作者供职于银联商务股份有限公司

编辑：葛辛晶

2008年11月1日，Satoshi Nakamoto（中本聪）在“metzdowd.com”网站的密码学邮件列表中发表了一篇题为《Bitcoin: A Peer-to-Peer Electronic Cash System》，即《比特币：一种点对点的电子现金系统》，史称“比特币白皮书”。业界也有人将其翻译为《比特币：基于对等网络的电子现金系统》。

“比特币白皮书”的说法欠妥

在百度百科上，“白皮书”被定义为是政府或议会正式发表的以白色封面装帧的重要文件或报告书。作为一种官方文件，“白皮书”代表了政府立场，讲究事实清楚、立场明确、行文规范、文字简练，没有文学色彩。

“白皮书”已经成为国际上公认的正式官方文书。各国文件分别有其惯用的颜色，封面用白色的就是“白皮书”。

“白皮书”最初是因为书的封皮和正文所用的纸皆为白色而得名。英语中“WHITE PAPER”和“WHITE BOOK”汉语均译做“白皮书”。但二者是有区别的，“WHITE PAPER”主要指政府发表的短篇幅报告，任何题材、任何组织机构均可使用，亦可用于包含背景材料的政治性官方声明。而“WHITE BOOK”篇幅较长，内容更为重要和充实，主要是有关重大事务的一种官方报告书。除英国外，其他国家在使用“WHITE BOOK”和“WHITE PAPER”时，往往未加严格区分。

“比特币白皮书”既非一国政府发布，也没有封皮可言，称之为“白皮书”似有不妥。当然，现在为了标榜某文档在该领域的地位，常常称之为“**白皮书”。

如果非要称之为“白皮书”，则我们可以称之为“比特币网络（互联网）白皮书”更为妥当，意为发布在网络（互联网）上的“白皮书”。

解读“比特币网络（互联网）白皮书”

在2019年春
季学期中央党校（国家行
政学院）中青年干部培训班上，习近平总书记
关于干部学习有一段论述：在学习理论上，干部要舍得花精力，全面系统学、及时跟进学、深入思考学、联系实际学。学习新时代中国特色社会主义思想，要深刻认识和领会其时代意义、理论意义、实践意义、世界意义，深刻理解其核心要义、精神实质、丰富内涵、实践要求。要紧密结合新时代新实践，紧密结合思想和工作实际，有针对性地重点学习，多思多想、学深悟透，知其然又知其所以然。学习理论最有效的办法是读原著、学原文、悟原理，强读强记，常学常新，往深里走、往实里走、往心里走，把自己摆进去、把职责摆进去、把工作摆进去，做到学、思、用贯通，知、信、行统一。

上升到哲学层面，道理都是相通的。下面，笔者就本着“读原著、学原文、悟原理”的理念，对“比特币网络（互联网）白皮书”进行一番解读。

业界更愿意把“比特币网络（互联网）白皮书”称为“一篇论文”。而既然是论文，那必然有结论。“白皮书”的结论是什么呢？

01

在“白皮书”摘要的开篇中写道，
“本文提出了一种完全通过点对点技术实现的电子现金系统，它使得在线支付能够直接由一方发起并支付给另外一方，中间不需要通过任何的金融机构”。

解读：摘要的第一句话传递了两个信息。

第一，提出一种电子现金系统的概念，该系统是通过点对点技术实现的。

第二，该系统可以不通过金融机构实现在线直接支付。

通过对比“白皮书”正文“简介”中的描述，“互联网上的贸易，几乎都需要借助金融机构作为可资信赖的第三方来处理电子支付信息”，可以得出另外一个隐藏的信息，即比特币系统是用于互联网贸易在线支付的电子现金系统。

这段话容易被忽略的一点是：中本聪只是表明“中间不需要通过任何的金融机构”，但并没有明确“不需要中介”。这为此后被解读为“去中介”埋下了隐患。

02

“白皮书”摘要中还提出
，“该网络通过随机散列（hashing）对全部交易加上时间戳（timestamps），将它们合并入一个不断延伸的基于随机散列的工作量证明（proof-of-work）的链条作为交易记录，除非重新完成全部的工作量证明，形成的交易记录将不可更改”。

解读：
首先，比特币的交易记录是一个链条，而“比特币网络（互联网）白皮书”中始终没有出现“账户” “记账”等描述。

其次，除非重新完成全部的工作量证明，否则形成的交易记录不可更改。值得一提的是，在实际运作过程中却可能出现意外，比特币、以太坊的硬分叉就是个例子。

03

“白皮书”简介中写道，
“我们无法实现完全不可逆的交易，因为金融机构总是不可避免地会出面协调争端”。

解读：
一方面，其目的是实现交易的不可逆。从银行的角度讲就是“调账”，出现交易差错或客户退货时需要调账。

其次，“金融机构总是不可避免地会出面协调争端”，但是文中并没提及比特币绝对不会有此类争端，更没有表明如果出现争端该怎么解决。

04

“白皮书”简介中提出，
“金融中介的存在，也会增加交易的成本，并且限制了实际可行的最小交易规模，也限制了日常的小额支付交易”。

解读：
一是“金融中介的存在会增加交易成本”，但事实是银行卡的交易成本低于现金。文中没有明确说比特币的交易成本比有金融中介参与的支付成本低。

二是对于最小交易规模的限制更多的是商家（银行卡推广初期，商户一般会有不成文的规定，如低于一定金额则不能刷卡），但随着非现金交易的推广普及，商家对于最小交易规模的限制也基本消除。最小交易规模的限制还取决于货币的计价标准，比如人民币的最小交易规模是分，以元计价的话就是精确到小数点后两位。比特

币的最小交易规模是聪，精确到小数点后8位。

如果仅仅看小数点后的位数，比特币肯定比人民币的最小交易规模小得多，但比特币当前的价格大幅上涨，截至8月14日，比特币收盘价为10022.97美元。

05

“白皮书”简介中还提及，
“潜在的损失还在于，很多商户和服务本身是无法退货的，如果缺乏不可逆的支付手段，互联网的贸易就大大受限”。

解读：
第一，文中未提及哪些商户和服务本身是无法退货的。笔者认为，其中包含数字音乐、数字电影等虚拟物品，同时也不排除还有一些灰色或违法交易。

第二，中国的互联网贸易实际上并没有因为缺乏不可逆的支付手段而影响了快速发展。

06

“白皮书”简介中明确，
“杜绝回滚（reverse）支付交易的可能，这就可以保护特定的卖家免于欺诈”。

解读：
比特币“杜绝回滚支付交易”的特性只是为了保护特定的卖家免于欺诈。而特定的卖家仅代表可以确定的互联网上的卖家，但并未说明其是否出售无法退货的商品和服务的商家。

07

“白皮书”简介中还提出，“对于想要保护买家的人来说，在此环境下设立通常的第三方担保机制也可谓轻松加愉快”。

解读：
一是如果设立通常的第三方担保机制用于保护买家可谓轻松加愉快，为什么对卖家不适用？

二是中本聪实际上已经意识到，比特币要想真正成为互联网贸易的电子现金，离不开与中介的合作。

综上所述“比特币网络（互联网）白皮书”的设计理念非常明显，那就是要创造一个点对点的适用于互联网贸易的电子现金系统。该系统可以实现交易的完全不可逆。而且，由于该系统不需要金融中介，因此可以降低交易成本。