比特币:一种点对点电子货币系统

中本聪
satoshin@gmx.com
www.bitcoin.org

摘要：点对点的电子货币将允许在线支付直接从一方发送到另一方，无需经过金融机构。数字签名提供了部分解决方案，但是如果仍然需要一个可信任的第三方来防止重复消费，那么主要的好处就失去了。我们提出了一个使用点对点网络的双向消费问题的解决方案。网络通过将交易散列到一个持续的基于散列的工作量证明链中来给交易添加时间戳，形成一个在不重新执行工作量证明的情况下无法更改的记录。最长的链不仅可以证明所见证的事件序列，还可以证明它来自最大的 CPU 功率池。只要 CPU 的大部分功率是由不合作攻击网络的节点控制的，它们就会产生最长的链并超过攻击者。网络本身需要最小的结构。消息以最佳方式广播，节点可以随意离开或重新加入网络，接受最长的工作量证明链作为它们离开时发生的事情的证据。

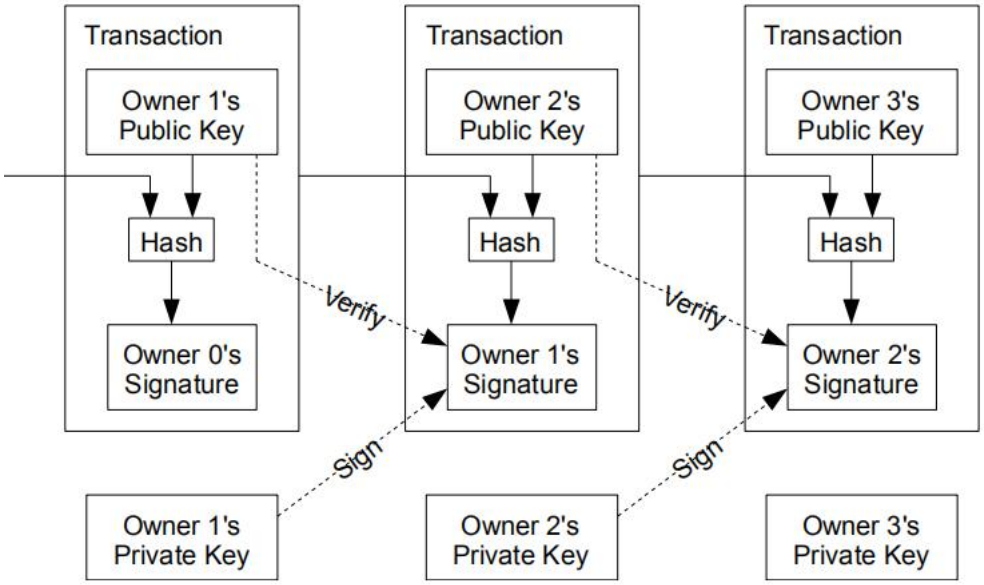
1. 介绍

互联网上的商业几乎完全依赖金融机构作为可信赖的第三方来处理电子支付。虽然该系统对于大多数事务都能很好地工作，但它仍然受到基于信任模型的固有弱点的影响。完全不可逆转的交易实际上是不可能的，因为金融机构无法避免调解纠纷。中介的成本增加了交易成本，限制了最小的实际交易规模，切断了小型非正式交易的可能性，对不可逆服务失去进行不可逆支付的能力，这是更广泛的成本。随着逆转的可能性，对信任的需求扩大了。商家必须对他们的顾客保持警惕，为了获取他们原本不需要的更多信息而与他们纠缠不休。一定比例的欺诈被认为是不可避免的。这些成本和支付的不确定性可以通过使用实物货币亲自避免，但没有一种机制可以在没有可信任方的通信通道上进行支付。

我们需要的是一个基于加密证明而不是信任的电子支付系统，允许任何两方直接进行交易，而不需要可信的第三方。在计算上无法逆转的交易可以保护卖家免遭欺诈，而常规的托管机制可以很容易地实现来保护买家。在本文中，我们提出了一种解决双花费问题的方法，使用一个点对点的分布式时间戳服务器来生成事务的时间顺序的计算证明。只要诚实的节点集体控制的 CPU 功率比任何协作的攻击节点组都多，系统就是安全的。

2. 交易

我们把电子货币定义为一系列数字签名。每个所有者通过数字签名前一次交易的散列和下一个所有者的公钥，并将它们添加到硬币的结尾，将硬币转移到下一个所有者。收款人可以验证签名以验证所有权链。

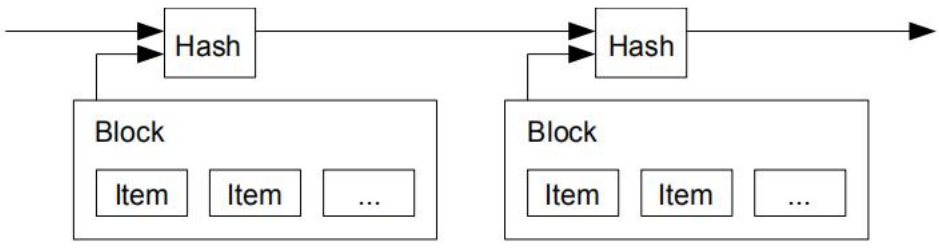


问题当然是收款人无法证实其中一个所有者没有双倍消费硬币。一个常见的解决方案是引入一个可信的中央权威机构，或铸币局，它检查每一个交易是否有双重消费。每次交易后，硬币必须返回铸币厂发行一枚新硬币，只有直接从铸币厂发行的硬币才被信任不会被重复使用。这种解决方案的问题在于，整个货币系统的命运取决于铸币厂的运营公司，每笔交易都必须经过铸币厂，就像银行一样。

我们需要一种方式让收款人知道以前的所有者没有签署任何早期的交易。就我们的目的而言，最早的交易是算数的，所以我们不关心后来的重复消费尝试。确认没有交易的唯一方法是了解所有的交易。在基于造币厂的模型中，造币厂知道所有的交易，并决定哪一个先到达。要在没有受信任方的情况下实现这一点，事务必须公开宣布，我们需要一个系统，让参与者对接收到的订单的单个历史记录达成一致。收款人需要证明在每次交易时，大多数节点都同意它是第一个收到的。

3. 时间戳服务器

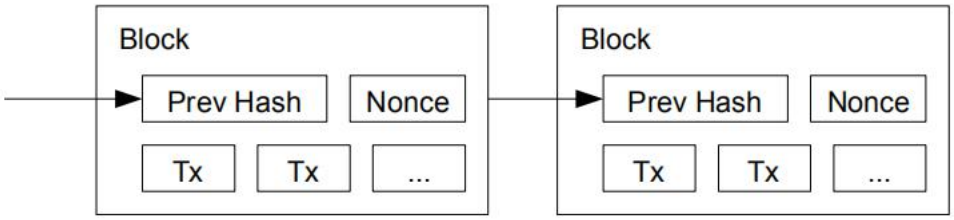
我们从时间戳服务器开始提出解决方案。时间戳服务器的工作方式是对要打时间戳的项目块进行散列，并广泛发布散列，比如在报纸或文章中。时间戳显然证明了数据在当时必须存在，以便进入散列。每个时间戳在其散列中包括前一个时间戳，形成一个链，每个额外的时间戳加强它之前的时间戳。



4. 工作量证明

要在对等基础上实现分布式时间戳服务器，我们需要使用类似 Adam Back 的哈希的工作量证明系统，而不是报纸或帖子。工作证明涉及到扫描一个值，当散列(例如使用 SHA- 256)时，散列以一些零位开始。所需的平均工作以所需零位数为指数，可以通过执行单个散列来验证。

对于我们的时间戳网络，我们通过在块中增加一个 nonce 来实现工作证明，直到找到一个给块哈希所需的零位的值为止。一旦 CPU 工作被花费以满足工作量证明，就不能在不重做工作的情况下更改块。由于后面的块是在它之后链接的，更改块的工作将包括在它之后重做所有的块。



工作量证明还解决了多数决策中确定代表性的问题。如果大多数是基于“一个 IP 地址一票”，那么任何人都可以分配许多 IP 地址，这就会被颠覆。工作证明本质上是“一个 CPU 一票”。多数决策由最长的链表示，最长的链具有最大的证明工作投入。如果大部分 CPU 功率由诚实节点控制，诚实链将增长最快，超过任何竞争链。为了修改过去的区块，攻击者必须重做区块及其后所有区块的工作量证明，然后追赶上诚实节点并超过它们的工作量。稍后我们将展示，随着后续块的加入，较慢的攻击者追赶的概率呈指数递减。

为了补偿不断增长的硬件速度和随着时间的推移对运行节点的不同兴趣，工作证明的难度由每小时平均块数的移动平均值决定。如果它们的生成速度太快，难度就会增加。

5. 网络

运行该网络的步骤如下：

1) 新的交易向全网进行广播；
2) 每一个节点都将收到的交易信息纳入一个区块中；
3) 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；
4) 当一个节点找到了一个工作量证明，它就向全网进行广播；
5) 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；
6) 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。节点始终都将最长的链条视为正确的链条，并持续工作和延长它。如果有两个节点同时广播不同版本的新区块，那么其他节点在接收到该区块的时间上将存在先后差别。当此情形，他们将在率先收到的区块基础上进行工作，但也会保留另外一个链条，以防后者变成最长的链条。该僵局（tie）的打破要等到下一个工作量证明被发现，而其中的一条链条被证实为是较长的一条，那么在另一条分支链条上工作的节点将转换阵营，开始在较长的链条上

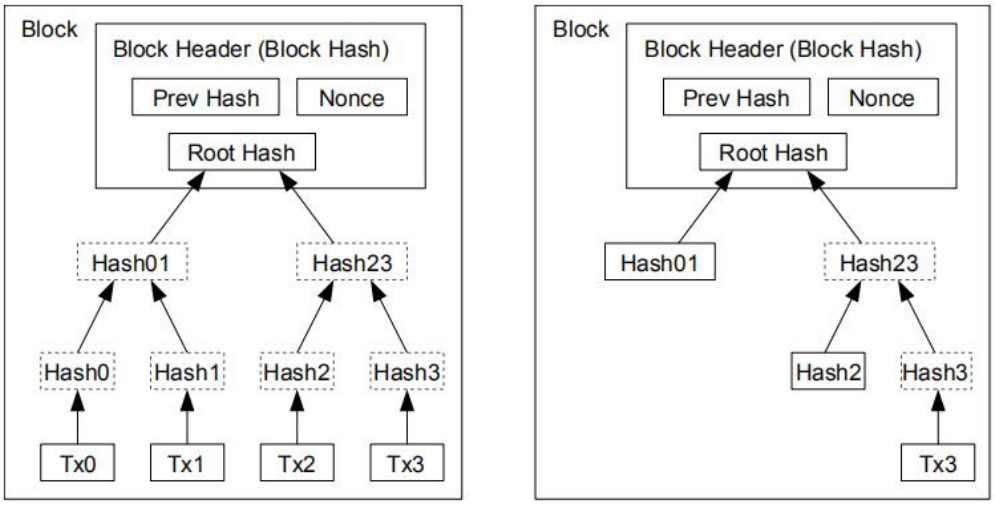
工作。 所谓“新的交易要广播”，实际上不需要抵达全部的节点。只要交易信息能够抵达足够多的节点，那么他们将很快被整合进一个区块中。而区块的广播对被丢弃的信息是具有容错能力的。如果一个节点没有收到某特定区块，那么该节点将会发现自己缺失了某个区块，也就可以提出自己下载该区块的请求。

6. 激励

我们约定如此：每个区块的第一笔交易进行特殊化处理，该交易产生一枚由该区块创造者拥有的新的电子货币。这样就增加了节点支持该网络的激励，并在没有中央集权机构发行货币的情况下，提供了一种将电子货币分配到流通领域的一种方法。这种将一定数量新货币持续增添到货币系统中的方法，非常类似于耗费资源去挖掘金矿并将黄金注入到流通领域。此时，CPU 的时间和电力消耗就是消耗的资源。 另外一个激励的来源则是交易费（transaction fees）。如果某笔交易的输出值小于输入值，那么差额就是交易费，该交易费将被增加到该区块的激励中。只要既定数量的电子货币已经进入流通，那么激励机制就可以逐渐转换为完全依靠交易费，那么本货币系统就能够免于通货膨胀。 激励系统也有助于鼓励节点保持诚实。如果有一个贪婪的攻击者能够调集比所有诚实节点加起来还要多的 CPU 计算力，那么他就面临一个选择：要么将其用于诚实工作产生新的电子货币，或者将其用于进行二次支付攻击。那么他就会发现，按照规则行事、诚实工作是更有利可图的。因为该等规则使得他能够拥有更多的电子货币，而不是破坏这个系统使得其自身财富的有效性受损

7. 回收硬盘空间

如果最近的交易已经被纳入了足够多的区块之中，那么就可以丢弃该交易之前的数据，以回收硬盘空间。为了同时确保不损害区块的随机散列值，交易信息被随机散列时，被构建成一种 Merkle 树 的形态，使得只有根(root)被纳入了区块的随机散列值。通过将该树（tree）的分支拔除（stubbing）的方法，老区块就能被压缩。而内部的随机散列值是不必保存的。

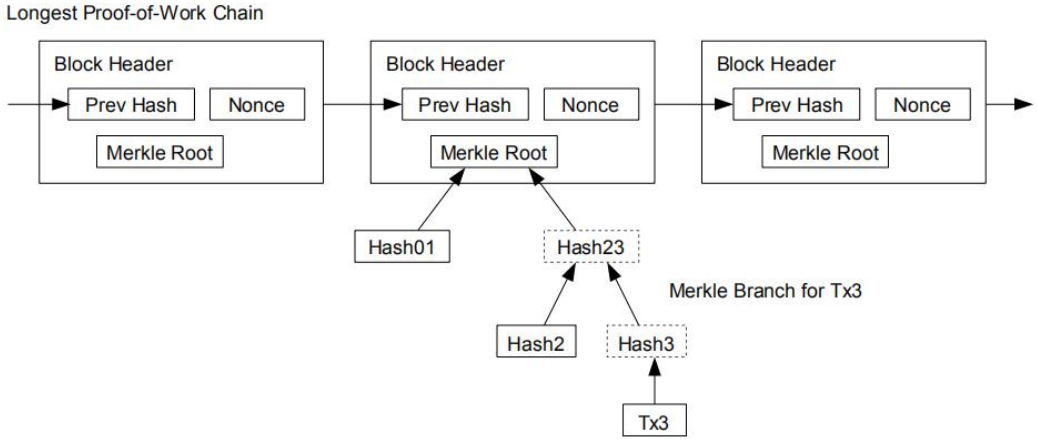


Transactions Hashed in a Merkle Tree　　After Pruning Tx0-2 from the Block

不含交易信息的区块头大小仅有 80 字节。如果我们设定区块生成的速率为每 10 分钟一个，那么每一年产生的数据位 4.2MB。（80 bytes * 6 * 24 * 365 = 4.2MB）。2008 年，PC 系统通常的内存容量为 2GB，按照摩尔定律的预言，即使将全部的区块头存储于内存之中都不是问题。

8. 简化的支付确认

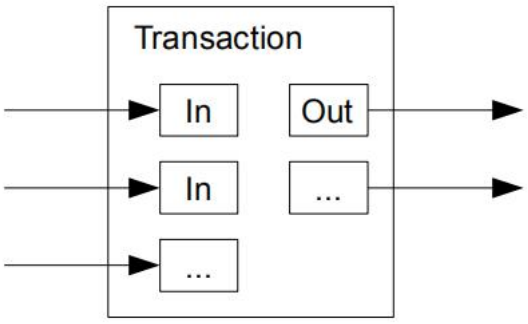
在不运行完整网络节点的情况下，也能够对支付进行检验。一个用户需要保留最长的工作量证明链条的区块头的拷贝，它可以不断向网络发起询问，直到它确信自己拥有最长的链条，并能够通过 merkle 的分支通向它被加上时间戳并纳入区块的那次交易。节点想要自行检验该交易的有效性原本是不可能的，但通过追溯到链条的某个位置，它就能看到某个节点曾经接受过它，并且于其后追加的区块也进一步证明全网曾经接受了它。



当此情形，只要诚实的节点控制了网络，检验机制就是可靠的。但是，当全网被一个计算力占优的攻击者攻击时，将变得较为脆弱。因为网络节点能够自行确认交易的有效性，只要攻击者能够持续地保持计算力优势，简化的机制会被攻击者焊接的交易欺骗。那么一个可行的策略就是，只要他们发现了一个无效的区块，就立刻发出警报，收到警报的用户将立刻开始下载被警告有问题的区块或交易的完整信息，以便对信息的不一致进行判定。对于日常会发生大量收付的商业机构，可能仍会希望运行他们自己的完整节点，以保持较大的独立完全性和检验的快速性。

9. 价值组合与分割

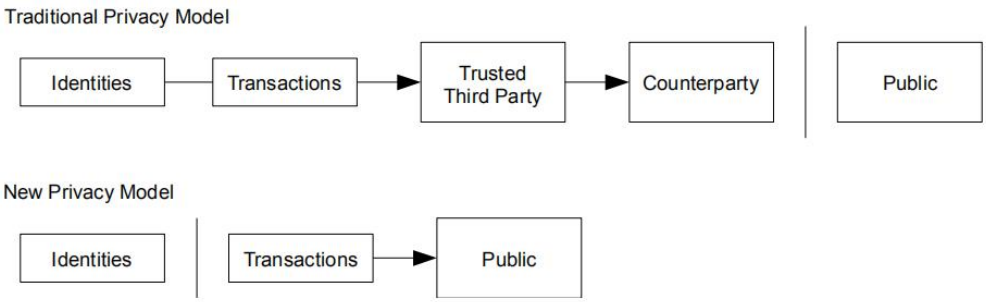
虽然可以单个单个地对电子货币进行处理，但是对于每一枚电子货币单独发起一次交易将是一种笨拙的办法。为了使得价值易于组合与分割，交易被设计为可以纳入多个输入和输出。一般而言是某次价值较大的前次交易构成的单一输入，或者由某几个价值较小的前次交易共同构成的并行输入，但是输出最多只有两个：一个用于支付，另一个用于找零（如有）。



需要指出的是，当一笔交易依赖于之前的多笔交易时，这些交易又各自依赖于多笔交易，但这并不存在任何问题。因为这个工作机制并不需要展开检验之前发生的所有交易历史。

10. 隐私

传统的造币厂模型为交易的参与者提供了一定程度的隐私保护，因为试图向可信任的第三方索取交易信息是严格受限的。但是如果将交易信息向全网进行广播，就意味着这样的方法失效了。但是隐私依然可以得到保护：将公钥保持为匿名。公众得知的信息仅仅是有某个人将一定数量的货币发所给了另外一个人，但是难以将该交易同特定的人联系在一起，也就是说，公众难以确信，这些人究竟是谁。这同股票交易所发布的信息是类似的，股票交易发生的时间、交易量是记录在案且可供查询的，但是交易双方的身份信息却不予透露。



作为额外的预防措施，使用者可以让每次交易都生成一个新的地址，以确保这些交易不被追溯到一个共同的所有者。但是由于并行输入的存在，一定程度上的追溯还是不可避免的，因为并行输入表明这些货币都属于同一个所有者。此时的风险在于，如果某个人的某一个公钥被确认属于他，那么就可以追溯出此人的其它很多交易。

11. 计算

设想如下场景：一个攻击者试图比诚实节点产生链条更快地制造替代性区块链。即便它达到了这一目的，但是整个系统也并非就此完全受制于攻击者的独断意志了，比方说凭空创造价值，或者掠夺本不属于攻击者的货币。这是因为节点将不会接受无效的交易，而诚实的节点永远不会接受一个包含了无效信息的区块。一个攻击者能做的，最多是更改他自己的交易信息，并试图拿回他刚刚付给别人的钱。 诚实链条和攻击者链条之间的竞赛，可以用二叉树随机漫步（Binomial Random Walk)来描述。成功事件定义为诚实链条延长了一个区块，使其领先性+1，而失败事件则是攻击者的链条被延长了一个区块，使得差距-1。 攻击者成功填补某一既定差距的可能性，可以近似地看做赌徒破产问题（Gambler’s Ruin problem）。假定一个赌徒拥有无限的透支信用，然后开始进行潜在次数为无穷的赌博，试图填补上自己的亏空。那么我们可以计算他填补上亏空的概率，也就是该攻击者赶上诚实链条。

12. 结论

我们在此提出了一种不需要信用中介的电子支付系统。我们首先讨论了通常的电子货币的电子签名原理，虽然这种系统为所有权提供了强有力的控制，但是不足以防止双重支付。为了解决这个问题，我们提出了一种采用工作量证明机制的点对点网络来记录交易的公开信息，只要诚实的节点能够控制绝大多数的 CPU 计算能力，

就能使得攻击者事实上难以改变交易记录。该网络的强健之处在于它结构上的简洁性。节点之间的工作大部分是彼此独立的，只需要很少的协同。每个节点都不需要明确自己的身份，由于交易信息的流动路径并无任何要求，所以只需要尽其最大努力传播即可。节点可以随时离开网络，而想重新加入网络也非常容易，因为只需要补充接收离开期间的工作量证明链条即可。节点通过自己的 CPU 计算力进行投票，表决他们对有效区块的确认，他们不断延长有效的区块链来表达自己的确认，并拒绝在无效的区块之后延长区块以表示拒绝。本框架包含了一个 P2P 电子货币系统所需要的全部规则和激励措施。