Whitfield Diffie 是 Sun 公司的前首席安全官，Martin Hellman 是斯坦福大学教授。他们俩发明的 Diffie-Hellman 算法是一种秘钥交换方法，交换秘钥后还需要其他算法来进行加密和解密。这个算法是今天互联网安全的基础。他俩的成就在于，告诉世人非对称加密以及公钥加密是可行的。

Whifield Diffie

他俩因此获得 2015 年的图灵奖。Hellman 也在 70 年代险些被美国军方关进监狱，要知道加密技术一直就是政府和军方的重要武器。密码科学家们要么为军方和政府工作，要么就要面对各来自政府的威胁，而后来密码朋克们，则赤裸裸的直接挑战强权。密码学和区块链的很大一部分，都是为了对抗强权，而且也是在对抗强权中发展起来的。中本聪至今还匿名，聪明且谨慎啊。

1978年，MIT 的 Ron Rivest、Adi Shamir 和 Len Adleman发明另一个公开钥匙系统，RSA

罗纳德·李维斯特（Ron Rivest）、阿迪·萨莫尔（Adi Shamir）和伦纳德·阿德曼（Leonard Adleman）都是麻省理工学院的研究人员， 1978 年共同发明 RSA，这是非对称的公钥加密技术，既可用于数据加密也可用于签名。RSA 是目前最流行的公钥加密算法。但实际上，RSA 并非最早出现的公钥加密技术，据传，英国人 Clifford Cocks 早在 1973 年就发现了类似的算法，但可惜的是，他是为英国国家通信总局工作的，所以他的发现被列为绝密，直到 1998 年才为世人所知。

RSA

2002 年，三人因 RSA 算法获图灵奖。

1982 年大卫乔姆提出不可追踪的密码学网络支付系统

大卫乔姆是美国人，但后来移居荷兰。他留着长发大胡子，一副神仙模样。就是他发明了乔姆盲签名，可以说他是密码货币的始祖。1982 年，据他说，他灵光一现，就发明了不可追踪的密码学网络支付系统，而这就是今天比特币的老祖宗。

大卫乔姆

1990 年大卫乔姆发明了 Ecash，这应该是第一种电子现金了，当时风头很劲，包括微软，维萨等大公司都要收购 Ecash。可惜，大卫乔姆的性格与他的形象一样特立独行，他的多疑、神经质、不近人情还有优柔寡断葬送了 ecash的未来。

中本聪对 ecash 不屑一顾，认为它依然是传统的中心化系统，必须依赖中心化的信用。

1985 年莱斯利·兰伯特 (Leslie Lamport) 等人提出的拜占庭将军问题 (Byzantine Generals Problem)

这真是区块链、比特币的最重要的核心问题，就是如何解决公开网络上的信任问题。1982 年Leslie Lamport 把军中各地军队彼此取得共识、决定是否出兵的过程，延伸至运算领域，设法建立具容错性的分布式系统，即使部分节点失效仍可确保系统正常运行，可让多个基于零信任基础的节点达成共识，并确保资讯传递的一致性。

莱斯利·兰伯特

中本聪最成功的地方，就是发明了 POW 工作量证明的方法，利用新币发行的刺激机制，解决了拜占庭将军问题，从而漂亮的实现了公开网络上的信任机制问题。

但中本聪的工作量证明并非彻底原创，他唯一的合作伙伴，哈克芬尼在 2005 年提出可重复使用的工作量证明机制（Reusable Proofs of Work，RPOW），乃是中本聪创意的母本。下面还有提及哈克芬尼。

莱斯利·兰伯特获得 2013 年图灵奖

1985年 Neal Koblitz 和 Victor Miller，首次将椭圆曲线应用于密码学，建立以公钥加密的算法。

Neal Koblitz 和 Victor Miller 在 1985 年分别提出这种算法，基于椭圆曲线数学的一种公钥密码的方法。ECC 能够提供比 RSA 更高级别的安全。

中本聪最令人信服的就是选择了一条曲线，而这条曲线并不在美国 RSA 的掌握之下。据斯诺登爆料后，大家才得以知晓，RSA 在很多加密技术中留有后门。而中本聪则神一般走位避开了 RSA 的陷阱。创建以太坊的天才少年 Vitalik 对中本聪并不那么敬仰，甚至评价他的 C++ 技巧很一般，但对中本聪选择的曲线，却大加赞扬。

2008 年 Neal Kin, Vladimir Oksman, 和 Charles Bry 申请专利：Updating And Distributing Encryption Keys invention

这三位都是德国人，他们在 2008 年申请了专利，分布式秘钥加密技术。有人怀疑他们是中本聪，因为中本聪的论文发表，bitcoin.org的注册都在这三位申请专利的前后脚，不得不令人怀疑。但这三位一口否认，Neal 甚至很无辜的问：比特币是什么东东? 然后他研究了一通后，发表的评论是，这玩意挺差劲的。 科学家相轻，莫过如此。但也可能 Neal 是想把中本聪给激出来。

1991 年 Stuart Haber 和 Scott Stornetta 发表论文： How to Time-Stamp a Digital Document

Stuart Haber, 和 Scott Stornetta 都是 HP 实验室的研究人员。他们提出用时间戳确保数位文件安全的协议。就是今天所谓区块链链条的雏形。这种技术，保证了数据的可追溯以及不可篡改。

1990 密码学匿名现金系统年大卫乔姆 ecash

大卫乔姆的故事看上文，他老人家还在荷兰搞着研究。

1991 年 Philip Zimmerman 发布 PGP (Pretty Good Privacy)

PGP 是用来做邮件加密的，它是一个基于 RSA 公钥加密体系的邮件加密系统，能够保证邮件内容不被篡改，同时让邮件接受者信任邮件来自发送者。

发明者菲尔·齐默尔曼（Philip Zimmermann）是美国人，他致力于写软件的同时，还反对美国政府侵犯公民的隐私权，在多年的对抗后，他离开了美国，到了瑞士。他未曾到过十八层地狱，所以对天堂低一点的楼层都忍受不了。

菲尔·齐默尔曼

哈尔芬尼是 PGP 公司的一员，也在 PGP 中做出主要的贡献。

PGP 是中本聪的最爱，他的邮件都是通过 PGP 发出。

1992年，蒂莫西·梅成立密码朋克

Tim May 曾是 Intel 的高级科学家和电子工程师，他同时还是科技和政治的专栏作家。他科学上的成就是解决了集成芯片上的 alpha 粒子问题。

Tim May

重要的是，他是密码朋克（cypherpunk）组织的发起人，1992 年在他加州的家里，发起了密码朋克邮件列表组织。共同发起人包括 Eric Hughes 与 John Gilmore。

列出这个伟大组织中最知名的几个名字：Tim May，Eric Hughes 与 John Gilmore，Jim Bell，David Chaum （大卫乔姆），Phil Zimmerman （PGP），Julian Assange（阿桑奇），Adam Back （亚当·拜克），Wei-Dai （名字是中国的，不知道人是否华裔。他在圈子中地位尊崇）和 Hal Finney （哈尔芬尼），Tim-Berners Lee 爵士 (万维网发明者)，John Perry Barlow (赛博自由主义政治活动家)和 Nick Szabo（尼克萨博，BitGold 发明人，智能合约的发明人）。

Tim May 作为密码朋友的发起人，享有巨大声誉。 尼克萨博在演讲的时候，一定会提起他。

1993年，埃里克·休斯(Eric Hughes) 正式提出密码朋克的概念。

在 Tim 和 Eric 创建了“密码朋克邮件名单”后的1993年，Eric Hughes 在《A Cypherpunk's Manifesto》中正式提出密码朋克的概念。它宣扬电脑化空间下的个体精神，使用强加密（密文）保护个人隐私。密码朋克提倡使用强加密算法，宣扬个体保持安全的私人性，他们反对任何政府规则的密码系统。他们宁愿容许罪犯和恐怖分子来开发和使用强加密系统，他们认为这是为个人隐私付出风险，必须接受。

1998 年 beenz.com 1999年 Flooz.com

俱往矣，俱往矣，在互联网刚刚兴起的时候，很多天才就开始打起了电子货币的主意，但无一例外，都死翘翘了。 Beenz 和 Flooz 都是当年的电子货币，正如中本聪所说：中心化的电子货币都是垃圾，必死无疑。 若是还依赖中心机构的信用，来发行电子货币，那么与网银有何区别？ 有何区别？

亚当·拜克(Adam Back)在1997年发明的哈希现金(Hashcash)算法机制

今天无数的电力耗费在比特币挖矿上，就要拜 Adam Back 所赐。是他与 1997 年提出了 HashCash 的算法机制。他的本意，是为了实现电子邮件的可信。发送电子邮件之前，需要运算一个数学题，这样发送大量垃圾邮件就会成本巨大。其实 DDOS 也可用这个方法来防范，在网站上每个点击之前，先算个数学题：=）。 这个思想，就被哈尔芬尼借鉴用来做可重复的工作量证明机制，随后，又被中本聪用到比特币中，完美的解决了拜占庭问题。

但是并非完美了，比特币为人诟病，最大的也就在于工作量证明，因为耗费能源太大。但中本聪早早就提出来了：只有大的矿机节点才会用于挖矿，大部分使用者只是做交易。

1998年，另一名密码朋克戴伟(Wei Dai)提出了匿名的、分布式的电子加密货币系统--B-money

Wei Dai 的地位也非常高，中本聪与之交流甚多，可以说他从 Wei Dai 那里借鉴了很多内容。 Wei Dai 是华裔，他为人低调，网上少有他的介绍。

1998 年 Wei Dai 提出了匿名的、分布式的电子加密货币系统--B-money。在比特币的官网上，B-money被认为是比特币的精神先导。

B-money的设计在很多关键的技术特质上与比特币非常相似，但是不能否认的是，B-money有些不切实际，其最大的现实困难在于货币的创造环节。

在B-money系统中，要求所有的账户持有者共同决定计算量的成本并就此达成一致意见。但计算技术发展是日新月异的，而且有时并不公开，计算量的成本这类信息并不准确、及时，也难以获得，因而B-money很难成为现实。

1998 年尼克萨博发布 Bitgold

和 Wei Dai 的 B-money 一样，尼克萨博的 Bitgold，比特金也并不成功。但尼克萨博可是密码朋克中最重要的成员，至今，很多人坚定的认为他就是中本聪，因为语义分析中，发现他的语言风格最靠近中本聪。

尼克萨博

尼克萨博是密码学者、程序员、律师，就是他提出了智能合约的概念，那还是 1995 年。 他对经济以及货币非常精通，当然他的 C++ 编程水平并不为人认可，也就因为 C++ 的水平不佳，很多人断定他不是中本聪，因为比特币是用 C++ 写出来的。

1999 年创立 Napster 的肖恩·范宁(Shawn Fanning)与肖恩·帕克(Shaun Parker)点对点网络技术的开发

几乎不用多介绍了，我们的快播，我们的迅雷，我们的一切种子，都要感谢 P2P。而 P2P 协议这一革命性的发明，来自肖恩·范宁(Shawn Fanning)与肖恩·帕克(Shaun Parker)。他们当年创建的 Napster 几乎颠覆了美国的音乐市场，虽然后来因为法律的原因 Napster 一蹶不振。但肖恩·帕克后来还有一个成就，那就是 Facebook，他是 Facebook 的创始人之一！

肖恩范宁

肖恩帕克

有了 P2P 协议，才有了后来的比特币，P2P 是去中心化系统中网络部分的精髓。

2005 年哈尔芬尼 Hal Finney 设计了工作量证明机制(PoW)的前身“可复用的工作量证明”(RPOW)

中本聪神龙见首不见尾，跟他联系的人，也都不知道他的真面目。他没有任何合伙人，只有哈克芬尼勉强算是。当中本聪在密码学小组中提及自己的思路时，惹得一片嘲讽，因为之前的各种电子货币都以惨败收场，没人相信一个30出头的无名之辈能够挑战此任务。再说，那个时候，太多民科提出了太多奇思异想，密码朋克们看都懒得看。只有哈尔芬尼，他是唯一的一个，立刻开始关注中本聪的思想。

哈尔芬尼

哈尔芬尼开始帮助中本聪，他是第一个运行比特币系统的人。他也是比特币系统中第一笔交易的收款人，当时，中本聪给他打过去了 70 枚比特币，只是为了测试。后来哈尔芬尼挖矿又陆续获得了几千枚比特币，但他随即停止了挖矿，因为他发现电脑太热了，他舍不得自己的笔记本。

但天不假寿，或者说天妒英才，哈尔芬尼后来得了一种病，ASL，也就是霍金那种病，在坚持了5年后，于 2014 年去世，时年 58 岁。不知道，在他去世之前，是否收到来自中本聪的问候。

哈尔芬尼死后身体接受了人体冷冻，也许几百年之后，他还会醒来，那个时候，也许地球上没有中心化的组织，而比特币已经成为主流货币之一。

Satoshi Nakamoto 2008 年发表《比特币:一种点对点的电子现金系统》

中本聪，无人知道他是谁，也无人知道他是一个人，还是一个团队。 2008 年出现在密码朋克邮件列表中，他如神龙一般，提出自己的创意。随后，他发表了自己的论文，著名的《比特币:一种点对点的电子现金系统》，系统的提出去中心化电子货币的理论。很快，他提交了可运行的比特币系统，迅速发展成为一个传奇。

在他的论文中，正式提出区块链的概念。也正因为比特币的流行，区块链的可用才为人关注。大众都是势力的，没有成功的证明，谁都不会相信。那些问你一项技术是否有成功案例的，都是庸才。

中本聪

中本聪如同武侠小说中的神侠，一切都在他的谋划之中，一切都在他的预料之中，诸葛亮的成功率都没有他高。至今，他的行为，他的言论，他的系统，无一漏洞。难怪，他经常说的一句话是：我真的懒得解释。

传奇！他就是传奇！

他说他已经有了其他好玩的东西，但愿过几年，他还能给人类一个惊喜。我们不用去猜，惊喜么一定是猜不到的。

中本聪将比特币控制权交给加文.安德烈森(Gavin Andresen)

2010 年 12 月 12 日中本聪最后一个帖子出现后，他就消失了，再未现身。之后加文.安德烈森以首席科学家的身份接管了比特币网络。

他一直担任两个角色：一是比特币核心的“首席开发”，二是基金会的“首席科学家”。

[日记本](applewebdata://852502C1-0A03-4F06-AE61-C08BDE152359/nb/625317)

© 著作权归作者所有

举报文章

关注 [灯下鼠](applewebdata://852502C1-0A03-4F06-AE61-C08BDE152359/u/7bd87904807a)

写了 281600 字，被 638 人关注，获得了 1124 个喜欢

围着光阴打转，油不尽，灯不枯。公众号“灯下鼠”

如果觉得我的文章对您有用，请随意赞赏。您的支持将鼓励我继续创作！

作者：灯下鼠

链接：http://www.jianshu.com/p/7d0327e18244

來源：简书

著作权归作者所有。商业转载请联系作者获得授权，非商业转载请注明出处。