比特币是如何记录交易的

记录事物的工具大体为两类：令牌和分类账

信息的移动意味着复制

信息存在于一个地方，要移动它，必须将它复制到另一个地方，并在原来的地方删除它。而在物理领域的移动则不同，你可以直接将东西从A移动到B。物理令牌是由原子组成的一个特定的实体，是无法（难以）复制的。而纯信息则没有这种特性，如果你可以读取信息，你就可以分毫不差的复制信息。

对物理令牌而言，交易发生的时间并不重要

一枚硬币，在你交易完成时，就从你手中转移到了对方手中。自然法则保证了这枚硬币不会在10:00花出，却在10:30才从你的手中转移到对方手中，也不会在你花出后，同时出现在你和对方的手中。从这个意义上讲，物理令牌具有无信任、无时间的特性。

数字令牌的移动存在时间差

数字令牌从本质上看，就是数字信息。正如前面所说信息要想移动，只能先复制再删除，不能做到物理世界中的直接移动。因此，需要记录交易的时间，在该时刻之后，这枚数字硬币的所有权便不属于你，尽管可能此时你的"钱包"中还存在这枚硬币的信息（复制删除的动作还没有结束）。由此来看，数字令牌不具备无信任、无时间的特性，也不是一个独特、单一、不可复制的实体，严格来说，数字"令牌"并不是令牌了。

所以，令牌这个方案在数字领域不可行。那么再来看看分类账是否可行呢?

数字分类账都存在潜在的双花问题

使用分类账交易的过程大体分为两步：记录交易和转移货币。双花问题存在于转移之前。一般来说，双花问题分为两种情况：一种是记账前双花，一笔钱花出去，由于延迟问题，本地交易记录还没有和集中式记账系统同步，你可以在系统记账前再次花出这笔钱；另一种是记账后的双花，一笔钱花出去，记账系统已经同步，但如果你攻击系统，在这笔钱真正被转移前从账本上删除了这笔交易记录，这笔钱将还属于你，你当然可以接着花。解决双花问题的通用方法是通过一个中心机构来列出交易记录，这个唯一账本由中心机构全权管理，即便出现双花问题，也可以由中心机构追回并追责。

去中心化不能存在中心机构

去中心化的系统应该是一个无监督、自信任的系统，不会有人或机构拥有更高的权利，每个节点都是完全平等的个体，我们所信任的就是这个自动化系统本身。其实真正重要的并不是中心系统本身，而是中心系统确定的时间，这个绝对的时间保证了账本上的交易记录有着唯一的顺序，有序的账本可以轻松找出并纠正错误。

去中心化的时间

在去中心化的分布式系统中，如何确定一个统一的时间呢？跟物理的文档不同，数字文档可以轻易被修改，而且修改也不会在物理存储介质上留下任何痕迹。在数字世界，我们可以不留痕迹的修改和伪造。信息的可修改性使得给数字文档加盖时间戳变得非常复杂，一些简单的方案根本不可行。比如这篇文章，简单的在文末加一个日期并没有什么用，因为任何人都可以修改这个日期。

Haber和Stornetta在他们1991年的论文中指出：数字时间戳就是要找到一个可行的计算过程使得改变一个数字文件的时间戳变得不可能。

不可预测的时间

编造日期是一个普遍问题，即使在非数字领域也是如此。绑架界所熟知的"报纸认证"是解决任意时间戳问题的通用解决方案。这种方法很有效，因为报纸很难造假且容易验证。报纸难以造假是因为他会引用昨天发生的事情，绑架者不可能在几个星期之前预测这些事情，所以这个带着保持的图片就可以证明被绑架人在报纸发行的时间还活着。比特币通过重新定义时间的概念解决了这个问题。比特币不用秒计时，而是区块。就好像没人可以预测明天的报纸头版一样，没人可以预测下一个人比特币区块的内容。你不能预测下一个区块包含哪些交易，因为你不能预测未来被广播的交易。更重要的是，你不能预测下一个区块是谁提出来的以及其工作量证明的解。

现在，通过不可预测的区块解决了编造未来时间情况，但过去的区块是已知的，仍然可以加盖过去的任意时间。

蝴蝶效应

"一只南美洲亚马逊河流域热带雨林中的蝴蝶，偶尔扇动几下翅膀，可以在两周以后引起美国得克萨斯州的一场龙卷风。"过去种种，皆成今我。历史上每一环都紧紧相扣，哪怕修改一丝一毫都会形成截然不同的今天。时间之所以重要，正是因为它与历史事件挂钩。比特币也是通过将区块串连起来，将昨日与今天捆绑，构成了一个不可修改的时间线。而这个串连的工具就是哈希函数，每一个区块的内容都打包成一个哈希值，这个哈希值也参与构成下一区块的内容，由此往复，这就形成了现在的区块链。

此时，比特币的时间便真正的不可伪造，交易的内容也不容修改，任何一部分的篡改都将导致被修改的区块以及之后的每一个区块的哈希值发生改变，哪里发生错误一目了然。

现在，我们就知道了比特币是如何记录交易的：用区块时间为交易加盖时间戳，交易又参与了时间的构成。