加密数字货币有着非常悠久的历史。这个冷知识专栏用几个主要人物和他们的创作，展示了一个加密数字货币的简明前传。

本书的序言《区块链：技术驱动金融》&quot；通往比特币的漫长道路&quot(杰里米克拉克/文)从技术和历史的角度阐述了加密数字货币的历史。这里参考他的梳理分析。在现实世界中现金可以很简单，需要防伪功能。现金就是一张纸。我可以在一张纸上写下&quot得到这张纸的人可以向我要一只羊&quot然后签上我的名字。签名是一种防伪措施。我&#039；我会给你纸条，当它涉及到你，我&#039；我要走了。

在数字世界里，情况变得复杂起来：这张纸条和上面的签名是一个数字文件，电子文件可以被完美复制无数次。给你这个电子文档之后，我可以给第三个人。。这就是所谓的双重支出问题。大卫郑初美提出了一个创造性的方案来解决数字世界中的这个问题。他的方法是使用这个逻辑：在一张纸上你选一个只有你自己知道的序列号，然后我签字。正如我不&#039；我不知道序列号，我不能&#039；不要把这张便条复制给别人。这就是密码学中所谓的盲签名。。这个想法形成了&quot第一个真正的电子货币方案&quot。1989年，大卫郑初美也创立了DigiCash，将他的想法商业化，但未能被大规模接受。这个方案的缺点是它需要工作。必须有一个所有参与者都信任的中央服务器来验证这些&quot数字笔记&quot。比特币白皮书中的

中本聪引用了前人的成果，如亚当贝克在1997年设计的HashCash和中国密码学家戴伟在1998年设计的BCoin。2010年，由于维基百科试图删除比特币条目，中本聪与其他人讨论如何修改条目描述，使其为维基百科所接受。他建议写：&quot比特币是戴伟的具体实现&#039；在1998年的cryptopunk和NickSaab&#039的比特黄金思想。"他说这是一个具体的实现，因为b币和比特币都只是在想法中。

这引出了区块链领域的一个重要人物，——计算机科学家尼克萨博。1998年，他提出了一个名为比特黄金的计划。在当前的区块链世界，尼克萨博有一个更重要的地位：萨博是&quot智能合同&quot1993年，他写了一篇关于&quot智能合同&quot。智能合约是区块链处理交易的核心方式。区块链应用程序的本质可以被视为智能合约的组合。

这个阶段的第四个重要人物是著名的密码学家哈尔芬尼(HalFinney)。他是&quotG&quot在著名的PGP加密和cryptopunk圈子里的一个前辈。。2004年，他使用工作量证明(POW)机制推出了自己的电子货币版本。在比特币的发展过程中，哈尔芬尼与中本聪有很多互动。比特币的第一次转移是中本聪向哈尔芬尼转移了10个比特币。

他们四个人的具体想法不同，但他们都有一个共同点，那就是他们都让计算机来做计算，因此&quot创建&quot电子现金。它们是比特币系统对计算机进行加密计算的工作量的证明，也是&quot采矿&quot。这很重要，有了这个想法。只有这样，集中式的服务器才能被去中心化的网络所取代，困扰数字货币的问题才得以解决。

更进一步。这个想法可以追溯到1992年由密码学家辛西娅德沃克和莫尼诺尔提出的一个减少垃圾邮件的方案。杰里米克拉克在他的书《区块链：技术驱动金融》中解释说：&quot想象一下，你每发一封邮件，电脑都要花几秒钟解决一道数学计算题。如果你没有附上答案，收件人&#039；的邮箱会自动忽略此邮件。"

最后中本聪综合了前人的创新，实现了一种在分配和交易上分散化的电子现金。

为什么以前的数字货币系统(比如郑初美&#039；s系统)失败？中本聪曾写道：自上世纪90年代以来，所有虚拟货币公司都失败了.我希望人们能看到，这些系统的失败显然是由于它们的集中控制。我猜我们第一次尝试建立一个分散的、不基于信任的系统。

这里他提到了两个相关的词，一个是去中心化，一个是非信任化。。分散式网络必须是非基于信任的。

以太坊的创始人维塔利克布特林(VitalikButerin)在《以太坊白皮书》中也很好地概述了这段历史。他围绕关键词&quot分散化&quot:&quot去中心化数字货币的概念，和财产登记的替代应用一样，是几十年前提出的。20世纪80年代和90年代的匿名电子现金协议其中大部分是根据乔&#039；s盲签技术。这些电子现金协议提供了高度私有的货币，但它们都不受欢迎，因为它们都依赖于一个集中的中介。

1998第一次，戴伟&#039；sB-coin提出了通过解决计算问题和分散共识来创造货币的思想，但提案并没有给出如何实现分散共识的具体方法。

2005年，芬尼引入了&quot可重复使用的工作量证明&quot(RPOW)。它同时运用了B币和亚当贝克的理念&#039；创建加密货币的困难散列现金问题。但是，这个概念又一次在理想化中迷失了，因为它依赖于可信计算作为后端。

2009去中心化的货币最早是由中本聪实现的，它通过现有的公钥加密方法来管理所有权，并使用一种叫做工作量证明的共识算法来记录谁拥有该货币。以上是《加密数字货币前传：从大卫郑初美到中本聪》的细节。更多关于数字货币的信息，请关注dadaqq.coM其他相关文章(www.dadaqq.coM)！