大家有没有听过一个段子：

一个CEO消失了快十年的公司，管理着几十万员工；

每个员工自私自利，争权夺利，公司运作10年风生水起；

一份代码上线，稳定运行10年，没出过bug；

遭到各国政府打压，无法禁止，覆盖全球100多个国家和地区；

没花过一分钱做营销预算，获取了3500万用户；

没融过一分钱，市值达到1700亿美元；

公司2009年上市，股价翻了300万倍。

把当中随便一条拿出来，都是现代商业上的奇迹，没有任何一个公司能够做到，但比特币做到了以上所有7条。在这段子里，改了一些数据，因为原本的数据已经再次膨胀，甚至又翻了几番，比特币的奇迹堪称前无古人后无来者，但又有多少人想到，在比特币在诞生之初，却更像是一场自由主义者们的社会实验。

大家都知道，比特币白皮书诞生于2008年

所以，我们就从，1992年说起！

1992年，前Inter高级科学家，蒂姆·梅(Timothy C. May）在自己的家里，发起了Crypto匿名邮件列表组织，通过匿名的邮件列表，交流包括数学、计算机、加密技术、文化艺术等的话题。

1993年，作为发起人之一的埃里克·休斯（Eric Hughes），发表了一篇名为《A Cypherpunk's

Manifesto》的文章，即密码朋克宣言，正式提出了密码朋克的核心主张：

“致力于建立匿名系统。用密码、匿名邮件转发系统、数字签名和电子货币来保护我们的隐私。”

由此也奠定了密码朋克后期主要的交流方向，1000多位来自世界各地密码学专家、天才程序员、数学黑客加入密码朋克，并在邮件列表中分享他们的研究成果。

密码朋克 Cypherpunk

这群世界上最聪明的自由主义者，在互联网产业的发展中拥有举足轻重的影响力！“维基解密”的创始人阿桑奇、万维网发明者Tim-Berners Lee、Facebook的创始人之一肖恩·帕克都是其密码朋克的成员。当然，也包括大家熟知的中本聪-Satoshi Nakamoto~

很多人都把比特币看做是一项伟大的发明，殊不知在它诞生前，密码朋克已经诞生了许多关于加密货币的研究和项目，“它们”或许没能真正成功，却给比特币的诞生，指明了方向！

其中最为著名的就是：

Ecash、Hash Cash、B-money

首先，我们来说Ecash
，在未来学家凯文凯利20年前的成名作：《失控》一书中有一个章节的名字就叫“电子货币”。

书中详细描述了很多关于密码朋克的人与事，作为密码朋克的“主教”级人物，大卫乔姆（David
Chaum）在书中详细介绍了他于1990年发明的的匿名现金系统——Ecash。

Ecash可以称得上是加密货币的始祖，虽然应用了公钥私钥的非对称加密（RSA）体系，但缺少了共识机制，Ecash依然是一个“中心化”网络，依然需要银行作为背书，虽然一时间风光无限！但是最终，由于产品没需求，后台没支持，这个项目在1998年破产。从今天的角度看，Ecash除了部分匿名的功能，其实它更像是微信或者支付宝，而David Chaum在《失控》中提出的关于无现金支付畅想，其实也是已经在很多过国家和地区实现。

这里再顺带说个八卦，我们的中本聪聪哥对于这位币圈始祖，一直都是种嗤之以鼻的态度，或者说，聪哥对中心化有着浓郁的怨念，只要是带有中心化属性的加密货币，聪哥必然怼之，然后留下一句：“懒得你和解释！”，在对手反应过来前悄然而去，气哭！

被此话“气哭”的BM

时间来到1997年

Hash Cash哈希现金诞生了，一篇名为《哈希现金邮资计划正式实施》的文章出现在了密码朋克成员的邮件列表中，哈希现金并不是某种“币”，而是发件人亚当·巴克(Adam Back)提出的一个解决邮件滥发问题的方案。

简单说就是发件方在每一封邮件发出时，都必须计算收件方提出的一个数值，对于动辄就要发送上百万垃圾邮件的人来说，代价就会变得很高，从而避免了垃圾邮件滥伐。但是，这个方案同时也造成了一个后果：后期算力的不断膨胀，这个弊端在比特币中成为了我们熟知的的挖矿机制：工作量证明POW(Proof of Work)

一年后，1998年，B-money诞生，B-money

一直被认为是比特币的精神先导，在比特币白皮书的结尾，中本聪第一个引用文献就是B-money。

设计者戴伟（Wei Dai），提出了世界上第一个分布式加密货币模型，当A向B转账时，使用私钥签名并且广播到全网，由全网用户帮忙记账，并通过“计算量成本”创造发行一个叫B-money的加密货币。

戴伟（Wei Dai），网传照片

是不是听起来已经和比特币的模型很相似了，但是，由于无法解决“双花”问题、节点信息不一致等问题，B-money一直停留在白皮书阶段没有真正的实施。

那在比特币中呢，中本聪通过最长链共识和时间戳解决了双花问题，B-moeny给比特币的最终完善提供了方向与框架，戴伟绝对当得上奠基者的名头，这里有个有意思的事情，大家知道以太坊的最小单位叫WEI（1 Ether = 10 的 18 次方 Wei），其实V神就在用这种方式向戴伟致敬！

时长所限，我们无法详细的介绍每一个位对比特币做出贡献的极客和科学家，他们也许只是因为信仰或者兴趣而聚集，但是他们在密码学、分布式系统、P2P等很多方面做出的研究给这个世界带来了无限可能。

他们就是引路的萤火，温暖着比特币诞生的前夜，而在不远处，一扇通往新世界的大门正待开启！