教你如何轻松学习区块链和比特币基础技术原理

背景

比特币的发展历程

自从2009年一个自称中本聪（对，是日本人...）的人在一个隐秘的密码学讨论组上发布了一篇叫做《比特币：一种点对点的电子现金系统》的报告，比特币就出现了，并且得到了越来越多人的关注。比特币从最初的几分钱到现在上万元的价格一路上涨，价格有过猛涨，有过大跌，但是价格的总体趋势是不断增加的。挖矿由一开始的个人电脑到后来的矿机，再到后来的矿池也经过了几代的发展。政策上得到了一些国家的支持，也有一些国家反对，还有一些国家对比特币的态度很暧昧。最有意思的是，2010年5月21日，在第一次比特币交易中，佛罗里达程序员Laszlo Hanyecz用1万BTC购买了价值25美元的披萨优惠券，这些比特币在最近价值已经上亿了。这些都见证了比特币神奇的发展历史。

区块链的前世今生

虽然比特币没有完全得到各国政府的认可，也并不是一个标准的金融组织，但是比特币十几年如如一日的挖矿活动从来没有停止过，比特币交易随时随地都在进行，无疑是一个成功的金融产品，从技术上，比特币的每一项技术点，例如：非对称密码学、P2P网络、共识机制、智能脚本等，都不是创新，但是这些技术组合形成的比特币就是一个大大的创新。

由于比特币的成功，比特币的核心技术区块链越来越多的得到大家的关注，以至于区块链被认为是互联网金融行业的下一个风口，各行各业都在研究区块链，并为区块链寻找使用场景，有个不恰当的例子，但是很生动，区块链技术就想是一个锤子，满世界的找钉子，好不容易找到的几个钉子，一看还是螺丝钉，还得换成螺丝刀才行，不过非得要用锤子砸进去，也不是不可以，就是有点费力气。

上面这个例子生动的说明了区块链技术的现状，比如，有的企业里面使用区块链做存储、有的企业里面使用区块链做客户的账务、也有的公司里面使用区块链保存电子资产，这些都是在为区块链找场景，虽然区块链还没有得到全面的应用，但是无疑区块链在金融领域已经初露头角。

另外一个现象是很多公司为了炒作新概念，声称产品使用了区块链，例如某某电子资产公司使用了区块链，仔细了解，人家使用的私有链，这让人觉得匪夷所思，私有的区块链是为了提高性能，肯定不是，区块链最难说清楚的就是性能，那是安全，私有的安全

在于私有产品的建设，不在于是否使用区块链，那么私有链的使用是为了什么呢？这里读者可自行YY。

实际上，区块链分为共有链、私有链和联盟链，共有链对参与的节点没有限制，整个系统运行在公网上，没有中央机构的控制，自由发展，自发组织，典型的案例就是比特币；私有链，顾名思义就是一个组织内部运行的区块链系统，这种系统运行在组织内，很难保证去中心化，在一个组织内本身就是个中心化的产物，因此，我一直认为凡事私有链都不要说具有去中心化的特点；联盟连，这是笔者最看好的一种形式，

我为什么要写这篇文章

比特币系统是当下最流行的电子货币之一，也有很多山寨币，但是思想甚至源码都是来自于比特币，朋友圈里有很多介绍性的文章，也有人试图通过漫画来生动的解释比特币的特性，但是始终不得要领，总是有些问题想不清楚，为了弄清楚这些问题，最近深入的研读了几本比特币的书籍以及中本聪本人发表的比特币论文，感觉茅塞顿开，迫不及待的与大家分享我的理解，希望与大家共同探讨、共同进步。

核心要点

比特币是什么

比特币是一种利用点对点技术实现的电子现金系统，它允许一个组织直接与另外一个组织进行在线支付，而不需要中间的权威的清算机构。

在比特币的世界里，如果你想拥有比特币，你需要申请一个比特币地址，就像你到银行存款，需要开立一个账户，然后，你就拥有这个账号，有了自己的账号，你可以向你的账号存款，别人也可以给你的账号转账，当你需要提款的时候或者给别人转账的时候，你需要出示一个能够打开这个地址的钥匙，也就是你的私钥，就像你在ATM上取款的时候需要提供密码一样。

与银行发行的法定货币不同，法定货币的发行是由各国央行来统一管理的，大家都相信央行是靠谱的，不会记错账，也不会被人攻击。然而，比特币的发行并不需要央行这样的权威机构，它允许一笔交易从一个组织直接结算给另外一个组织，省去了权威机构结算的环节，提高了交易和结算的效率，节省了交易的成本，尤其是跨境交易的成本。

一个点对点的在线交易系统如何保证交易的匿名性、正确性、不可篡改性？又是如何防止双重支付和防止作弊和攻击的呢？

下面的章节将为大家通过最通俗的语言解开比特币的神秘面纱，让你从逻辑上理解比特币是如何工作的，让学习比特币不留死角，让比特币的方方面面清晰的呈现在你的脑海里。

区块链技术的核心要点

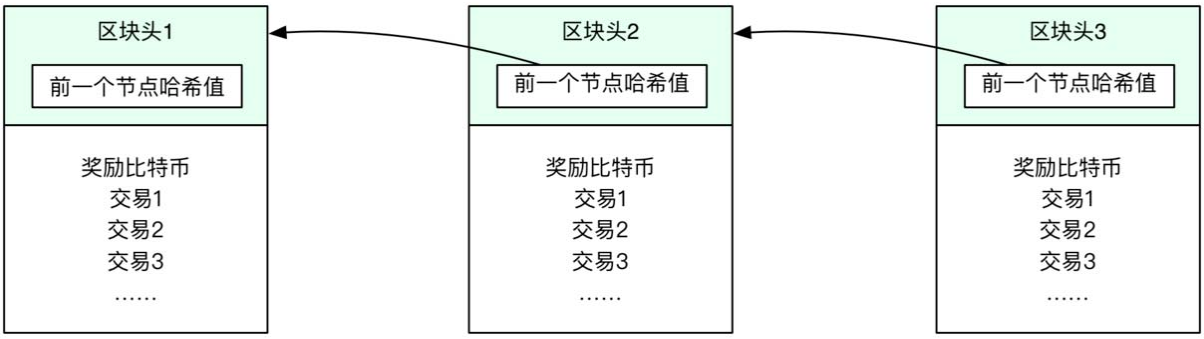
本节介绍区块链技术中最核心的几个要点，这包括：区块链存储、密匙和地址、解锁脚本、挖矿过程、共识机制、P2P网络等。

区块链是如何存储的？

对于一个现金账户系统，首先要解决的是如何记账，把账记在哪里，账户如何存储等。例如，你在中国银行存款，中国银行为你开立账户，你的账户就存储在中国银行的服务器上，而你在建设银行存款，建设银行为你开立账户，你的账户就存储在建设银行的服务器上。如果你需要转账给同一个银行的其他人的账户，你需要通过这个银行为你转账和结算，如果你需要转账给其他银行的其他人的账户，你需要通过银联为你转账和结算，尽管一个普通用户感知不到如此多的过程，不过这些步骤确实是存在的，从这个过程中我们看到记账的账户系统是专用的，是中心化的，归某一个组织所有并维护，通常这个组织是权威的、可信赖的。

而比特币并没有中心化的记账系统，而是通过分布式的区块链来记载比特币的拥有权和交易信息。每个比特币的参与者都拥有一份相同的区块链副本，区块链包含着多个随着时间排序的块，后一个块通过哈希指针指向前一个块，形成一个链，从链的顶端通过这个指针，可以一直找到底端第一个块，第一个块成为创世纪块。每个区块记录着前一个区块的哈希散列值，实际上是前一个节点头的哈希散列值，如果想改变一个区块包含的交易，必须改变这个区块之后所有的交易，由于每个区块的产生是需要条件和时间的，并且条件相当苛刻（后续会在共识机制相关的文章中详细说明），因此，一个区块一旦产生，并且被区块链的节点所接受，并且在这个节点之后又产生了一定数量的区块，那么这个区块基本是不可篡改的。

区块链示意图如下：



从上图可见，区块链是由多个区块组成，每个区块是由区块头和区块体组成的，每一个区块头包含着区块的元信息，同时也包含一个指向前一个区块头哈希值的指针，这个指针是防止区块链被篡改的关键信息。区块体包含比特币的交易信息，第一个交易是特殊交易，是奖励给挖矿节点的酬劳，这也是唯一一种可以产生比特币的方式，也就是发行比特币的方式，其余的交易都是转账交易，比特币从一个地址支付给另外一个地址，这也是实现比特币价值转移的唯一方式。总结来看，比特币只有发行和转账两种交易，比特币产生以后只能从一个人转账给另外一个人，而不能凭空消失，比特币发行的总量是有限的，一共2100万，因此是一种通缩性货币，后续我们会在相关的文章中详细介绍比特并的通缩特性。

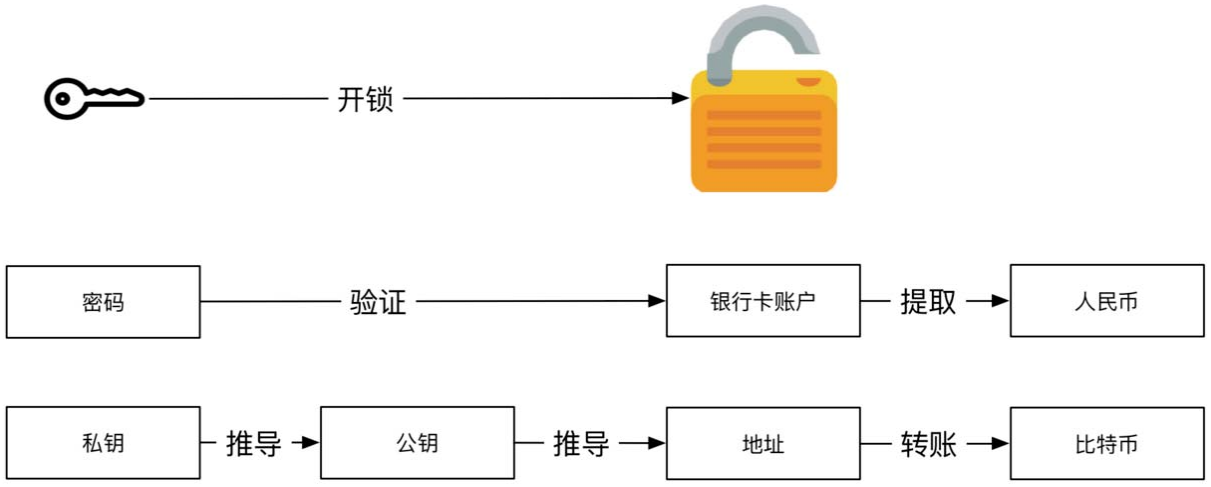
比特币的拥有者如何证明自己拥有比特币？

上一节介绍了区块链的存储，区块链实际上是比特币的账本，记录着谁拥有多少比特币，只不过这个账本是保存在互联网上的、分布式的，并不是由一个中心机构或者服务器来存储。有了账本，剩下的问题就是比特币的拥有者如何证明自己拥有比特币？就像你在银行开立了一个账户，等你想给其他人转账的时候，你需要在ATM上插入卡，然后输入密码。卡就相当于比特币的地址，密码就相当于比特币的秘钥，有了正确的地址和秘钥，就可以对外宣称自己对比特币的拥有权，就可以把比特币转账给其他人来做一笔转账交易。

在ATM上提取一笔现金，输入密码解锁账户，我们相信ATM机不会泄露密码。那么在比特币的世界里，我们如何通过私钥来校验一个地址上的比特币的归属权呢？

比特币的归属权是通过加密领域技术来实现的，我们先来了解下加密领域的原理，加密领域大体上经过了3个阶段，第一个阶段拼算法，把加密逻辑写在一个非常高深的代码里，后来发现无论把多么复杂的逻辑写在代码里，总有高手可以破解。于是产生了对称秘钥加密，对称秘钥加密通过一个对称的秘钥进行加密数据，然后传输或者保存，需要的时候再通过同一个秘钥进行解密还原原来数据，缺点是秘钥是共享的，无法安全的保存秘钥，尤其是跨组织的场景。后来，聪明的安全科学家们发明了非对称加密算法，例如：RSA，非对称算法拥有一对秘钥，一个公钥和一个私钥，私钥可以推导出公钥，但是公钥不能推导出私钥，公钥加密的数据私钥可以解密，私钥加密的数据公钥可以解密，如果组织A向组织B传递数据，那么组织A使用公钥进行加密，组织B使用私钥进行解密，因此，组织B需要小心的保存好私钥，而公钥是公开的，这是典型的非对称加密场景，能够有效的防止数据被偷窥、被篡改。非对称加密还有另外一个场景，就是签名，签名是加密场景的逆向场景，商户B通过自己的私钥加密数据，然后把加密的数据传递给商户A，商户A通过公钥进行解密，如果解密的数据正确，则说明数据是由A发送的，有效的保证了数据的防篡改，从这两个场景我们看到，公钥是公开的，可发给任何人，私钥是私密的，用来解密或者签名的。

比特币证明归属权的示意图如下：



从上图可见，现实生活中我们用钥匙打开锁头，我们用密码在ATM上提取现金，那么在比特币系统里，我们通过秘钥来实现比特币的转账，实现价值的转移。

更具体来讲，一笔比特币交易会把一定数量的脚本锁定在一个地址，声明拥有这个地址的用户会通过密匙的签名来证明自己拥有这个地址，然后，花费这笔比特币，这笔比特

币被花费后并不会消失，会被锁定在其他人的地址上，其他人可以使用同样的方法来花费这笔比特币。

从上面的过程，我们总结了两个动作，锁定与解锁，这和我们平时锁锁头和开锁头是对应的，在比特币系统里是通过锁定脚本和解锁脚本来实现的。

1. 锁定脚本把比特币关联在一个比特币地址上，证明了比特币归属这个地址。
2. 解锁脚本提供证明，证明这个地址归我所有，这个比特币也归我所有，我可以用来支付。

下面我们举一个例子详细说明：

用户Alice在比特币里地址A上拥有10个比特币，Alice与Bob想做一笔交易，Bob把自己家的汽车卖给了Alice，Alice需要向Bob支付10个比特币，Bob的比特币地址是B。

在之前的交易中，Alice拥有的10个比特币被锁定在Alice的比特币地址A上，其来源可能是挖矿所得或者别人转账而来，我们会在后续详细描述如何获得比特币，这里我们只关注证明Alice拥有比特币的交易的锁定脚本。

锁定脚本的逻辑格式为：

比特币数量	来源	锁定地址
10	挖矿所得	地址A

如果想花费这个锁定脚本，需要的解锁脚本如下:

解锁地址	解锁
地址A	地址A的公钥、地址A用私钥对前一区块头哈希散列值的签名

具体的解锁过程如下：

1. 使用地址A的公匙推导出地址，与地址A对比，如果一致则证明公匙提供正确，进入下一步。
2. 使用地址A的公匙解密签名，如果获得的值与前一区块的哈希散列值一致，则证明解锁成功，可以花费地址上的10个比特币。

其实，锁定和解锁脚本是通过逆波兰表示法的基于堆栈的脚本实现的，由于本文篇幅有限，这里不展开介绍，会在后续的文章中详细介绍锁定和解锁脚本的原理和流程。

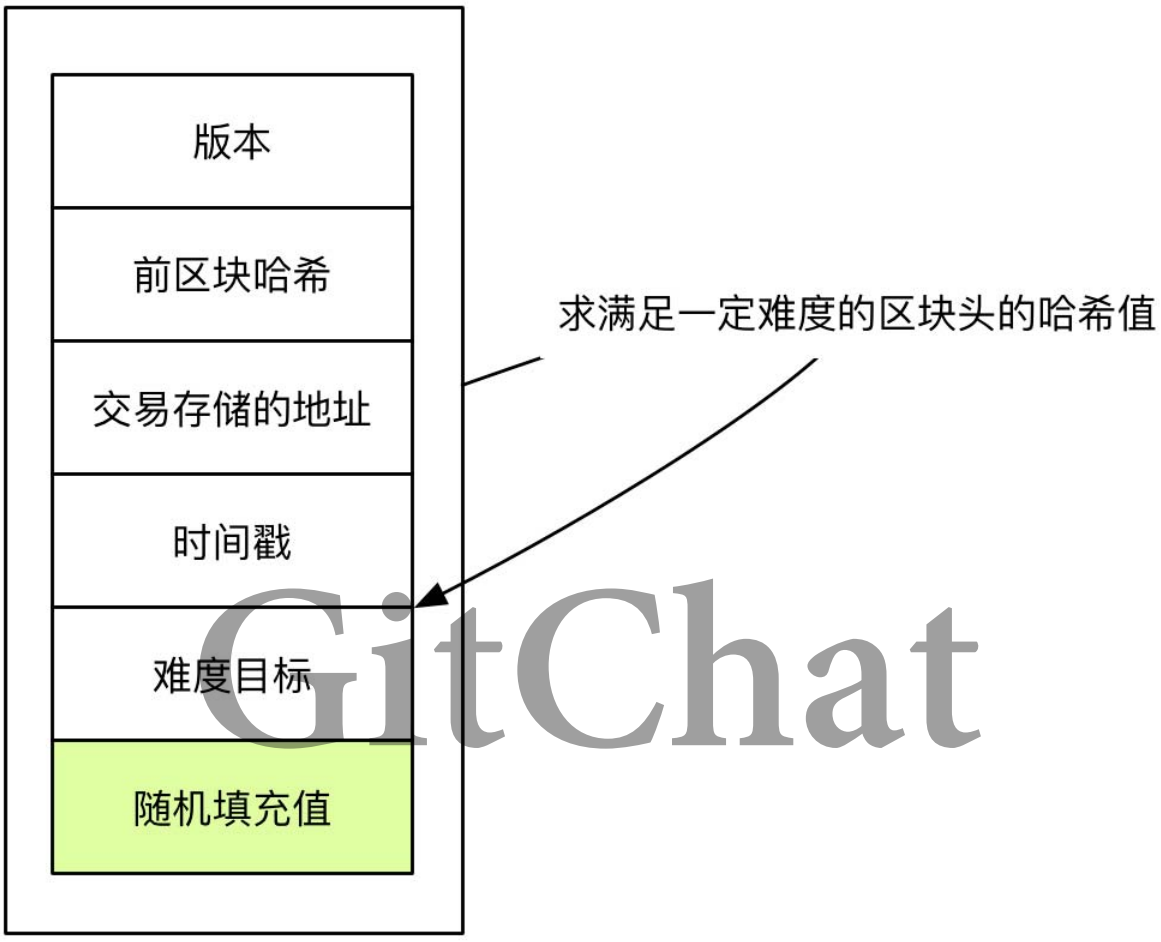
挖矿

上一节介绍了比特币使用分布式存储的区块链作为记账系统，也解决了大家关于如何声明比特币的拥有权，以及把比特币支付给其他人的过程。现在我们遇到了新的问题，既

然区块链是分布式的记账系统，每个参与的节点都有一份拷贝，那么谁来负责把一笔交易记到区块链呢？

这不得不引入一个新的概念，就是共识机制，比特币是通过工作量证明的共识机制来决定记账权的，通俗来讲，谁证明了自己的工作量最大，谁就负责记账。

工作量证明示意图如下：



工作量大小是通过计算符合某一个标准的比特币区块头的哈希散列值来体现的。试图争夺记账权的节点称为挖矿节点，挖矿节点会把网络节点上发来的交易进行验证（网络传播机制会在下一节中介绍），验证后会存入缓冲区，形成一定的交易存储结构（交易使用Merkle树存储，后续问斩各种介绍），放在区块体中，然后根据区块的基本信息构造区块头，区块头通常包含前一个区块的哈希散列值、Merkle根（后续文章会详细介绍）、时间戳、难度目标、以及一个填充的随机值。这里面的随机值是随机产生并且填充的，挖矿过程就是求出一个能够填充本区块头的随机值，让区块头的哈希散列值符合某一个标准，例如：哈希散列值的前某些位为0，难度目标就是用来表达哈希散列值标准的难度系数，可以通过概率算法计算出难度值与挖矿成功的可能性。

网络上的每一个矿机接收并验证了一批交易，然后就开始进行挖矿，视图计算满足某一难度值的区块头的哈希散列值，如果计算成功，则挖矿成功，向全网广播挖矿所得，全网节点验证后，把这个区块连接到区块的最上端，并且在全网达成一致。矿机需要反复的试验随机填充值来进行求解，一般采用产生随机数，尝试把产生的随机数填充到区块

头，然后计算哈希，后续文章会介绍矿机联盟，矿机联盟会把随机数分成多个小区间，分配给联盟中的成员，共同求解。

除了上面介绍的工作量证明机制，还有权益证明、股份制的权益证明共识机制等，后续我会在共识机制的专题文章中与大家分享。

P2P网络

前面两节介绍了比特币的账户体系和记账机制，这节我们讨论比特币的分布式区块链账本是如何在网络上传输，交易又是如何在网络上传输并得到验证的。

比特币网络中的节点都是对等的，没有中心化的服务器，节点有不同的类型，不同的类型有不同的职责，我们会在将来的文章中详细介绍，这里我们只介绍全节点，也就是比特币核心客户端的工作机制。

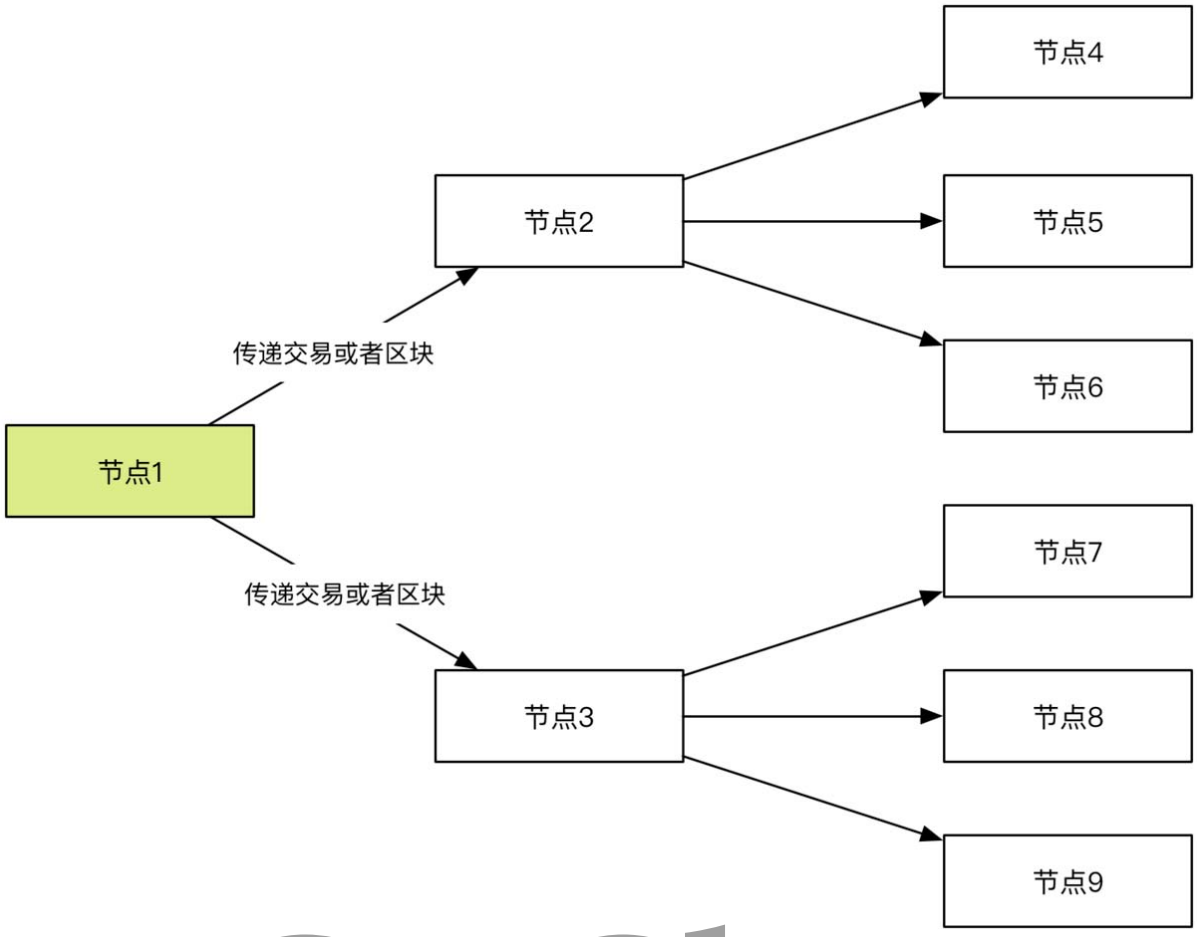
比特币中的全节点除了存储完整区块链，还具有矿工、钱包、路由节点等的角色，他们的职责如下：

1. 矿工：就像挖矿的工人一样，做的是体力活，不断的尝试在构造的区块头的随机字段上填充数字，来找到满足一定标准的哈希散列值，如果找到，把此区块连接到区块链的最上端，并且把合法的区块链发送给邻接节点。

2. 钱包：区块链记载了创币交易和转账交易，这有别于通常意义的账户系统，通常意义的账户系统记录账户余额，而区块链里面只记录了交易，没有余额，钱包就是用来从区块链中算出某个地址拥有区块的余额，如果你学过关系型数据库，你可以把区块链理解为数据库的索引，也可以认为是一本书的目录。

3. 路由节点：负责在去中心化的网络环境中传递交易和区块，一个节点创建一笔交易，并发送给相邻的节点，相邻的节点验证后，再发送给相邻的节点，很快会传遍网络。如果一个节点通过挖矿，找到一个符合标准的区块，这个节点也会用相同的方式传递给相邻节点，然后相邻节点再继续传播下去，让网络的所有节点都达成一致。

P2P网络传播的示意图如下：



我们会在后续的文章中详细介绍比特币P2P网络的工作机制，包括节点分类、节点发现、节点连接和广播等。

区块链学习如何进阶

由于篇幅有限，前文介绍了比特币的三大基础概念，包括区块链、挖矿与P2P网络，然而比特币是个庞大的系统，初学者可能对方方面面都有疑问，这涉及到如何防止双重支付、智能合约、区块链分叉、通缩特性、锁定和解锁脚本、交易的Merkle树存储、交易的存储格式、区块链被攻击的概率、挖矿难度与挖矿成功时间、更多的共识机制、创币交易和转账交易、比特币的性能、不同类型的挖矿节点、以及比特币的应用场景等。

笔者曾经鼓动小伙伴们加入我的比特币和区块链技术研究微信群，

那时候比特别才5000块，是人民币呀 :) 这是一个自由的分享群，每人都参与发言，任何人可以抛出问题，接下来问题是这个样子的，一共有50多个问题，oh..my gosh，多吗？不少？想了解答案吗？想！那就立即跳过问题看后面我分享的材料，看完秒懂这些问题，让你理解比特币和区块链不留死角，是在吹牛吗？嗯，也许不是，看吧，看完真的秒懂。

1. 比特币在哪里？
2. 比特币多少钱？
3. 如何购买比特币？
4. 现在有哪些区块链交易平台？
5. 比特币安全吗？
6. 比特币如何保存？
7. 比特币是世界货币吗？
8. 比特币和区块链的关系？
9. 比特币是谁发明的？
10. 中本聪是谁？
11. 比特币一共有多少个？
12. 现在已经挖了多少比特币了？
13. 产生比特币有多少途径？
14. 哪个国家承认比特币？中国承认比特币吗？
15. 挖矿是什么？如何挖矿？
16. 都谁可以挖矿？
17. 怎么验证一个矿机挖到矿了？
18. 密码学的基本原理？算法加密、对称加密、非对称加密。
19. 比特币的私钥、公匙、公钥哈希、钱包地址都啥关系？
20. 什么是智能合约？
21. 为什么要没10分钟挖矿成功一次？如何保持每10分钟一次，而不是20分钟一次？
22. 区块是怎么连接一起的？又怎么防止篡改的？
23. 挖矿的难度值是怎么确定的？怎么调整的？

24. 比特币为什么是通缩的？比特币挖完了咋办？
25. 共识机制包含哪些？pow、pos、dpos
26. 比特币交易是怎么达成的？包括生产交易和转账交易
27. 区块头的结构？区块头是如何互相串联成链的？
28. 交易是如何存储的，又如何加入一个块的？
29. 账本在哪里？如何获得和存储账本？账本有多大？
30. 什么是Merkle树？如何验证交易？
31. 比特币真的是去中心化吗？
32. 比特币如何使用P2P网络？
33. 比特币的性能如何？每秒只能做7笔交易，交易确认速度真的是10分钟吗？
34. 什么是软分叉和硬分叉？
35. 什么是50%攻击？
36. 公共的账本为什么说没人能更改得了呢？
37. 比特币钱包都有哪些rest api可用？
38. 一个人如何证明自己就是某个地址的拥有者？
39. 比特币与虚拟货币的关系？比特币与法币的关系？
40. 什么是共有链、私有链、联盟链？
41. 什么是侧链、染色链？
42. 什么是莱特币、狗狗币？
43. 区块链除了应用在比特币还有哪些应用场景？
44. 区块链是一项创新吗？
45. 比特币p2p网络节点都有哪些类型？
46. 比特币交易是如何收费的？根据交易数量、金额还是？
47. 那么大的账本每个节点都要下载吗？
48. 比特币钱包真的有钱包吗？什么是纸钱包？
49. 比特币如何保证交易的匿名性？交易所又是如何进行实名认证合规的？
50. 中本聪是如何用数学上的泊松定理证明交易的被攻击的概率的？
51. 比特币还有bug吗？
52. 比特币一笔交易有多大的限制？
53. 什么叫支付到脚本？什么叫支付到公钥哈希？
54. 大家站在扩容派还是保守派的一端？

最正宗的资料

如行业内一个前辈所说，最正宗和最正经的学习比特币和区块链的资料莫过于中本聪发布的比特币论文，我对新技术的学习一直都是先看论文，再看具体的实现或者产品，听到前辈这句话让我感觉像找到了知己一样，一直坚持认为上来就某某框架、某某高大上开源项目、某某微服务实现大规模高并发平台的套路总觉得有点构造空中花园的野路子，于是，马上立刻就把我学习的比特币和区块链资料分享出来，希望能够让更多的人从比特别最原始的概念开始学习，打下良好的基础，再扩展学习会有水到渠成的感觉。

读者可以从下面的连接下载原始论文：

> 中本聪比特币论文[英文版] 密码:x0f8

> 中本聪比特币论文[中文版] 密码: 29fx

精通比特币必看的书籍

学习上面的论文更多的能够帮助你对理论的理解，这篇论文的内容包括了比特币和区块链最核心的思想，那么如果你想从技术上更深入的学习比特别，或者想了解比特别和区块链的实现层次的细节，那么我推荐《精通比特币》这本书，幸好这本书也有中文版。

读者可以从下面的连接下载这本书：

> 精通比特币 密码: bbdb

这本书详细的介绍了P2P网络、交易的过程、钱包的构造、智能合约、共识机制、密码学原理、脚本支付、网络分裂的解决办法等，书中内容可以解决文章开始的所有的问题。

技术进阶的资料

前文说了，虽然论文是一项新技术的灵魂和核心，路边的野花真的就不要了吗？可以时而的换个口味，读读别的文章，看看别人的PPT，学学别人学习途径，还是很有价值的，这里介绍几个对学习比特币有帮助的资料。

1. 一个故事告诉你比特币的原理及运作机制

   > 这是一篇使用比喻讲解比特币的文章，喜欢听故事的看这个就好。

2. 中国区块链技术和产业发展论坛标准(密码：xa8y)

   > 这是国内一个组织制定的区块链标准，想不通这个标准的作用在哪里? :)

3. 区块链与数字货币技术(密码:cu7y)

   > 这是广泛传播的一个比特币和区块链PPT，内容面很广，可以用作导读。

4. 布比区块链产品白皮书(密码:uico)

   > 这是国内一家使用区块链做保存电子资产服务的公司的白皮书，指的阅读。

5. 只能合约PPT(密码:v362)

> 这是一个直接上代码讲解只能合约的PPT，比较难理解，得边看边查资料。

6. 区块链技术指南(密码:2qvg)

> 技术指南比较全面的讲解区块链技术的方方面面。

本文小结

本文从比特币和区块链技术的背景说起，介绍了比特币和区块链技术的来龙去脉，然后，为读者讲解了区块链技术的核心原理，这包括密码学原理、智能合约、P2P网络、解锁脚本等，最后提供了笔者在区块链研究群里收集的初学者常见的问题，并向导读者带着这些问题去阅读笔者提供的资料。阅读完这本书，并读完笔者提供的资料，无论你是技术人员还是业务人员，无论你是初学者还是有一定的基础，都会对比特币和区块链的技术原理有更深入的认识和理解。