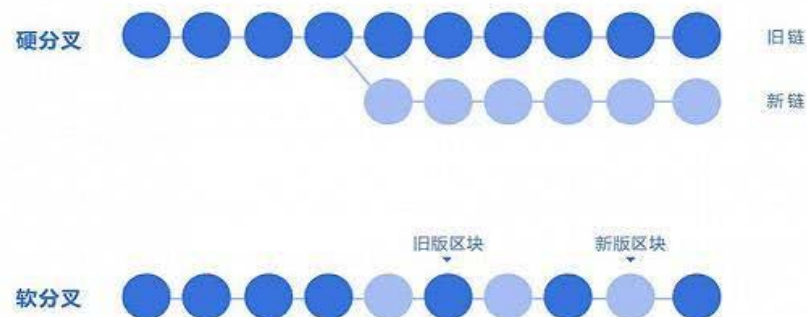


图1.17. 比特币软/硬分叉示意图
信息来源: 百度图片

1.6 比特币的分叉

1. 软分叉

软分叉由于向前兼容,新旧节点仍然运行在同一条区块链上,并不会产生两条链,对整个系统影响相对较小。到目前为止,比特币发生过多次软分叉,如 BIP-34, BIP-65, BIP-66, BIP-9

此处以 BIP-34 为例,简单说明软分叉的过程。在旧版本中,存在一个无意义的字段“coinbase data”,矿工不会去验证该字段的内容。BIP-34 升级的新版本则要求该字段必须包含区块高度,同时将版本信息由“1”修改为“2”。该升级共包含三个阶段。

第一个阶段:矿工将版本号修改为“2”,此时所有矿工验证区块时,按照旧的规则验证,即不关心“coinbase data”字段内容,所有矿工不论以新规则还是旧规则打包区块,均可以被整个网络接受。

1.6 比特币的分叉

第二阶段：如果最新产生的 1 000 个区块中，版本号为“2”的区块个数超过 75% 时，则要求版本号为“2”的矿工必须按照新的规则打包区块，升级的矿工收到版本号为“2”的区块时，只会接受“coinbase data”字段包含区块高度的区块，对于版本号为“1”的区块，仍然不校验该字段并接受。

第三阶段：如果最新产生的 1 000 个区块中，版本号为“2”的区块个数超过 95% ，则升级的矿工只接受版本号为“2”的区块，并会对“coinbase data”字段进行校验，版本号为“1”的区块则不被接受，以此来逼迫剩余少量矿工进行升级。

软分叉虽然对系统的影响较小，但是为了保证向前兼容，不能新增字段，只能在现有数据结构下修改，即可升级的内容非常有限。同时，因为这些限制，软分叉一般升级方案比较复杂，复杂的方案往往更容易产生 BUG，并且可维护性很差。

1.6 比特币的分叉

2. 硬分叉

硬分叉相比软分叉则会“暴力”很多,由于不向前兼容,旧版本矿工无法验证新版本的区块而拒绝接受,仍然按照旧的逻辑只接受旧版本矿工打包的区块。而新版本产生的区块则会被新版本矿工接受,因此新版本矿工保存的区块会和旧版本矿工保存的区块产生差别,即会形成两条链。

硬分叉修改余地很大,方案设计比较简单,但是如果整个网络中有两种不同的意见,就会导致整个生态的分裂。当前比特币影响最广泛的硬分叉事件即为2017年8月1日的硬分叉,比特币由一条链分叉产生一条新的链“比特现金(Bitcoin Cash, BCH)”。

这次硬分叉的起因是开发者与矿工在比特币扩容方案上的分歧。比特币区块大小为1MB,按照每10分钟一个区块的速度,全球每秒只能完成大约7笔交易。比特币发展初期,1MB的区块足够打包出块间隔内产生的所有交易,但是在比特币如此火爆的今天,这种处理速度显然达不到要求。

1.6 比特币的分叉

为了解决以上问题,经过社区讨论,最终形成了两个改进方案,分别是扩容方案和隔离见证方案。

扩容方案的想法比较直接,既然现在因为区块太小而导致交易处理速度低下,那就直接扩大区块的容量,使其能容纳更多的交易。原来 1MB 不够用,那么就扩成 2MB、8MB,甚至直接扩到 32MB。

隔离见证方案的想法是,将交易分为两部分,一部分是交易信息,另一部分是见证信息,这两部分信息分开进行处理。好比一辆车太小,要搭车的人太多,于是让车上所有人将背包和行李放在另一辆跟着的货车上,这样原来的车就可以容纳更多的人了。

支持扩容方案的主要是矿工们。采用扩容方案,矿工可以在每个区块中包含更多的交易,从而获取更多的手续费,然而若使用隔离见证的扩容方案,小额的交易将不通过区块确认,矿工的手续费收益会大幅降低,因此矿工更倾向于支持扩容方案。

1.6 比特币的分叉

隔离见证方案的支持者主要是比特币开发团队的部分核心成员。他们认为,扩容方案是一个“扬汤止沸”的方案,毕竟不可能无限制地对区块的容量进行扩大。同时,区块的变大会使得挖矿的门槛提高,从而降低普通矿工的参与度,导致比特币系统的去中心化程度减弱。

2016年2月和2017年3月,争议双方两次进行商讨,希望双方各退一步,接受一个折中的方案,该方案中,区块容量将会被扩大到2MB,同时也对比特币部署隔离见证的方案。但是,由于期间有参与方反悔或者反对,导致最终没有达成共识,这也给“硬分叉”埋下了伏笔。

在2017年8月1日,比特大陆投资的矿池ViaBTC团队,采用比特大陆提出的UAHF(用户激活的硬分叉)方案,挖出了第一个区块,对比特币区块链进行了硬分叉。自此,与比特币竞争的分叉币比特币现金诞生。比特币现金区块链的区块容量达到了8MB,且没有采用隔离见证方案。

分叉后称为**比特币现金 (BCH)**, 随后比特币黄金 (BTG)、比特币钻石 (BCD)、超级比特币(SBTC)等数字货币出现。

目 录

- 1.0. 引言
- 1.1. 比特币的诞生
- 1.2. 疯狂的比特币
- 1.3. 比特币的通俗故事
- 1.4. 比特币的交易
- 1.5. 比特币的挖矿
- 1.6. 比特币的分叉
- 1.7. 其它密码货币

1.7 其它密码货币

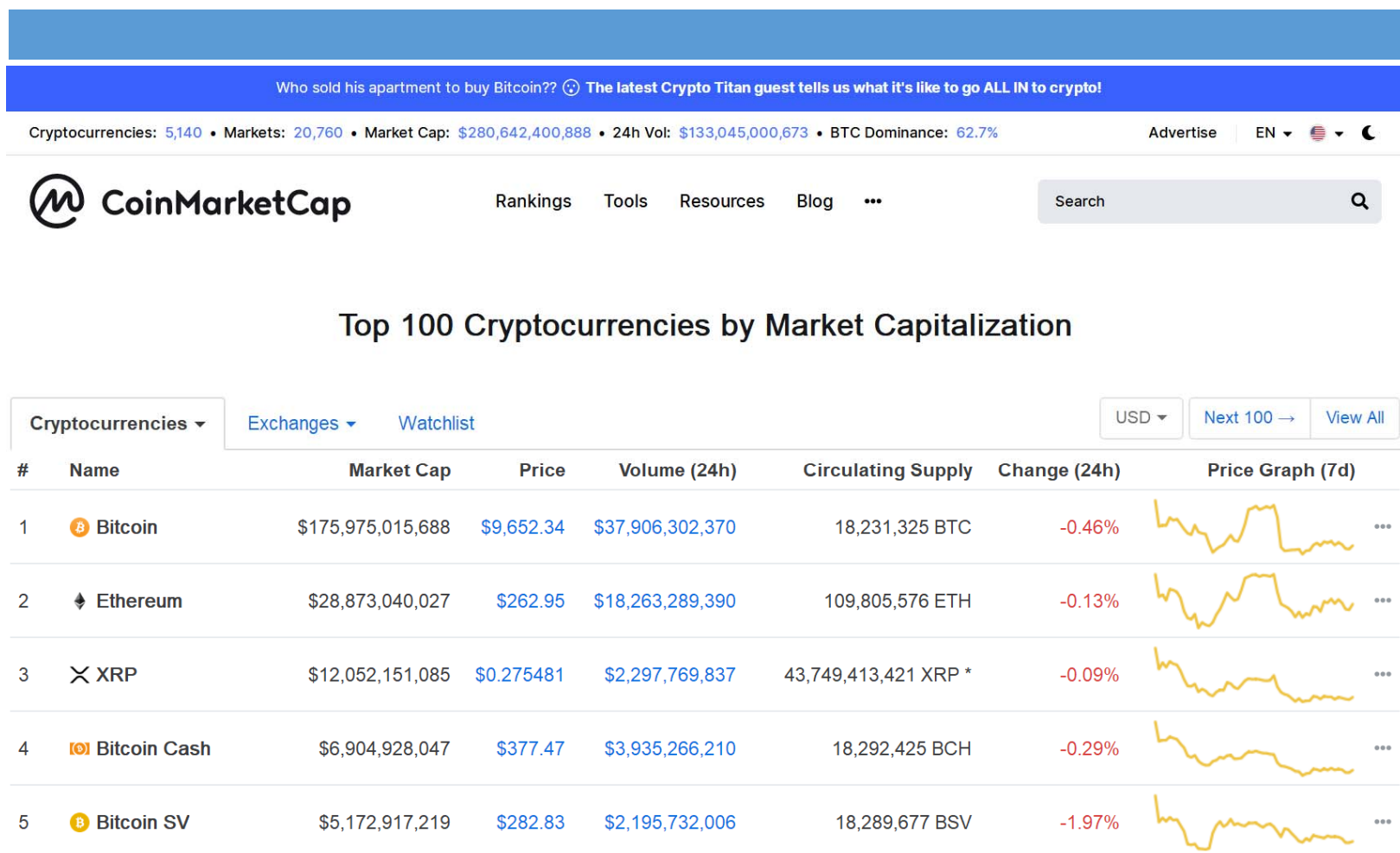


图1.17. 数字货币市值(2020年2月22日21:09)
信息来源: <https://coinmarketcap.com/>

1.7 其它密码货币

以太坊（英文Ethereum）是一个开源的有智能合约功能的公共区块链平台，通过其专用密码货币以太币（Ether，简称“ETH”）提供去中心化的以太虚拟机（Ethereum Virtual Machine）来处理点对点合约。

以太坊的概念首次在2013至2014年间由程序员Vitalik Buterin受比特币启发后提出，大意为“下一代加密货币与去中心化应用平台”，在2014年通过ICO众筹开始得以发展。截至到2020年2月22日，以太币是市值第二高的密码货币，仅次于比特币。

以太坊可以用来创建去中心化的程序、自治组织和**智能合约**，据纽约时报的报导，在2016年5月已经有数十个可用的程序。预期的应用目标涵盖金融、物联网、农田到餐桌（farm-to-table）、智能电网、体育赌博等。去中心化自治组织有潜力让许多原本无法运行或成本过高的营运模型成为可能。

1.7 其它密码货币

Zcash 是首个使用零知识证明机制的区块链系统。零知识证明简单点讲,就是证明者能够在不向验证者提供任何有用的信息的情况下,使验证者相信某个论断是正确的,所以 Zcash 可提供完全的支付保密性。Zcash 是比特币的分支,保留了比特币原有的模式,不同之处在于,Zcash 交易能够自动隐藏区块链上所有交易的发送者、接受者及数额。只有那些拥有查看密钥的人才能看到交易的内容。用户拥有完全的控制权,他们可自行选择向其他人提供查看密钥。

门罗币(Monero, XMR)是另一个比较流行的隐私保护的加密数字货币,它同样具有隐藏地址、保护用户的隐私与匿名的功能。与 Zcash 不同,门罗币采用环签名方式保护用户隐私。环签名环中一个成员利用他的私钥和其他成员的公钥进行签名,但却不需要征得其他成员的允许,而验证者只知道签名来自这个环,但不知道谁是真正的签名者,这个方式解决了对签名者完全匿名的问题。

1.7 其它密码货币

- 莱特币是一种基于“点对点”(peer-to-peer)技术的密码货币，是MIT/X11许可下的一个开源软件项目，由一名曾任职于谷歌的程序员(李启威)设计并编程实现，2011年1月9日发布运行，被认为是第一山寨币。
- 莱特币旨在改进比特币，与其相比，莱特币具有三种显著特点：
 - ◆ 第一，莱特币网络每2.5分钟（而不是10分钟）就可以处理一个块，因此可以提供更快的交易确认。
 - ◆ 第二，莱特币网络预期产出8400万个莱特币，是比特币网络发行货币量的四倍之多。
 - ◆ 第三，莱特币在其工作量证明算法中使用了由Colin Percival首次提出的Script算法，这使得相比于比特币，更能抵抗矿机、矿池造成的中心化问题。



谢谢!

