2017-12-14

比特币基本原理

0. 比特币的诞生

比特币的诞生应该算在2008年的11月1号的那一天，一个化名为"中本聪"的人在网上发表了一篇论文。 在这篇论文里，他详细的描述了一种崭新的货币体系，他将之命名为"比特币"。

随后，次年的1月3日，首个比特币程序在中本聪的手里诞生，与之一起诞生的是最早挖矿所得的50个比特币。在那之后他开始逐渐淡出，直到彻底的消失。

人们至今也没找出这个叫中本聪的人的真实身份，即使如今的运营商、互联网巨头与政府已将人们在网络上的行迹牢牢掌握在了手里。

他在发言时会经常切换美式和英式英语，他随机在全天不同的时间上线，以隐瞒自己的国籍和时区；他隐藏自己的ip地址，加密自己的邮件，故意伪造一些写作

和发言风格来混淆视听；此外他还是一名造诣颇深的密码学专家，对了，他发表论文的地方就叫做 “密码学邮件列表”。

所以比特币从诞生时起就带上了一种黑客精神：对抗任何势力所强加的审查。

当然我们也可以这么看： 如果一个发明了匿名货币系统的黑客，却连自我身份都不能匿名的话，那整件事会变成一个笑话。

但是所幸，中本聪没让我们失望。

1. 什么是货币

我发现要讲清楚什么是比特币，这一节是无论如何也跑不了的了。我不是什么经济领域的专家，我只能很粗浅且只能在很直观的意义上讲述这个问题。（不过就标题所表达出来的本文主旨而言，似乎也足够了）

高中的课本里有讲过(还记得吗?)，货币是储存价值的媒介，一种东西要成为货币，最重要的，他必须满足：

1. 稀缺性。

   这就是为什么黄金可以而沙子不能被当作货币的原因。稀缺性可以理解为获得它的难度，越是稀缺要获得它就越难。 一个直观的认识是这样的：假设你一个月的薪水是5000元，它意味着人民币的稀缺程度恰好到了这样一个度，即你要付出一个月的劳动才能获得5000个一元。 你不会同意以5000粒沙子来支付你的薪水，是因为与其通过劳动一个月来获得它，你大可以去沙滩走一圈就轻轻松松地得到了。

   那么现在的金融系统是如何保证货币的稀缺性的呢？控制发行。货币的发行是被牢牢掌握在中央银行手中的，这样货币的发行量才能做到可控(所以你现在知道了，私自印钞是违法的）。回到刚刚那个例子, 你同意以5000元来支付你一个月的薪水，是因为人民币发行量刚好到了这个度。如果此时的人民币发行量翻倍了，稀缺度相应降低, 这时候你就应该要求以1万元来支付你的薪水了(但市场的响应往往不会这么快，在这期间你的财富其实是被剥夺了 - - 你的劳动本该获得一万元却只得到5000元的回报)。

2. 交易性

> 货币存在的目的当然是为了交易。就像很多人告诉你的那样，钱是用来花的，不是用来带进棺材的。所以除了满足稀缺性以外，一种东西它越是方便交易，那么他就越符合理想货币的标准。所以在货币史上，银元代替了贝壳，纸币代替了银元，数字货币正逐渐取代纸币。
>
> 这里所说的"交易"，是指财产从一方转移到另一方，即一方的财产减少相应的另一方增多。对实物货币来说，它发生得非常自然，甲要给100元乙，当100元钞票从甲的手里转移到乙的手里的那一瞬间，交易完成了，甲的财产减去了100元而乙的财产增加了100元，这个过程中没有第三方的参与，完全是甲和乙之间的私密行为；然而当交易发生在数字货币层面上时，就没这么简单了，甲要给100元给乙，如何确保交易完成了呢？假设甲和乙在各自的电脑上记录了自己的财富数额的话，那么如何确保乙在给自己增加了100元的时候甲如实地给自己减去了100元呢？这个时候我们不得不要引入第三方了 - - 我们称之为"银行"的那个家伙。 当甲要转移100元给乙时，他不是直接给乙而是给银行， "请把我的100元转给乙"，于是银行在甲的帐目上扣掉100元，再在乙的帐目上加上这100元。(我们假设它慷慨地不收取任何交易费)

以上所说的就是现代货币系统的一个粗廓模型，这个模型最大的弊端在于：人们不得不去信任一个中心系统。

数字货币的交易必须依赖银行，而一个人的银行账号可能会被审查、限制甚至是剥夺。当一方想要给另一方转移自己的财富时，银行可以收取高昂的费用或者直接拒绝(比如你试试汇一笔钱给美国的亲戚）。

货币的发行必须依赖中央银行。好吧，这已经是一个广为人知的秘密了：货币一直在贬值，或者说货币一直在超额发行(想想20年前的100块跟现在的100块)。我引用两段话， 一段来自凯恩斯,

> 通过连续的通货膨胀过程，政府可以秘密地、不为人知地没收公民财富的一部分。用这种办法可以任意剥夺人民的财富，在使多数人贫穷的过程中，却使少数人暴富。

另一段，出自哈耶克,

> 政府无法克制滥发货币的冲动

那么有没有可能设计出一套货币系统，在这个系统里我们不需要一个中心机构，不用被迫去信任任何的第三方， 使货币的发行透明可控，货币的交易私密而安全呢?

你猜?

2. 什么是比特币

所以我们现在可以回答到了，比特币是一个发行去中心化和交易去中心化的电子货币系统。在这个系统里，货币的发行量是透明且可预期的，货币的交易利用整个网络的协同合作来保证交易的安全。

下面我将逐步拆解比特币的原理。需要注意的是，比特币作为一个已经实际在使用的产品，它本身有着非常丰富的细节。本篇目的是向没有技术背景的读者讲述比特币的基本原理，因此并不会涉及到这些细节。比如说钱包的地址其实并不是公钥，而是公钥的二次哈希值； 区块链的难度要求并不是简单的把所有区块链的内容做一次哈希运算；等等。但是为了叙述的简洁性，在不影响对基本原理的讲解下这些都做了简化处理，希望大家能够理解。

2.0. 比特币网络 – 由众多运行着比特币程序的节点组成

比特币是一个由众多平等的节点组成的网络。

一个节点就是一个比特币程序，任何能够连上网和具有一定计算能力的机器都能运行这个程序 - - 所以你家里的电脑也可以作为比特币网络里的节点:)

节点之间是可以互相通讯的，同时比特币有一套机制可以让一个节点向其他所有节点发出消息，这个行为被称为"广播"。

2.1. 区块链 – 一个公共的账簿

我们先回到银行的例子。银行最基本的功能，无非是维护一个账簿，而这个账簿只需如实记录每一笔交易而已。比如X年X月X日，王小明转了30块钱给张大毛；Y年Y月Y日，张大毛转了12块钱给李小豆，诸如此类。 根据这个账簿我们可以查到一个人的所有交易记录，因而也就能推算出这个人此刻的账户余额为多少。比如李小豆从建银行帐号开始，转进的交易合计500元，转出的交易合计300元，那么可以算出此时李小豆账户余额一定是200元。

维护好这个账簿，并且作为唯一的维护者(只有银行才有权力查看和修改)， 银行作为一个交易中心的职责就完成了。

比特币也有账簿，但是与银行不同的是，这个账簿是公开的，任何人可以去查看和审核它。

这个账簿被称为**区块链**。你可以把区块链想象成一个小册子，册子的每一页写满了交易信息，并且不断有新的页加入进来。

2.2 钱包 – 由一对公钥和私钥构成的的账户

上面一小节，解释了什么是比特币的账簿。这一小节将解释这个账簿里资金的归属权问题，亦即比特币的帐户系统。

比特币里的帐户跟银行的帐户有本质的区别。

在银行账户下，银行记录下了该账户所有者的身份信息(回想一下你去银行开户时提交的资料：照片、身份证、电话号码、家庭住址....)，因而只要你能向银行证明你的身份，你也就获得了你名下财产的所有权。在这种模型下，银行扮演了一个全知全能的上帝角色：他知晓现实人们的财富信息。我们除了祈祷上帝不要把我们的信息泄露出去或者利用它干坏事以外，别无他法。

在比特币的世界里，并没有银行这样一个机构，它不会强制人们暴露自己的身份以换取资金的安全。比特币的帐户只是简单的由两串数字构成，分别被称为“公钥”和“私钥”，除此之外再无其他。

这个两个数字所具有的数学特性 - **一个被私钥加密过的数据只能通过公钥来解开，所谓的非对称加密** - 使它们能够完美的实现一个帐户(比特币世界里被称为钱包)需要的功能。

我们把公钥作为帐户地址 - - 在比特币世界里也称钱包地址 - - 它类似于银行系统里的帐号，就是当你告诉别人“请给我的帐号打300块钱”时，需要告诉别人的那一串数字。对银行来说，它是“招商银行6214850200251100”，对比特币而言，它是“1Hyg1CvfZZNjsjgu9H98GF6zeCX4hX812y ”。

私钥，是证明钱包所有权的*唯一*凭证，你通过证明你是该钱包的私钥持有者来获得该钱包的所有权。注意，和银行账号的密码不同的是，你丢失了密码还可以通过证实自己的身份来找回，但你一旦丢失了密钥那这个钱包里的资金就再也找不回了。

因为公钥和私钥所具备的非对称加密的美妙特性，钱包的所有者并不需要通过出示私钥来证明自己持有它。他只需要出示一段用私钥加密过的文字，验证者能用公钥(即钱包地址)解开这段文字即能证明。

那么怎么生成一对这样的数字呢?

相比于银行开户的繁琐手续，你唯一需要的只是一个实现了该功能的数学软件。

感谢数学。

2.3 区块 – 有难度要求的账簿页

前面提到，区块链就是一个账簿，一个区块就是这个账簿里固定大小的一页。(比特币规定区块大小不超过1M，而一笔交易大约250字节大小，因此一个区块平均能写下4000笔左右交易。)

区块链是公共的，每个人都可以下载，验算和查看区块链里的交易信息。同时每个人也都可以向区块链增加区块，只是我们需要一种机制来防止坏人们通过提交大量的区块来拖垮整个网络。这个机制的核心在于我们要使区块的构造变得有代价，代价大到不可能在短时间内构造出大量的区块。

比特币要求，一个合法的区块必须满足:

1. 该区块内的交易必须都是合法的，即签名必须正确,钱包余额必须大于等于转出的数额等等;

2. 该区块必须使区块链具有某种特征的哈希值.

   哈希值是一种数学运算(感谢数学！)，你可以简单理解为对数据的摘要，不同的数据有不同的哈希值，即使两个数据只相差一个字节，他们对应的哈希值也会截然不同。

比特币通过"要求区块链的哈希值具有某种特征"来控制构造区块的难度，这个特征其实就是要求哈希值开头的几位数字为0. 比方说当前比特币要求哈希值前4位必须为0，我们用P表示当前的区块链，用B表示当前构造的区块，那么P + B的哈希值前4位必须为0该区块B才能被允许加入区块链中。 这里要注意三点， 1. 要构造出这样一个区块没有捷径，必须通过大量的计算，一遍一遍的往B里放随机数直到P + B的哈希值满足要求为止。相同的难度要求, 算力(计算能力)越大的，

率先构造出满足要求的区块的概率就越大 2. 哈希值前面为0的位数越多，要构造出这个区块的难度就越大。

好了，我们现在有了控制区块构造难度的工具了，那么比特币通过什么样的规则来控制难度呢?

比特币规定区块链应保持在平均每两周时间增加2016个区块(也就是平均10分钟一个)的速度上。 也就是说，每增加2016个区块，系统就会算出产生这2016个区块的时间，如果它小于两周那么就提高接下来2016个区块的难度(比如从要求哈希值前3个必须为0提高到前4个为0)， 如果它大于两周就降低难度(比如从要求4个0降低到3个0), 这样从长远来看，就使区块链平均以每10分钟一个的速度增加了。

也因此可以推论，区块链的难度要求与全网构造区块的算力成正相关关系。也就是说，参与构造区块的算力增加那么难度要求就会提高，相反则会降低，这样才能使区块链以固定的速度增加。

上面提到，让构造区块变得有难度，是为了防止被坏人攻击。同时，它还有一个作用是防止坏人们将一笔钱花两次(所谓双花问题)。 我们看如下一个比特币的应用场景:

小张要用比特币在小李那里网购一个商品，

1. 小李用数学软件生成好一个比特币钱包，并将该钱包地址(公钥)告诉小张。
2. 小张选取了自己一个有足够余额的钱包，并用这个钱包的私钥签发了一笔交易(该交易把一部分比特币发到小李的钱包地址上)，然后把交易广播给全网络。
3. 网络中的一些节点把该交易收纳到当前正在构造的区块中。 第一个成功构造出合法区块的节点把该区块广播给全网络，得到全网络的认可被加到区块链上。
4. 小李发现区块链上已经有一个区块包含了指向自己钱包地址的交易，并且交易金额正确。 小李随即给小张发货。
5. 小张发现小李已经发货，这时他开始重新构造一笔交易，试图把刚刚发给小李的钱发到自己另外的一个钱包里。这个时候他不能再把这笔交易广播出去了，因为网络中的其它节点会发现该交易是不合法(花掉一笔已经花掉的钱)

而直接拒绝掉， 小李只能自己构造一个包含了该交易的区块，并且试图说服网络中的其它节点他的这个节点才是合法而刚刚那个(包含发给小李交易的区块)是不合法的， 这样就能实现他一笔钱花两次的目的。

比特币规定当区块链发生分叉时(即出现了两个或以上互斥的合法区块)时，应该追随最长的那条。 那意味着小张要实现自己双花目的，他必须在产生了小李那个区块后，马上构造出两个区块来，才能说服其他节点跟随自己的这条链。 要达到这个目的，当前时间内他必须拥有(或者接近拥有了)全网51%的算力, 才能抢在其他所有节点之前构造出两个区块出来。

2.4 矿工 – 通过挖矿来争夺记账权的区块链维护者们

前一节我们讲到，区块链的难度实际上是对区块链的保护，这个难度要求越高区块链就越免于被坏人攻击。换个方式表述就是，全网构造区块的算力保障了区块链的安全，全网的算力越高，那么坏人们获得全网51%算力的难度就越大，因此越不容易被攻击。

那么我们如何激励节点们贡献出自己的cpu跟电力来提高全网的算力呢？ 答案是区块奖励。

比特币规定，成功构造出合法区块的节点会获得一部分比特币作为奖励，这部分比特币是系统生成的，他类似于淘金业里的挖矿，通过辛勤的劳动增加了黄金(比特币)的流通总量，因此构造区块的过程被称为“挖矿”，企图通过挖矿来获得区块奖励的节点被称为“矿工”。

挖矿的意义:

1. 它激励节点们贡献出算力来保护网络
2. 它实现了一种公平的方式发行比特币，因为不存在一个中央发行机构。

除了区块奖励外，交易者还可以通过额外支付一笔交易费给矿工们来鼓励他们将自己的交易收纳到它的区块里。这样当区块奖励趋于0时(比特币总量2100万枚，意味着越到后面区块奖励会越少), 因为有交易费的存在，矿工们也会继续维护整个网络。值得注意的是这里的交易费跟银行转账费有所不同，银行的转账费是由银行自上而下规定的，比特币的交易费是由使用者自由设置自下而上竞争的结果(如果当前交易数量很多而你给的交易费太低的话，可能不会被矿工们收取。）

亦即，矿工成功挖到区块时，他将获得 1）区块奖励 2）该区块内所有交易的交易费。

2.5 总结

比特币的核心是一个公共的账簿–区块链，每个人都可以核算查看这个账簿里的交易信息。这个账簿里不会记录任何真实世界里的个人信息，比特币保护了使用者的隐私。

通过非对称加密，用户可以不用出示密钥就可以证实自己是该密钥的持有者。因此提供了一个安全的不用信赖任何第三方(对比银行，你必须信赖它不把你的账号密码泄漏出去)的方式发起一笔交易。

因为比特币是开放的，意味着任何人都可以攻击比特币网络。通过控制区块的难度，使比特币网络免疫于大部分的攻击除非攻击者获取了接近全网51%的算力。而矿工们是比特币网络的保护者，比特币通过区块奖励和交易费的方式激励他们贡献出自己的cpu，组成巨大的算力屏障，使得任何组织或个人想要发起51%算力攻击都成为不可能。

3. 结束语

刚刚过去的2018年1月3日，是比特币诞生的第9年。比特币的第一个区块正是在9年前的这一天向全世界宣告了它的诞生。在这个创世区块里，中本聪意味深长的写下了一句话，正是当天泰晤士报的头版标题:

> 2009年1月3日，财政大臣正准备第二次拯救银行。

那一年美国次贷危机。 9年过去了，很多人已经忘了这场全球金融危机的肇因，同时对于比特币所描绘的自由远景也不屑一顾。但是我相信，人们之所以认为这样的自由不重要，是因为他们从未得过这样的自由。

9年过去了，比特币完成了很多事，还有更多的事尚未完成。就像丘吉尔曾说过的那样，

> 这不是结束,这甚至不是结束的开始,但这毕竟是开始的结束.