目 录

[1. 区块链的故事-大卫·乔姆 1](#_Toc46629358)

[2. 区块链的故事-尼克·萨博 5](#_Toc46629359)

[3. 区块链的故事-戴维 9](#_Toc46629360)

[4. 区块链的故事-哈尔·芬尼 11](#_Toc46629361)

[5. 区块链的故事-中本聪 14](#_Toc46629362)

[6. 区块链的故事-中本聪是谁 16](#_Toc46629363)

[7. 区块链的故事-比特币的主要历史 20](#_Toc46629364)

[8. 区块链的故事-Diffie-Hellman 密钥交换 24](#_Toc46629365)

[9. 区块链的故事-RSA 28](#_Toc46629366)

[10. 区块链的故事-ECC 非对称加密 32](#_Toc46629367)

[11. 区块链的故事-图灵与英格玛 34](#_Toc46629368)

[12. 区块链的故事-对称加密 36](#_Toc46629369)

[13. 区块链的故事-密码朋克小组 38](#_Toc46629370)

[14. 区块链的故事-15 44](#_Toc46629371)

[15. 区块链的故事-UTXO 48](#_Toc46629372)

# 区块链的故事-大卫·乔姆

2016 年 6 月，斯坦福大学举办了一次会议，Real World Crypto，这会议之目的，要将密码学学者与开发工程师拉在一起，促进这两个群体之间的对话。 会议上，密码学家大卫·乔姆 （David Chaum）带来了一种新技术，他称之为 PrivaTegrity。 大卫·乔姆刚及花甲之年，他面如重枣，且须发皆白，颇有点仙风道骨的劲头。不过，他修炼一生之术，非刀非剑，而是密码学。



乔姆老先生骄傲地声称，他的 PrivaTegrity 技术将彻底终结 “密码斗争”。

美国的科技界与政府之间，一向有些小过节，尤其是与警局之类的强力机构。起因很简单，FBI 破案抓人，时不时总得求着科技界帮忙，修个电脑，破解个密码什么的，而美国的科技界，向来就傲娇，对这些抓差派活，既不踊跃，也不积极，甚至很有抵触情绪。

就在 2016 年 2 月，FBI 与苹果还激烈地掐了一架。 FBI 要苹果公司帮助破解恐怖分子的 iPhone，苹果说 “不干，不干，就不干。” FBI 大怒：“你敢不干？” 苹果：“不干不干，干不了！ 能干也不干！” 双方就开始吐口水，这就是所谓的 “密码斗争”。

乔姆的一生，都在研究如何保护 “个人隐私”，他敌视 FBI 这样的强权部门，认为这些机构是个人隐私的天敌。 早在上个世纪 80 年代，互联网还处在幼年期，他就察觉到网络将给个人隐私带来的祸患。 所以，他在伯克利读博士期间，就开始研究密码学，早早立志要以保护个人隐私为己任。

在密码学界，大卫·乔姆的地位极高，把他列入世界前五，怕是没有什么争议的。他出生在美国，在伯克利大学读书，之后短暂任教于纽约大学和伯克利大学。 在 80 年代后期，乔姆周游世界，途中他爱上了荷兰，就此定居阿姆斯特丹。

乔姆从伯克利大学的研究生涯开始，30 年来，一直下功夫的密码学技术，都可用一个词来概括 - “不可追踪”。他发明的算法中，名气最大的 “盲签名”，就是一种 “不可追踪” 的数字签名技术。

数字签名技术，是用 RSA 之类的算法，对数字文件进行运算，获得一个数字消息，即签名，用来证明该数字文件，确实无误地来自于某人。这和用墨水笔对纸质文件签名，以表示确认并无不同。

而盲签名技术，让签名者看不到被签名的数字文件。与现实世界类比，盲签名就是在信封里放一张复写纸，签名者在信封上签名时，他的签名笔迹便透过复写纸印到文件上。使用文件的人，拆开信封，便可取得签了名的文件。

这种盲签名技术，又引出了乔姆最得意，也是最失败的产品 - eCash。乔姆发明该产品的本意，是要研制一种支付系统，让银行无从追踪用户的支付信息。说的直白一点，就是在计算机和网络上，实现了纸质钞票的匿名性。

在 eCash 体系下，用户从银行获得数字现金，就用到了盲签名技术。银行的计算机，给用户发放一笔数字现金，要用数字签名来授权，但银行并不清楚该笔数字现金是给予了哪位用户。

简单展开一下，eCash 是用数字货币实现了纸钞的防追踪性。 王美丽到银行取钱，银行从她的账户上扣除 1 万元，同时给她 1 万元纸钞。 王美丽持 1 万元纸钞在商场购物，店家并不查验王美丽的身份，也并不记录王美丽的购物信息，店家只关心纸钞的真实性。之后，店家把 1 万元纸钞存进银行，银行也并不知道这 1 万元来自于王美丽。

而当代的电子支付系统，一律都是可追踪的，你的每一笔消费都留有详细完备的记录。根据王美丽的刷卡信息，银行几乎能够勾勒出她完整的人生历程。

eCash 系统除了保护用户隐私，让银行无法收集用户的支付记录之外，还解决了数字货币的一个基本问题，即如何防止数字货币被盗用。 RSA 这样的非对称加密算法，是其中的关键。

非对称加密算法，乃是近代密码学大厦的根基。

eCash， 及其后的数字货币发明浪潮，就是一场如何玩好非对称加密算法的游戏。

乔姆在发明了 eCash 系统之后，对此技术极具信心，他敏锐地感觉到这是一个巨大的商业机会。于是，他摇身一变，从傲娇的科研人员华丽转身，成了一名光荣的创业者和 CEO。他的公司名叫 DigiCash，这是一家注定要在科技史上留名的企业，只是，人们难以评价这家公司是成功，还是失败。

DigiCash 成立于 1989 年，倒闭于 1999 年。

后来，乔姆在接受采访的时候，把 DigiCash 的故事叙述成一场科技超前于时代的悲剧。但他的同事们似乎并不同意，很多他的老部下、老同事们，认为乔姆性情有点固执，而且多疑善变，这才是 DigiCash 一手好牌打烂的主要原因。

我们只是旁观者，自然难辨是非。但从资料中可以看到，当年要购买 DigiCash 的公司如过江之鲫。让我们再次围观当年 DigiCash 的盛况：

ING 高盛 微软 网景 ABN-Amro银行 Visa

在比尔盖茨与乔姆的接触中，比尔提出过计划，要将 eCash 集成到 Windows 95 中。据说是乔姆的固执态度，让这笔交易最终泡汤。 人们不得不认为，这是一个非常遗憾的故事。

毫无疑问，乔姆是伟大的密码学家，但他是不是一个伟大的商人，恐怕要打上一个大大的问号。

乔姆的 eCash 用盲签名实现了数字货币的不可追踪性，用 RSA 算法让数字货币能够在网络上交易，是他给了数字货币以生命。他是当之无愧的数字货币之父。今天，数字 Token 满天飞，但少有人知，乔姆乃是 Token 之父。以太坊的白皮书中，V 神 Vitalik 在开篇即提了一句乔姆，令人欣慰。

可惜的是，乔姆的数字货币，还有一个小小的缺憾，那就是 eCash 还需要依赖银行系统。 必须依赖银行系统的中心数据库，eCash 才能验证一笔钱是否已经花掉。

乔姆是天才的密码学者，全天下排名，他位列前五，但他没有解决数字货币的去中心化问题。不仅乔姆没有搞定此事，之后，整整 20 年中，无数密码学家，都在思索这个问题，但一直无解，很多高手沮丧之下，甚至断言 P2P 环境下的数字货币是不可能的。

乔姆最光辉的成就，可不是 eCash，而是早在 1979 年就发明的 Mix Network。今天，我们有着五花八门的加密通讯软件，究其根源，鼻祖就是 Mix Network。 用最简单的比喻来说，Mix Network 就是把一封信套在多层信封中，经由每层信封的收信人递交下一层信封收信人。最终的信息接受者，也就是最后一层信的接受者，无从知晓信件来自何方。中间层信封的收信人，也因无法解密再下一层信封的信息，对除了自己和自己的上下家之外的其它接收人，一概一无所知。

流行极广，甚至成为暗网神器的 Tor 洋葱加密网络，也是继承发扬了 Mix Network。Tor 在本书后面的章节中还会出现。

在 Mix Network 上，乔姆所践行的信仰，一样还是 “不可追踪”。

2016 年的 Real World Crypto 会议上，他推出的 PrivaTegrity 技术，引入一种被他称之为 cMix 的全新混合网络，其效率将远超他几十年前创造的 Mix Network 加密体制。然而惊人的区别还在于，cMix 所有的消息都要经过 9 台服务器执行加密运算。

更惊人的是，乔姆所谓他终结了 “密码斗争” 的终极办法，是在 cMix 中留有一道后门。这 9 台服务器若是一致同意，则可以将任何 cMix 消息解密。而乔姆说，他会将 9 台服务器分别放置在 9 个不同的国家，美国只有 1 台，需要 9 个国家达成司法上的一致，才能对解密的权力进行控制。

这已经不仅仅是技术的事了，这已经进入政治与法律的领域。 密码学的历史，一直就是技术开道，政治与法律随行。

乔姆期待他的技术能左右国际权力的分配，一派指点江山的气概，但愿乔姆的理想能够实现。

# 区块链的故事-尼克·萨博

二战及二战之前的密码学家，多数都是高校的学者，且有很多是为政府工作的。 到了现代，涌现了众多另类密码学者，他们身份独立，并不为政府工作，甚至在观点与行动上敌视政府。 二战前后，密码学完全是政府手中的武器，用于军事与政治。 而现代密码学，则成了众多独立密码学家用来保护个人隐私的武器。

所以，现代密码学大家们，往往学以致用，吃自家狗粮，用自己研究出来的密码技术，把自己的身份隐私严严实实的保护起来。

乔姆他老人家虽然以 “不可追踪” 技术为终身课题，且武功又居于世界前五，他若想躲起来，怕是谁都难觅其踪。

幸运的是，他老人家虽然性格倔强，刚愎多疑，但对于抛头露面并不抵触，甚至是欣然的。 从网络上可以找到他多张照片，维基百科上他的简历也很清楚，认真找，还能挖掘出长篇大论对他的文字采访以及视频资料。 为他写个全本传记都不是什么难事。

要给尼克·萨博 （Nick Sazbo）写传记，就有些困难了。

萨博是 “智能合约” 概念的发明人，也是 “比特黄金”，一种数字货币概念的发明人。“比特黄金” 是自乔姆的 eCash 之后，成功将数字货币推进到 P2P 大门口的概念。可惜，“比特黄金” 仅停留在概念阶段，并没有写出代码来。 在 “比特黄金” 这个产品上，萨博所经历的处境，与今天的连续创业者们颇为相似：就缺两个程序员了。 萨博曾经在论坛上诚征开发高手，来合作实现“比特黄金”，可惜无人揭榜。

萨博并非不能写程序，他的名片上清楚印着身份，乃是计算机科学家、法律学者、密码学家。萨博真是一个博大精深的杂家，他的文章中显示他对技术、历史、法律、经济、政治都有很深厚的知识积累。而在计算机和密码学领域，他的兴趣集中在安全、可靠、信任等方面。

用算法和密码学来创造计算机和网络上的商业、货币、合约，是他追求的目标。

他对 “不可追踪” 之类的隐私保护事业，似乎兴趣不大，然而，他却比乔姆更重视个人隐私。在网上，只能找到一两张他的照片。外貌上看，他倒是很像一位伐木工，面容粗粝，身材雄伟。 据传，他是匈牙利人。还据传，他是华盛顿大学的法学教授，但被他否认了。



被他否认的还有另一个传言，有板有眼的说他是中本聪，是比特币的发明者。 Aston 大学的语言分析专家，判断他是中本聪，因为从语言上，他与中本聪的英语风格最为相符。

然而，程序代码这玩意是个硬杠杠。多少名满天下的互联网豪杰们，都躲着程序代码走。能不能写代码，是技术威虎山上，最后一道暗语，通过了才是一伙的。

萨博虽然是科学家，但并不擅长 C++，而中本聪的比特币系统用的 C++。

1998 年，尼克·萨博在他的博客上贴出了一篇小文，文章标题叫做 《比特黄金》，该文短小精悍，共计 980 个英文词。此文是有划时代意义的，它设计了一种概念，无需依赖对第三方的信任，便可以在线生成不可复制的、具有价值的数字货币。

不依赖对第三方的信任，就此成为众多密码学者的最高追求。

尼克·萨博设计比特黄金的目标，是在线模拟真实的黄金。黄金的特性众所周知，因存量有限和生产困难而稀缺，所以具有极高价值，黄金的价值不依赖第三方，任何人掏出的黄金，都值钱。当然黄金也有一些缺点，比如难以携带，检验成本较高。 所以，尼克·萨博希望用密码学制造在线的 “比特黄金”，具有黄金的优点，又能避开黄金的缺点。

在比特黄金中，尼克·萨博引入了 “可复用的工作量证明”、“分布式时间戳”、“分布式产权登记” 几项技术。工作量证明，其原理很简单，就是用计算机来计算一个数学题，耗费一定的计算机工时，这种工时就作为 “比特黄金” 价值的来源，与淘金者耗费体力挖矿生产黄金一个道理。最初的工作量证明，是亚当·贝克 （Adam Back）发明，用来防止垃圾邮件，每次发送一个邮件前，CPU 需要忙碌几秒钟计算一个数学题，这就如同花费了一定的成本。

可复用的工作量证明，则更进一步，将 “工作量证明” 所耗费的 CPU 工时记录下来，且可以传递给他人，他人可以再次花费出去，这样一来，“可复用的工作量证明” 与黄金更加相似。

“分布式时间戳” 为 “可复用工作量证明” 生产出的 “比特黄金” 标记上时间，尼克·萨博考虑到随着计算机的快速发展，不同时代的计算机工时成本并不一致。而盖上 “时间戳”，则可以明确某个时间段生产出来的 “比特黄金” 的成本与价值。

“分布式产权登记” 则用来记录 “比特黄金” 的归属权，这件事在乔姆的 eCash 中已经解决，就是用非对称加密算法进行签名。只是在 “比特黄金” 上，尼克·萨博提出要用分布式的产权登记，以实现在 P2P 环境下的应用。

这也是尼克·萨博的比特黄金一文中不完善之处，理想很美好，现实很骨感，怎么才能实现产权的分布式登记？ 尼克·萨博并未详细阐述。

还有一个不完善之处是，比特黄金没有解释如何进行交易，因此也就压根没提数字货币都要面对的最大挑战：双花问题。

计算机与网络上的数字文件，是可以任意复制的，数字货币生产出来后，复制多份，发送给多人，怎么办？尼克·萨博的 “比特黄金” 并没有解决这些问题。

尼克·萨博的第二个巨大成就是 “智能合约”。 他是律法学者，对合同法有着浓厚的兴趣，如何将合同、契约引入计算机中，就成了他研究的目标。

做区块链开发，在今天，指两种不同的工作，其工作内容和所用技术迥异。一种是开发区块链协议，目的是写出底层区块链协议，做的是中本聪的工作。 另一种是在区块链上开发智能合约，目的是写出应用，用的语言多是脚本语言。若做个便于理解的比喻，则区块链如同操作系统，而智能合约如同操作系统上的 Word，Excel 等应用。

1994 年尼克·萨博在论文 《智能合约：数字市场的基石》 中正式提出 “智能合约” 的概念。该文很长，约 6000 多字，一如萨博一贯的文风，行文在经济、政治、历史、计算机、密码各种学科中跳跃。还好的是，萨博从来不喜在文章中铺陈公式和算法，也很少引用代码，所以他的文章不怎么烧脑。

合约是人们在社会中建立关系的重要工具，人们在合约中做出各种承诺。合约不仅限于商业关系，生活中各种关系都可能涉及合约，比如一贯被冠以神圣，歌为浪漫的婚姻，实质上便是一种合约。

合约对于市场经济而言，更是最基础的奠基石，没有合约精神，则自由市场无从建立。 合约这种看似理所当然的事物，却蕴涵着既复杂又深刻，让人们难以理解的精神。尼克·萨博定然是哈耶克的粉丝，他不止一次在文章中提及哈耶克。 按照哈耶克的思想，合约与产权一样，是在人类在几千年的社会活动中自然形成的。若让人们凭借理性去创造出合约的概念，那是近乎不可能的。

而尼克·萨博发明的 “智能合约”，道理很简单，就是用数字的方式来构造与执行合约。此处敲黑板，划重点，萨博所说数字方式，并不是把纸质合同扫描了存储到计算机中，或者在线填写一张合同表单，那是合同的 “信息化”，而非 “智能合约”。 智能合约的要义在于，合约的条款，要化为数字化的代码协议，可在计算机上执行。

萨博为 “智能合约” 举了一个原始的例子，就是我们常用的 “自动售货机”。 投入 5 块钱，机器执行合约，吐出一罐可乐。 更多的例子还有刷卡机、银行汇款系统、网银系统等，都可算作智能合约的初始形态。当然，并非所有的软硬件计算机系统，都能算得上智能合约。 “自动售货机” 可归入智能合约，本质在于，这机器系统，代表商业关系中的一方，执行了对另一方的合约承诺：你给我 5 块钱，我承诺给你一罐可乐。

要让 “智能合约” 遍布世界，嵌入到各种设备设施中，则用密码学构建的协议就大有必要。 如同在纸质合约中，需要清楚的列出所有条款，参与合约的各方还要无误的理解合约条款，之后各方才会签字。但在传统的计算机和网络环境下，中心化的软件系统，难以做到多方对条款的平等协商。密码学构建的协议，则开辟了一条道路，为网络上实现纸质合同的全流程，提供了技术上的可能性。

尼克·萨博的智能合约概念，深远地影响了数字货币、区块链等技术与产品的发展。今天，我们在区块链上开发智能合约，其思想与原则依然来自 20 多年前尼克·萨博的文章。

尼克·萨博的“比特黄金”与“智能合约”，都只停留在论文的阶段，没能从技术上得以实现。岁月如水，20 年转瞬即逝， 2009 年比特币实现了 “比特黄金” 的构想，2016 年以太坊则实现了 “智能合约” 的全部内涵与精神。今天，尼克·萨博还是以太坊的顾问，他还活跃在区块链领域。

这就足以证明他并非中本聪。

作者：灯下鼠  
链接：https://www.jianshu.com/p/ba0349f1dc9a  
来源：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。

# 区块链的故事-戴维

在基础科学领域，华人的建树一点都不少。但要说起在离经叛道、藐视陈规的密码学领域，那华人的身影就是凤毛麟角了。毕竟，华人还是以好孩子形象示人的居多，特立独行的反抗精神少。幸运的是，有这么一位华人，他在比特币的诞生中，扮演了极为重要的角色。

他就是戴维（ Wei Dai）。从成就上论，他所提出的 B-Money，几乎能算是比特币的前身。中本聪本人都承认这一点，这是有实锤证据的，在 2008 年 8 月 22 日，中本聪给戴维的邮件中，中本聪是这样说的：“我马上要发布一篇论文，这篇论文把你的 B-Money 完善成为实际可运行的系统。” 2009 年 1 月 10 日，中本聪刚刚发布了比特币系统 0.1 版，他再次写邮件给戴维，声称：“比特币系统解决了 B-Money 要解决的所有问题”。

1998 年戴维发表了论文 B-Money。 在文中，他提出了分布式账本的概念，参与网络的各方维持一致的数据库，数据库中记录所有账户的余额。 至于如何保障众多数据库节点的一致性，戴维并未提出思路。

B-Money 中货币的发行机制，也是通过工作量证明，即使用计算机解答算术题，根据所耗费计算机的工时作为成本，以衡量出货币的价值。

戴维与萨博在货币发行上，都继承自哈希现金，沿袭了工作量证明的思路，即计算机运行的工时成本与货币价值挂钩。而到了中本聪的比特币，虽然也使用了工作量证明，但那只是为了达成共识，比特币的价值不再与 CPU 工作量的成本挂钩。然而最有意思的是，随着比特币的流行，矿机大规模部署成为商业模式，矿机的工作量或者说电费，依然自发与比特币价值挂上了钩。背后并非代码的强制力量在指挥，而是自由市场那只看不见的手在发挥作用。

B-Money 比萨博的比特黄金更加详细，对货币交易的机制，做了认真的描述。当然，戴维并未深入探讨如何保证交易的一致性，对于双花问题，他也并未触及。

B-Money 更加前瞻性的是，它提出了 “合约” 的概念，B-Money 系统不仅运行数字货币，还可以执行合约。这几乎就是今天的区块链的应用架构了。

戴维在 B-Money 的开篇，即开宗明义，声称自己热爱蒂姆·梅（Tim May）关于 “密码学无政府主义” 的主张，他认为在一个密码学支撑下的无政府社区，暴力是无处容身的。

而要运行这样一个社区，那就需要给社区创造一种货币，还要有一种执行合约的手段，这在传统社会中，都是由政府的强力来保证的。 而戴维的 B-Money 要用技术替代政府的强力。较之尼克·萨博，戴维的理想主义浓度要高上一倍。

戴维在蒂姆·梅创建的密码朋克小组中，享有很高的地位。但在网络上找不到他的照片，也找不到他的详细信息。他有一个主页，就叫[weidai.com](http://weidai.com/)， 上面朴素地列出了他的论文，别无其他。

然而区块链之热潮，让戴维也难躲强大的人肉搜索。据传，戴维的父亲也是一代科技高手，移民到美国后，创立了自己的软件公司，并成功将公司卖给了微软。 在上个世纪，戴维的父亲曾陪同比尔·盖茨来到中国，开启了微软公司在中国的事业。

随着比特币与区块链的热潮高涨，一众密码学大师们也纷纷下海，或创业、或站台，加入淘金之大潮。而戴维至今依然过着隐士般的生活，从来见不到他处于聚光灯下，也见不到他接受媒体采访，更与任何商业行为毫无瓜葛。从淡泊名利这个中国式的传统审美角度看，他完全满足了我们对大师的所有想象。

他在气质上，是最靠近中本聪的人。

作者：灯下鼠  
链接：https://www.jianshu.com/p/92da0774d5c2  
来源：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。

# 区块链的故事-哈尔·芬尼

ALS 是世界五大绝症之一，俗称 “渐冻人症”，2014 年网络上热闹过一阵子的 “冰桶挑战” 就是为 ALS 病人筹款。很多人了解 ALS，是因为一个伟大的物理科学家霍金。他于 2017 年去世，从发病到去世历经 55 年，医生评价霍金教授是幸运的，大多数 ALS 患者在发病后三到五年内死亡。

哈尔·芬尼（Hal Finney）于 2014 年 8 月 24 日，病逝于洛杉矶郊区的家中。他死于 ALS，他没有霍金那么幸运，从发病到去世仅仅 5 年。这位伟大的密码学家、伟大的程序员在人生的最后岁月中，依然保持了乐观，并且还在坚持编程。若身患绝症，普通人会发出的哀叹常常是：“为什么得病的是我”，芬尼则不然。芬尼不仅拥有高超的技术，无疑也拥有美丽优雅的灵魂，他坐在轮椅上，靠管子进食，靠管子呼吸，但他说： “总的来看，我还是幸运的，我对生活还是满意的。”

在比特币的发展历程中，哈尔·芬尼至关重要。**他是第一个赞许中本聪，认真研究中本聪论文的人**。要知道，从乔姆之后，涌现出了无数异想天开的构思，妄图实现更高明的数字货币。 密码学圈子内，面对层出不穷的民科，大牛们早已麻木。中本聪作为一个无名小卒，按照年龄在 2008 年也只是小伙子，他的论文自然无法引起大师们的重视。哈尔·芬尼是头一个热情点赞的人，那时候他绝对是密码圈内的老鸟了。

芬尼说：“比特币的思路真的很赞。它假设诚实用户的 CPU 算力能够压倒攻击者的算力，以此为基础构建系统的安全，我太喜欢这个创意了。”

当时，中本聪将论文贴在了一个密码学主题的邮件组中，时间是 2018 年 10 月 1 日。几天后，哈尔·芬尼写了很长的邮件，对中本聪的论文做了细致的评价。在伟大事业的开端，参与者通常并没有澎湃的激情，也没有狂热的冲动，他们的讨论是波澜不惊的平静，就像夏日黄昏微微袭来的阵阵凉风，身在其中也无人知晓撼动天地的雷电就蕴藏其间。10 年之后再读这些讨论的文字，这两位聪明人仿佛还坐在电脑旁边，用键盘交流着闪光的思想。今天早已物是人非，比特币已成大器，人却一个隐匿，一个逝去，不由得令人感慨万千。

在邮件的末尾，哈尔建议中本聪，写出更详细的文档。 而中本聪回答：“**我写代码，也许更快些。**”

这是两个程序员之间的对话。 中本聪与哈尔·芬尼都是非常高明的程序员。

哈尔·芬尼生于 1956 年，1979 年毕业于加州理工，获得工程学士学位。他曾在一家游戏公司里开发视频游戏，那家公司的传统业务是做玩具，有一个知名的产品叫 “芭比娃娃”。1991 年，他遇到了菲尔·齐默曼（Phil Zimmermann），成为菲尔的第一个雇员。他们开发的产品就是大名鼎鼎的 PGP （Pretty Good Privacy），这是第一款用于保护用户隐私的通信工具，可以对论坛消息、邮件、电脑文件，乃至硬盘进行加密和签名。 PGP 在密码学历史上，是一款开天辟地的产品，围绕着它，菲尔等开发者与美国政府展开了一段可歌可泣的斗争，后文还会叙及。

哈尔·芬尼的家位于洛杉矶郊外的圣芭芭拉，那是一所很小的房子，他与家人生活在一起。他的办公室只不过是客厅的一个角落，办公桌上堆满了电脑及屏幕，周围显得凌乱，家具也有些陈旧过时。哈尔是很优秀的程序员，他又是典型的理想主义者，对金钱和物质享受都不甚热切。他关注个人隐私，对美国政府不很信任，参与开发 PGP，还有自己发明的 “可复用的工作量证明”，意图都在于保护个人隐私。



2004 年，哈尔提出了 RPOW（Reusable Proof of Work） 的理论，他延续了哈希现金（HashCash）的 POW 思路，让计算机做算术题消耗工时，以工时证明投入成本，并发行数字货币。只是 RPOW 的数字货币，比哈希现金更进一步，哈希现金只能一次性消费，而 RPOW 则可以流转，可以多次消费。

哈尔与尼克·萨博、戴维保持着紧密的联系，他们经常讨论密码学及数字货币的问题。 尼克·萨博的比特黄金，戴维的 B-Money 都只停留在概念阶段，只有哈尔的 RPOW 开发出了软件，现在还可以在 Github 上找到 RPOW 源代码。哈尔是一个真正的优秀程序员。

哈尔对数字货币有过深入的思考，并实际开发过数字货币，所以，他一看到中本聪的比特币论文，就大加赞赏。拥有这样的判断力，并非易事。同为密码圈内资深专家的 John Levine 压根不信这套理论，他认为将安全寄托在可信节点的算力强过恶意节点的算力，是不可靠的。 另一位 James Donald 也提出质疑，认为区块数据过大，这是是无法逾越的障碍。所以，当哈尔这样一个老兵，挺身而出为中本聪撑腰，可想而知中本聪的感受。

2009 年 1 月 9 日，中本聪发布了比特币的第一个版本，0.1 版本。第三天，也就是 11 号，哈尔回邮件表示祝贺。也就在这个邮件中，哈尔对比特币的前景做了一个狂野的猜测。他写道，如果比特币非常成功，全球的财富都用比特币来表达，则 2100 万个比特币共计价值 100 万亿到 300 万亿美元，那么每个比特币价值为 1000 万美元。

什么叫远见？ 这就是远见！

哈尔是第一个运行比特币系统的人，他成功的挖掘出了比特币。而且在 1 月 12 日测试比特币时，他收到了来自中本聪的一笔转账， 10 个比特币，这是比特币网络上的第一笔交易。 在随后的几天中，哈尔持续运行比特币系统，并给中本聪提了几个 bug，中本聪根据哈尔的报告修改了软件。 哈尔在自己的笔记本上持续运行了几天矿机，获得了约几千个比特币。笔记本风扇的噪音，还有发烫的外壳，让他有点烦恼，于是他关了比特币客户端，这让他后来有点后悔。

随后，哈尔就消失了一阵子。从中本聪那边来看，一定会感到很奇怪。哈尔对于比特币如此热情，为何就再无消息了？

就在 2009 年，哈尔运行比特币系统之后不久，他就病了。 2009 年 8 月，他被确诊患上了渐冻人症。后来他在回忆中说，自己还欠中本聪 10 个比特币，因为患病也就没有还给他。

哈尔没有霍金那么幸运，他的病程发展很快。 他瘫痪了，通过一根管子进食，通过另一根管子呼吸。他有一台霍金那样的电脑，跟踪他的眼球来操纵轮椅。他的声音是通过语音合成器发出的。他还能编程，只是速度是以前的 1/50。

他接受了自己的病状后，又开始关注比特币，他将自己的几千个比特币转移到了离线钱包中。而比特币也开始关注他，因为他的密码学及编程能力，人们自然将他当成了中本聪的最佳人选。最为诡异的情节是，人们发现了一位中本聪候选人，名叫多利安中本聪，恰好是日裔美国人，恰好也是工程师，而最不可思议的是，这位多利安中本聪是哈尔的邻居，就住在距离哈尔家 1.6 公里外。人们为此甚是怀疑，这之间一定有着某种密谋或联系，也许多利安是中本聪，哈尔是帮助他的人，也许哈尔是真中本聪，借用了邻居多利安的名字，但一切都没有真凭实据。

2013 年，哈尔的病已经很严重。他却接到了一个威胁电话，电话那边的人要敲诈他一大笔比特币。哈尔的家人报了警，警察来后检查了哈尔的家。据说警察检查的时候，哈尔坐在轮椅上，被推到院子里，在露天的星光下呆了大半夜，身上仅盖着一条薄毯。哈尔一生致力于保护个人隐私不受政府的侵害，而在最后的时刻，还是由政府和警察保护了他，保护他免受小毛贼的侵犯，这真是让人长叹。现实的世界里，充满了无奈，善良与和平的人们，总是摆脱不了暴力的纠缠，要么被暴力保护，要么被暴力侵犯。

2014 年 8 月 28 日，从医学上，确认哈尔死亡。随后哈尔的身体被冷冻，安放在三米高的液氮容器中，他成了人体冷冻技术的第一位用户。哈尔是第一个参与 PGP 开发的人，也是第一个运行比特币的人，现在他又成为了第一个冷冻人。

哈尔没有死，哈尔只是被加密了。在我们今天的区块链上，哈尔的状态是死亡，但我们相信未来，相信未来的算力，那会是我们难以想象的强大算力，它一定能够改写生死，哈尔将复活，他还会继续编程，他还有机会把 10 个比特币还给中本聪。

# 区块链的故事-中本聪

这本是武侠小说中的情节，无名小辈单挑了少林武当，扫地老僧收服了邪魔外道。人们读及总要心花怒放，为剧情的反转而欢欣鼓舞，还有从身份代入的幻想中获得快感与满足。

当武侠小说中的情节，发生在科技界，就是史无前例了。翻遍科技史，我们再也找不到这样的例子，成就如此之大，却隐姓埋名。中本聪真的视功名财富如粪土？几千亿美元的价值，神一般的地位，就这样全数弃之不顾？中本聪所掌握的比特币，以 2017 年底的价格计算，价值 190 亿美元，他位列全球财富榜第 44 位。

但他从未动用过一个比特币，除了为测试而转移给哈尔的那 10 个币。

2008 年 8 月 22 日中本聪发了第一个邮件给戴维，询问戴维关于 B-Money 的事，他要在文中引用 B-Money 论文。

2008 年 11 月 1 日，中本聪在一个密码学邮件组中，发了一个邮件。 2011 年 4 月份，中本聪在比特币社区论坛发布最后一个公开的帖子，声称：“我已经搞别的去了”。

他在之前就已把比特币开发的工作，交给了盖文·安德森（Gavin Andresen），把[bitcoin.org](http://bitcoin.org/)网站交给了马尔蒂·马尔米（Martti Malmi）。2011 年 4 月份之后，可能他还与盖文保持了一小段时间的邮件联系，最终，中本聪彻底人间蒸发了。

中本聪留下了 31000 行代码、1 份白皮书、约 500 个帖子和邮件（共计 10 万字），从此销声匿迹，再无音信。

中本聪还曾出没在一个 P2P Foundation 论坛上，在那上面，根据注册信息，他是住在日本的男子，生日 1975 年 4 月 5 日。人们很简单就推翻了这些信息的真实性。首先，中本聪的英语极其流利，肯定不会是日本人。而他所留的生日，更是深藏玄机。 4 月 5 日，在美国历史上曾经发生过一件大事。那还是 1933 年，美国正处于大萧条之中，这个新生的国家从未经过如此打击，从 1929 年黑色星期五的股灾开始，经济一路走低，民众在失业与饥饿中，普遍失去了信心。1933 年富兰克林罗斯福就任总统，大刀阔斧采取了 “罗斯福新政”。其中，不乏异常激进的手段。他于 1933 年 4 月 5 日发布政府令，宣布禁止民众持有黄金，并强制以 20.67 美元的价格收购美国民众手中的黄金。

罗斯福新政对于经济的作用，一向是有争议的。 普遍的观点认为，罗斯福新政拯救了美国经济，从 1933 年之后美国经济开始复苏。 但有一些经济学家，以奥地利自由经济学派为主，则对此持怀疑态度，认为经济复苏并非罗斯福新政之功，恰恰相反，罗斯福新政延迟了经济复苏的速度。

但有一个观点则争议很少，人们普遍认为罗斯福没收民众黄金，是美国历史上政府最严重的违宪行为，这是美国政府对民众最赤裸的掠夺。

而中本聪的生年 1975 年，恰好又是福特总统签署 “黄金合法化” 法令的年份，美国人民再次获得了黄金的合法拥有权。

中本聪是真正的密码学家，一个编造的生日，也成了他的檄文。 他并非纯粹的技术狂人，他所创造的比特币，寄托了深重的社会理想。

在比特币的创世区块中，中本聪留下了一句话，这句话来自 2009 年 1 月 3 日泰晤士报头版文章的标题：2009 年 1 月 3 日，财政大臣正处于实施第二轮银行紧急援助的边缘。 更加清楚的表明了中本聪对银行体系的嘲讽态度。

中本聪的目标乃是挑战现有的金融秩序，站在中央银行体系、货币发行机制，以及支付方式之前，他就像唐吉坷德一样，发起了攻击，不过他的武器是数学和密码学，另一个不同是，他比唐吉坷德更聪明，也更强大，也许勇气比唐吉坷德要小一点，还要更谨慎一些。

难道中本聪真的是淡泊名利吗？错了!  他之所以隐姓埋名，完全为的保护自己。 如果他公开自己的身份，也许早已为 FBI 逮捕，在监狱中安度余年了。 发明比特币这桩事，往严重了说，可以算是伪造货币，美国法律明令禁止私人发行货币与法币美元竞争。 即便往宽松了论，不按伪造货币追究，也可以因为比特币方便了毒品与军火买卖，而判他的罪。美国司法史上，有这样的案例。

比特币是第一个与法币竞争的货币系统。

乔姆的 eCash，还是依托在银行体系上，可以安全地归类到法定货币的支付渠道、支付手段中。  尼克·萨博的比特黄金、戴维的 B-Money 只是纸上理论，并未真正实现。 而亚当·贝克的哈希现金以及哈尔的 RPOW 虽然都有货币的影子，但其目标乃是用于计算机系统，用于电子邮件之类系统的防攻击中，并无挑战金融体系的意图。

比特币能够威胁到当前的金融体系，威胁到金融权力。

中本聪，他比余则成还要小心。中本聪所拥有的武器，那可远超余副站长了，电视剧潜伏发生的那个时代没有非对称加密，若有，我们的余副站长绝对可以高枕无忧，不必每日紧锁眉头、提心吊胆。

# 区块链的故事-中本聪是谁

中本聪所用的英文名是 Satoshi Nakamoto，在日本，人们翻译他的名字为中本哲史，Satoshi 可以对应多个中文字：聪、智、慧、哲、敏。总之就是聪明的意思啦。

再憨厚的人，也不会相信，这是个真名。

但比特币的创造者，起的这个假名字，还是给一位真叫 “中本聪” 的人，带来了不少麻烦。

2014 年 3 月，美国新闻周刊的一位记者，Leah McGrath Goodman 发文称自己找到了中本聪本尊。该中本聪全名叫多利安·中本，居住加州洛杉矶的郊区，是一位退休的工程师，曾为美国军方工作过。 记者 Leah 的思维很直线，他寻找中本聪，就直接到美国公民数据库中搜索叫 “中本聪” 的人。结果一下子就找到了，Leah 大喜过望，直扑而去。而在交流过程中，这位木讷的中本聪很不配合，说 “我已经不再参与它了，不能讨论它” ，这让 Leah 再次大喜过望，认定多利安就是比特币的发明人。一时闹得鸡飞狗跳，沸沸扬扬。后来多利安否认了，他错以为记者所问的，是他曾经参加的军方项目。

事情的走向随之开始诡异了。中本聪在 P2P 基金会论坛上的账号，打破了 3 年的沉默，发了一个帖子说 “我不是多利安”。但随后论坛官方澄清，中本聪的这个账号，已经被黑掉了，这个发言帖子并非来自中本聪本人。

诡异并未终止在这里。随之人们发现，比特币的重要参与者，也是第一个运行比特币的密码学家哈尔·芬尼，就住在多利安家旁边！

多利安并非中本聪，这个很容易推论出来。比特币的发明者不会那么直白，用上自己的本名。另外，多利安的英语很笨拙，而中本聪则使用完美无瑕的英语。

但是，假设哈尔·芬尼是中本聪，或者是中本聪小组的一员，哈尔·芬尼随手用了下自己邻居的名字，这要算是一种可能。

现在，我们有了两位候选人，他们都可能是中本聪： 多利安中本，哈尔·芬尼。

多利安中本，这个推测可称之为 “躺枪” 候选人。仅仅是同名同姓而已，其他的别无相似之关联。

哈尔·芬尼，则可算是 “非常嫌疑” 候选人，毕竟当时他就在现场，他靠的最近！ 哈尔·芬尼的密码学和编程能力，让他成为我们已知人选中最匹配的了。 虽则戴维在接受采访时认为，只有他与尼克·萨博，具备这个可能性。但戴维指的是密码学及高层设计的能力，而非 C++ 代码能力。

尼克·萨博一直被认为是中本聪的强力人选。萨博在 2011 年也曾经说过，在中本聪之前，只有他自己，戴维还有哈尔·芬尼三人对数字货币的创意具有巨大热情，并积极的付诸行动。从兴趣、密码学及创造性上，他可以是中本聪的。

2013 年有人对中本聪的文本做文本风格上的分析，并与尼克·萨博的文本进行了比较。结论是非常相近，这也让人们更加怀疑尼克·萨博就是中本聪。但尼克·萨博本人否定了。

而戴维也认为尼克·萨博不会是中本聪。因为中本聪在联系他讨论比特币时，压根儿就未曾听闻过尼克·萨博的比特黄金。戴维的这个理由似乎并不成立，尼克·萨博若要藏匿身份，恰恰要不提自己的比特黄金才是。但戴维的另一个理由，却是无可辩驳的，戴维说尼克·萨博并不以 C++ 技能见长。

但戴维可是真正的 C++ 高手，他是 Crypto++ 库的开发者，在密码软件领域硕果累累。中本聪在邮件中，对戴维非常尊重。 但戴维在后来说，他猜测中本聪并未读过他的 B-Money 论文，只是在写比特币论文时，引用了一下 B-Money 概念，戴维认为自己对比特币并无真正贡献。

戴维与哈尔·芬尼一样，在密码学、编程能力上，都足以成为中本聪。那么戴维是否中本聪？

记者曾经采访戴维，戴维倒也没有谦虚，他说放眼望去，天下英雄能做出比特币的，只有尼克·萨博和自己。 记者追问，那既然尼克·萨博不是，您岂不是中本聪唯一候选人么？ 戴维回答：“中本聪出来之后，就有了第三个人。” 他还是否认了。

也有人对戴维的华人身份做了引申，认为“中本聪”乃是 “中国人本来聪明” 的意思，所以中本聪一定就是戴维。 拜托啦，有一点点民族自豪感是好的，但这中本聪英文是 Satoshi Nakamoto，是中国人自己翻译成中本聪的好不？如果韩国人愿意，也可以翻译成韩本聪的，别说韩国人不会这么干，他们的民族自豪感那是远超中国，堪称宇宙第一。

好，现在我们又多了两位候选人：尼克·萨博；戴维。

尼克·萨博可谓是 “形似” 候选人。他在密码学界的地位，以及他的思想，都足以成为中本聪，只是需要个大神级的程序员配合他。当然还有他的语言风格是那么像中本聪。

而戴维，则不论从技术来说，还是学界地位来看，都足以创造出比特币。再论自由思想的激进程度，甚至他低调行事的风格，都与中本聪是那么相像。戴维可谓是 “神似” 候选人。

望月新一是数学家，住在日本东京，在京都大学任教授，在数学领域有着杰出的贡献。他自己创造了一套艰深的数学理论，并籍此解决了 ABC 猜想。 2013 年计算机大牛，也是超文本（Hypertext）的发明者特德·尼尔森声称望月新一乃是中本聪。这个推测毫无逻辑，仅仅因为望月新一是天下头一号聪明人，那他就是中本聪，这推理太霸道，简直让人无言以对。望月新一是理论数学家，而中本聪不仅是学者，还是工程实现的高手。再说，望月新一这样的数学家，应该是不喜欢去写代码的，更不愿意去做软件的。

澳大利亚企业家克雷格·赖特（Craig Wright）于 2015 年接受电视采访，声称自己是中本聪，随后他的家遭到警察搜查。据传说，他给出了技术层面的证据，但无人验证。克雷格·赖特的公开声明也前后矛盾，顾此失彼，完全是莫名其妙的。众多区块链圈内人士，包括以太坊发明人维塔利卡（ Vitalik），闪电网络发明人约瑟夫·朴恩（Joseph Poon）都对克雷格·赖特的技术演讲嗤之以鼻。 只是，不知道为何，比特币的首席开发者盖文，却支持克雷格·赖特。无论如何，说克雷格·赖特是中本聪，听起来都像是一个闹剧。不是故意要歧视企业家，但让一个企业家去开发出比特币这样的系统？您是逗呢吧？

望月新一可算是 “莫名其妙” 候选人。 而克雷格·赖特，算他是 “无厘头” 候选人吧。

还有三个候选人，他们来自德国，是一个小组，名字是 Neal King、Vladimir Oksman 和 Charles Bry。一个记者发现，在中本聪论文中，有这样一个 “computational impractical to reverse” 非常罕见的词组，而这个词组出现在这三个人的一份专利申请中，专利内容恰恰是关于密码的更新和分发的。另外，中本聪的[bitcoin.org](http://bitcoin.org/)域名刚好是这份专利申请提交的三天后注册的。[bitcoin.org](http://bitcoin.org/)注册地为芬兰，而这三人中的一位曾在六个月前去过芬兰。同样，这三人也都否认自己是中本聪，而且这三位对比特币也不大认可。这要是真的，那这情节可真是草蛇灰线，玄机深藏，线索暗伏千里之外了，那记者也堪称福尔摩斯附体。

这三位，可称之为 “福尔摩斯” 的候选人。

Jed mcCaled 也是中本聪的合格候选人，他是优秀的 C++ 程序员，创造过电驴，又创办了第一个比特币交易所 Mt.Gox，后来连续创建了 Ripple、Stellar，都是区块链领域的成功项目。而且，巧合的是，他也是 P2P 基金会论坛的活跃会员，中本聪就在该论坛上活动。2005 年到 2010 年，比特币诞生的那段时间，他似乎没有任何工作，也许正在埋头开发比特币。但，Jed 创业那么多，为何单单要隐藏比特币这段历史呢？只要经营过商业的人，肯定都不会躲开聚光灯，这会成为一种刻在骨子里的本能的！ 影响力就是利润，每个企业家都懂的。再说，中本聪隐姓埋名发明了比特币，然后公开建设了比特币交易所，这个逻辑也委实难以说通。

Jed 可称之为 “档期符合” 候选人。

现在我们一共有了 8 组候选人。按可能性先后排序，列表如下：

Dai Wei - 神似

哈尔·芬尼 - 非常嫌疑

Jed mcCaled - 档期符合

尼克·萨博 - 形似

多利安中本 - 躺枪

望月新一 - 莫名其妙

克雷格·赖特 - 无厘头

Neal King、Vladimir Oksman 和 Charles Bry - 福尔摩斯

但最有可能的猜测是，中本聪并非上面的各位大佬们，而是另有其人，很可能他只是一名默默无闻的密码学家。不过，默默无闻并不是说他是民科，须知，无论从论文还是从代码上分析，我们都可以判断出中本聪是一位货真价实的学者。另有一种论调说中本聪是一群人，这个也有些不可信，中本聪在论坛上的文章以及讨论，表现出了一个人完整的个性，一群人很难群演出这种个性上的一致。 若中本聪是世界上最杰出的那几百位密码学者之一，他可能默默无名的搞出了比特币，但很有可能在后期，戴维、哈尔·芬尼、尼克·萨博等大师已经知晓其身份，只是众人皆为其隐瞒而已。

2016 年在无厘头的克雷格·赖特在新闻上闹得轰轰烈烈时，以中本聪邮件注册的账户，在 Linux 基金会论坛上，有一个发帖说：“我不是克雷格·赖特，我们都是中本聪。” 人们虽然都怀疑这句话并非出自中本聪，但我们依然可以引用这句话，说一句：“**人人都是中本聪**。”

# 区块链的故事-比特币的主要历史

2008 年 11 月 1 日，中本聪在论坛上发表白皮书。

2009 年 1 月， 中本聪发布比特币 0.1 版。

2009 年 1 月 3 日，中本聪挖掘出第一个区块。

2009 年 1 月中，哈尔·芬尼第一个下载比特币客户端并运行。

2009 年 1 月 12 日，哈尔·芬尼收到来自中本聪的 10 个比特币，这是第一笔交易。

2009 年秋天，比特币网站的维护者马迪，用 5050 个比特币，交换了 5.02 美元。

2010 年 5 月 22 日，拉斯洛用 10000 个比特币换了 2 个披萨。

2010 年 7 月 18 日，MT.GOX 上线运行。

2011 年 4 月，“比特币耶稣” 罗杰大举买入比特币，将价格从 1.89 美元拉升到 3.30 美元。

2011 年夏， 《时代周刊》及《福布斯》分别长篇报道比特币，引发社会对比特币的关注。

2012 年，多重签名软分叉。

2013 年 4 月 1 日 比特币突破百元大关。

2013 年 3 月，比特币第一次分叉。

2013 年 10 月 FBI 关闭 “丝路” 网站，并抓捕“丝路”的老板。FBI 没收 26000 个比特币。

2013 年 10 月首个比特币 ATM 在加拿大问世。

2013 年 11 月 维珍航空接受比特币订票。

2013 年 12 月中国央行宣布不接受比特币，比特币跌至 600 美元。

2016 年 6 月比特币 CSV 分叉。

2017 年 8 月 比特币现金从比特币系统中分离出来，成为独立的数字货币。

2017年 11 月比特币上涨至 20000 美元。

2017 年 12 月比特币价格下跌，进入漫长的疲软期。

2018 年，比特币价格长期盘桓在 3000 - 4000 美元区间。

**比特币的意义**

乔姆在创造数字货币时，追求的是 “不可追溯”，目标是为了保护个人隐私。到了密码朋克小组中，尼克·萨博、戴维等人除了保护个人隐私这个小目标之外，浓浓的乌托邦主义理想就冉冉升起。尼克·萨博一直的研究，要在网络上建设稳固可信的商业关系与合同关系。而戴维则要为无政府的社区提供货币。

中本聪无疑也是一个无政府主义者，他对英国银行业的嘲讽，永远烙在了创世区块中，好在英国绅士们并不介意，几百年来英国绅士是最善于接受批评的。中本聪的本意，清清楚楚写在比特币论文中，他要设计一种不依赖第三方信任的电子货币系统。

伟大的事物出现后，在人们手中的用途，总有个飘忽不定的过程。如同周星驰喜剧片中间谍的装备，看上去是只皮鞋，实质上是个吹风机。非对称密码学出现后，最直接的用途，自然是用作消息加密。然而谁又能想到，它被用来创造数字货币。

比特币是一个创举，人们从此进入数字货币时代。然而比特币所打开的那扇门，后面又藏着何种仙山丽景，在今天谁又能看清楚呢？

互联网角度

因为比特币，互联网第一次开始承载、传递、流通价值。在此之前，互联网只能传递信息，价值只能依靠银行、淘宝、腾讯这样中心化的组织来记录。

从此之后，在互联网上，人们一样可以运作现实世界中的各种商业行为。比如，不通过银行，直接付 100 元钱给你的理发师，或者在网上与你的合作伙伴签署一个关于股权的合约。效率当然更高，而且，合约条款可自动执行。

比特币开始，互联网才进入 2.0，互联网才刚刚走进青春期。

科技角度

比特币是密码学结出的硕果。在人类历史上，密码学一直就是战争、商业竞争中最重要的武器，在二战期间，密码学可以说左右了战争的走向。 从密码朋克小组将密码学带入民用，密码学开始为世界进入数码时代作了巨大的助推。

随着人工智能、物联网技术的发展，人们已经站在了机器时代这样一个新纪元之前。比特币以及由此出现的区块链，则为机器时代的社会信用、人类组织形式、机器交互提前做了准备。

社会角度

人类社会的组织模式，以及计算机系统的架构模式，一直以来都是中心化的。比如建立一个公司，都是先有 CEO，然后再层层分设经理，权力由上而下传递。而比特币系统的 P2P 模式，还有区块链的去中心化模式，将给人类的社会组织形式，带来新的工具，一种去中心化的工具。

去中心化与中心化不是彼此排斥、非此即彼的关系，而是可以并存的。二者都是人们可用的工具，如何选择，依然由人们的自由意志决定。

经济学角度

中本聪是否读过哈耶克的书，我们找不到证据。尼克·萨博的文中，倒是常常引用哈耶克的话。 奥地利学派经济学者倡导自由经济，看重市场的作用。哈耶克有一本书，就叫做《货币的非国家化》，更是提出激进的自由市场理念，认为货币的发行可以不由央行垄断，而是商业机构都可发行货币。

这与中本聪在比特币系统中的理念无疑是相符的。 对金融体系、银行系统的不信任，当是中本聪设计比特币的出发点。而 2008 年正是全世界爆发经济危机的时点，人们普遍处在恐慌与失望的情绪中。

伦理角度

财产权，是人类社会文明的基石之一。而用暴力保护财产，保护人们的人身安全与自由，是人类历史上唯一的手段。任何一间房子，任何一个人，都要受到某个政府和某支军队的保护。

而比特币系统，则是人类社会上，罕见的，不受暴力保护，也未被暴力消灭的价值系统。这给了我们以信心，也许未来的人类不必再依赖暴力手段才能对财产、人身安全与自由进行保护。

哲学角度

哈耶克有一个独创的思想，他认为人类的习俗、法律、宗教这些规则，都不是人类理性的发明，换句话说，并非出自聪明人的设计，而是在人类社会中自发演进出来的。所以，面对人类社会，不要过于相信理性的力量，而是要尊重既有的规则。

深度学习给人工智能带来了巨大突破，其原理是让机器从数据中拟合出多个线性函数，从而对数据进行分类和决策。 其本质是人们自知无法找到准确的数学函数，来描述数据的规律，于是便把决策的权力交给机器。

人们对于彼此之间的信任，耗费了太多的精力和成本。中本聪在比特币的论文中，论述了 “无信任” 的商业模式，我们不再将商业关系建立在对人的信任之上，而是让机器来执行吧。

这是人们通过理性的思考，放弃了对自身理性的偏执和自信，将权力交与机器。

**比特币与区块链**

在中本聪的论文中，并没有 “Blockchain” 一词，而是两个词 “Block” 与 “Chain”。他在开发程序的时候，把数据文件都放在了一个叫做 Blockchain 的文件夹内，由此 Blockchain 成了比特币系统所用技术的代名词。

而今天，Blockchain 一词因其颇具形象的画面感，而成为以比特币为开端，一大类基于密码学的去中心化技术的统称。

区块也好，链也好，都是中本聪用来实现 “点对点电子货币” 的技术手段，实质上都并非去中心化技术的本质。但是，不必纠缠于名词，内涵会给名词以新的含义，正如火车早已用电，但我们依然称之为火车一样。

比特币带来了区块链技术，而区块链将带我们走向新的世界。

作者：灯下鼠  
链接：https://www.jianshu.com/p/9d7c05ee6664  
来源：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。

# 区块链的故事-Diffie-Hellman 密钥交换

惠特菲尔德·迪菲（Whitfield Diffie）出生于 1944 年，留着披肩长发，胡须半尺，须发尽皆雪白如银，看上去潇洒磊落，却又不拘一格，乃是风清扬、令狐冲一流的人物，他自称是 “离经叛道者”。

他从小喜爱数学，后来在麻省理工读了数学专业，于学业上他并不很用心，对学校留的作业没什么兴趣。他的兴趣在于研究密码学，尤其是密码分发问题。使用传统的对称加密算法，密钥的安全交付成了加密工作中最薄弱的一环，为了分发密码所耗费的人力及物力巨大。军方、政府、银行都维持着庞大的密码运送团队，团队中的人必须绝对可信，薪资自然也就不低，这些人走南闯北四处运送密钥。



就这样，密码分发问题一直困扰着密码学家们，也困扰着密码的重度用户 - 各国的政府和军方。

迪菲思考了很久，希望能够想出个方案来颠覆这个行业，解放那些忙碌不堪的密码分发员。他热爱自由，于是他不上班，自由自在，号称专门研究密钥分发问题。

1974 年，迪菲听闻有人和他一样，对密码分发问题感兴趣，那个人叫做马丁·赫尔曼（Martin Hellman），在斯坦福大学做教授。 迪菲不亏是北美令狐冲，他当晚就驱车 5000 公里去找赫尔曼。马丁接到迪菲电话，是不是把他当传销不好说，总之，大教授勉强答应了见面半小时。

赫尔曼从面相上看，儒雅斯文，一派学者气象。 但人不可貌相，实际上他一直是积极的社会活动家，在 “远离战争”、“反对核武器” 这一类的社会活动中都有他的身影。



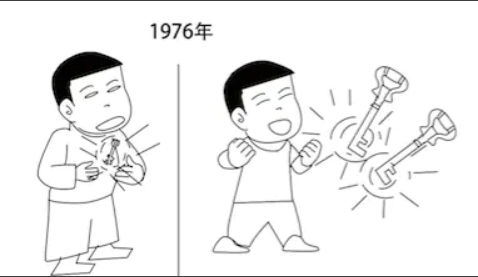
这次见面的结果是，当晚赫尔曼就把迪菲带回了家，和家人一起吃晚饭。

而另一个成果是，两人情投意合，义结金兰，发誓要一起研究密码分发技术。他们碰到的第一个难题是，两人都太穷了。赫尔曼是个穷教授，而迪菲干脆没有固定收入。 两人毕竟聪明，合计了一下，一致同意，对付贫穷最好的办法就是考研。于是赫尔曼运用自己仅有的那点权力，把迪菲招为自己的博士研究生。实际上，迪菲比赫尔曼还大一岁。

迪菲一向不守陈规，在学校也不乐意做作业，到最后，那个博士也没毕业。他擅长的是提出创新的主意。早在 1973 年，迪菲就提出了非对称加密的思想来，可惜无人能够实现。

迪菲与赫尔曼努力的方向是密码交换问题。

人类在密码学上的研究，可以截然划分为两个阶段。在迪菲和赫尔曼的成果之前，可以称之为原始密码时代，所用技术全是对称加密。所谓对称加密，就是加密与解密，用同一个密钥。举例来说，一个简单的加密方法，是把  A 加密成为 B， 把 C 加密成为 D。（A - B，C - D) 就是这个加密方法的密钥，对密文解密，也需要这个密钥。

  
如果用生活中钥匙与锁做比的话，那么钥匙是密码，锁是消息。合上锁，需要钥匙。打开锁，也需要钥匙，这就是对称加密。

再举一个影视剧的例子，潜伏里余则成收到广播中的数字，根据数字和规则，从一本书上寻找对应的文字。那本书，就是密钥。加密方和解密方，都需要那本书。

这种原始的方法，其中最让人痛苦的问题有二，其一是密码的分发，如何给余则成送去那本书。对于经常需要更改密码的情况，送密码的代价就非常高。 其二是密码一旦被截获，则一切全完。

在人们的直觉中，两人之间要想使用密码通信，那么必须约定密钥。两人必须鬼鬼祟祟的见一面，避开人群，偷偷摸摸交换个密码、钥匙什么的。这难道还有什么可怀疑的？

然而在人们找到方法打破这个直觉之前，一个思想实验，给了人们巨大的启示。 思想实验非常神奇，物理学家们都爱用，比如薛定谔的猫就是最著名的思想实验。爱因斯坦、费曼等物理大牛更是用思想实验斗法，你讲一个故事，我讲一个故事。思想实验不涉及科学与技术的细节，但故事其中的逻辑却能对科学与技术问题进行推演，仿佛战争之前的沙盘推演。而且，谁不爱听故事呢？

这个思想实验是这样的。

爱丽丝和鲍勃，是一对情侣，住在临近的两个村子里，双方父母不同意两人的恋情，两人都被锁在家中，只能通过信件诉衷情。 爱丽丝要送情书给鲍勃，又不愿意让邮递员看到信件内容。在人们直觉的思维中，爱丽丝和鲍勃可以用一个加锁的盒子来寄信，两人都有这个锁的钥匙，就可以了。 但是，爱丽丝需要先把钥匙送给鲍勃。有送钥匙的功夫，别说情书可以亲自送过去了，两人私奔都可以了。

有没有这种可能，爱丽丝在见不到鲍勃的情况下，也能安全把信件送到鲍勃手里，且邮递员偷窥不到信件内容？

爱丽丝很聪明，她想到了方法。她把信件放到盒子里，然后用一把锁锁上，钥匙只有一把，在她手里。邮递员把盒子送给了鲍勃，邮递员因为没有钥匙，打不开盒子，所以偷窥不了。鲍勃收到盒子后，也无法打开盒子。但鲍勃拿出另一把锁，在盒子上再锁一道，钥匙也只有一把，在他手里。 鲍勃让邮递员将盒子送回爱丽丝手中。爱丽丝收到盒子后，用自己的钥匙，把自己的那把锁打开，让邮递员把盒子再交回鲍勃手中。鲍勃收到盒子后，盒子上只有一把鲍勃自己的那把锁，鲍勃摸出钥匙，颤抖地打开盒子，拿出情书信件阅读，沉浸在幸福中。当然，他还是要防备下邮递员，他来回跑了三趟，又没看到信，怒气之下起了杀心，把我们一场科技的思想实验，反转成凶杀故事也没准。

就这样，看似有违我们直觉的难题，就解决了。迪菲和赫尔曼，他们这些科学家认为，既然思想实验的逻辑可以走通，那么只要找到合适的数学方法，就一定能实现。迪菲与赫尔曼把目光放到了单向函数上，所谓单向函数，就是算法是不可逆的函数。做个比喻，我们很容易就可知道，黄色油漆与蓝色油漆混到一起，能够得到什么颜色，我们只要把两种油漆倒在一起搅拌一下即可。但若是给我们一桶绿色油漆，让我们分辨出是哪两种油漆混合而成，以及两种油漆的混合比例，那就困难无比了。

寻找这个数学方法，用去了迪菲和赫尔曼两年时间，最终的攻克，归功于赫尔曼。他天才的发现，取模运算，也就是做除法找余数的运算，具有单向函数的特性。用这个取模函数，爱丽丝与鲍勃，可以公开的交换数字，最终生成共同的密钥，只有他俩知道。邮递员眼睁睁看着他俩一桶桶的送油漆，就是分离不出油漆的配方，也就得不到密钥。

其实还有第三人，拉尔夫·默克尔（Ralph Merkle），他也参与了这个工作。默克尔在此之前便已在密钥分发技术上，成就非凡。 他有过一个理论叫 Merkle 难题，那是对称加密的原始时代所能达到的最高成就，我们还是用思想实验的方法说明这个理论。

爱丽丝要送情书给鲍勃，他们用的对称加密，所以必须约定密钥。 爱丽丝找到 1 万把锁，每把锁有2 把钥匙，在锁和钥匙上一一标上号码。每把锁的钥匙，爱丽丝都留下一把。把 1 万把锁和另外的 1万把钥匙，一一对应放进 1 万个密封的盒子，盒子上并不锁死，但是要打开盒子，需要拧盒子的螺丝，每个盒子打开都需要 10 分钟。爱丽丝委托邮递员，送这 1 万个盒子给鲍勃，倒霉的邮递员怨气冲天，但还是送去了。 鲍勃看到 1 万个盒子，并没有惊慌，他沉着地选择了一个盒子，随意选择的一个，然后用 10 分钟拧下盒子上的螺丝，拿到了那把锁，假设那锁上标号是 #6800。鲍勃用 # 6800 的锁与钥匙，锁上一个盒子，盒子里装着信件，委托邮递员送给爱丽丝。 爱丽丝收到盒子后，根据锁上标号 #6800，找到 #6800 钥匙，打开盒子，阅读情书，沉浸在幸福中。

若是邮递员要打开鲍勃的盒子，他就得一个个打开 1 万个盒子（此处物理的盒子与数字的盒子，逻辑上难以彻底对应。对于物理盒子，在邮递员从爱丽丝拿到 1 万个盒子时，他便需打开所有 1 万个盒子，每个盒子 10 分钟，并复制所有钥匙。拿到鲍勃的信件盒子后，由于并不知道 6800 对应哪一把钥匙，他只能一把把去试。而在数字世界中，此时邮递员依然拥有从爱丽丝处拿到的 1 万个盒子的原始副本），每个盒子 10 分钟，然后一把把钥匙试那个 # 6800 的锁。如果运气好，他大约需要打开 5000 个盒子，也就是 5 万分钟。

Merkle 难题，几乎算是在对称加密技术下，分发密钥问题的最佳方法了，但对称加密的潜力也就到此为止，再无它途。

1976 年迪菲与赫尔曼联名的论文 《密码学的新方向》，是一个新纪元的开始，从此这个世界走进了非对称加密时代。这篇论文几乎奠定了互联网传输安全的基础。实际上，这篇论文中，默克尔也有贡献，只是那时他还年轻，只是赫尔曼的博士生。2015 年图灵奖颁给了迪菲与赫尔曼，默克尔也因此无缘图灵奖这至高荣誉。

但默克尔也许并不在意，他自己的发明 Merkle Tree，是区块链上最基础的技术之一。每一次区块链上的数据校验，都在致敬他。

# 区块链的故事-RSA

迪菲与赫尔曼完美地解决了密钥分发的难题，从此，交换密钥就很简单了，爱丽丝与鲍勃完全可以可以在村头大喇叭里喊话，就能够交换出一个密钥。但加密的方式，依然是对称加密的。

DH 协议交换密钥虽然方便，但依然有一些不尽人意的麻烦处，爱丽丝还是要与鲍勃对着嚷嚷半天，二人才能生成密钥。当爱丽丝想要交换密钥的时候，若是鲍勃正在睡觉，那爱丽丝的情书，还是送不出去。

迪菲与赫尔曼在他们的论文中，为未来的加密方法指出了方向。 通过单向函数，设计出非对称加密，才是终极解决方案。 所谓非对称加密，就是一把钥匙用来合上锁，另一把钥匙用来开锁，两把钥匙不同。锁死的钥匙，不能开锁。开锁的钥匙，不能合锁。

麻省理工的三位科学家，他们是罗纳德·李维斯特（Ron Rivest）、阿迪·萨莫尔（Adi Shamir）和伦纳德·阿德曼（Leonard Adleman），他们读了迪菲与赫尔曼的论文，深感兴趣，便开始研究。迪菲与赫尔曼未能搞定的算法，自他们三人之手，诞生了。



2002 年，这三位大师因为 RSA 的发明，获得了图灵奖。 但不要以为 RSA 就是他们的全部，这三位是真正的大师，每一位的学术生涯都是硕果累累。让我们用仰视的目光探索大师们的高度。

李维斯特还发明了 RC2, RC4, RC 5, RC 6 算法，以及著名的 MD2, MD3, MD4, MD5 算法。他还写了一本书，叫 《算法导论》，程序员们都曾经在这本书上磨损了无数的脑细胞。

萨莫尔发明了 Feige-Fiat-Shamir 认证协议，还发现了微分密码分析法。

阿德曼则更加传奇，他开创了 DNA 计算学说，用 DNA 计算机解决了 “旅行推销员” 问题。 他的学生 Cohen 发明了计算机病毒，所以他算是计算机病毒的爷爷了。他还是爱滋病免疫学大师级专家，在数学、计算机科学、分子生物学、爱滋病研究等每一个方面都作出的卓越贡献。

1976 年，这三位都在麻省理工的计算机科学实验室工作，他们构成的小组堪称完美。李维斯特和萨莫尔两位是计算机学家，他们俩不断提出新的思路来，而阿德曼是极其高明的数学家，总能给李维斯特和萨莫尔挑出毛病来。

一年过后，1977 年，李维斯特在一次聚会后，躺在沙发上醒酒，他辗转反侧，无法入睡。在半睡半醒、将吐未吐之间，突然一道闪电在脑中劈下，他找到了方法。一整夜时间，他就写出了论文来。次晨，他把论文交给阿德曼，阿德曼这次再也找不到错误来了。

在论文的名字上，这三位还着实君子谦让了一番。 李维斯特将其命名为 Adleman-Rivest-Shamir，而伟大的阿德曼则要求将自己的名字去掉，因为这是李维斯特的发明。 最终争议的结果是，阿德曼名字列在第三，于是这个算法成了 RSA。

RSA 算法基于一个十分简单的数论事实：将两个大素数相乘十分容易，但想要对其乘积进行因式分解却极其困难，因此可以将乘积公开，用作加密密钥。

例如，选择两个质数，一个是 17159，另一个是 10247，则两数乘积为 175828273。 乘积 175828273 就是加密公钥，而 （17159，10247）则是解密的私钥。

公钥 175828273 人人都可获取，但若要破解密文，则需要将 175828273 分解出 17159 和 10247，这是非常困难的。

1977 年 RSA 公布的时候，数学家、科普作家马丁加德纳在 《科学美国人》 杂志上公布了一个公钥：

114 381 625 757 888 867 669 235 779 976 146 612 010 218 296 721 242 362 562 842 935 706 935 245 733 897 830 597 123 563 958 705 058 989 075 147 599 290 026 879 543 541

马丁悬赏读者对这个公钥进行破解。漫长的 17 年后，1994 年 4 月 26 日，一个 600 人组成的爱好者小组才宣称找到了私钥。私钥是：

p：3 490 529 510 847 650 949 147 849 619 903 898 133 417 764 638 493 387 843 990 820 577

q：32 769 132 993 266 709 549 961 988 190 834 461 413 177 642 967 992 942 539 798 288 533

这个耗时 17 年的破解，针对的只是 129 位的公钥，今天 RSA 已经使用 2048 位的公钥，这几乎要用上全世界计算机的算力，并耗费上几十亿年才能破解。

**RSA 的安全性依赖于大数分解，但其破解难度是否等同于大数分解，则一直未能得到理论上的证明，因为未曾证明过破解 RSA 就一定需要作大数分解。**

RSA 依然存在弱点，由于进行的都是大数计算，使得 RSA 最快的情况也比普通的对称加密慢上多倍，无论是软件还是硬件实现。速度一直是 RSA 的缺陷。一般来说只用于少量数据加密。

RSA 还有一个弱点，这个在下文中还会提及。

在密码学上，美国的学者们忙的不亦乐乎，成果一个接一个。但老牌帝国英国在密码学上，也并不是全无建树，毕竟那是图灵的故乡，是图灵带领密码学者们在布莱切里公园战胜德国英格玛加密机的国度。

英国人也发明了 RSA，只是被埋没了。

60 年代，英国军方也在为密码分发问题感到苦恼。1969 年，密码学家詹姆斯埃利斯正在为军方工作，他接到了这个密钥分发的课题。他想到了一个主意，用单向函数实现非对称加密，但是他找不到这个函数。政府通讯总部的很多天才们，加入进来，一起寻找单向函数。但三年过去了，这些聪明的脑袋，并没有什么收获，大家都有些沮丧，这样一个单项函数，是否存在？

往往这个时候，就需要初生牛犊来救场了。科克斯就是一头勇猛的牛犊，他是位年轻的数学家，非常纯粹，立志献身缪斯女神的那种。 虽然年轻，但他有一个巨大优势，当时他对此单向函数难题一无所知，压根儿不知道老师们三年来一无所获。于是懵懵懂懂的闯进了地雷阵。

面对如此凶险的地雷阵，科克斯近乎一跃而过。只用了半个小时，就解决了这个问题，然后他下班回家了，并没有把这个太当回事，领导交代的一个工作而已，无非端茶倒水扫地解数学题，早点干完，回家路上还能买到新出炉的面包。他完全不知道自己创造了历史。科克斯是如此纯粹的数学家，后来他听闻同事们送上的赞誉，还对此感到有些不好意思。在他眼里，数学应该如哈代所说，是无用的学问，而他用数学解决了具体的问题，这是令人羞愧的。

可惜的是，科克斯的发明太早了，当时的计算机算力太弱，并不能实现非对称的加解密。所以，军方没有应用非对称加密算法。詹姆斯与科克斯把非对称加密的理论发展到完善，但是他们不能说出去，军方要求所有的工作内容都必须保密，他们甚至不能申请专利。

军方虽然对工作成果的保密要求非常严格，但对工作成果本身却不很在意。后来，英国通讯总部发现了美国人的 RSA 算法，觉得好棒棒哦。他们压根就忘记了詹姆斯与科克斯的 RSA。通讯总部赞叹之余，扒拉了一下自己的知识库，才发现自己的员工科克斯早已发明了 RSA 类似的算法。 官僚机构真是人类的好朋友，总能给人们制造各种笑料，虽然其本意是要制造威权的。

科克斯对此并不介怀，他甚至是这样说的：“埋没就埋没吧，我又不想当网红，要粉丝干嘛？那些粉丝能吃？” 原话不是这样的，但表达的意思基本如此。

迪菲在 1982 年专程去英国见詹姆斯，两人惺惺相惜，真是英雄相见恨晚。可惜詹姆斯依然不能透漏他们对 RSA 的研究，他只告诉了迪菲：“你们做的比我们要好。” 全球各国的科学家们，可以比出谁更好，但全球各国的官僚们，却很难比出谁更颟顸，他们不分高下。

# 区块链的故事-ECC 非对称加密

RSA 是第一个非对称加密算法，也是迄今为止，最优秀、应用最广泛的非对称加密算法。它有一个非常重要的优点：原理简单，易于理解，而且操作方便。

但 RSA 的弱点也很明显，那就是运算的速度很慢。与同一安全级别的对称加密算法比较，RSA 要慢几百倍。所以在实际应用中，通常会结合 RSA 与对称加密算法，用 RSA 加密对称加密算法的密钥，然后用密钥对消息进行对称加密。

1985 年一种新的非对称加密算法出现。华盛顿大学的 Neal Koblitz 与普林斯顿大学的 Victor Saul Miller 分别独自提出了 ECC 椭圆曲线算法。 这种算法比 RSA 的单位安全强度更高，ECC 使用 256 位密钥可以达到 RSA 使用 3072 位密钥的效果。 但 ECC 的缺点是原理非常复杂，其背后的数学理论极其深奥，并非 RSA 那样具备高中数学即可理解的简单。

ECC 需要的密钥较小，且签名速度快，但验正签名速度慢，这一点正与 RSA 相反。 今天 ECC 已经得到了广泛的应用，**我国的国密 SM2 就是基于 ECC 算法。**

ECC 的效率与 RSA 的效率有一个形象的比较：破解一个 228 字节的 RSA 密钥，需要的能量少于煮沸一勺水的能量；而破解一个 228 字节的椭圆曲线密钥，需要的能量则足够煮沸地球上所有的水。

比特币系统中的非对称加密，应用的就是 ECC 加密算法系列。

Neal Koblitz 也是一位真正的数学家，对于数学有着很深的感情。 1984 年他收到来自荷兰数学家 Hendrik Willem Lenstra 的一封信，在信中，Hendrik 提出了一种应用椭圆曲线进行大数分解的方法。Neal 对此方法大加赞赏，评价说此方法既聪明，又优雅，还很容易理解，可以说将数学在密码学领域的应用，提升到了一个新的水平。

Neal Koblitz 也随之受到启发，他开始思考，是否可以基于椭圆曲线设计一整套加密算法呢？他很快写出来论文，而同期另外一位数学家，Victor Miller，他当时为 IBM 工作，也独自提出了同样的理论。所以，椭圆曲线加密算法，是这两位数学家分别独立创造出来的。

由此可以看到，数学家们之间的交流是多么重要，RSA,、ECC 都是两拨人在同一时期分头发现的。 Neal Koblitz 也曾经建议，密码学家和计算机学家，要经常读别人的文章，不要兴高采烈提出一个理论，却发现早就有人写出过论文了。 Neal Koblitz 作为数学家，对密码学家颇有点瞧不上。他说，数学家如同大象，看时间的流逝很慢。而密码学家和计算机学家，则像蜂鸟一样，看时间的流逝很快。他用的语言很文艺，实则批评很尖锐，意思是说密码学家和计算机学家非常急功近利。急急忙忙写文章，就像蜂鸟振翅一样，写出的只能是些没有价值的垃圾。

如果可以对 Neal Koblitz 的文章妄加解释的话，那么可以认为在 Koblitz 眼中存在一条歧视链。 数学家歧视密码学家，密码学家歧视计算机学家。

Neal Koblitz 的研究横跨数学及密码学，所以他有充分的资格对这些学科发表评论。 在他眼中，80 年代的密码学是一个朝气蓬勃的学科，极其刺激，因为那时候美国国家安全局要垄断密码学的研究，这密码学就成了一个禁地。 不禁还好，一听说是禁地，数学家和密码学家们原本没兴趣的，也都露出了 “邪恶的” 笑容。所以，80 年代，密码学研究真是轰轰烈烈，自由的精神、特立独行的个性，在密码学者身上比比皆是。 Neal Koblitz 对 DH 发明者迪菲就非常认可，认为他是杰出的、不落俗套的自由主义者。

然而密码学家们 “坏孩子” 式的兴奋并未持续很久。美国国家安全局 NSA 并非笨蛋，他们发现大棒不好使，很快就改变了策略。80 年代后期，NSA 设立了基金，用于资助密码学研究的项目，用胡萝卜政策替代了大棒子政策。 有钱自然是好事，数学家和密码学家们踊跃地申请基金。

Neal Koblitz 曾经写过一篇文章，讲述了数学与密码学之间的紧张关系。Neal Koblitz 是数学家，而数学大师哈代曾经这样评论过数论，说数论因远离现实生活而保持了它的优雅与纯净。数学家们常常因为数学本身的审美而感到自豪。 但另一方面，密码学又给 Neal Koblitz 这样的数学家一个在现实世界中驰骋的机会。 Neal Koblitz 引述过 NSA 一位官员的话 “数学家的密码学算法如果有漏洞，那么再写一篇论文就是，但在现实世界中密码失效，则可能丢失百万美金或者造成特工丧命”。 也许 在 Neal Koblitz 的心中也有紧张的关系，一面为了数学的审美而骄傲，另一面为 ECC 在现实世界中的功用而自豪。

# 区块链的故事-图灵与英格玛

在1975 年之前，也就是迪菲与赫尔曼发明 DH 算法之前，人类 6000 年的历史中，密码学跟数学几乎没什么关系。 密码学中用到的那点子数学概念，都是平庸乏味的。迪菲与赫尔曼算是开启了密码学的新时代。

在那 6000 年的黑暗历史中，还有一个例外，就是图灵，他在破解密文时用上了复杂的统计学。

图灵是计算机之父，也是人工智能之父，还是密码学历史上最耀眼的大师。二战中盟军的胜利，图灵的贡献可谓卓越。而对整个人类的科技发展，他也做出了无可比拟、无可替代的贡献。然而，他的个人生活、他的命运，却是一个悲剧。用一句话流行的句式来说，英国欠他一个道歉，全世界人民欠他一句谢谢。

2013 年，英国女王向图灵颁发皇家赦免，英国司法部长宣布，图灵因同性恋遭致的判决是不公的。

我们的叙述，要将时间退回到半个多世纪以前。 1952 年 3 月 21 日，英国柴郡法院判决图灵因严重猥亵行为而有罪。法院给了图灵两个选择，要么入狱，要么接受化学阉割，图灵选择了后者。

图灵违反的法律是 1885 年刑法修正案第 II 条 “严重猥亵罪”，该法条严禁男性之间的身体接触，不论在公共场合还是私人场合。

文明的这列火车，行驶在平行的两根轨道上，一条是科学、技术，一条是伦理、法律、习俗。仅仅相隔半个世纪，1950 年的文明与今天的文明，差距最大的并不是科技，而是对人的尊重。难以想象，在英国，竟然存在过如此粗暴干涉个人自由的法律。

图灵与密码的关系，起因源自二战中德英之间的密码对抗。二战英德之战爆发后，围绕着一款叫英格玛机的加密机，英德之间展开了漫长而艰苦的竞赛。 英格玛机的故事，漫长而曲折，其中涉及国家及人物众多，命运各自跌宕起伏，精彩与复杂的程度完全不输于英格玛机技术上的精彩和复杂。

长话短说，德国人本就擅长机械，在二战期间他们所使用的恩格玛机，可以说是那个时代最登峰造极的密码系统了。恩格玛机本质上依然是一种替代加密法，将一个字母替换成另一个字母。只是德国人对机械与电子的天分，将其发展成了恐怖的复杂机器。恩格玛机使用三个转子、两个插线板、一个反射器，还有复杂的转换关系，实现了近乎无穷的加密可能性。一台恩格玛机器一共可以提供约 10,000,000,000,000,000，即一亿亿种可能的密钥！如果要暴力破解，一秒钟验算一种密钥，则需耗时三万年。

恩格玛机最初是德国发明家亚瑟·斯雪比尤斯于 1918 年发明。亚瑟·斯雪比尤斯也是一个企业家，只是不很成功。他发明恩格玛机，纯粹为了挣钱。 1918 年，他为恩格玛机申请了专利，认为这台机器将会有巨大的市场，军方需要它，商业企业也会需要它。然而很遗憾，商业企业根本没人愿意出钱买，军方对其热情也很小。要知道，按照现在的币值换算，一台恩格玛机要值 20000 英镑。直到 1925 年才有政府部门开始采购恩格玛机，随之这些部门认识到了恩格玛的威力。在之后的 20 年里，恩格玛机卖到德国政府和军方近 20000 台，在二战初期，这种机器让英国的解密者完全陷入了泥潭沼泽中。

1939 年图灵来到布莱切利庄园，这里聚集了一众数学家、密码学家及语言学家，为了破解恩格玛机密码体系。

图灵观察到恩格玛机体系的两个弱点：

其一是任何一个字母，在恩格玛机上不会加密成为其自身

其二是德国的一些密文电报中，有一些周期性固定不变的内容，比如每天的天气预报

基于这两个弱点，图灵设计了名为 “炸弹” 的密码破译机，实质上根据恩格玛体系的两个弱点，对所有可能的转子和插线板进行穷举试算。图灵设计的机器成功破解了德国的恩格玛机器。

后来英国人改进了恩格玛机，对其弱点进行了修正，让加密后的字母，也可以成为其自身。 英国人制造的机器叫 Typex，这可以称之为加强版的恩格玛机。德国人尝试破解 Typex，但无计可施，最终放弃。

恩格玛机器是对称加密时代的最高峰，这个时代持续了几千年，在这几千年中，一直是密码破解师占上风。可以说，没有任何密码体系，是牢不可破的，只要是对称加密，则都可以破解。

# 区块链的故事-对称加密

在人类演进发展出书写的技能后，几乎同时，加密就成为了人们的通讯技术。

最早的加密技术，是隐文术。有历史记载的加密活动，出现在公元前五世纪，希腊与波斯的战争中。希腊人在木板上写字，在字上涂蜡盖住字迹，以此安全传送波斯军队的信息到希腊。还有记载，把字写在间谍剃光的头皮上，然后等间谍长出头发覆盖了字迹，再亲身将自己送到接受方。我国古代，也出现过蜡丸藏书等故事。这些方法，主要的手段就是将要传送的字迹隐藏。隐文术严格来说，算不上密码，是一种明文传送。只要敌方得知隐藏的方法，一切秘密便大白于天下。

而真正的密码技术，有两种，一种是替换，一种是易位。易位密码术最早出现在公元前五世纪，将羊皮纸缠绕在棍子上，沿着棍子纵向写字，这样解下羊皮纸后，其上的字迹横着读就是无意义的乱码。接收方用同样规格的棍子，缠上羊皮纸，则可以纵向读出正确的信息来。

替换密码技术出现在公元前四世纪。婆罗门学者记载了将字母两两替换的方法，可以对信息进行加密。

在易位技术中，字母不变，但字母的相对位置变化；在替换技术中，字母的位置不变，但字母改变。

高卢记中记载，凯撒曾经设计了一套密码，将每个字母往后挪动三位。比如 A 加密成为 D， B 加密成为 E。 这就是凯撒移位密码。

这基本的原理，构成了之后几千年加密的技术基础。人们在历史上设计了更加复杂的密码替换方法，更加复杂的密钥，以及用机械及电子方式加密，但基本原理就是如此。

替换密码的安全性建立在密钥上，只要密钥被敌方获取，则可以轻松解开密文。而密钥可以构成数量庞大的组合，因此在没有更先进的解密方法出现之前，替换密码几乎是安全的。

而之后发明的，对替换密码术的破解方法，原理也很简单。每一种语言，其中的每个字母，都有固定的出现频率。正如 A 这个字母在英语中出现的频率约为 8%，而 E 在英语中出现最频繁，约为 13%。这样，对密文中出现的字母进行频率统计，根据一致的频率替换成正确的字母，就可以翻译成明文了。

在非对称加密出现之前，对称加密与解密的斗争中，加密者一直处在下风。即便如上文所提的恩格玛机，那是对称加密技术的最顶峰，也最终在图灵的统计学和机器运算面前，崩溃了。

计算机的出现，与密码学有着千丝万缕的联系。现在公认的计算机之母，是宾夕法尼亚大学埃克特、莫克利研制的 ENIAC。 实际上，有一位英国数学家，也是图灵的同事，叫马克斯纽曼，他拓展了图灵 “万能机器” 的概念，设计出了可编程计算机，并由工程师汤米佛劳尔斯制造完成，这台机器共有 1500 个电子管。可惜的是，这台机器被英国军方销毁，连图纸也被烧掉。 所以可以说是密码学者，发明了计算机。

计算机出现后，加密与解密的工作，就自然转移到了计算机上。无疑计算机的计算速度和计算能力，也给加密解密技术带来了更宽阔的天地。

计算机只处理二进制数，也就是 0 与 1，所以所有的信息都要转化成为 0 与 1。使用计算机加密，其过程依然按照古老的原则进行，与凯撒时代并无区别。无非就是替换与易位。随着计算机在商业上应用的普及，为了能够广泛使用密文传递信息，建立一套加密的标准，就成了当务之急。

菲斯特尔是德国人，1930 年代流亡来到美国。因为他是来自德国的流亡者，经历了坎坷的努力，方才能够在美国参与密码研究。 事实证明，美国用他用对了。 他在 IBM 实验室发明了后来大名鼎鼎的 DES 算法。 DES 算法是一种对称加密标准，计算机将电文处理成为二进制后，进行分组、加密、替换、易位各种复杂处理，重复操作总计 16 次。解密的那一端，根据共同的密钥，反向处理实现解密。 1976 年 DES 算法成为美国加密的标准。但美国 NSA 要求民用 DES 的密钥数必须控制在 10 的 18 次方以内。

DES 升级后的版本 3DES，现在是全球最流行的加密算法。

# 区块链的故事-密码朋克小组

上个世纪六七十年代，社会思潮丰富多彩，或者说风云激荡，西方的年轻人热衷于反抗些什么，以消除不满与苦闷。朋克运动应运而生，最初的形式是一帮搞乐队的酷小孩，穿着奇装异服，弹唱暴躁而反叛的摇滚。后来朋克就成了一种精神，成了年轻人对抗传统，发泄不满，乃至反对一切，为了反对而反对的一种精神。

朋克精神，就是反抗传统。 然而时间久了，反抗本身也成了一种传统，就此流传下来。

到了 80 年代，个人计算机开始流行，网络始露头角。另外一个新发明， 非对称加密也在 80 年代进入实用阶段。

谢天谢地！ 那些缺乏音乐细胞，搞不了摇滚，偏爱理工科技而被鄙视为书呆子的年轻人，终于有了自己的武器与阵地。他们骨子里的那反抗精神，终于也有了可以发泄的手段。就此，朋克精神进入技术与网络领域。

1992 年，Eric Hughes, Timothy C. May 和 John Gilmore 三个小伙伴聚在一起，他们都热爱密码学，他们商量着要用密码技术反抗点什么。于是他们约定，成立一个 “造反” 小组。当时，他们是在旧金山湾区的一间办公室里，蓝天白云，风和日丽，气候美妙无比。

三个人是清一色的技术高手，在密码技术上的造诣都很深。 在普通人看来，非对称加密的出现，无非一种新技术罢了。但在这三人眼中，非对称加密带来的是一个全新的疆界，一个自由主义者借以藏身的乌托邦。

只有精通非对称加密技术，且洞察当时的技术发展趋势，才能懂得他们所言非虚。 在 PC 与网络流行之前，人们的通讯方式无非信件、电话、电报，这些原始形式的通信，有一个好处，再强权的机构也无法进行大规模的监控，因为拆信，监听电话，截获电报都只能人工来做，费时费力，绝无可能对全社会进行大规模监控。 计算机与网络的流行，给人们带来了网络通信，而这种数字化通信也给强权机构的监控带来的便利，针对通讯数据的自动化监控成为可能。

传统的对称加密技术，需要大规模的密钥分发，只有政府与大公司才能承担的起成本。 而非对称加密技术的出现，让民用的加密也可以固若金汤，再强大的机构也无法破解两个市民之间的加密通信。

斗争由此而来。在三个小伙伴看来，RSA 这样的非对称加密技术，给了人们保护隐私的权力，从此不再担忧被政府监控。有了非对称加密技术，你就可以在网络的世界上，拥有自己独立的王国，自由自在，不受打扰，不受侵犯。

小组成立之后，第一次聚会上，Jude Milhon 惊呼：“你们就是一群密码朋克呀。” Jude Milhon 是个女孩，她是活跃的女权分子，也是一名黑客，后创办了密码朋克杂志 Mondo 2000。她提出过一个口号： “女孩也需要调制解调器”，真是新时代的 “不爱红妆爱武装”。

从此，小组的名字就叫 “密码朋克小组”， 他们也自称密码朋克。

1993 年 Eric Hughes 为小组起草的 “密码朋克宣言” 是密码朋克们的行动纲领。Eric 在宣言中声称 “在互联网时代，一个开放的社会需要隐私；我们不能指望政府、企业或者其他冷冰冰的大组织赐我们以隐私权；我们必须自行护卫自己的隐私；我们自己会写代码，我们要写出软件来！”

之后，他们搞了个邮件组，通过电子邮件讨论各种问题，主题涉猎极其广泛，包括数学、密码学、计算机、政治、哲学，还会有一些个人之间的争论。当时流行的一些小说作品，也是密码朋克们讨论的热点，例如乔治奥威尔的 《1984》，John Brunner 的 《冲击波骑手》，Ayn Rand 的 《阿拉斯加耸耸肩》，还有 Vernor Vinge 的 《真名实姓》，这是他们的最爱。  《真名实姓》 中的大魔头 “邮件人” 假扮成英国的语言风格，并且设计了多层伪装，这个形象无疑是中本聪模仿的对象。

到了 1994 年的时候，邮件组中成员已有 700 多人， 1997 年则达到 2000 人。Eric 设计了一个匿名邮件转发系统，所有密码朋克小组的邮件，都通过服务器进行转发，转发过程就隐藏了邮件发送的地址，实现了不可追踪。

听上去，他们只是一群技术爱好者，有必要搞的这么神神秘秘的么? 大家讨论点密码技术，都得算是有为、有追求的好青年，该发大红花呀，躲躲闪闪藏猫猫干嘛？ 情况并非如此简单，实际上，他们这个小组，是在法律的边缘游走和试探。

在 90 年代之前，密码学一直是美国政府手中的武器，美国政府以国家安全、防范犯罪为名义，牢牢的控制着先进的密码技术。美国政府不允许密码技术出口，限制民用密钥的强度，甚至立法授权政府部门随时可以对任何民用密文进行解密。针锋相对的，美国出现了不少民间的团体，对抗政府，要求公民的隐私权。密码朋克的一干兄弟们，之后就扛起了反抗的大旗。

实际上，这一波保护公民隐私的浪潮，其发端还要更早。1985 年，密码学家乔姆的文章 《非实名的安全：打倒老大哥的交易系统》，就已经提出了匿名的现金系统及商誉系统的概念。乔姆发明的各种系统，包括电子货币，以及加密通讯工具，都是为了保护个人隐私。

1990 年 John Perry Barlow 建立电子前沿基金会，宣布互联网是一个独立世界，不受任何政治力量的管辖。 John Gilmore 也是密码朋克的创始人之一。 这个基金会，为网络隐私诉讼、关涉隐私保护技术的官司提供民间资金支持。

密码朋克与密码邮件组，将这一波浪潮推高到社会运动的层面。现在回头看去，这个邮件组真是星光璀璨。当年他们在一起，只是出于兴趣、爱好以及共同的价值观，也许他们并未想到，他们中的很多人，已经影响了历史的进程。20 年过去，当我们看到这些名字，依然会生神往之心，当年的密码朋克邮件组该是怎样的盛况啊。

对密码朋克邮件组中一些重要的人物简做说明，以彰彼时之辉煌。

Tim·C·May 是密码朋克的发起人，他也是 intel 的高级科学家，在 Intel 公司为芯片技术解决了 alpha 粒子问题。 他有一篇著名的 “密码无政府主义者宣言”。在文中他提出，密码学将对社会和经济的各个方面造成巨大变革。他算是戴维、尼克·萨博眼中的 “带头大哥”。

Eric Hughes 是美国的数学家，也是一位程序员。他起草了著名的 “密码朋克宣言”。人们一向将他与梅并列，是密码朋克小组的两个创始人之一。

John Gilmore 不仅参与创建了密码朋克，还创建了电子前沿基金会。他在开源软件领域贡献甚大，他发起了 Cygnus Solutions 公司，为开源软件提供支持，后该公司并入红帽软件。 他也是 GNU 的主要成员。他参与制定了 DHCP 协议。他是 SUN 公司的第五位员工。

Jacob Applebaum 是个神奇的家伙，他的职业真是要一个很大的数组才能记录清楚。 他是新闻记者、计算机安全专家、艺术家、社会活动家、黑客。人们肯定会好奇，他该如何分配自己的时间。他还是 Tor 洋葱网络的创始人之一，也一度对外代表维基解密。 多年来，美国执法部门一直盯着他，他是某些部门眼中的犯罪嫌疑人。

Julian Assange 是 “维基解密” 的创始人，也是全球知名黑客。他在密码朋克中影响巨大。在计算机领域，他的成就包括开发 TCP 端口扫描器 strobe.c，参与开发 PostgreSQL，开发 NNTPCache，开发 “否定加密法”。阿桑奇因为维基解密这个事业，而受到多国指控。

Adam Back 是 “哈希现金” 的发明者，也是中本聪最早通过邮件联系的人。是他让中本聪去接触戴维。 现在他创立的公司 Blockstream，致力于开发侧链技术，也近乎将比特币开发的权力控制在手。

Bram Cohen 美国程序员， BitTorrent 协议发明人。

Tim BernersLee 英国牛津大学的教授、计算机科学家、工程师。 他发明了 “world wide web ” 万维网。1989 年他提出了万维网的概念，并成功通过 HTTP 协议实现计算机之间的通讯。

哈尔·芬尼是美国密码学家、工程师。他是 PGP 早期的主程序员，后发明了 RPOW，也是中本聪最早的支持者，第一个运行了比特币客户端。

Tim Hudson 是 OpenSSL 的发明人。而 OpenSSL 可称之为互联网的血液，比特币中也应用的 OpenSSL。

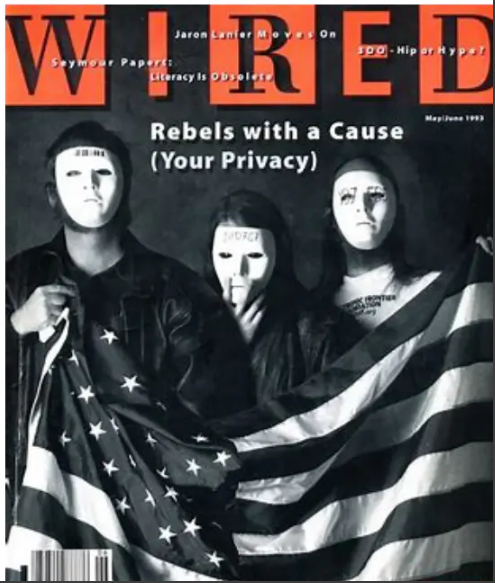
Matt Blaze，贝尔实验室的科学家，破解了美国政府用来监控通讯的芯片 Clipper Chip。

Nick Sazbo 是美国律师、法律学者、密码学者、计算机科学家。尼克提出了 “智能合约” 概念，影响了区块链的技术架构。他在 1998 年的文章中提出了 “比特黄金”，可称之为比特币的思想蓝本。

当然，还包括比特币的发明者：中本聪。

据 John Gilmore 的统计，从 1996 至 1999 约 800 天里，这个邮件组共计处理了 24,575 封消息。 每天大约 30 封。

1993 年，知名 IT 杂志 Wired （连线）在封面报道了 Eric Hughes, Tim May, John Gilmore 三位小伙伴。在封面上，他们三位举着美国国旗，脸上遮盖着白色的塑料面具。密码朋克的形象从此定格，并走进大众视线。



“密码朋克宣言” 中声称 “密码朋克以写代码为使命”，这个稍微有点涉嫌虚假宣传。小组中人并非个个都会写代码， 实际上，仅有十分之一的密码朋克能够开发代码，能够做密码技术相关的开发则更少，仅只 5%。

密码朋克小组中研究开发的技术包括邮件匿名转发系统、PGP、电子货币，以及各种算法。

朋克的精神核心是反抗，密码朋克们反抗的方式并非仅有技术，他们挺身而出，与美国当局进行了多次正面冲突，那些冲突虽称不上 “你死我活”，毕竟大部分都是在法律框架之内的斗争，但形容为刀光剑影则并不为过。

1994年，“密码朋克” 成员 Phil Karn （贝尔实验室研究员）起诉美国国务院。起因是关于  Bruce Schneier 的一本书 “应用密码学”。 美国国务院法令认为，书的出口是合法的，这没问题，但若是你将书中的代码写到磁盘里，未经许可送出国外，那就是违法了。Phil Karn 就觉得，这太过无厘头了，脑子进水了吧。 这场官司打了好多年，最后不了了之，法院连判决都未给出来。 到了 2000 年，美国已经实质上废除了密码学代码出口的所有相关禁令。

1995 年一个世纪大诉讼开始了，人们称之为 Bernstein v. US。 Daniel Bernstein 是加利福尼亚州大学伯克利分校学生，他开发了一套名叫 Snuffle 的加密系统，准备发表论文并公布源代码。然而美国的法律不允许他公开源代码，由此一场世纪大案拉开了序幕。  EFF 作为 Bernstein 的代理人出现，另有 7 位大律师主动为 Bernstein 辩护。 经过 4 年的漫长诉讼，最终，第九巡回上诉法庭判决，软件源代码也是一种言论，受宪法第一修正案的保护，美国政府不许代码公开的法令是违宪的。Bernstein 大获全胜。

1996 年，密码朋克成员  Peter Junger，诉美国商务部。Peter Junger 是 Case Western Reserve 大学的教授，他开了一堂关于计算机法律的课，由于美国商务部关于密码技术出口的禁令，他的课堂不能接纳非美国公民。经历了漫长的诉讼过程，在 Bernstein v. US 案胜诉之后，第六巡回法庭也宣布密码技术源代码受第一修正案的保护。从此，外国的留学生可以在美国的课堂公开学习密码学技术。

这些诉讼，影响深远，对美国乃至全球科技界的发展，都可称得上至关重要。从此，密码学技术，再也不是美国政府和军队的禁脔，开始在民间跨越国界，广泛传播。

学术研究、技术研发、诉诸社会活动和法律武器的诉讼，都为密码朋克们取得了理想中的成果。 在保护个人隐私这个使命上，他们成功了。

然而密码朋克们毕竟是理想主义者，他们的一些行动都是出于热血与激情，结果也就容易谬之千里。

James Dalton Bell 也许是最难缠的密码朋克。1996 年他发表了一篇论文，用非对称加密技术设计了一套匿名电商系统，用来投标招募杀手，执行谋杀政客的任务。在这件事上，作为一名密码朋克，他走的有点远了。 以 Tim May 为领袖的密码朋克们，只是要将现实世界的言论自由、隐私自由，通过密码技术搬到网络世界。 而  James Dalton Bell 则走到了反方向，希冀将网络世界的无限自由，带到现实世界。 美国的执法部门并未对他的论文采取什么行动，但很快，他因为税务问题被捕，在监狱中度过了 1 年，出狱后，他继续纠缠上诉，随之多次被捕，他一共在监狱中度过了 10 年时间。

密码朋克们希望建设一个自由的乌托邦，免于遭受强权对隐私的侵犯。然而，通常来说，这个乌托邦是在网络上，通过密码技术构建起来的。 但 Ryan Lackey 却走的更远。他在英国费利克斯托港口 7 英里的大海上，找到了一个人造小岛，那是在二战期间建设的防空平台，离洋面 60 英尺，共有 550 平方米。 平台早已废弃，锈迹斑斑。  Ryan Lackey 在这个平台上建设了一个机房，幻想这就是一个没有强权，没有法律的世外桃源。 他在乌托邦里呆了 2 年，最终因为缺乏资金，缺乏贷款，也没有业务，而不得不终止这个项目。

正如《真名实姓》中所描写的情节，当 “滑头先生” 控制了全球的网络与计算机，如上帝般拥有了绝对权力，却通过计算模拟发现，也许自己的统治将比现有的权力更恶劣。他的伙伴埃莉所说：“到头来咱俩还不如人类组成的现存政府。 这些事你下不了手，我也一样。” 现实中也一样，密码朋克小组的大部分成员，都是正直善良的技术狂人。

密码朋克们抗争的社会活动，为世人争取权利，让人们在网络时代能够享有隐私权。他们所创造的技术，保护着我们，在网络上为我们构筑了安全的家园。当比特币系统在密码朋克小组出现的时候，这个家园发展到了令人炫目的程度。

# 区块链的故事-区块链

2008 年 11 月 1 日，一个网名叫做中本聪的人，在密码邮件小组中，发了一个邮件。邮件中声称他设计了一种基于点对点的现金系统，叫比特币。在邮件中他给出了比特币论文的地址。然而比特币论文中，并没有区块链一词，只有单独的 “区块” 与 “链” 频繁出现。

过了年，2009 年 1 月 9 日，这个叫中本聪的人，在密码邮件小组里，发布了比特币 0.1 版本。这个基于 C++ 的程序，在 Windows 上可以运行，并在磁盘上创建了一个叫 Blockchain 的目录。由此，人们称比特币所用的技术为 “区块链”。

比特币所用的技术非常繁杂，涉及了众多密码学技术、计算机技术、数学算法，很难找到一个合适的词来恰当定义它。 区块链只是它交易记录的数据结构，并非其核心的本质，但区块链这个词，指代物体的形状，非常形象，画面感强，也就流行下来了。也有人意图另起一词，但难以取代区块链。

如果按照比特币中所涵盖的技术特性来描述，也可以将其中的技术系列称之为 “共识账本” 来突出它共识机制与记账功能； 还可以将其称之为 “P2P 交易” 以描述其功用； 还可以称之为 “POW” 以说明它解决双花问题的思路；还可以称之为 “公信链” 以彰显其实现网络信任的特性； 总之，都是描述了其技术特性的一个方面。

比特币按照中本聪论文标题所述，是一种点对点的电子现金系统，P2P 点对点可以是其技术的精髓，而中本聪在邮件中，则称这种货币在去中心化体系下，无需中心服务器，也无需对第三方的信任，便可自行运转。 那么完全可以将 “去中心化” 视为其技术的核心。我们由此可以定义区块链为 “去中心化” 的系列技术。

比特币是区块链技术的来源，但区块链技术系列并非发源自比特币，而是有着悠久的历史。 比特币乃是各种密码学、计算机算法、去中心化技术的集大成者。

比特币从本质上，近乎完美的达成了一个伟大的使命： 让价值在计算机、网络这个数字世界中自由的流动。换成通俗的话来解释，就是它实现了两个目标：

你所拥有的数字货币，可以随意在网络上存储和传播，除了你，别人花不了它

你所拥有的数字货币，你无法任意复制，无法双花，也就是无法支付给多人

从此，在一个去中心化的数字世界中，价值有了容身之地。

换个角度来说，在计算机网络上，人们实现了黄金、纸钞、纸质合同的商业模式。在黄金和纸钞的时代中，人们将黄金和纸钞存在家中，交易的时候，是 “人-人” 的模式。 而到了计算机银行联网时代，人们的货币是存在银行中的，交易的时候，是 “人 - 银行 - 人”的模式。而区块链时代的到来，人们在数字世界中，再次回归 “人-人” 模式。

从此，在互联网的数字世界中，每个组织、乃至每个个体，都可以构建自己的价值王国。

**交易-区块-链**

我们每天都要与钱，也就是货币打交道。我们拥有货币，以及使用货币的方式，发生了翻天覆地的变化，但我们大多数人却习以为常，并无知觉。

在货币漫长的历史上，一直到几十年前，计算机与网络流行之前，人们习惯于实物货币。 货币要么以金、银、铜等贵金属的各种形态呈现，要么就是国家印刷的纸钞。实物货币有几个特点：

人们持有货币，就是持有货币实物。古代的金银铜要用钱箱保存，大财主还要挖地窖。 纸币则用钱包与保险柜保存。

交易的过程，就是货币实物转移的过程。不管是递过去几个铜钱，还是从钱包里抽一张100元人民币，都是货币实物的交接。

实物货币的发行主体大多是主权国家，但货币在民间的流通是自由自在的。一张 100 元人民币，可以经过张三、李四、王五等无数人。

用实物货币进行支付，是没有数据记录的。张三在小商店中支付 100 给李四，李四并不认识张三，也不需要留下张三的身份证信息。

在计算机和网络流行之后，数字技术统治了人们的生活。支付开始依赖 ATM、信用卡、网络银行、手机 App 等电子方式。电子支付的便捷性深受人们喜爱，很快便主宰了市场。电子支付有如下特点：

人们不再持有实体货币，人们拥有的货币，体现为银行数据库中一个账户上的余额。

支付的过程，只是账户余额的增减。张三支付李四 100 元，则张三银行账户余额减少 100 元，李四账户增加 100元。

人们之间的支付过程，完全依赖银行系统。而银行间的结算，则依赖更高的机构，比如央行或者 VISA 组织。

所有的支付行为，都有数据记录。不论是刷信用卡，还是网银支付，消费记录近乎透明的勾勒出消费者的全部生活。

这是一个深刻的变化，人们获得了电子支付的便捷，却也牺牲了很多权利。 所持有的货币，全部托付给银行，给了银行巨大的作恶空间，为了防范与约束银行，政府制订了汗牛充栋的监管法规。 再有，人们的交易隐私，彻底丧失，在银行面前，消费者是透明的。

这种牺牲，是受限于技术的无奈之举。人们只能在权衡利弊后，宁愿牺牲隐私，牺牲对货币的控制权，来换得支付的便捷性。因为，依靠过去的技术，人们并不知道，如何在数字网络世界中，实现个人对货币的控制权，实现个人隐私的保护。

比特币的诞生，解决了这个难题。 比特币，在数字世界中，让个体消费者不再依赖银行，不必将货币委托给银行，也再无必要去担心交易过程中会暴露隐私。

当人们称比特币为虚拟货币的时候，在概念上有颠倒黑白之嫌。比之银行的余额制，比特币这样的数字货币，具有浓厚的实体货币的实在性。 什么样的货币才是百分百的虚拟？ 当然应该是银行的余额制货币。

比特币所构造的模型，迥异于传统银行的余额制，也不同于古老的金银铸币和纸钞。它创造性的用交易记录为货币的载体。

比特币系统中，并不存在单独的 “比特币”，比特币是以交易记录的形式存在的。 例如张三支付李四 1 个比特币，则系统中记录一条交易记录；

张三 支付 李四 1

区块则是将多笔交易数据打包在一起，形成的数据体。可以理解区块为一个账本，账本里记录了多笔交易。

单笔交易的字节数，最基本的大小为 250 B，当然实际发生的交易，会大于这个数值。

一个区块大小被中本聪限定最大为 1 M，那么我们就可以算出来，一个区块最多可以容纳 1048576/250 = 4194 笔交易。

还是以账本做比喻，中本聪限定了一个账本最多只有 1024 页。而一个最基本的交易要占用四分之一页。那么一个账本最多就是 4194 笔交易。

据统计，最大的一个区块，发生在 2015 年 7 月 1日，高度为 363270 的区块，共录入了 4509 笔交易，大小恰好是 1 M。

每本账本记满了交易后，记账人就在账本封面上，贴上时间封条，盖上自己的印章。 最重要的一个步骤是，在账本上记录前一个账本的编号，这样账本之间就构成了一个首尾相连的账本链条。

这样构成的账本链条，有一个特点，越老的账本，其中的交易越难以篡改。若要更改 2015 年高度为 363270 中的一笔交易，那么就要将 2015 年该账本之后的所有账本，全数改掉，重新记账才可做到。

而禁止篡改历史记录的目的，是为了防止双花，也就是防止把同一笔钱，两次支付到不同的地址。

# 区块链的故事-UTXO

比特币是一种货币，但这个系统中并不存在一枚金光闪闪的 “币”。 中本聪在设计的时候，让比特币以交易记录的形式出现。你并非拥有一个比特币，而是拥有别人转给你比特币的一笔记录。这个记录叫做 UTXO （Unspent Transaction Output - 未花费的输出）。

听起来拗口，但说穿了，和古老的现金模式在本质上有相似之处。你打开你的钱包，发现里面有 1 张 100 元，2 张 50 元， 1 张 10 元，这些钞票就是你的 UTXO （Unspent Transaction Output - 未花费的输出）。如果你想知道自己一共有多少钱，并没有一个余额表给你查看，你需要将钞票从钱包里拿出来，一五一十的点清楚。 如果你要付钱给别人，也是在钱包中的 UTXO 钞票挑出一张交给别人。

我们被银行的余额制荼毒太久，脑袋中的思维极易被余额制所固化。

但比特币的 UTXO 比黄金、纸钞等实物货币，更进了一步。它抛弃了类似纸钞这样的独立实体，而是用交易记录来体现货币。

让我们设想一个故事，1000 人乘飞机降落到了无人荒岛，建设了一个与世隔绝的社会。 他们耕种、打猎、纺织，开展各种经济活动，并且建设了自由市场，开展贸易。但荒岛上没有印钞机，也没有黄金，用什么做货币呢？难道真用贝壳做货币？可是这荒岛上那贝壳真是遍地都是，不具备稀缺性

其中有一位叫中本聪的聪明人，他深思熟虑之后，提了一个建议。干脆我们不用实物做货币，改用记账的方式来表征货币。 比如，Alice 要买 Bob 的大麦 100 斤，Bob 标价 10 美元，他们来到荒岛之前都用美元，所以现在也沿用美元计价。 那么 Alice 支付 Bob 10 美元。记录在纸上为：

Alice  支付  Bob 10 美元 20170909

Bob 收到这张纸条记录，这就是 Bob 的一张 UTXO。 Bob 在需要支付其他人，比如 Eva 款项的时 候，就可以用这张 UTXO 记录去支付，这笔交易可以呈现为：

在 90011 这笔交易中，Bob 支付 Eva 10 美元，记录在交易信息的右边。 Bob 为了支付这 10 美元，从自己的 UTXO 库中，找到了 Alice 支付他的这笔收入，假设交易编号为 90000。 Bob 用这笔收入的 UTXO 作为支付 Eva 10 美元的输入。

而 Bob 支付 Eva 的 10 美元，在交易记录到达 Eva 后，便成为了 Eva 的 UTXO。

在复杂的交易中， 比如 Eva 需要支付 12 美元到不同的人，她从 UTXO 记录中，找到了两条记录，分别是 10 美元和 3 美元。 Eva 用这两笔 UTXO 共计 13 美元，支付给 TOM、Jason 和 Alice 共 12 美元。但还多余的 1 美元怎么处理？ 在比特币系统中，没有对方找零这么一说的。 解决方法是 Eva  在交易中构造一个输出给自己支付 1 美元。交易的信息如下：

所以，一笔交易的输出，就会形成收款方的 UTXO，而收款方使用 UTXO 支付的时候，这个输出将 成为新交易中的输入。

作者：灯下鼠  
链接：https://www.jianshu.com/p/05bc8c9fdb59  
来源：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。