区块链的诞生

1976年，**惠特菲尔德·迪菲**(Whitfield Diffie)和**马丁·赫尔曼**（Martin Hellman）两位密码学大师发表了论文**《密码学的新方向》**。

论文覆盖了未来几十年密码学所有新的进展领域，**包括非对称加密、椭圆曲线算法、哈希等一些手段**，奠定了迄今为止整个密码学的发展方向，也**对区块链的技术和比特币的诞生起到决定性作用。**

同年，哈耶克出版了他人生中最后一本经济学方面的专著：**《货币的非国家化》**。

《货币的非国家化》的思想挑战了一直以来的“国家发行货币”，提出非主权货币、竞争发行货币等理念，其实就是今天说的**去中心化货币**的精神。

1977年，罗纳德·李维斯特（Ronald L. Rivest）、阿迪·萨莫尔（Adi Shamir）、伦纳德·阿德曼（Leonard M. Adleman）**这三个人真正提出了一个公钥加密/数字签名算法即RSA算法**。

1980 年，Merkle Ralf（拉尔夫）提出了 Merkle-Tree 这种数据结构和相应的算法。

后来的主要用途之一是分布式网络中数据同步正确性的校验，这也是比特币中引入用来做区块同步校验的重要手段。

1982 年，**兰波特（Lamport）提出拜占廷将军问题引出了我们的分布式计算和共识思想**。

也标志着分布式计算的可靠性理论和实践进入到了实质性阶段。

同年，大卫·乔姆提出了密码学支付系统 ECash，可以看出，**随着密码学的进展，眼光敏锐的人已经开始尝试将其运用到货币、支付相关的领域了**，应该说 ECash 是密码学货币最早的先驱之一。

1985 年，Koblitz 和 Miller 各自独立提出了著名的**椭圆曲线加密（ECC）算法**，解决了当时之前 RSA 算法计算量过大的问题。

1997 年，英国的密码学家亚当·贝克（Adam Back）发明了**哈希现金**（Hashcash）。

其中用到了工作量证明系统（Proof of Work），该概念最早出现在1993年。

工作量证明系统是比特币的核心理念之一。

同年，1997年哈伯和斯托尼塔提出了一个用时间戳的方法保证数字文件安全的协议。

时间戳最大的特点就是当一个虚拟货币被交易时，被盖上时间戳，它就不能被改动。

经过1976年-1997年整整二十年的积累，终于在1998年密码学货币的完整思想成立。

1998年，戴伟（Wei Dai）、尼克·萨博同时提出**密码学货币**的概念。

到这一步，我们的区块链技术才能讲出一个基本完整的故事。

但是历史也总是喜欢和我们玩捉迷藏。

虽然戴伟的B-Money被称为比特币的精神先驱，而尼克·萨博发明的Bitgold，提出**工作量证明机制**，用户通过竞争性地解决数学难题，然后将解答的结果用加密算法串联在一起公开发布，**构建出一个产权认证系统。**

提纲和中本聪的比特币论文里列出的特性非常接近，以至于有人曾经怀疑萨博就是中本聪。

二

2008 年美国次贷危机爆发，美国为了避免由第四大投资银行雷曼兄弟的倒闭引发金融机构连锁反应而实行量化宽松政策，即**疯狂加印钞票**。

人类开始思索有没有一种货币**可以保障人民财产权不背侵犯、货币可以超越主权，不被第三方机构控制，也不会超发、滥发**。

就是在这样的背景下，2008 年由中本聪发表的一篇论文**《比特币：一种点对点的电子现金系统》**，文中描述了一个全新的数字货币系统：比特币。

至此比特币的底层技术区块链正式诞生。