密码学历史及近 40 年人物技术里程碑(公号回复“密码学”下载 PDF 资料，欢迎转发、赞赏、支持科普)

秦陇纪

简介：密码学历史及近 40 年人物技术里程碑。(公号回复“密码学”，文末“阅读原文”可下载 31 图 17k 字 19 页 PDF 资料，欢迎转发、赞赏支持科普。)蓝色链接“科学 Sciences”**关注**后下方菜单项有文章分类页。**作者**：秦陇纪。**来源**：参考古千峰等文章，数据简化社区秦陇纪微信群聊公众号，引文出处附参考文献。**主编译者**：秦陇纪，数据简化、科学 Sciences、知识简化新媒体创立者，数据简化社区创始人 OS 架构师/C/Java/Python/Prolog 程序员，IT 教师。每天大量中英文阅读/设计开发调试/文章汇译编简化，时间精力人力有限，欢迎转发/赞赏/加入支持社区。**版权声明**：科普文章仅供学习研究，公开资料©版权归原作者，请勿用于商业非法目的。秦陇纪 2018 数据简化 DataSimp 综合汇译编，投稿合作、转载授权、侵权错误(包括原文错误)等请联系 DataSimp@126.com 沟通。**欢迎转发**：“数据简化 DataSimp、科学 Sciences、知识简化”新媒体聚集**专业领域一线研究员**：研究技术时也传播知识、专业视角解释和普及科学现象和原理，展现自然社会生活之科学面。秦陇纪发起期待您参与各领域~ 强烈谴责超市银行、学校医院、政府公司肆意收集、滥用、倒卖公民姓名、身份证号手机号、单位家庭住址、生物信息等隐私数据！

目录

密码学历史及近 40 年人物技术里程碑(13926 字)

科学 Sciences 导读：密码学是研究保密通信的一门科学——不安全环境中，如何把所要传输的信息发给接收者之前进行秘密转换，以防止第三者对信息的窃取。从凯撒的字母替换，二战时期德英、美日间情报较量，非对称公私钥，RSA 算法，时间戳，哈希现金，到时下流行的比特协议、比特币，关于秘密通信的历史，精彩无比。有人设计密码，有人破译密码，在这场智与智的较量中，产生无数经典。本文是零起点科普，我们先了解若干最经典的密码，一起感受密码学里的艺术；然后在 B 部分继续了解近 40 年来密码学人物和技术里程碑。

信息时代，密码无处不在。生活中我们经常会用到各种**口令(password)**，如银行取款、保险柜、电脑登陆、邮箱、QQ、微博等用到的(不是真正意义上的密码)。后来口令做了变换，需要解密才能使用，出现了**密码**。比如，网络信息的加解密传输、应用，时下流行各种比特币类技术，没有密码

学技术和探索，就不会有**比特币**和**区块链**。但如果研究区块链技术只从比特币开始未免太局限，比特币之前的知识图谱、密码学，才是比特币时代先行者与科学家们理解区块链技术的关键所在。

密码学是研究保密通信的一门科学，研究在不安全的环境中，如何把所要传输的信息发给接收者之前进行秘密转换以防止第三者对信息的窃取。各种密码技术也随处可见，为**密码学者**们津津乐道。此前很长一段时间，密码学作为一门行走在暗处的黑色艺术，一直不为大众所知，只在少数专业者间流传。从凯撒的字母替换，二战时期德英、美日间情报较量，非对称公私钥，RSA 算法，时间戳，哈希现金，到时下流行的比特协议、比特币，关于秘密通信的历史，精彩无比。有人设计密码，就有人破译密码，在这场智与智的较量中，产生无数经典。让我们先了解几个最经典的密码，一起感受密码学里的艺术；然后在 B 部分继续了解近 40 年来密码学人物和技术里程碑。

A 从艺术到科学——密码学发展历程(5750 字)

从艺术到科学——密码学的发展历程

文|秦陇纪，源|中科院物理所 2017-09-07 等，科学 Sciences20181107Wed

密码学包括**密码编码学**和**密码分析学**，这两个分支形成既对立又统一的矛盾体，安全的密码机制促使更强大的分析方法的发展，而强大的分析方法又强迫更加安全的密码机制的诞生，二者在相互斗争中共同进步，所以说密码学的发展史汇聚了人类文明的聪明才智。

讨论加密问题时需要基于一个通信模型，假设通信双方 Aaron 和 Bob 通过一个不安全信道进行通信，攻击者 Carson 窃听他们间的交流，这种窃听总是防不胜防。所以 Aaron 和 Bob 需要将他们之间交流的消息处理成只有他们自己看得懂的“文字”，让 Carson 眼中只能看到一堆乱码。

在**古典密码学**中，主要使用替换的手段进行加密，最早的加密算法可以追溯到古罗马时期的**凯撒大帝**使用的凯撒密码和**武王**伐纣时的阴符阴书。

BC60 年，凯撒密码 Caesar cipher

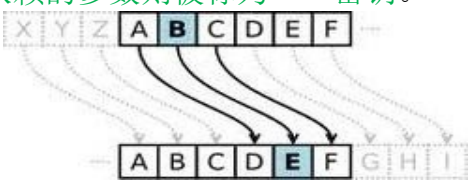
约公元前 60 年罗马共和时期，**尤里乌斯•凯撒**被森图利亚大会选举为罗马共和国的执政官。作为一名杰出军事领袖，**恺撒**深知指挥官对前方将领的命令对于一场战争的重要性，这些信息绝对不能让敌方知道，于是他设计了一种对重要军事信息进行加密的方法，即使这些信息被截获，敌方也不一定能看懂——这就是著名的**凯撒密码**，也算是最早的密码实例。他用此加密方法与将军们进行联系，又称恺撒加密、恺撒变换、变换加密。凯撒密码是一种单表替换加密技术，**明文**中的所有字母都在字母表上向后(或向前)移动若干位，下例是向后移动 3 位得到**密文**：

明文：goodgoodstudydaydayup

密钥：3

密文：jrrgjrrgvwxgbgdbgdbxs

这种密码中，字母表中 A 到 W 每个字母在加密时用该字母后面第三位那个字母代替，字母 XYZ 分别被替换成 ABC。凯撒在这里是将字母向右移动了三位(如下图)。比如，在三个移位的情况下，信息 DOG(这种需要加密的信息统称“明文”)就变换成 GRJ(这种经加密后产生的的信息统称“密文”)；密文 FDW 对应的明文则是 CAT。可以看到，加密、解密过程都是以字母移位的位数为参照的。这种在加密和解密的算法中依赖的参数则被称为——密钥。



移位个数的选择并非限制在三位，从1到25任何数的移位都能产生类似效果。只要通信双方事先约定好，这个选择就很任意。很明显的是，移位方法最多是25种，这成为凯撒密码的致命弱点。穷举25种移位方法，得到25组新编码，必有一种编码是真实情报内容，由于其它24组多是是毫无意义的字母组合，所以凯撒密码很容易就能被破译。

凯撒在当时成功地使用了这种密码，还在《高卢战记》中颇为得意的记录下了这个加密设计，他的敌人并没有意识到他在使用密码，也就没有识破这种古典加密手段。

改进后的移位加密法

凯撒密码缺点暴露后，有人对它做出改进：用**随机顺序排列的字母表**，替代正常顺序的字母表。这种简单代换方法达26!种，这个看起来不大的数字，数量级达到了10^{26}，也就是说穷举法破译已经失效了。但是，这种方法并非无懈可击，当它对一段比较长的英文信息加密时，依然容易被破译。这是英语本身的统计特性决定的。

众所周知，英语单词中字母的出现次数具有**统计特性**。每个字母的使用频率不同且差别很大。一篇文章中字母出现的相对预期频率可以通过统计大量英语文章确定出来的。比如，英语文章中**E**的出现频率最高，大约是12.7%；而**J**的出现频率最低，只有0.1%左右。当使用上述简单代换密码时，字母表中特定字母总是被同一个字母代替，导致密文中字母出现的频率也会出现同样的不平衡性，再加上破译者对发密方背景的了解，要确定密文中包含的信息依然不是一件困难的事。

一个好的解决办法是用多个密文符号来表示同一个字母。每个字母有不同数量的的密文符号替代，替代者的数量与每个字母在英语统计中的频率成正比。例如，字母a在书面英语大约占8%的比例，所以我们可以分配8个符号来表示它。明文中出现的字母a在密文中可以被这8个符号中任一个替换。这样一来，每个符号在密文中的频率都在1%左右。类似处理所有英文字母。这样设计出的一套字母替换表，打乱了密文中的英语统计特性。但由于每个密文符号只代表唯一的明文符号，也会带来风险：对于一个给定的密钥，破译者能汇编出一部已知的明文与密文相对应的词典。

好几个世纪以来，上述的几种加密法保证了信息的安全。不过自从频度分析这种方法被引进到欧洲后，密码破译者终于占据了上风。苏格兰**玛丽女王**的悲剧充分诠释了这种密码的弱点。

1586 年，“不可破译”的密码

1586年，英国政府破译了苏格兰**玛丽**女王和同党谋反的密信，玛丽女王惨遭吊死。而她使用的就是字母替换这种单码加密法。这个事件也正式宣告上述密码已经全部失效。[1]

同年，一位名叫**维热纳尔**的法国外交家出版了一本《密码理论》，介绍一种以他自己名字命名的新密码，而这本书一直无人问津。直到两百年后莫尔斯电码流行开来，为了防止电报员泄露信息和间谍窥探秘密，维热纳尔密码才被广泛应用。

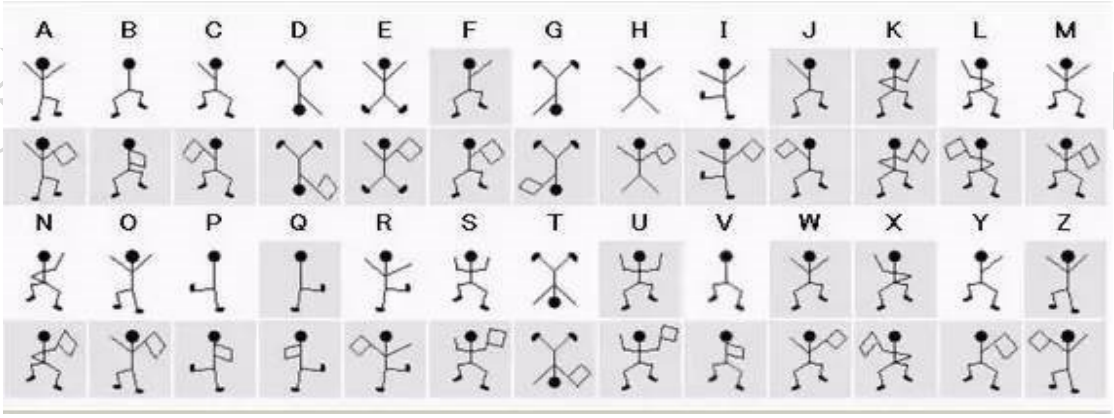
维热纳尔密码一度被认为是无法破译的，以致让一些掌握这种密码的人洋洋自喜，不过很快，以建立了现代计算机的理论框架而闻名于世的怪才**查尔斯•巴贝奇**解决了这个难题。

事情起源于一个布里斯托尔的一个牙医**赛瓦特**。这个牙医其实对密码学知之甚少，1854年，他声称发明了一种新密码，并写信给《艺术协会杂志》企图获取专利。而他只不过是将**维热纳尔密码**重新包装了而已。**巴贝奇**写信揭露这个事实，赛维特却不愿承认，甚至为难巴贝奇让他破解这个密码。其实能否破解密码和密码是不是新创造的毫无关系，但这已足以激起巴贝奇的好奇心了。很快，他就成功破解了维热纳尔密码。

对于这样重要的成果，巴贝奇却没有发表它。这也符合他的性格：他一直是这种懒洋洋的态度。而更重要的原因恐怕是英国政府要求巴贝奇保密，从而让他们可以在这方面领先全世界9年——直到1863年**卡西斯基**也发现了破译方法并将它发表。有趣的是，在美国的南北战争期间，南方联军仍然在使用黄铜密码盘生成维热纳尔密码，自始至终都只主要使用三个密钥，而那个时候这密码早就被破译了，所以**北方政府**在情报战上一直是笑而不语的。

维热纳尔密码的原理

稍微复杂些的还有多表替换的**维吉尼亚密码码**，又叫做维热纳尔密。这种替换加密虽然乍看之下混乱无序，但通过统计手段就能恢复出密钥，比如统计密文字母的频率，并与自然语言中各个字母出现的频率相对比，从而揭示隐藏在乱序密文后面的加密规律。福尔摩斯探案集中的《跳舞的小人》章，介绍了用简单小人图案来代替英文字母，福尔摩斯破译的方法就是频率分析法。

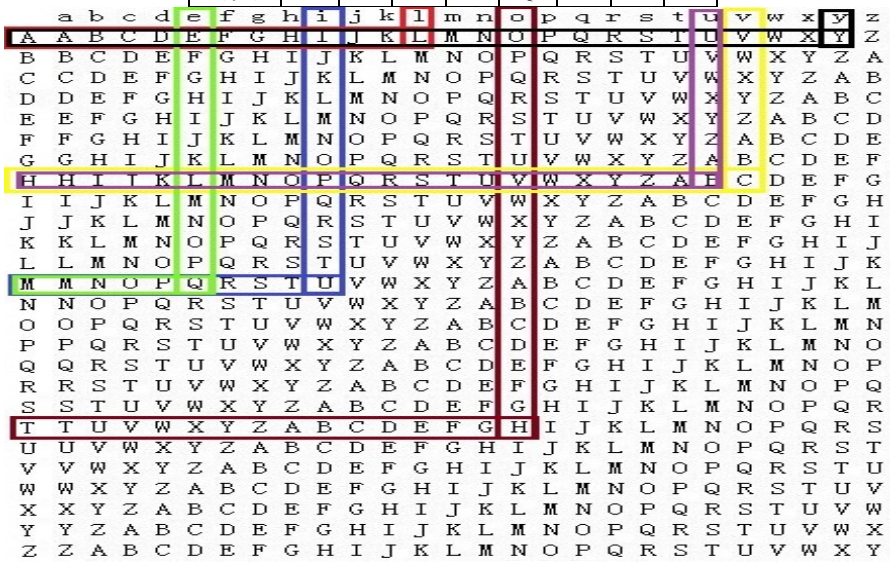


下面我们来对密码机制给出一个严格的定义，一个密码机制是由以下五部分组成[2]：

1. 明文空间 P：所有可能的明文组成的有限集；
2. 密文空间 C：所有可能的密文组成的有限集；
3. 密钥空间 K：所有可能的密钥组成的有限集；
4. 加密法则 E；
5. 解密法则 D；对任意的密钥 k，都存在一个加密法则 ek 和相应的解密法则 dk，且对任意明文 x，均有 dk(ek(x))=x。

维热纳尔密码的加密过程是这样的：首先选择一个无重复字母的**密钥词**(比如MATH)，重复密钥词直至它成为一个和明文信息一样长的字母序列，再利用下面这种方阵加密这条信息。为加密第一个字母I，此时它下方对应的**密钥词**是M，于是，加密I时由M对应的那行中读出i列下的字母即U，类似地，得出所有**密文**：

信息	I	L	O	V	E	Y	O	U
密钥	M	A	T	H	M	A	T	H
密文	U	L	H	C	Q	Y	H	B



这无疑是一种高明的加密手段，维热纳尔密码用严格的轮换方式重复使用一串简单的代换密码，很好的伪装了基础语言中的字母频率。它还有很多变化，比如有一种可以允许密钥词中出现重复字母。每种变化都会产生一些新的特征，从而引发破译方式的变化。[2]

查尔斯•巴贝奇是破译维热纳尔密码的第一人，他的思路是：在已知**密码周期**(即所使用的密码组件数目，显然，上述版本的维热纳尔密码周期就是密钥词长度)为p的情况下，将密文改写成p行，使得每一列按原来的密文顺序排列，例如，p=3，密文c1c2c3c4c5c6c7c8c9…就排列成：

c1 c4 c7…
c2 c5 c8…
c3 c6 c9…

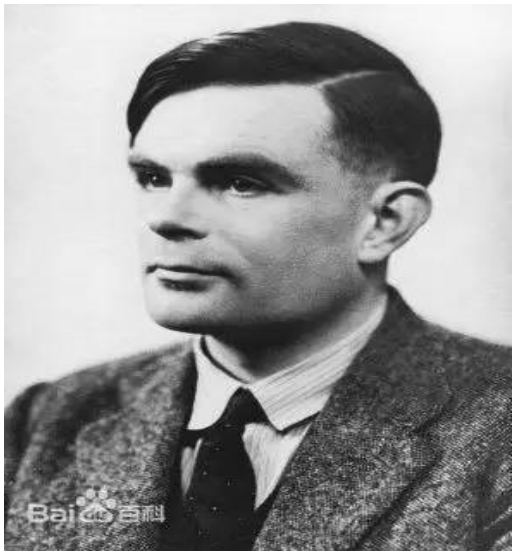
这样排列后，每行都是使用同一简单代换密码所得出的，如此就可以对每一行都使用上一节提到过的统计分析了。事实上，对每一行而言，这种简单的代换密码正是凯撒密码。

所以，对于维热纳尔密码的破译者来说，关键就在于确定周期p，巴贝奇则用了一种精巧的方法：在密文中搜索重复的字符串，它意味着两个重复模式之间的距离可能等于周期的整数倍！

难题又被破解！密码编译者需要再次寻找新方法，继续这场智的较量。

19 世纪，公开密码机制

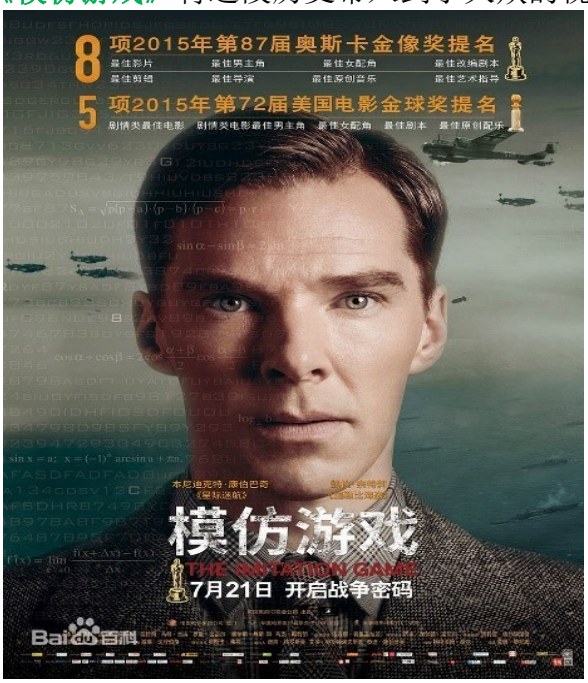
如何保证一个密码机制的安全性呢？一般认为不让别人知道明文是以何种方式加密的就行了，也就是说将加密算法保密。但这个方法并不可靠，因为加密算法的种类毕竟是有限的，穷举起来不是没有可能。一旦知道了是用何种算法进行加密，破解也就是分分钟的事儿。因此，19 世纪荷兰语言学家和密码学家**奥古斯特·柯克霍夫**提出：密码机制的安全性不依赖于算法的保密性，密码系统应该就算被所有人知道系统的运作步骤，只要密钥不泄露，就仍然是安全的。公开加密算法相当于让所有人都能来分析破译，对算法本身的安全性提出了更高的要求，而一旦攻击成功，结果一般会公开发表，算法的使用者能及时做出调整，避免更大的损失。现在大多数民用保密都使用公开的算法，但用于政府或军事机密的加密算法通常仍是保密。



图灵

密码学与战争

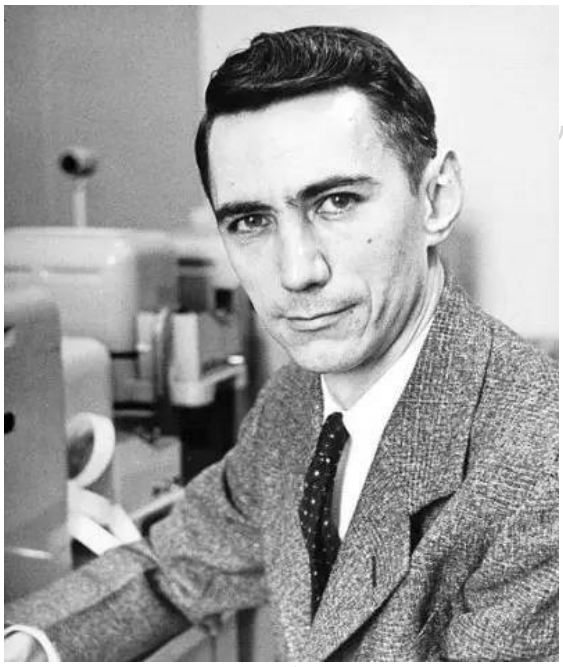
对密码学需求最高的莫过于军事领域，在战争中信息最为宝贵，一条简短消息的泄露可能会决定一场战争的输赢和成千上万条性命，第二次世界大战的时候正是**波兰**和**英国**密码学家破译了**德军**使用的恩尼格玛(ENIGMA)密码机，才使得战局出现转机，拯救了更多人的生命，其中的代表人物就是**图灵**，2014 年上映的电影《模仿游戏》将这段历史带入到了大众的视野。



模仿游戏

1949 年，从艺术到科学

1949 年，**香农**发表了论文《保密系统的信息理论》[3]，该文提出了混淆(confusion)和扩散(diffusion)两大设计原则，为**对称密码学**(主要研究发送者的加密密钥和接收者的解密密钥相同或容易相互导出的密码体制)建立了理论基础，从此密码学成为一门科学。



香农

对称密码学主要由分组密码和流密码构成，在**分组密码算法**中，明文消息被分成若干个分组，加密和解密都是对这些分组进行操作，而**流密码**则是使用一个密钥流生成器产生一串与消息等长的密钥比特流，再与明文进行异或操作，流密码一次只加密一个比特，与分组密码相比，流密码需要更大的处理能力，所以说流密码更适用于硬件平台实现，分组密码更适用于软件平台实现。经典的分组密码算法有 DES 和 AES，流密码算法有 Trivium 和我国学者自主设计的祖冲之算法(ZUC)。

在分组密码的设计中，充分利用扩散和混淆，可以有效地抵抗对手根据密文的统计特性推测明文或密钥。扩散就是让明文中的每一位影响密文中的许多位，或者说让密文中的每一位受明文中的许多位的影响。这样可以隐蔽明文的统计特性。当然，理想的情况是让明文中的每一位影响密文中的所有位，或者说让密文中的每一位受明文中所有位的影响。比如 AES 中 ShiftRows 部分。混淆就是将密文与密钥之间的统计关系变得尽可能复杂，使得对手即使获取了关于密文的一些统计特性，也无法推测密钥。使用复杂的非线性代替变换可以达到比较好的混淆效果，比如使用多个 S 盒，而简单的线性代替变换得到的混淆效果则不理想，比如凯撒密码。乘积和迭代有助于实现扩散和混淆，当然这个过程应该是可逆的。

1976 年，密码学的新方向——公钥密码学

1976 年，**Whitfield Diffie** 和 **Martin Hellman** 发表了论文《密码学的新方向》[4]，标志着公钥密码学的诞生，他们也因此获得了 2015 年的图灵奖。

公钥密码体制的特点是采用两个相关的密钥将加密与解密操作分开，一个密钥是公开的，称为公钥，用于加密；另一个密钥保密，为用户专有，称为私钥，用于解密。公钥密码与之前的密码学完全不同，因为公钥算法的基础不再是香农提出的代替和置换，而是基于一种特殊的数学函数——单向陷门函数。单向陷门函数的特点是：易计算，但难求逆，即满足以下几点：

1.若 k 和 x 已知，求 y = fk(x)容易计算；
2.若 k 和 y 已知，求 x = fk-1(Y) 容易计算；
3.若 y 已知但 k 未知，则求 x = fk-1 (y)是不可行的。
这里的容易计算是指能在多项式时间内解决，计算上不可行是指计算的时间复杂度是指数级的。

最经典的公钥加密算法莫过于 1978 年由 Rivest，Shamir 和 Adleman 用数论方法构造的 RSA 算法[5]，它是迄今为止理论上最成熟最完善的公钥密码体制，并已得到广泛应用。RSA 算法的安全性可以归约到大整数分解的困难性，即给定两个大素数，将它们相乘很容易，但是给出它们的乘积，再找出它们的因子就很困难。目前为止，世界上尚未有任何可靠的攻击 RSA 算法的手段，只要其密钥长度足够长而且使用方法得当，用 RSA 加密的信息是不能被破解的。这就是为什么 WannaCry 病毒那么令人束手无策。

2017 年，WannaCry 勒索病毒

2017 年 5 月，WannaCry 勒索病毒在全球爆发，中国大陆部分高校学生反映电脑被病毒攻击，文档被恶意加密。勒索病毒肆虐，俨然是一场全球性互联网灾难，给广大电脑用户造成了巨大损失。

最新统计数据显示，100 多个国家和地区超过 10 万台电脑遭到了勒索病毒攻击、感染。[6]

WannaCry 是一种“蠕虫式”勒索病毒软件，它使用 AES-128 和 RSA 加密算法恶意加密用户软件以勒索比特币。AES-128 和 RSA 算法本来是非常优秀的对称加密算法，用于加密通信信息避免被敌手获取，但在坏人手中却被用来恶意加密用户的文件，成了勒索工具。也正是因为 AES-128 和 RSA 的强大的安全性，导致至今除了像亡羊补牢一样修复系统漏洞避免感染之外没有彻底的解决办法。

那么 AES 和 RSA 又是何种利器，竟让全世界都束手无策？要想了解 AES 和 RSA 等更加细致的内容，请接着看 B 部分列举的近 40 年密码学人物、技术里程碑，加深理解什么是加密、密码学。

B 密码学历史及近 40 年人物技术里程碑(7386 字)

我们将要公开发布我们的代码，让密码朋克战友们能够使用软件。我们的代码，对全球所有人免费。如果你们要封杀我们所写的软件，我们也毫不在意。我们清楚，软件是无法被销毁的，彻底的分布式系统永不停机。——《密码朋克宣言》

密码学 40 年丨重要历史与人物

文|古千峰，科学 Sciences20181019Fri

作者：古千峰，美国区块链媒体BTC Media亚太区CTO，前Ripple开发者，分布式商业的理论建立者与实践者，十五年外贸与企业管理经验，高级经济师，区块链讲师。

当代加密学始于Whitfield Diffie与Martin Hellman于1976年发表的《密码学的新方向》，他们在该论文中首次提出了公钥的概念以及通过公私钥方式进行安全通讯的方案。Whitfield Diffie与Martin

Hellman是当代密码学的奠基者，并因对密码学的杰出贡献在2015年获得图灵奖。

10月31日是**中本聪**发表《比特币：一种点对点的电子现金系统》论文10周年，他巧妙组合了当时的各种加密学技术，推出了比特币的设计。到2008年**中本聪**发表论文前30多年时间里，相继诞生RSA加密、椭圆曲线加密、零知识证明、盲签名技术、HTTP协议、BT协议、Kademlia……并出现了各种形式的对数字货币的探索。没有这些技术和探索，不会有比特币和区块链，饮水思源，需要感谢前比特币时代的这些先行者与科学家们。而对于技术工作者，如果研究区块链技术就只从比特币开始的话，未免局限，比特币之前的知识图谱、密码学，才是理解区块链技术的关键所在。

比特币白皮书之前的重要历史与人物

比特币关键技术发展过程：

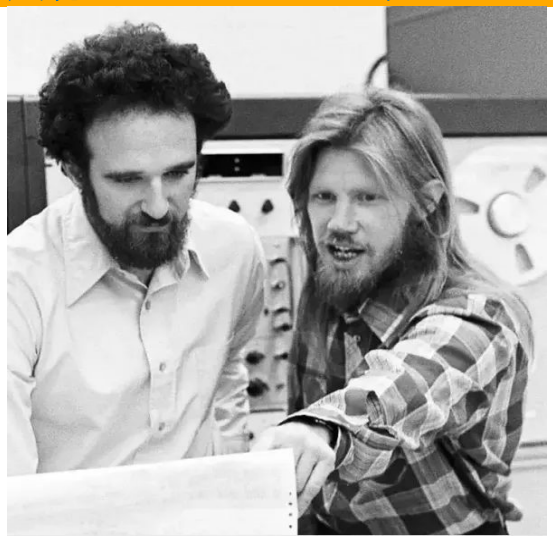
加密：*DH协议—RSA算法—椭圆曲线加密算法*

点对点网络：*Napster—BitTorrent协议— Kademlia*

工作量证明：*哈希现金机制—RPoW—PoW*

数字货币：*eCash—Bmoney—BitGold—比特币*

1976 年，DH 协议，公私钥出现——Whitfield Diffie 与 Martin Hellman



1976年以前，所有的加密都采用对称加密算法(加密和解密使用同样的规则)，这种算法最大的弱点就是必须把加密规则告诉对方，否则无法解密，在这种情况下，如何安全的传递密钥是难以解决的问题。

1976年，Whitfield Diffie与Martin Hellman发表《密码学的新方向》，***他们论文中提出了一种崭新的构思：加密和解密可以使用不同的规则(非对称加密)***，从而在不直接传递密钥的情况下完成解密。

论文中的公钥密码思想和DH(Diffie-Hellman)密钥交换协议在密码学中具有划时代的意义，公私钥的出现成功解决了密钥传递问题，它们是互联网安全协议的基础，也是互联网能够获得如此成功的重要原因。

值得一提的是，该论文还以公钥密码思想为核心，预测了密码学未来的发展方向：利用计算复杂性问题构造单向陷门函数，进一步可以构造公钥密码学，而公钥密码学可以实现加密和认证功能。

1977 年，RSA 算法——Ron Rivest、Adi Shamir 与 Len Adleman

Diffie和Hellman给出了一种协议，表明非对称加密是可行的，但他们并没有提出具体的加密算法。1977年，三位数学家Rivest、Shamir和Adleman完成了这件事，他们设计的RSA算法成功实现了非***对称加密，这标志着公钥密码思想在实际中是可以实现的。***

RSA算法基于一个简单的数论事实：将两个大质数相乘十分容易，但是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作为加密密钥。极大整数做因数分解的难度决定了RSA算法的可靠性，到目前为止，世界上还没有任何可靠的攻击RSA算法的方式。

从诞生之日起，RSA 算法便是最受欢迎的非对称加密算法，只要有计算机网络的地方就有它。2002 年，Rivest、Shamir 和 Adleman 因共同提出了 RSA 算法获得图灵奖。

1982 年，拜占庭将军问题——Leslie Lamport

1982年，Leslie Lampor在论文**《The Byzantine Generals Problem》**中提出了拜占庭将军问题，以拜占庭帝国与周边邻邦的战争故事作为背景，研究如何让各邦将军达成进攻与撤退的共识，解决叛徒的容错性问题，保证信息传递的一致性问题。

拜占庭***将军问题是一种分布式对等网络的通信容错问题***，解决该问题就是通过确定由谁发起信息，以及如何实现信息统一同步来保障分布式系统能够达成一致。

Leslie在论文中提出了几种解决方案，FTMP、MMFCS、SIFT等容错架构也陆续出现，但如今应用的最为广泛的是1999年由Miguel Castro与Barbara Liskov提出的实用拜占庭容错算法(PBFT)。

1982 年，盲签名技术，数字现金 eCash 诞生——David Chaum

David Chaum 被认为是数字货币的先驱者，他在1982 年的论文**《Blind Signatures for Untraceable Payment》**中提出了盲签名技术和基于该技术的匿名数字现金eCash。1990 年，David Chaum创建了 DigiCash 公司实现eCash。

eCash首次给出了在网络上匿名传递价值的方式，它通过银行的加密签名，以数字形式存储货币，用户可以将这种数字现金自由转移，且无需暴露自身信息。但从严格意义上讲，eCash不是数字货

币，而是一种中心化信用的数字现金。

盲签名技术是指在签名之前使消息的内容失明，签名者在无法看到原始内容的前提下对信息签名。该技术可以实现对所签名内容的保护，还因无法将签名内容与签名结果对应，实现防追踪。

1985 年，零知识证明——Shafi Goldwasser、Silvio Micali 与 Charles Rackoff

1985年，Shafi Goldwasser，Silvio Micali和Charles Rackoff在论文**《The Knowledge Complexity of Interactive Proof-Systems》**中首次提出了零知识证明(Zero-knowledge proofs)，它是一种特殊的交互式证明，指的是证明者可以向验证者证明自己知道X的值，但不需要向验证者透露除了“自己知道X的值”外的任何信息。

零知识证明是密码学家设计的最强大的工具之一，可被用于密钥交换、NP 问题、身份验证、数字签名、水印检测中。***“我不能告诉你这个秘密，但我可以向你证明我知道这个秘密”。***

应用广泛的zk-SNARK(zero-knowledge succint non-interactive arguments of knowledge，零知识、简洁、非交互的知识论证)是零知识证明的一种，使证明者能够简洁地使任何验证者相信其给定论断有效，并且实现计算零知识，不显示验证内容，不需要证明者与验证者之间进行交互。

在数字货币系统中，zk-SNARK可以实现让矿工知道一笔交易是有效的，但却不知道这笔交易的发起者、接收者以及转账金额等隐私信息。

1985 年，椭圆曲线加密算法——Neal Koblitz 与 Victor Miller

椭圆曲线加密算法是在1985年由Neal Koblitz和Victor Miller分别独立提出的，它是一种基于椭圆曲线的非对称加密算法，其安全性依赖于解决椭圆曲线离散对数问题的困难性。

椭圆曲线加密算法的主要优势在于某些情况下，它使用更小的密钥提供与其他加密算法相当的或更高等级的安全；另一个优势是它可以定义群之间的双线性映射，而双线性映射在密码学中有着大量应用。

1989 年，万维网，HTTP 协议——Tim Berners-Lee

万维网(World Wide Web，WWW)是一个由许多互相链接的超文本组成的系统，是人们在互联网上进行交互的主要工具，它是Tim Berners-Lee在1989年发明的。

Tim 发明了三项关键技术让超文本可以连接到网上：统一资源标识符(URL)；超文本标记语言(HTML)；超文本传输协议(HTTP)。

1990年，Tim Berners-Lee成功利用互联网实现了HTTP客户端与服务器的第一次通讯，而万维网讯息收集中心Info.cern.ch，是世界上第一个网站及网站服务器。

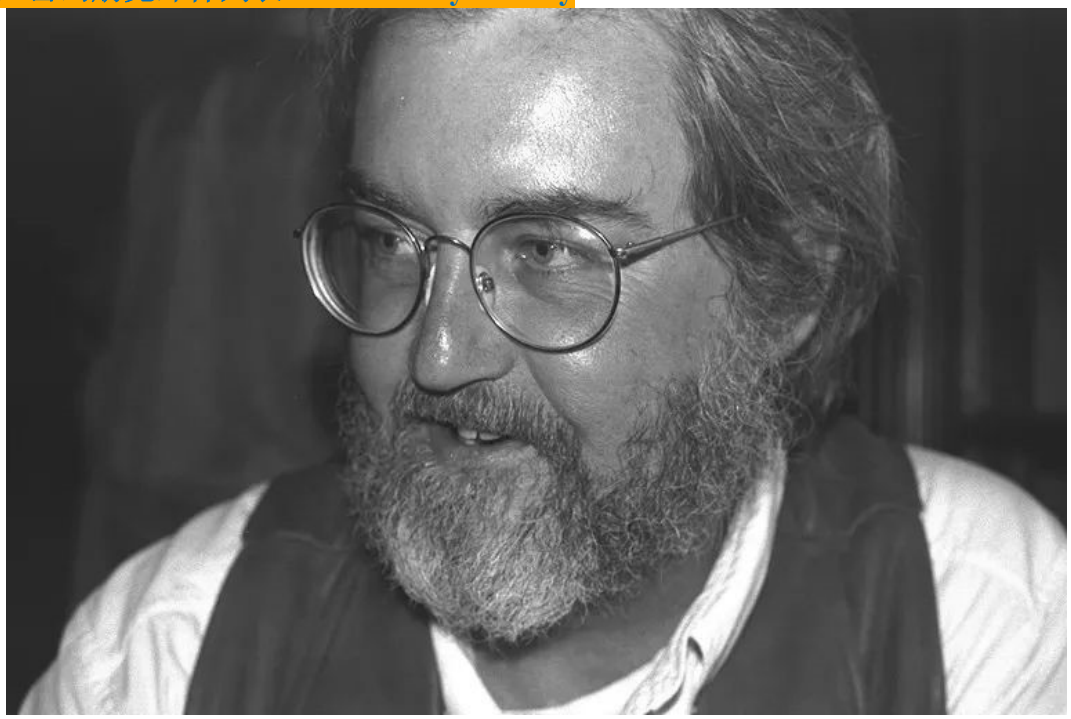
1991 年，用时间戳保证数据安全的协议——Stuart Haber 与 W. Scott Stornetta

Stuart Haber W. Scott Stornetta

1991年，密码朋克成员Stuart Haber 与W. Scott Stornetta发表了论文**《How to time-stamp a digital document》**，在这篇文章中他们提出了一个用时间戳的方式来保证数字文件安全的协议。***该协议用时间戳表达文件创建的先后顺序，并要求在文件创建后其时间戳不能改动，从而使得文件被篡改的可能性为零。***可信时间戳由算力时间源负责保障时间的授时和守时监测，任何机构包括时间戳中心不能对时间进行修改。

中本聪在比特币中引入了该协议：时间戳服务器对以区块形式存在的一组数据实施随机散列并加上时间戳，该时间戳能够证实特定数据必然于某特定时刻是的确存在的，因为只有在该时刻存在了才能获取相应的随机散列值。每个时间戳将前一个时间戳纳入其随机散列值中，每一个随后的时间戳都对之前的一个时间戳进行增强，从而形成一个链条。

1992 年，密码朋克邮件列表——Timothy C. May



Timothy C. May是密码朋克运动的发起人之一，也是英特尔早期资深的科学家。1992年，他建立了密码朋克邮件列表，全世界的密码学家、程序员、极客在这里通过加密电子邮件进行交流。***该组织早期成员有维基解密主编 Julian Paul Assange、BitTorrent 协议发明者 Bram Cohen、万维网发明者 Tim Berners-Lee，以及包括 Adam Back 、戴维、Nick Szabo、中本聪在内的数字货币的开拓者。可以说没有密码朋友邮件列表，就没有数字货币。***

2008 年，中本聪在密码朋克邮件列表发布了比特币白皮书。

1993 年，《密码朋克宣言》——Eric Hughes

1993 年， Eric Hughes 发表了《密码朋克宣言》，“cypherpunk”一词首次出现；1994 年 Timothy C. May 发表了《密码朋克常见问题解答》。

Eric Hughes 在宣言中写道：写代码，是密码朋克的使命。我们深知总要有人写软件来保护隐私。只有我们亲自动手，我们才能拥有隐私权，我们一定会开发这样的软件。 我们将要公开发布***我们的代码，让密码朋克战友们能够使用软件。 我们的代码，对全球所有人免费。如果你们要封杀我们所写的软件，我们也毫不在意。我们清楚，软件是无法被销毁的，彻底的分布式系统永不停机。***

《连线》杂志报道了这些隐匿于世界各地、为人类隐私事业战斗的人们，称“密码朋克正在与 FBI、NSA 作战。他们的战争将决定 21 世纪是否还会有隐私存在。”

1997 年，哈希现金机制——Adam Back

1997 年 3 月，Adam Back 在密码朋克邮件列表发送了一封主题为《A partial hash collision based postage scheme》的邮件，提出了哈希现金机制(HashCash)。

哈希现金是一种工作量证明机制，用于抵抗邮件的拒绝服务攻击及垃圾邮件网关滥用。如今被广泛应用于挖矿算法，戴伟的 B-money、Nick Szabo 的 BitGold，这些比特币的先行者都是在哈希现金的框架下挖矿。Hashcash 也为 RPoW 和 PoW 的提出奠定了基础。

工作量证明机制的核心特征之一是不对称性：工作量对于请求方是有一定难度的，对于验证方则是容易的。哈希现金机制采用安全哈希算法 SHA1 实现工作量证明。

1998 年，B-money——戴伟

1998 年 11 月，同样是在在密码朋克邮件列表中，戴维发布了 B-money 白皮书。这是一种匿名的、分布式的电子加密货币系统，强调点对点的交易和不可更改的交易记录。

B-money 是第一种真正意义上的数字加密货币，比特币的去中心化的结算架构、匿名交易、点对点网络，在 B-money 中已经全部出现，不过它没有真正进入应用领域。

在比特币白皮书中，第一个被引用的资料是 B-money；在以太坊中，ETH 的最小单位被命名为 Wei，以示对戴伟的敬意。

1998 年，BitGold——Nick Szabo

Nick Szabo 在 1998 年发明了数字货币 BitGold，使用了工作量证明机制。在白皮书中，Nick 是这么描述的：比特金通过使用被称为“解题功能”、“工作功能证明”或“安全基准功能”客户端，以一段字符串计算另一段字符串，计算结果就是它的工作量证明。

不过，Nick Szabo 更被大众知晓的身份是“智能合约之父”，1996 年，他在论文《Smart Contracts: Building Blocks for Digital Markets》中提出了智能合约概念。

智能合约是一套以数字形式定义的承诺 ，包括合约参与方可以在上面执行这些承诺的协议，其基本理念是把合约条款嵌入到硬件和软件中。Vitalik Buterin 在以太坊中实施了智能合约这一想法。

1999 年，P2P——Sean Parker 与 Shawn Fanning

1999 年，18 岁的 Shawn Fanning 与 19 岁 Sean Parker 成立在线音乐服务 Napster。Napster 是第一个被广泛应用的 P2P(Peer-to-Peer，点对点网络、对等网络)音乐共享服务，它把 P2P 技术变成了主流，是对下载方式的一次革命。

P2P 是无中心服务器、依靠用户群交换信息的一个互联网体系，它的每个用户端既是节点，也是服务器。P2P 在隐私要求高的网络中和文件共享领域得到了广泛的应用，也是比特币最重要的基础技术之一。

P2P 这一概念最早出现在 1969 年 4 月 7 日的第一份 RFC(Request For Comments)文档中，RFC 是互联网工程任务组(IETF)发布的一系列备忘录，后来演变为用来记录互联网规范、协议、过程等的标准文件。

2001 年，BitTorrent 协议——Bram Cohen

2001 年 4 月，Bram Cohen 发布了 BitTorrent 协议，并在 2001 年 7 月正式应用。

BitTorrent 协议是架构于 TCP/IP 协议之上的一个 P2P 文件传输通信协议。它把文件虚拟分成大小相等的块，并把每个块的索引信息和哈希验证码写入种子文件。下载者根据种子文件告知对方自己已有的块，然后交换没有的数据。

使用 BitTorrent 协议，下载的人越多提供的带宽越多，下载速度也就越快；同时，拥有完整文件的用户也会越来越多，文件的“寿命”会不断延长。

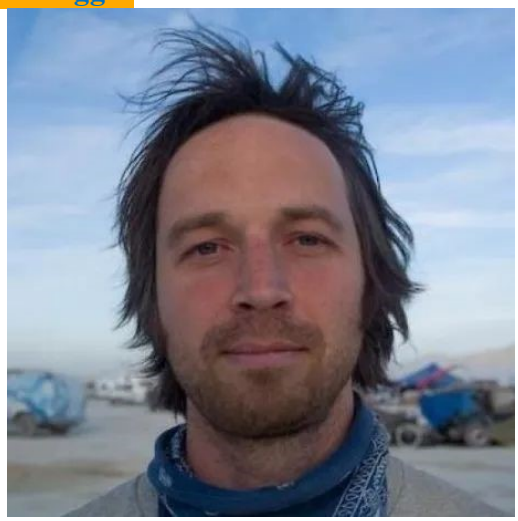
2002 年，Kademlia——Petar Maymounkov 与 David Mazières


2002 年，Petar Maymounkov 与 David Mazières 发表了论文《Kademlia: A Peer-to-peer Information System Based on the XOR Metric》，提出了 Kademlia。Kademlia 是第三代 P2P 网络的节点动态管理和路由协议，通过分布式哈希表实现信息的存储和检索。

相比之前的两代协议，***Kademlia 以全局唯一 ID 标记 P2P 网络节点，以节点 ID 异或(XOR)值度量节点之间距离，***并通过距离分割子树构建路由表，建立起一种全新的网络拓扑结构，相比于其他算法更加简单和高效。

2005 年，BitTtorrent 实现基于 Kademlia 协议的分布式哈希表技术，eMule 也实现了基于 Kademlia 的 类似技术。以太坊使用 Kademlia 作为分布式网络的底层算法。

2004 年，Ripplepay——Ryan Fugger



2004 年，Ryan Fugger 开发出去中心化货币支付协议 Ripplepay，它是 Ripple 协议的前身。Ryan 最初的想法是革新传统交易模式，构建可通过全球网络为用户提供安全快捷支付服务的系统。

2012 年，Chris Larsen 与 Jed McCaleb 向 Ryan 提出数字货币的理念，随后三人共同成立了 OpenCoin，开发新的支付协议 Ripple，它是一个实时结算系统和货币兑换与汇款网络，基于分布式开源互联网协议、共识总账和原生货币 XRP。

2014 年 Ripple 与德国互联网银行 Fidor 合作，这是它的第一家银行用户，4 个月后它获得两家美国银行的支持，在当年 12 月，它又与银行支付网络 Earthport 达成合作。如今，Ripple 可以支持 27 个国家的实时全球支付。

2005 年，RPoW——Hal Finney

2005 年，Hal Finney 设计出了 RPoW(Reusable Proofs of Work ，可复用工作量证明)，RPoW 是 PoW 的前身。Finney 将 Adam Back 的哈希现金机制完善成一种可重复利用的工作量证明，并用于数字货币实验中。

Hal Finney 是一位密码学先锋，***PGP(Pretty Good Privacy)计划的核心参与者，PGP 旨在使世界各地的人们能够以除接收者之外的任何人都无法阅读的方式进行加密通信。***

Finney 是唯一一个立刻关注中本聪提出比特币想法的人，他在 Bitcoin 发布的当天就下载了，是除中本聪外第一个运行 Bitcoin 的人，此外，Finney 也是第一笔比特币交易的收款人。

2008 年 10 月 31 日，Satoshi Nakamoto 发布比特币白皮书：

《比特币：一种点对点的电子现金系统》

Bitcoin: A Peer-to-Peer Electronic Cash System

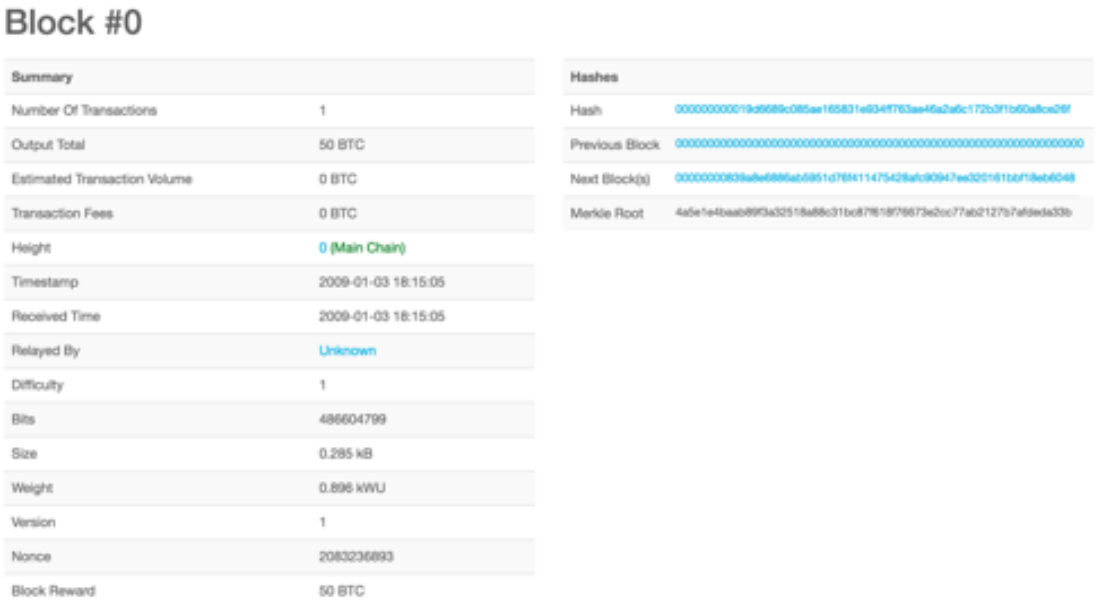
Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest

2009 年 1 月 3 日，比特币“创世区块” Block #0 挖出

在区块中，Satoshi Nakamoto 写下：

The Times 03/Jan/2009 Chancellor on brink of second bailout for banks.



Block #0

Summary	
Number Of Transactions	1
Output Total	50 BTC
Estimated Transaction Volume	0 BTC
Transaction Fees	0 BTC
Height	0 (Main Chain)
Timestamp	2009-01-03 18:15:05
Received Time	2009-01-03 18:15:05
Relayed By	Unknown
Difficulty	1
Bits	486604799
Size	0.285 kB
Weight	0.896 kWU
Version	1
Nonce	2083236893
Block Reward	50 BTC

Hashes	
Hash	000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f
Previous Block	0000000000000000000000000000000000000000000000000000000000000000
Next Block(s)	00000000839a8e6886ab5951d76f411475428afc90947ee320161bbf18eb6048
Merkle Root	4a5e1e4baab89f3a32518a88c31bc87f618f78673e2cc77ab2127b7afdeda33b

随着人类科技水平的进步，计算机的计算能力增长得越来越快，这无疑给密码分析提供了有力的工具，因此对密码机制的安全性提出了更高的要求，驱动着**密码从业者**不断推陈出新，保卫**网络空间**的安全。同时还要提高警惕，不要让密码算法这柄利剑伤害到用户本身，避免类似于 WannaCry 的勒索病毒再次爆发。最后，**信息安全**最薄弱的环节其实是**用户**本身，相当对的安全事件不是由于技术的漏洞，而是人的疏忽，所以希望大家都能重视**密码学**，保护自身在网络空间的安全。

—END—

参考文献(909 字)

1. 秦某．从艺术到科学——密码学的发展历程．[EB/OL]中科院物理所，http://www.sohu.com/a/190323227_224832，2017-09-07.
2. Stinson D R. Cryptography: theory and practice[M]. CRC press,2005.
3. Shannon C E. Communication theory of secrecy systems[J]. Bell Labs Technical Journal, 1949, 28(4):656-715.
4. Diffie W, Hellman M. New directions in cryptography[J]. IEEE transactions on Information Theory, 1976, 22(6):644-654.
5. Rivest R L, Shamir A, Adleman L. A method for obtaining digital signatures and public-key cryptosystems[J].Communications of the ACM, 1978, 21(2):120-126.
6. 腾讯新闻：全球爆发电脑勒索病毒 中国多所大学校园网被攻击 http://news.qq.com/a/20170513/001170.htm
7. 吴师傅．密码往事．[EB/OL]；果壳网，https://www.guokr.com/article/43508/，2011-06-14．
8. 古千峰．密码学 40 年丨重要历史与人物．[EB/OL]；云头条企鹅号，http://8btc.com/thread-242744-1-1.html，2018-11-07．
x. 秦陇纪．数据简化社区 Python 官网 Web 框架概述；数据简化社区 2018 年全球数据库总结及 18 种主流数据库介绍；数据科学与大数据技术专业概论；人工智能研究现状及教育应用；信息社会的数据资源概论；纯文本数据溯源与简化之神经网络训练；大数据简化之技术体系．[EB/OL]；数据简化 DataSimp(微信公众号)，http://www.datasimp.org，2017-06-06．

Appx.数据简化 DataSimp 社区简介(835 字)

信息社会之**数据、信息、知识、理论**持续累积，远超**个人认知学习**的时间、精力和能力。应对大数据时代的数据爆炸、信息爆炸、知识爆炸，解决之道重在**数据简化(DataSimplification)**：简化减少知识、媒体、社交数据，使信息、数据、知识越来越简单，符合人与设备的负荷。**数据简化 2018 年会议**(DS2018)聚焦**数据简化技术(DataSimplificationTechniques)**：对各类数据从采集、处理、存储、阅读、分析、逻辑、形式等方面**做简化**，应用于信息及数据系统、知识工程、各类数据库、物理空间表征、生物医学数据，数学统计、自然语言处理、机器学习技术、人工智能等领域。欢迎投稿**数据科学技术、简化实例相关论文**提交电子版(最好有 PDF 格式)。填写申请表加入**数据简化 DataSimp** 社区成员，应至少一篇数据智能、编程开发 IT 文章：①高质量原创或翻译美欧数据**科技论文**；②社区网站义工或完善 **S 圈型**黑白静态和三彩色动态社区 **LOGO 图标**。**论文投稿**、加入**数据简化社区**，详情访问 www.datasimp.org 社区网站，网站维护请投会员邮箱 DataSimp@163.com。请关注公众号“数据简化 DataSimp”留言，或加微信 QinlongGEcai(备注：姓名/单位-职务/学校-专业/手机号)，免费加入**投稿群**或**“科学 Sciences 学术文献”**读者微信群等。长按下图“识别图中二维码”关注三个公众号(搜名称也行，关注后底部菜单有文章分类页链接)：

数据技术公众号“**数据简化 DataSimp**”：

科普公众号“**科学 Sciences**”：

社会教育知识公众号“**知识简化**”：