加密数字货币有着非常漫长的历史，这个冷知识专栏用几个主要人物和他们的创造，来展示一个简明的加密数字货币前传。《区块链：技术驱动金融》一书的前言“通往比特币的漫长道路”（杰里米·克拉克/文）从技术与历史的角度对加密数字货币的历史进行了详细的阐述，这里参考了他的梳理分析。1)
1983年，大卫·乔姆（David Chaum）最早提出把加密技术用在数字现金上

在物理世界中，现金可以非常简单，它需要的是防伪功能。现金是一张纸条，我可以在一张纸条上写“拿到这张纸条的人可以找我领取一只羊”，然后签上自己的名字。签名就是防伪措施。我把纸条拿给你，纸条到你手中，我就没有了。

在数字世界中，情况开始变得复杂：这张纸条和上面的签名是一个数字文件，而电子文件可以被无数次地完美复制。把这个电子文件给你之后，我还可以再把这个电子文件给第三个人。这就是所谓的双重支付（double spending）问题。

大卫·乔姆提出了一个创造性的方案，在数字世界里解决了这个难题。他的方法是采用这样的逻辑：在一张纸条上，你选择一个只有你知道的序列号，然后我在上面签名。由于我不知道这个序列号，因此我没法再复制一份这张纸条给另一个人。这就是密码学上所谓的盲签（blind signature）。这个思路形成了“第一个真正意义上的电子货币方案”。1989年，大卫·乔姆还创建了数字现金公司（DigiCash）来把自己的想法商业化，但未能被大规模接受。

这个方案的缺点是，它要运转起来，就必须有一个所有参与者都信任的中心化服务器来进行这些“数字纸条”的验证。2) 1997～1998年，亚当·贝克（Adam Back）与哈希现金（HashCash）、戴伟（Wei Dai）与B币（B-Money）、尼克·萨博（Nick Szabo）与比特黄金（bit gold）、哈尔·芬尼（Hal Finney）与工作量证明（POW）

在比特币白皮书中，中本聪引用了1997年亚当·贝克设计的哈希现金、1998年华裔密码学家戴伟设计的B币等前人的成果。2010年，由于维基百科试图删除比特币词条，因此中本聪与人讨论了如何修改词条描述以让维基百科接受，他建议这样写：“比特币是戴伟在1998年在密码朋克中所提到的B币构想和尼克·萨博提出的比特黄金的具体实现。”他说是具体实现，是因为B币和比特黄金都只是停留在构想中。

这就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。他在1998年提出了名为比特黄金的方案。在现在的区块链世界中，尼克·萨博有着更为重要的位置：萨博是“智能合约”（smart contract）的提出者，1993年他写出了“智能合约”论文。智能合约是区块链处理交易的核心方式，区块链应用的实质可被看成是

一个个智能合约的组合。

这一阶段的第四个重要人物是知名密码学家哈尔·芬尼，他是著名的PGP加密中的“G”，是密码朋克圈中的前辈。他在2004年推出了自己版本的采用工作量证明（POW）机制的电子货币。在比特币开发过程中，哈尔·芬尼与中本聪有很多互动，比特币的第一笔转账就是中本聪转了10个比特币给哈尔·芬尼。

他们四人的具体设想各有不同，但有一个共同点，即都是让计算机进行计算，从而“创造”电子现金，它们是比特币系统让计算机进行加密计算的工作量证明和“挖矿”的创意来源。这非常重要，有了这个想法，中心化服务器才可以被去中心网络所取代，困扰数字货币的难题被解决了。再往前，这个想法可追溯到1992年密码学家辛提亚·沃克（Cynthia Dwork）、摩尼·纳欧尔（Moni Naor）提出来的用于减少垃圾邮件的一个方案，对此杰里米·克拉克在《区块链：技术驱动金融》一书中解释说：“设想你每次发送邮件时，计算机都不得不花几秒钟解决一道数学计算题目。如果你没能附上答案，收件人的邮箱会自动忽略这封邮件”。3)
2008年10月，中本聪发布论文“比特币：一个点对点电子现金系统”

最终，中本聪把前人的创新综合起来，实现了一种在发行和交易上都去中心化的电子现金。

对于前人的数字货币系统（比如乔姆的系统）为什么会失败，中本聪曾经写道：自20世纪90年代以来所有的虚拟货币公司全都失败了……我希望，人们可以看到，这些系统之所以失败，显然是因为它们的中心化控制这一特性。我想，我们正在首次尝试建立一个去中心化的、非基于信任的系统。

这里他提到了两个相关的词，一是去中心化（decentralized），二是非基于信任的（non-trust-based）。去中心网络一定是非基于信任的。以太坊创始人维塔利克·布特林（Vitalik Buterin）在以太坊白皮书中也很好地概述了这段历史，他是围绕“去中心化”这个关键词展开论述的：“去中心化的数字货币概念，正如财产登记这样的替代应用一样，早在几十年以前就被提出来了。

20世纪八九十年代的匿名电子现金协议，大部分是以乔姆的盲签技术为基础的。这些电子现金协议提供具有高