加密战争33年：始于拜登，终于拜登

作者：Chao



2024年深秋，华盛顿特区。金黄的枫叶正从白宫的梧桐树上缓缓飘落，拜登总统站在椭圆形办公室的窗前，望着这个他即将告别的城市。

三十三年前，在不远处的国会山，作为参议员的他提出了那个著名的S.266法案。那时的他绝不会想到，这个看似普通的法案，会成为一场持续三十多年"加密战争"的导火索。更不会想到，这场战争最终会在他担任总统的最后时刻，以密码朋克们的胜利而告终。

这是一个关于失败与胜利、压制与反抗、集权与自由的故事，一个跨越了整整一个世代的史诗。在这场持续了三十多年的战争中，一群怀揣着数学理想的极客，最终改变了人类文明的进程。

### 第一部分：战争前夜

#### 冷战的余烬

这个故事要从更早说起。

1975年，IBM研究实验室。一群科学家正在开发一种革命性的加密算法，这就是后来著名的DES（数据加密标准）。此时的计算机产业正处于关键时刻：个人电脑即将走入千家万户，而加密技术将决定这场革命的走向。

但就在这项工作即将完成时，美国国家安全局（NSA）突然介入。他们以国家安全为由，要求将密钥长度从128位缩减到56位。这个看似技术性的改动，实际上让算法的安全性降低了数万亿倍。

在冷战的阴影下，没有人敢于质疑这个决定。加密技术被视为军事装备，必须严格管控。但随着个人电脑革命的推进，这种冷战思维开始与新时代的需求产生尖锁的矛盾。

#### 战争开启

1991年春，NSA的一份内部报告写道："随着个人电脑的普及和互联网的发展，加密技术的扩散将成为国家安全的重大威胁。我们必须在这个问题失控之前采取行动。"

这份报告最终落在了参议员乔·拜登的办公桌上。作为司法委员会的重要成员，他决定采取行动。他提出了S.266法案《1991年综合反犯罪法案》。法案第1126条要求："电子通信服务提供商和设备制造商有义务确保政府能够获得加密通信的明文内容。"

表面上，这是一个针对犯罪的法案。但实际上，这是政府第一次试图通过立法来控制整个数字世界的钥匙。

### 第二章：代码即武器

#### 车库里的反抗

就在华盛顿的政客们讨论这个法案时，在科罗拉多州的一个车库里，程序员Phil Zimmermann正在进行着一场静默的革命。他开发的PGP（Pretty Good Privacy）软件，能让普通人使用军用级别的加密技术。

当Zimmermann听说S.266法案时，他意识到必须在法案通过之前完成PGP。这变成了一场与时间赛跑的战役。

但完成开发只是第一步。美国政府将加密软件列为军需品，禁止出口。面对这个障碍，Zimmermann想出了一个天才的主意：将PGP的源代码印刷成书籍出版。

这就是著名的"齐默尔曼出版社"事件。因为根据美国宪法第一修正案，出版物受言论自由的保护。政府可以管制软件，但无法禁止一本数学书籍的出口。

很快，这本看似晦涩的技术书籍在全球流传。在世界各地，程序员们购买这本书，将印刷的代码重新输入电脑。PGP像一股不可阻挡的暗流，悄然流向全球每个角落。

#### 学术界的声音

学术界也提出了反对。1992年初，当国会就加密技术管制举行系列听证会时，学术界的众多专家站出来明确反对建立后门机制。他们的核心论点很简单：加密系统要么是安全的，要么是不安全的，不存在中间状态。

在科技界、学术界的强大反对声浪下，S.266法案最终未能通过。这是加密自由的第一次胜利，但政府显然不会轻易放弃。

### 第三章：密码朋克崛起

#### 新兴力量的诞生

1992年，加州伯克利。

在Sun公司第五号员工John Gilmore的家中，一群关心隐私和加密技术的人开始定期聚会。这些聚会吸引了二三十位来自湾区的技术专家，其中包括英特尔科学家Timothy May和密码学家Eric Hughes。每个月，这群人都会在Gilmore家的会议室讨论密码学、隐私权和数字时代的公民自由。

这些聚会很快发展成为了密码朋克运动的发源地。参与者们意识到，S.266法案的出现预示着一场关于数字时代公民自由的持久战。几次会面后，他们决定不让物理限制成为障碍，于是创建了密码朋克邮件列表。这个名字来源于"密码"（Cypher）和"朋克"（Punk）的结合。很快，这个邮件列表吸引了数百名成员，包括计算机科学家、密码学家和自由主义者。

#### 数字时代的独立宣言

1993年3月，Eric Hughes发表了《密码朋克宣言》。这份后来被视为数字时代独立宣言的文件开篇写道：

"隐私是在一个开放的社会维持开放所必需的。隐私不是秘密。一个隐私事务是某个你不想让全世界都知道的事情，但不是一个你不想让任何人知道的事情。隐私是选择性地向世界展示自己的能力。"

这段话迅速在早期互联网上传播。它准确表达了一个新兴群体的核心理念：在数字时代，隐私不是特权，而是基本人权。而保护这项权利的工具，就是加密技术。

#### 政府的反扑

密码朋克的崛起让克林顿政府感到不安。1993年4月，白宫推出了一项新计划：Clipper Chip。

这是一个精心设计的陷阱。政府声称这个加密芯片将同时满足隐私保护和执法需求。他们甚至说服了AT&T承诺采购100万片。

但这个计划很快就遭遇了致命打击。1994年6月，AT&T的研究员Matt Blaze发表了一篇论文，证明Clipper Chip的安全性形同虚设。这个发现让政府陷入尴尬，AT&T也随即放弃了采购计划。

更重要的是，这件事让公众第一次清晰地认识到：政府控制的加密系统是不可信的。

在这些公开的战斗之下，还有更深层的暗流在涌动。1994年，阿姆斯特丹。一群密码朋克秘密集会。他们讨论的是一个更具颠覆性的想法：数字货币。

"政府控制加密的真正原因是想控制金钱，"一位与会者说，"如果我们能创造一种不受控制的货币，那才是真正的革命。"

### 第四章：制度的演变

#### 网景的困境

1995年，硅谷。

一个名叫网景的公司正在改写历史。这家由24岁的Marc Andreessen和经验丰富的Jim Clark共同创立的公司，将互联网带入了普通人的生活。8月9日，网景上市。开盘价28美元，收盘达到58.25美元，公司市值一夜之间突破29亿美元。这是互联网时代的开端。

在这个关键时期，网景团队开发了SSL加密协议。但由于美国政府的出口管制，他们不得不发布两个版本：

美国版：使用128位强加密

国际版：只能使用40位加密

这种双重标准很快被证明是灾难性的。一位法国学生用8天时间就破解了40位的SSL。这个新闻震惊了商业界。"这就是政府管制的结果，"网景的工程师们愤怒地说，"他们不是在保护安全，而是在制造漏洞。"

2009年，网景公司的联合创始人Marc Andreessen与Ben Horowitz共同创立了a16z风险投资公司，随后A16z迅速成为了加密领域最活跃的投资机构之一。作为企业，Marc Andreessen不得不屈服于政府的要求。但作为一个投资人，Marc Andreessen继续支持着这场加密战争。

#### 开源运动的崛起

加密战争中，还有一个意想不到的盟友：开源运动。

1991年，一个名叫林纳斯·托瓦兹的芬兰学生发布了Linux的第一个版本。为了避开美国的出口管制，他特意将加密模块放在核心之外。这个看似妥协的决定，反而让Linux得以在全球自由传播。

开源运动改变了整个科技世界的格局。那些曾经被视为理想主义的密码朋克理念，开始在现实中开花结果：

代码应该是自由的

知识应该共享

去中心化是未来

微软的比尔·盖茨将开源称为"计算机病毒"，但他错了，开源成为了未来。

密码战争也极大地支持了开源运动本身。1996年，在丹尼尔·伯恩斯坦诉美国政府对加密软件的出口管制一案中，法院首次裁定：计算机代码是受宪法第一修正案保护的言论形式。这个具有里程碑意义的判决，为开源运动扫清了法律障碍。如今，开源软件已经成为互联网的根基。

#### 战争的第一阶段结束

到1999年，形势已经不可逆转。克林顿政府最终放松了延续了数十年的加密技术出口管制。当时的《经济学人》杂志评论说："这不仅是一场关于技术的战争，更是一场关于自由的战争。"

战争的成果正在改变世界：

PGP成为电子邮件加密的标准

SSL/TLS保护了所有的网上交易

Linux和开源软件改变了整个科技行业

加密技术成为了数字时代的基础设施

但这仅仅是开始。密码朋克们的目光已经投向了一个更具野心的目标：货币体系本身。

### 第五章：货币战争

#### 数字货币的先驱

1990年，密码学家David Chaum创立了DigiCash公司，开启了密码学与电子支付结合的先河。DigiCash通过"盲签名"技术创造了一个既能保护隐私又能防止双重支付的系统。虽然这家公司最终在1998年宣告破产，但它的影响深远。

接下来的十年，一系列开创性的构想相继出现：

1997年，Adam Back发明了Hashcash。这个最初用于对抗垃圾邮件的系统，首次将"工作量证明"的概念实用化。

1998年，Wei Dai发表了B-money提案。这是第一个完整描述的分布式数字货币系统，参与者通过解决计算难题来创造货币，也就是我们熟悉的PoW。Wei Dai的贡献如此重要，以至于多年后以太坊创始人Vitalik Buterin将以太坊的最小货币单位命名为"Wei"，以表达对这位先驱的敬意。

1998年到2005年间，Nick Szabo提出了BitGold设想。他不仅将工作量证明与价值存储巧妙结合，更提出了"智能合约"的革命性概念。

#### 比特币的诞生

这些先驱者的工作看似都触碰到了梦想的边缘，却始终缺少最后一块拼图。如何在没有中心化机构的情况下，让所有参与者对交易达成共识？这个问题困扰了密码学家们整整20年。

2008年10月31日，一个化名中本聪的神秘人物，在密码学邮件列表上发布了比特币白皮书。这个方案巧妙地整合了多项既有技术：

采用了类似Hashcash的工作量证明系统

借鉴了B-money的去中心化设计理念

使用Merkle树进行交易验证

创新性地提出了区块链来解决双重支付问题

这个新系统解决了此前所有数字货币方案都未能解决的问题：如何在完全去中心化的情况下达成共识。

更重要的是，这个方案选择的发布时机非常微妙。就在一个月前，雷曼兄弟轰然倒塌，全球金融危机全面爆发。人们开始质疑传统金融体系的稳定性。

2009年1月3日，比特币的创世区块诞生。中本聪在区块中写下了一句话："The Times 03/Jan/2009 Chancellor on brink of second bailout for banks"

这句来自《泰晤士报》的头条，不仅是对区块产生时间的记录，更是对传统金融体系的无声控诉。

第一笔比特币交易的接收者，正是曾在DigiCash实习过的Hal Finney。当他在2009年1月收到中本聪发来的10个比特币时，他在推特上简单地写道："正在运行比特币。"

这条普通的推文，成为了数字货币历史上最著名的记录之一。从DigiCash的实验室，到密码朋克的邮件列表，再到比特币的诞生，一场酝酿了近二十年的革命终于找到了它的新形态。

#### 第一次冲突

2011年，比特币首次引起了华盛顿的注意。

维基解密在遭到信用卡公司和银行封锁后，开始接受比特币捐款。这让世界第一次看到了比特币的真正力量：它不可审查，不可封锁。

参议员Charles Schumer随即在新闻发布会上发出警告，称比特币是"数字形式的洗钱工具"。这是美国政府首次公开针对比特币表态。

#### 风暴来临

2013年，一场意外的危机让比特币获得了新的认同。

塞浦路斯银行业危机爆发，政府直接从储户账户中强制征收存款。这让全世界都看到了传统金融体系的脆弱性：你的存款，并不真正属于你。

比特币价格首次突破1000美元。但随之而来的是政府更严厉的打击。同年，FBI查封了暗网市场"丝绸之路"，缉获了144,000枚比特币。政府似乎在证明：比特币就是犯罪分子的工具。

#### 制度的反扑

2014年，加密货币遭遇了第一次重大危机。全球最大的比特币交易所Mt.Gox突然关闭，85万枚比特币凭空消失。这相当于当时全网比特币的7%。

各国政府以保护投资者为由，开始加强监管。2015年，纽约州推出了严格的BitLicense制度，这个被称为"数字货币业者照妖镜"的监管框架，迫使多家加密货币公司离开纽约。

但每一次危机，都让这个行业变得更加强大，更重要的是，这些危机证明了一个关键点：即便中心化的交易所可能失败，比特币网络本身依然坚如磐石。这正是去中心化设计的价值所在。

#### 制度性突破

2017年标志着加密货币的一个重要转折点。这一年，比特币从1000美元一路飙升到20000美元。但更重要的是制度性的突破：芝加哥商品交易所(CME)和芝加哥期权交易所(CBOE)推出了比特币期货合约。

这标志着华尔街开始正式接纳这个曾经的地下资产。监管机构的态度也开始微妙变化，从完全否定转向尝试理解和规范。

但真正的转折发生在2020年。新冠疫情爆发，各国开启了史无前例的货币扩张。在这个背景下，机构投资者开始重新审视比特币的价值。

8月，MicroStrategy首席执行官Michael Saylor宣布将公司储备资金转换为比特币。这一决定在企业界引发了连锁反应。到2021年2月，特斯拉宣布购入15亿美元比特币，这个消息震动了整个金融界。

### 第六章：最后的战役

2021年，拜登政府对加密行业发起了全面围剿。这一次，政府的打击比以往任何时候都更有组织、更全面三十三年前，S.266法案失败后，政府就再也无法阻止加密技术的发展。现在，他们试图通过监管来控制加密货币。

但形势已经不同。在表面的监管风暴下，加密货币已经深深植入了现代社会的每个角落：超过5000万美国人持有加密货币，主流支付公司纷纷接入加密支付，华尔街已经建立起完整的加密货币业务线，传统金融机构开始为客户提供加密货币服务。

更重要的是，新一代人已经完全接受了密码朋克的理念。对他们来说，去中心化和数字主权不是革命性的概念，而是理所当然的事情。这种观念的转变比任何技术创新都更具深远意义。

2022年，加密市场经历了一场严重危机。FTX的轰然倒塌让整个行业陷入寒冬。2023年，加密行业开始复苏。每一次危机都让行业变得更加成熟，更加规范。监管机构的态度也开始发生微妙变化，从单纯的打压转向寻求合理的监管框架。

#### 历史的转折

2024年，一个具有讽刺意味的转折出现了。特朗普将支持加密创新作为重要的竞选政策，他承诺将为加密行业创造更友好的监管环境。他的竞选搭档、俄亥俄州参议员J.D. Vance本人就是比特币的持有者，多年来一直站在加密创新的前线。他们以横扫的形势赢得了这次总统大选。

三十三年前，当拜登提出S.266法案时，他认为自己在捍卫秩序。但历史总是充满讽刺：正是这个法案，成为了一场改变人类文明的革命的导火索。现在，他即将将总统之位交给一位支持加密的继任者。这个转折来得如此自然：当一场革命最终胜利时，连曾经的对手也不得不承认它的价值。

但对密码朋克们来说，赢得政府的认可从来就不是终极目标。正如中本聪当年所说，比特币是一个可以让每个人都获得金融主权的工具。政府的态度只是路上的一个路标，见证着加密技术如何从地下运动走向大众生活，如何从技术实验发展为改变世界的力量。

从最初的密码学家和程序员的抵抗，到今天数以亿计的人使用加密货币；从车库里的极客实验，到撼动全球金融体系的力量；从被视为乌托邦的理想，到即将成为新世界的根基。在这场持续了一个世代的战争中，密码朋克们一次次被低估。他们被称为理想主义者、极端分子、甚至是罪犯。但他们只是倔强地相信：数学的真理终将战胜政治的权力，去中心化的自由终将战胜中心化的控制。

现在，他们的梦想正在成为现实。加密技术不再是隐藏在黑暗中的武器，而是照亮新文明的火炬。它正在重构人类社会的每一个层面：当钱包变成密码， 当契约由程序执行， 当组织被代码管理， 当信任建立在数学之上， 这个世界就站在了一个新文明的门前。

在未来的历史书上，2024年也许会被记录为加密革命的胜利之年。但真正的胜利不在于某个政府的认可，而在于千千万万普通人的觉醒。

这是密码朋克们的礼物，一个由代码构建、数学保护的新世界。在这个世界里，自由、隐私、信任都不再是口号，而是在每一行代码、每一个区块、每一次点对点的连接之中。