

# 数字极权时代生存手记

自序	4
前言	9
第一章 必要的前期准备	12
第一节 获取美区 Apple ID	13
第二节 获取 Google Voice	18
第三节 注册美区 Paypal	22
第二章 如何突破网络封锁	23
第四节 “翻墙”基本原理	24
第五节 V2Ray	26
第六节 Shadowsocks	35
第七节 其他翻墙手段概要与评析	40
第三章 加密即时通讯应用	46
第八节 加密通讯应用概论	48
第九节 Telegram 使用指南	50
第四章 个人信息保护指南	67
第十节 个人信息保护指南	67
第十一节 墙外社交媒体使用建议	83
第五章 信息难民自救指南	86
第十二节 404 信息保存	86
第十三节 404 信息获取	89
第六章 番外	91
第十四讲 去中心化网络	91
第十五讲 加密数字货币	96
附录	98

哪敢与世无争，分明是这个世界逼着人去争！

——岳昕《我在公开信后的一周里》

# 自序

自序·数字极权的铁幕下，我们已退无可退

《数字极权时代生存手记》收录了我自 2017 年以来在网络代理、信息安全等方面的学习与实践成果的记录。

编程随想在《为啥朝廷总抓不到俺——十年反党活动的安全经验汇总》一文中这样写道：“（在墙内）很多具备政治素质的人，缺乏信息安全的技能；所以他们无法利用互联网与党国斗争。”信息知识与技能的意义还不止于此。数字极权之所以能够毫无阻力地在中国推进，离不开大众在个人数据权利问题上的集体无意识。大多数中国民众对国家机器与科技巨头合力实施的大规模监控所知甚少，对个人隐私信息的去向漠不关心，再加上官媒“用隐私换取便利、安全”的洗脑宣传，使得整个国家在数字极权主义的邪路上越走越远。

信息技术可以为专制政府所用来强化管控，反过来也可以民众所用来扩展自由。网络代理可以帮助人们自由地获取未经审查的信息，端对端加密通信可以保证私密对话不受服务商与政府的监控，多重代理带来的网络匿名可以提供更大限度的言论自由，加密技术的普及与对网络封锁的破坏可以提升了当局实施舆情管控的成本。被统治阶级的群体性觉醒构成了反抗的前提，信息技能的运用则可以构成反抗的手段。因此，当信息知识与技能成为互联网时代的每一个个体的基本生活常识和能力时，它可以对数字利维坦提出有力的挑战，这或许就是普及信息技能的意义所在。

## 一、GFW 必须被打破

互联网技术拓展了信息传播的深度与广度，一度被寄望能给中国社会带来民主。然而与互联网在中国普及相同步的是防火长城（Great Firewall, GFW）的建设，它试图在互联网空间实行闭关锁国的政策，审查屏蔽一切与中共意见相左的境外网站，把中国人圈禁在从万维网中硬生生划出的“大中华局域网”中。在本国网络空间，中共当局藉维护国家安全之由大发专制淫威 [1] [2] [3] [4]，压制一切异见，扼杀多元价值，对异议者动辄禁言删号乃至逮捕拘禁、定罪判刑，迫使墙内民众学会自我审查而畏于发声；另一方面又开动宣传机器，使得民众只能获取当局希望他们接触的单一信息与强加给他们的价值观念，今日头条、腾讯新闻和各大国产手机浏览器每日置顶的习近平报道与“声名在外”的数字化红宝书“学习强国” App [5] [6] 就是显例。中共通过封锁、审查、禁烟、灌输多管齐下，以软硬手段相结合的方式推动洗脑政策与信息时代相适应，最终达到把中国人打造成闭目塞听、头脑简单、思想与党中央高度一致的木头人的效果。

GFW 不是一天建成的，中国互联网的原住民最早可以不受限制访问 Twitter、YouTube、中文维基百科等境外网站。GFW 加码的亲历者与见证者拥有着对于网络审查现状的认知，这是寻找手段突破封锁的前提。而对在 GFW 后成长起来的新世代而言，许会因为坚持独立精神而在墙内平台屡遭迫害，不得已出逃墙外成为“信息难民”；而更多的人难以认知“墙”的存在，或是将自我审查内化为习惯，“不会主动寻找敏感的信息，因为他们在成长中对信息审查已习以为常”[7]，在信息壁垒和官方意识形态狼奶的灌输下成长为“粉红”和“战狼”，深种文革思维，高扬“爱国无罪”，沐浴“盛世狂欢”，他们将翻墙者视为反动的异端，给墙外网站的批评声音贴上反华势力的恶毒攻击的标签。因此，先行者有必要向身边的人传授自己的翻墙“手艺”，让他们也能轻松便捷地跨过 GFW，自由地在完整、开放的国际互联网上查看一切未经中共当局审查的信息，还互联网以本该有的面目。只有让更多的人倾听到不同的声音，才有让洗脑政策的受害者吐净狼奶，意识到完整互联网远不止“中华局域网”的一亩三分地，才有可能弥合信息不对称的鸿沟，进而为不同派别间开展良性对话创造可能性。需要承认的是翻墙手段本身只是提供带来改变的可能性，不必然带来变革的结果，正如“战狼”有时也会翻墙，但只不过那是在上演“帝吧出征”的闹剧；但是推广翻墙术仍是有益的尝试。清醒者若是不付出抵御愚民政策的努力，听任同伴继续沉睡，自然永远无法改变网络审查的现状。

## 二、穹顶之下，莫非天网

人工智能和大数据等新兴科技为实现利维坦对社会生活全方位控制提供了全新的手段，数字科技与极权政体的联姻将人类带向前所未有的反乌托邦，而新疆已然不幸成为了“先驱”——当局要求所有居民在手机上安装能够自动扫描和上传文件数据的净网卫士 APP [8]，使用数以千计的监控摄像头配合面部识别和大数据分析以便实时掌控所有居民的一举一动 [9] [10]。我们纵然无法左右“新疆再教育营”的存废，但至少应当清醒地认识到这个国家正在发生的一切、我们的同胞所经历的一切，而不是听信外交部和官媒所谓“去极端化”、“职业培训”的无耻谰言。如果汉人觉得事不关己而对中共当局在新疆的倒行逆施听之任之，同样的灾难迟早也会降临到他们的头上。被冠以“雪亮工程”[11] [12] [13] 之名的监控天网正在内地铺开，“内地新疆化”并非空穴来风。大规模监控的实质是专制统治者监视臣民、巩固统治的工具，它所带来的只有民众的恐惧，而不是官方所允诺的安全与社会稳定。

在中国强制性的网络实名制下，网警可以轻而易举地将你在国内网络平台的发言与你的真实身份相关联；警察时刻在幕后监视着微信上发生的一切 [14]，你甚至会因为在朋友圈的言论而遭受牢狱之灾 [15]。正在建设的社会信用体系表明了当局掌控全面个人活动的企图。特定严重失信人黑名单等措施确实起到了打击不诚信行为的效果，但它同时也被当局用于迫害持异见者和访民群体 [16]，藉大数据之手制造人道灾难。

### 三、“哪里有压迫，哪里就有反抗”

就如同毛泽东所说的“我是一个知识分子，当一个小教员，也没学过军事，怎么知道打仗呢？就是由于国民党搞白色恐怖，把工会、农会都打掉，把五万共产党员杀了一批，抓了一批，我们才拿起枪来，上山打游击”一样——我是个码农行业的门外汉，也没学过计算机科学，怎么知道注册美区 Apple ID、租虚拟服务器搭建翻墙工具、用 Telegram 替代微信、翻墙上中国数字时代了解祖国呢？就是由于共产党搞赤色恐怖，把网络上对自己不利的言论都删掉，把境外网站的 IP 地址封锁了一批，TCP 关键词屏蔽了一批，VPN 应用下架了一批，我才爬墙自救起来，最后还把经历写成了这本书。

自 Telegram 被中国当局封锁后，要想在中国大陆使用 Telegram 自然离不开翻墙这一大前提，于是就有了本书的第二章“如何突破网络封锁”。翻墙不是我新学会的技能，不过我在 2017 年中时于偶然间得知了 Shadowsocks，使得日常性使用墙外服务成为了可能，并使我幸运地躲过了当年发生的国内 VPN 厂商被迫关停、苹果在中国区 App Store 下架 VPN 应用以及之后“十九大”前的 GFW 升级带来的断网冲击。之后，我从购买 Shadowsocks 商业服务转为借助 HyperApp 在 VPS 上自建 ShadowsocksR，再到命令行下自建 V2Ray，在升级“爱国上网”方式对抗党国的网络封锁和管制的道路越行越远，从此一发不可收拾。

移动端的翻墙离不开广义的 VPN 客户端的使用，而中国 App Store 的 VPN 应用下架潮迫使我注册了美区的 Apple ID 和 PayPal 以便获取和更新 VPN 和纽约时报等其他被中共认为威胁其统治而勒令下架的应用程序，这是本书第一节“获取美区 Apple ID”和第三节“注册美区 PayPal”的由来。

2017 年末上海携程员工亲子园虐童事件、红黄蓝幼儿园虐童事件、北京清退“低端人口”事件、北京亮出天际线行动、京津冀煤改气导致供暖危机，再到 2018 年的修宪取消主席任期限制、#MeToo（中国）系列运动（沈阳事件、北大岳昕事件、……）、长春长生生物问题疫苗事件、P2P 网络借贷平台集中爆雷、深圳佳士工运，这些曾经被送上舆论风口浪尖的热点话题的命运逃不过在微博、微信等墙内社交媒体上的大规模删帖封号的命运，留下一片刺眼的红色和“404”。在中国特色权贵资本主义运作模式下，权力与资本合谋劫掠财富，政府积极扩张权力的同时又拒不承担责任，一贯奉行“解决提出问题的人而非解决问题本身”的行事逻辑，以“稳定压倒一切”与维护国家安全的名义维护特权阶级的统治地位与既得利益，通过信息封锁和舆情管制来奴化民众，悍然制造无人堪作见证的历史。需知中共当局迫害的不仅仅是那些被控“煽动颠覆国家政权”的民运人士、人权律师和自由派学者，而是生活在极权体制下每一个平民。如果任由受害者被噤声，问题被掩盖，悲剧注定重演。

我曾在微博上追踪一批因为关注北京切除事件频繁被销号后又“转世”的博主，并曾尝试备份预感会被删的敏感题材的微博和微信公众号文章，也是在这个时候接触到

了新闻网站 [中国数字时代](#) 和它那句极为讽刺的“在这里，了解祖国”的口号。我坚信，信息传播的自由是人与生俱来的自然权利，中共当局将真相揭发与理性讨论诬指为谣言而一并绞杀的无耻企图必须被粉碎。本书第五章“信息难民自救指南”，便是拜网信办和中宣部之赐。

#### 四、选择适合自己的解决方案

解决方案的选择应取决于用户的直接需求，而效率和安全强弱同时受到方案选择与具体使用方法的影响。本书所提供的方案接近于“数字移民”，在效率与安全的权衡上更倾向于前者。在网络代理方式的选择上，V2Ray 和 Shadowsocks 可以有效地突破 GFW，但这类翻墙方法在匿名性上可能存在不足——如果你选择商业服务，服务商可以在服务器上看到你所有的访问记录；如果选择自建，你很难保证你对 VPS 所做的安全防护措施足以抵挡潜在的攻击。另一方面，承诺服务器零日志的 VPN 服务固然能够提供较强的匿名性，但它们所采用的除 OpenVPN 协议修改版之外的 VPN 协议都能被 GFW 识别屏蔽，并不能满足中国用户翻墙的需求，这是本书将 V2Ray 和 Shadowsocks 放在前面的原因。在加密即时通讯应用的选择上，本书推荐的 Telegram 也不能保证绝对的安全，因为即便是端对端加密模式也可能遭到中间人攻击。Telegram 上不存在政府的审查和监控，拥有一定规模的中文用户群体，频道和超级群聊使它在信息传播上具有显著优势，这使它相对更适合作为大陆民众习惯使用的微信 (WeChat) 的替代品。

如果你对个人隐私保护或匿名性有更高的要求，建议阅读 [编程随想](#)、[Cryptoboy404](#) 和 [iYouPort](#) 的博客。对于人权律师、新闻记者、NGO 工作者、访民等从事高风险活动的群体，应当参考 [《数字安全实用手册》](#) 等专业性更强的作品。

衷心祝愿每一位读者都能获得免于自我审查与恐惧的自由。

- [1] [Solidot | 网信办启动“剑网 2018”专项行动](#) (2018-07-16)
- [2] [Solidot | 网信办关停三款短视频应用，B 站宣布增加审查人员](#) (2018-07-27)
- [3] [Solidot | 网信办加强舆论监管](#) (2018-11-16)
- [4] [Solidot | 网信办禁止转世账号](#) (2018-11-16)
- [5] [美国之音 | 习近平“红宝书”“学习强国”手机软件由阿里巴巴开发操作](#) (2018-02-18)
- [6] [BBC News 中文 | “学习强国”：习近平“红宝书”登上 App 排行榜首](#) (2018-02-16)
- [7] [ABC NEWS | 与西方隔绝：在“墙”内长大的中国新世代](#) (2018-11-11)
- [8] [Solidot | 净网卫士被发现明文传输收集的数据](#) (2018-04-10)
- [9] [德国之声 | 脸部辨识结合大数据 250 万新疆居民难逃中国掌心](#) (2018-02-18)
- [10] [Solidot | 中国公司的人脸识别数据库外泄](#) (2019-02-15)
- [11] [【立此存照】雪亮工程：视频监控入户到人 - 中国数字时代](#) (2018-03-30)

- [12] [特大号 | 2018安防监控、雪亮工程项目盘点! - 中国数字时代](#) (2019-01-03)
- [13] [自由亚洲 | 2022年中国每人“拥有”两个监控探头 - 中国数字时代](#) (2019-02-04)
- [14] [【立此存照】网安部门监控清华大学学生组织的报告书 - 中国数字时代](#) (2017-12-04)
- [15] [Solidot | 网民因在朋友圈骂交警被拘 8 天](#) (2019-01-10)
- [16] [【网络民议】“母亲成了诈骗受害者，反而被禁止坐高铁” - 中国数字时代](#) (2019-02-16)

#### \*阅读需知

本书之所以称为“手记”，而非“教程”、“指南”，一来是因为我自身只是半路出家、勉强实现从无到有的“老白”，不能保证书中原创内容的专业可靠；二来详实严谨的优质教程或科普文在国际互联网上并不少见，我依样画葫芦重抄一遍前辈的教程显然是没有意义的。所以我对本书的定位是文献与超链接综述，意在摘引相关作者的创作、维基百科的词条解释来告诉事实 A、技术 B 或工具 C 的存在；至于深入了解技术 B 的原理或者学会运用工具 C，需要读者阅读链接的教程并善于运用搜索引擎从完整互联网上获取更多的信息，仅靠本书的内容是不够的。

本书将通过 PDF、Gitbook 和 Telegraph 三种渠道分发，不同渠道的发行版在排版等细节上存在差异。



## 前言

[ABC NEWS | 为何我决意在微信上作一个沉默的观察者](#) (2018-11-04)

[ABC NEWS | 澳洲中文社交媒体上的假新闻：核辐射秘密和致癌咖啡](#) (2018-07-23)

[ABC NEWS | “从不讲述全部真相”：中国媒体进军国际的民主威胁](#) (2019-02-09)

[BBC | 从档案袋到信用评级 中国是否正走向“奥威尔式”监控社会](#) (2018-10-17)

[编程随想 | 为啥朝廷总抓不到俺——十年反党活动的安全经验汇总](#) (2019-01-30)

[China's Surveillance State Should Scare Everyone](#) (2018-02)

[端传媒 | “南方傻瓜”甄江华：黑暗中行走的抗争者](#) (2017-12-12)

[端传媒 | 中国大数据四问：官商民集体狂欢的背后，“数据利维坦”正在降临？](#) (2018-02-21)

[端传媒 | 异乡人——竺晶莹：从“盛世”中出走，那些与我同行的中国年轻人](#) (2018-03-16)

[端传媒 | 江雪：微信个人帐号被封记](#) (2018-04-10)

[端传媒 | 大数据权利之争：对不起，你的数据属于你，但我们有权使用](#) (2018-04-17)

[風傳媒 | 自由之家：中国国安部门大肆扩张网路管理 迫害维权人士与分享资讯公民](#) (2019-01-30)

[华尔街日报中文网 | 中国科技巨头的副业：做政府监视的“眼睛”](#) (2017-12-04)

[美国之音 | 报告：警惕中国互联网管控模式威胁全球信息自由](#) (2019-02-05)

[纽约时报中文网 | 中国的威权主义未来：人工智能与无孔不入的监控](#) (2018-07-10)

[泡泡 | 老大哥并没有一直在看，反而比这更可怕——监视之恶（一）你可能还没完全理解奥威尔](#)

[泡泡 | 为什么必需拒绝大数据——监视之恶（二）公私监控伙伴关系](#)

[泡泡 | “冰河”已在你心里，这就是他们的目的 —— 监视之恶 \(三\) 历史和现实，拆穿谎言](#)

[泡泡 | 可怕的“连点成线”和互联网审查 —— 监视之恶 \(四\) “反恐”歧途](#)

[泡泡 | “六行字足够绞死你”，这不是玩笑 —— 监视之恶 \(五\) 数据指控](#)

[泡泡 | “计算机和狗”之辩，为什么要批评美国？ —— 监视之恶 \(六\) 破解荒唐的狡辩 \(上\)](#)

[泡泡 | 为什么要求解散国安局？ —— 监视之恶 \(六\) 立法监管不可能，应该怎么办 \(下\)](#)

[Solidot | 网信办称互联网需要秩序 \(2017-11-17\)](#)

[Solidot | 院士称 IPv6 时代将真正能实现网络实名制 \(2017-11-29\)](#)

[Solidot | 每个人都应该对中国计划中的全面监视感到害怕 \(2018-02-05\)](#)

[Solidot | 数以千计的公司正在监视你 \(2018-04-01\)](#)

[Solidot | 中国政府开始部署步态识别技术 \(2018-11-07\)](#)

[Solidot | 加州大学警告教职工和学生在中国不要使用微信 \(2019-01-02\)](#)

[Solidot | 网信办启动为期半年的网络生态治理专项行动 \(2019-01-03\)](#)

[Solidot | 深度学习之父担心中国的 AI \(2019-02-06\)](#)

[网信办：网络直播先审后播、加强弹幕实时管理、黑名单须上报 - 中国数字时代 \(2016-11-03\)](#)

[池见新草 | 在告密与监控中慢慢长大：中国学校的日常 - 中国数字时代 \(2018-05-22\)](#)

[后窗工作室 | 被教室天眼扫描的中学生 - 中国数字时代 \(2018-05-26\)](#)

[量子位 | 这是AI? 这是爱? 这是能全方位监控学生的“智能校服” - 中国数字时代 \(2018-12-24\)](#)

源点credit | 中国的社会信用体系与公众舆论 - 中国数字时代 (2019-01-31)

人民日报 | 将弹幕划入先审后播范围是一大亮点 - 中国数字时代 (2019-02-14)

ZDNet | 中共承包商在新疆记录维族人行踪 256万条个人信息在网上“裸奔”数月 - 中国数字时代 (2019-02-16)

## 第一章 必要的前期准备

### 第一节 获取美区 Apple ID

- 一、为什么需要美区 Apple ID ?
  - (一) 获取被下架应用
  - (二) 逃离“云上贵州”
- 二、换区还是注册新 ID?
- 三、如何获取美区 Apple ID
  - (一) 注册美区 Apple ID 教程
  - (二) 中国区 Apple ID 迁移至美区教程
  - (三) 如何实现原生 IP 全局代理
- 四、美区 Apple ID 的日常使用
  - (一) 如何使用美区 Apple ID 购买 app
  - (二) App Store 快速换区

### 第二节 获取 Google Voice

- 一、Google Voice 是什么?
- 二、为什么选择 Google Voice?
- 三、Google Voice 号码的用途
- 四、如何获取 Google Voice 号码?
  - (一) Google Voice 号码申请教程
  - (二) Google Voice 号码购买教程
- 五、如何长期保留 Google Voice 号码
- 六、Google Voice 日常使用

### 第三节 注册美区 Paypal

- 一、为什么需要美区 PayPal ?
- 二、如何注册美区 PayPal ?

## 第一节 获取美区 Apple ID

### 一、为什么需要美区 Apple ID？

#### (一) 获取被下架应用

中国网民广泛使用虚拟私人网络 (Virtual Private Network, VPN) 及类似工具来规避 GFW 的封锁，直接访问不受审查的国际互联网。自 2017 年以来中共当局加大了对 VPN 打击力度。2017 年 1 月 22 日，工信部发布了《工业和信息化部关于清理规范互联网网络接入服务市场的通知》，规定用户未经主批准不得自行建立或租用 VPN。2017 年 6 月 22 日，知名 VPN 服务商 Green 发布公告被迫停止服务。2017 年 7 月底，Apple 在中国区 App Store 下架了数百款 VPN 应用，2017 年 11 月 21 日 Apple 回复参议院 Cruz 和 Leahy 的问询时承认已下架了 674 款 VPN 应用，现在中国用户必须需要借助其他国家/地区的 Apple ID 登录外区 App Store 才能获取 VPN 应用。



#### [美国之音 | GreenVPN停止服务页面](#)

除了 VPN 之外，Apple 还在中国区 App Store 下架了纽约时报和 Skype，你同样只能在外区商店获取这些应用。

#### (二) 逃离“云上贵州”

迫于中国出台的《网络安全法》要求网络服务提供者将数据储存在本地的强制规定，Apple 在 2018 年 2 月底将中国区的 iCloud 服务转交“云上贵州”运营。新的 iCloud 隐私条款增加了要求用户“理解并同意，苹果公司和云上贵州有权访问您在此服务中存储的所有数据，包括根据适用法律向对方和在彼此之间共享、交换和披露s所有用户数据（包括内容）的权利。”此举显然降低了中国强力部门获取本国苹果用户数据的门槛，

如果你对“云上贵州”感到不安，那么你同样需要一个外区 Apple ID，然后将自己的云端数据转移到外区 iCloud 上。



### iCloud 新老用户条款对比

参见：

- [Solidot | iCloud（中国）将由云上贵州运营](#)
- [中国数字时代 | 【立此存照】iCloud 将由贵州政府掌控国企运营 可访问所有数据](#)

## 二、换区还是注册新 ID?

获取美区 Apple ID 的方式主要有将中国区 Apple ID 迁移至美国区（简称“换区”）和注册新的美区 Apple ID 两种。

美区 Apple ID 的作用在于下载 VPN 等在中国区商店被下架的应用，并保证你的 iCloud 数据不受中国政府直接控制。Bilibili、网易云音乐、共享单车类应用和部分游戏等只供中国区 App Store，如果你有这些应用的使用需求则还需保留中国区 Apple ID。编者建议同时使用中国区、美国区两个账号，并将美区 Apple ID 作为主力使用，必要时切换登录中国区 Apple ID 购买所需的应用。

## 三、如何获取美区 Apple ID

## (一) 注册美区 Apple ID 教程

- [App Store 注册美区 Apple ID 帐号终极指南 | archive 存档](#)

- [91yun | 教程：一步步教你如何注册美区 Apple ID，到美区 APP Store 下载应用](#)

- [VPNASK: VPN翻墙程序在中国区 App Store 被苹果下架，你只需要申请一个美国区 Apple ID 就可以恢复正常! | YouTube 视频教程](#)

## (二) 中国区 Apple ID 迁移至美区教程

★ [更改 Apple ID 国家或地区 - Apple 支持](#)

- [坚果极客：全局代理+原生IP，手机上也能更改Apple ID地区！](#)

## (三) 如何实现原生 IP 全局代理

注册新 Apple ID 与 Apple ID 换区时都必须提供付款方式，并且仅支持对应国家/地区银行发行的信用卡或借记卡。以美国为例，只有美国银行发行的银行卡才能在美国 App Store 消费，由中国银行发卡的银联+Visa/Mastercard 双标卡或单标卡是不被支持的。

如果你没有对应国家的信用卡，必须在注册或换区时使用对应国家地区原生 IP 全局代理以保证“支付方式”中显示“None”选项。对于“先有鸡还是先有蛋”的问题，下面就不同的场景提供几种解决方法。

场景 1: 使用 iPhone 注册美区 Apple ID，该 iPhone 上已经安装有可用的 VPN 应用或者 Shadowsocks/V2Ray 客户端且有可用的节点

**【无需额外步骤】**注册时打开 VPN / Shadowsocks 客户端使用全局代理 (Global) 模式即可。

场景 2: 使用 iPhone 注册美区 Apple ID，该 iPhone 上未安装任何可用的 VPN 应用

解决方法 2.1

**【下载、使用中国区 VPN 救急】**在中国区 App Store 中搜索“VPN”还能找到漏网之鱼，你可以使用提供美国线路的 VPN 服务来救急。

解决方法 2.2

请已有美国 VPN/Shadowsocks/V2Ray 节点或者肉身位于美国的 iPhone 用户代为注册。

### 解决方法 2.3

如果无法独立注册美区 Apple ID 作为过渡，可以考虑在淘宝购买美区 Apple ID 账号。购买使用此类产品存在风险，建议只用作临时使用。

## 四、美区 Apple ID 的日常使用

### (一) 如何使用美区 Apple ID 购买 app

1. 【充值】使用 Visa/Mastercard 双币卡在 [Apple 官网](#) 购买美区 iTunes Gift Card 礼品卡，或者在美国的超市、便利店购买实体礼品卡进行充值。

\*注意是用于 iTunes 和 App Store 的礼品卡，勿将其与购买硬件的 Apple Store 礼品卡混淆。

参见：

- [Apprcn: 使用双币信用卡在苹果官网购买美区 Gift Card 礼品卡](#)

2. 在淘宝、闲鱼等平台购买美区 Gift Card 礼品卡（请尽量选择小面额卡以规避风险），充值后使用。

3. 家庭共享

4. 找人代付（借助 App Store 的赠送礼品功能）

### (二) App Store 快速换区

#### 1. 捷径动作

在 App Store 下载自动化流程应用 捷径/Shortcuts（原 Workflow）后打开链接 [AppStore换区](#) 以获取。

#### 2. Pin - JSBox Lite - 区域切换

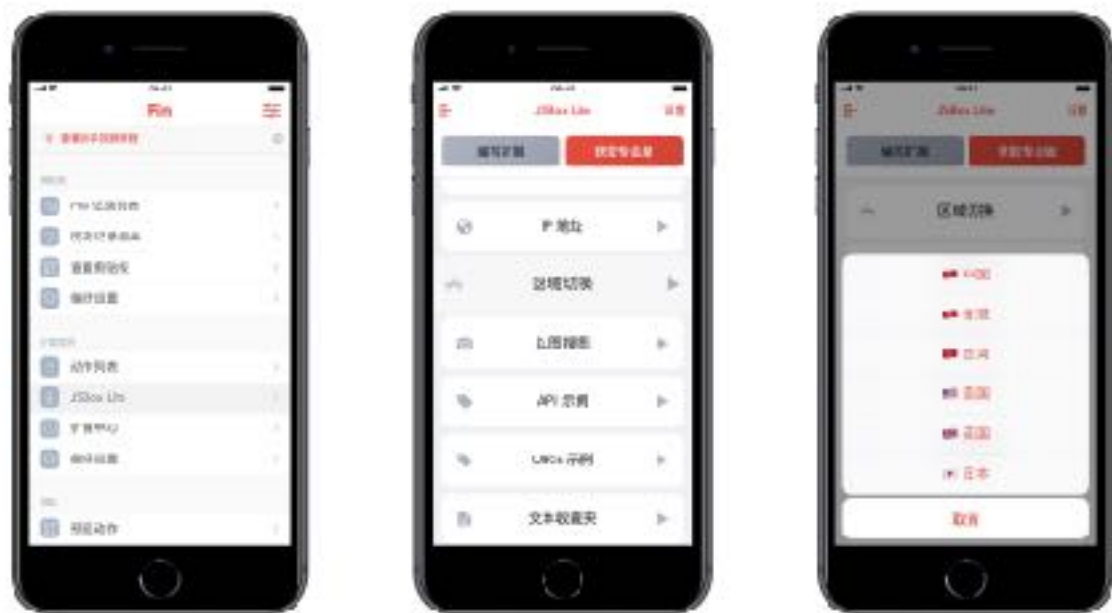
Pin (iOS) ¥18 / \$2.99

智能剪贴板应用 Pin 3.0 新上线了「xTeko 实验室」（现已改名为「JSBox Lite」），支持基于 Javascript 的扩展程序。JSBOX Lite 内置的“商店”提供的「区域切换」扩展支持一键切换至 中国/香港/台湾/美国/英国/日本区 App Store 商店。

操作方法 1：下拉打开 iOS 通知中心插件 Widget，点按 JSBox Lite 菜单中的「区域切换」进入

操作方法 2：或进入 Pin 应用，JSBox Lite > 商店 > 工具 > 区域切换（点按右侧的“▶”按钮以运行）





### 3. JSBox - 区域切换

如果你有能力自行编写 JavaScript 脚本，可以考虑购买使用功能更全面的 JSBox。

补充：

1. 可参考 Telegram 频道 [ShadowrocketNews](#) 以获取更多 Apple ID 换区及注册的信息
2. 强烈建议在注册 Apple ID 时使用 Gmail 等国外邮箱作为账号。
3. 如果你已经下载了 VPN 应用并打算继续使用中国区 Apple ID，你可以通过以下两种方法在不换区/不切换 Apple ID 的前提下更新中国区已下架的 VPN 应用：

方法1. 【卸载、重装应用】（仅适用于运行 iOS 11 及以上系统的设备）设置 > 通用 > iPhone/iPad 储存空间 > （全部显示）> 选中需要更新的应用 > 卸载应用（Offload App）> 重新安装应用

参见 [iOS 11 免换区更新其它区或已下架 App | 每日一技 - 少数派 | archive 存档](#)

方法2. 【iMazing】在 Mac/Windows PC 上下载使用 iMazing 获取已下架应用的 IPA（iMazing 可以理解为 iTunes 的第三方客户端）

以下教程来自 Telegram 频道“Shadowrocket News”，原链接 <https://t.me/ShadowrocketNews/199>

iMazing 下载 IPA 教程（编者注：以 Shadowrocket 为例）

使用 iMazing 进行下载安装（<https://imazing.com>）

1. 下载安装 iMazing，试用即可
2. 连接手机
3. 在左侧找到 Apps
4. 点击 Manage Apps 按钮
5. 确认右上角的 Apple ID 为 Shadowrocket 的购买 ID，不是的话选择 Log Out 重新登录

6. 选择 Add from App Store
7. 搜索关键字 Shadowrocket 下载并安装

方法3. 【TestFlight】使用应用的 TestFlight（简称“TF”）版本也可以实现不切换 Apple ID 使用最新版应用。

## 第二节 获取 Google Voice

\* Google Voice 号码是为之后注册 Telegram 准备的，并非必需品。如果你已经拥有境外号码可以跳过本节内容。

### 一、Google Voice 是什么？

Google Voice 是由 Google 推出的 VoIP 服务，它允许用户使用 Google 提供的免费号码或付费指定的号码来集成用户个人的众多电话号码，并在美国和加拿大提供的免费语音通话和短信服务。

### 二、为什么选择 Google Voice？

Google Voice 的优势在于支持免费、长期保留号码。

TextNow 等虚拟号码服务只提供临时号码。Telegram 每次登录账户都需要接收短信验证码，如果你使用临时性虚拟号码或者出境时购买的临时电话卡号码注册 Telegram，当号码过期被回收或者临时电话卡到期后你若中途登出 Telegram 账户，再次登录时就会因收不到短信验证码而无法登录。

Voxox、Pinger、FreeTone 等虚拟号码服务商提供的是订阅制服务，你可能需要每年支付十几美元的费用来保留你的虚拟号码。

参见 Yhio 酱的推文

<https://twitter.com/yh1318447499/status/1077898341193703424?s=12>

“针对最近推友因为绑定+86手机号出现的各种问题 还是要提醒推友们 ①一定不要绑定+86的手机号和国内邮箱，可以绑定Google Voice, Voxox, Pinger, 或者freetone ②开启登录两步验证 Google验证器挺好用的 🤖 虽然网络没法做到完全匿名，但是咱们还是要尽最大努力保护自己，快到年关了希望推们都平平安安的”

### 三、Google Voice 号码的用途

1. Google Voice 可用于匿名注册加密即时通讯应用 Telegram，原理部分会在 Telegram 的章节提及。
2. Google Voice 可作为国外网络服务的验证号码及接受验证短信，例如美区 PayPal 等。不过 Twitter 等部分网站会识别出 Google Voice 的虚拟号码属性，并且不支持将虚拟号码作为验证号码以防止用户滥用。

### 四、如何获取 Google Voice 号码?

获取 Google Voice 号码主要有在线申请 Google Voice 号码和向号码拥有者付费购买号码两种方式。

注：你需要拥有 Google 账号（Gmail 账号）才能登录 Google Voice 服务。建议在手机 Gmail 客户端应用注册新账号以提高成功率，注册完成后建议立即添加「验证邮箱」以确保变更代理 IP 后还能正常登录。

#### （一）Google Voice 号码申请教程

Google Voice 号码本身是免费申请的，但随着用户数量增多其申请难度也水涨船高。申请时往往会显示失败，需要持续点击不断尝试，并可使用鼠标连击脚本或应用用以辅助申请，但仍不能保证成功申请。如果你长时间尝试都无法获取号码，可以考虑购买一个 Google Voice 号码。

参见：

- [墙洞说：免费申请 Google Voice 美国电话号码 | archive 存档](#)

#### （二）Google Voice 号码购买教程

Google Voice 号码原本在淘宝平台有售，普通号码（非靓号）的售价一般在 CNY ¥15 - ¥20 之间，但此类店铺不定期会遭到淘宝封杀。

以下是 Telegram 群聊 [Google Voice 交流群](#) 的 [置顶消息](#) 中提供的几位卖家：

@BHGchinaboy (JUN LEE)

@daydzcom (北美快运)

@gv\_special (C Y) 主要售卖 gv 靓号

@Googlevoice\_00 (Google Voice)

其他购买渠道请自行搜索。

Google Voice 卖家发送的商品信息一般包含以下要素：Gmail 账号、Gmail 登录密码、验证邮箱和 Google Voice 号码。部分卖家允许你修改密码和验证邮箱后直接使用；部分卖家需要回收其 Gmail 账号再利用，会要求你将 Google Voice 号码移转到自己的账户上。

参见 Google Voice 号码移转视频教程（需翻墙）[Transferring a Google Voice Number](#)

附 Telegram 群聊 Google Voice 交流群 [置顶消息](#) 中的部分教程链接：

- [Google Voice 申请快速入门](#)
- [如何利用脚本辅助申请Google Voice号码](#)
- [在手机APP上使用GV号收发短信、接拨电话](#)
- [长久保留申请的 Google Voice 号码](#)
- [谷歌帐号的注册和如何防止被封](#)
- [谨慎绑定新版谷歌语音](#)
- [在国内如何使用 Google Voice ?](#)
- [Google Voice 转移](#)（此为 Telegram 群聊中的一份 pdf）
- [Goolge Voice 申请详细方法及注意事项](#)
- [Google voice注册美国手机号](#)

## 五、如何长期保留 Google Voice 号码

Google 会回收超过半年未使用的 Google Voice 号码，对此你可使用 IFTTT 脚本 [Keep Google Voice](#)，令其每月自动拨打你的号码来起到长期保留 Google Voice 号码的作用。

IFTTT 是互联网自动化服务平台，是“if this then that”的首字母缩写，读作“ift”（相当于“gift”的“g”不发音）。初次使用 IFTTT 需要注册，也可以直接使用 Google 或 Facebook 账户登录。

参见：[长久保留申请的 Google Voice 号码](#)



除 IFTTT 的脚本外，你还可以将自己的 Google Voice 号码与其他网络服务相绑定，从而可以定期或者频繁收到来自该服务商的通知短信，避免号码被回收。

参见：[印象笔记|科技 NEWS 活跃 Google Voice，防止被回收的方法：定期拨打电话或发短信出去](#)

拨打电话：

- \* 中文播放新闻：+1 (641)793-7058
- \* Apple 软件升级中心：+1 (888)840-8433
- \* 微软客户服务：+1 (800)642-7676
- \* 美国之音：+1 (712)775-9189

发送短信：

- \* Cloudflare 查 DNS：+1 (833)672-1001

## 六、Google Voice 日常使用

你可以使用 Gmail 邮箱接收来自 Google Voice 的短信消息，无需打开网页版 Google Voice。

在移动设备上你可以使用谷歌环聊（Hangouts）应用。

参见：

- [数字移民 | 获取一个美国手机号，Google Voice 攻略全记录 \(2018-08-30\)](#)

## 第三节 注册美区 Paypal

### 一、为什么需要美区 PayPal ?

PayPal 是第三方电子支付平台，类似于中国大陆的支付宝。美国的网络服务往往需要美国的信用卡和 PayPal 作为支付手段，而美区 PayPal 作为第三方平台支持中国国内的 Visa/Matercard 双币信用卡付款，帮助中国用户走出来没有美国信用卡可用的窘境。此外使用 PayPal 而非中国国内的支付宝可避免相关交易信息被阿里和 Big Brother 获取，更利于保护个人人身安全。

美区 PayPal 可用于绑定美区 Apple ID，还可用于支付虚拟专用服务器（VPS）的租赁费用。如果你选择购买礼品卡为 Apple ID 充值，也不想 VPS 上自行搭建 Shadowsocks/V2Ray 翻墙服务，则没有必要注册美区 PayPal，大可略过本小节。

### 二、如何注册美区 PayPal ?

美区 PayPal 注册时需要提供美国的手机号码，这里可以用到上节的 Google Voice 虚拟号码。此外注册过程中并没有什么难点。

参见：

- [教程：美区 Apple ID 绑定 Paypal，无需美国信用卡也能买买买](#) (2018-01-11)
- [数字移民 | 教程：美区 Apple ID 绑定 Paypal，无需美国信用卡也能买买买](#) (2018-06-04)

## 第二章 如何突破网络封锁

### 第四节 “翻墙”基本原理

### 第五节 V2Ray

#### 一、V2Ray 简介

##### (一) V2Ray 的定位

##### (二) V2Ray 的优缺点

###### 1. V2Ray 的优势

###### 2. V2Ray 的缺点

##### (三) Project V 官网与交流群

##### (四) V2Ray 获取渠道

##### (五) 小结

#### 二、如何使用 V2Ray

##### (一) 服务器端

###### 1. 购买 V2Ray 节点

###### 2. 租用 VPS 自建 V2Ray

##### (二) 客户端

#### 三、捐助支持 Project V

### 第六节 Shadowsocks

#### 一、Shadowsocks 发展简史

#### 二、Shadowsocks 与 VPN 的区别

##### (一) 涉及目的

##### (二) 代理模式

##### (三) 流量特征

##### (四) 直观体验

#### 三、如何使用 Shadowsocks

##### (一) 服务器端

###### 1. 购买商业服务

###### 2. 使用共享节点

###### 3. 租用 VPS 自建 Shadowsocks

##### (二) 客户端

###### 1. 客户端的选择

###### 2. 客户端的使用

### 第七节 其他翻墙手段概要与评析

#### 一、翻墙手段一览

#### 二、对部分翻墙手段的评析

##### (一) VPN

##### (二) 自由门、无界网络

##### (三) Lantern 蓝灯

- (四) Psiphon 赛风
- (五) 翻墙浏览器与浏览器插件
- (六) Tor + Meek
- (七) Outline
- (八) Project Fi

### 三、通用翻墙手段难易度汇总

## 第四节 “翻墙”基本原理

“翻墙”的前提是知道“墙”/ GFW 的存在。根据维基百科对“防火长城/ GFW”这一词条的界定，防火长城 (Great Firewall, GFW) 是中华人民共和国政府在其互联网边界审查系统的统称。此系统起步于1998年，其英文名称得自于2002年5月17日 Charles R. Smith所写的一篇关于中国网络审查的文章《The Great Firewall of China》，取与 Great Wall (长城) 相谐的效果，简写为 Great Firewall，缩写 GFW。随着使用的拓广，中文“墙”和英文“GFW”有时也被用作动词，网友所说的“被墙”即指网站内容被防火长城所屏蔽或者指服务器的通讯被封，“翻墙”也被引申为突破网络审查浏览境内外被屏蔽的网站或使用服务的行为。

参见：

- 品葱：防火长城 (GFW) 的设计原理是什么？
- 端传媒：道高一尺，墙高一丈：互联网封锁是如何升级的
- 阅后即焚：GFW的前世今生，一部GFW之父方滨兴的发家史

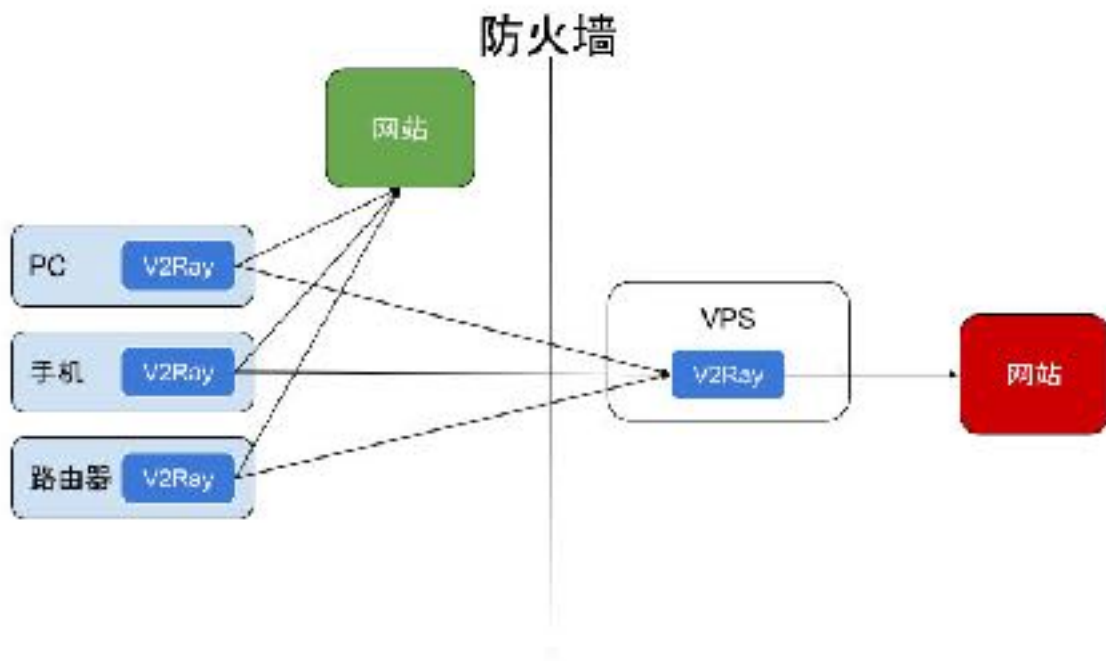
被 GFW 屏蔽的网站包括但不限于不受中国政府（或者说是中共）欢迎的网站，具体名单参见 维基百科 - 中华人民共和国被封锁网站列表、中国数字时代 - 翻墙必读 - 被墙网站。GreatFire Analyzer 提供网站是否被 GFW 屏蔽的测试。

GFW 并不是实体的墙，而是一系列网络封锁手段的统称，包括“域名解析服务 (DNS) 缓存污染、针对境外的 IP 地址封锁、IP 地址特定端口封锁、无状态 TCP 连接重置、对加密连接的干扰、TCP 关键字阻断、对破网软件的反制、间歇性完全封锁、深度包检测、针对 IPv6 协议的审查、对电子邮件通讯的拦截和网络攻击”。

翻墙的方式有数十种之多，但其基本原理不外乎通过连接代理服务器来绕开 GFW 的封锁（比如你无法访问谷歌的服务器 A，但你可以直接访问未被 GFW 屏蔽的境外代理服务器 B，由不受 GFW 之限的 B 访问 A，然后再将从 A 处取得的数据转发



给你)，这一过程中使用的代理模式主要由 Socks、HTTP 和 VPN 三种。关于 GFW 封锁技术与翻墙手段的演进，推荐阅读 Project V (V2Ray) 开发者 Victoria Raymond 的 [v2ray: 简单介绍一下网络连接的封锁与反封锁 一文](#)。



V2Ray 单服务器模式示意图

图片来自 Project V 官网 [原图地址 \(已失效\)](#)

参见 [Project V - 使用方式 - 工作机制 - 单服务器模式](#)

\*在中国大陆，不少人用“科学上网”来指称“翻墙”以规避审查，2017 年又新生了“爱国上网”一词。出于维护言论自由、拒绝自我审查，以及避免“黑话”太多给新人造成困惑的综合考量，本书通篇采用直白的“翻墙”一词，特此说明。



## 第五节 V2Ray

### 一、V2Ray 简介

V2Ray 是一个模块化的代理软件包。

#### (一) V2Ray 的定位

V2Ray 将自身定位为一个功能强大的平台，而非单纯的协议或软件，它除了自有的 Vmess 协议外还直接支持 Shadowsocks、Socks 等协议。它可以让使用者自行选择各种模式和组合，通过不同的设定来达到不同的代理效果，以此对抗变化着的 GFW。

参见：[V2Ray 的模块化](#)

#### (二) V2Ray 的优缺点

参见 [V2Ray 白话文教程 - 前言](#)

#### 1. V2Ray 的优势：

“ (1) 更完善的协议: V2Ray 使用了新的自行研发的 VMess 协议，改正了 Shadowsocks 一些已有的缺点，更难被墙检测到

(2) 更强大的性能: 网络性能更好，具体数据可以看 V2Ray 官方博客

(3) 更丰富的功能: 以下是部分 V2Ray 的功能

mKCP: KCP 协议在 V2Ray 上的实现，不必另行安装 kcptun

动态端口: 动态改变通信的端口，对抗对长时间大流量端口的限速封锁

路由功能: 可以随意设定指定数据包的流向，去广告、反跟踪都可以

传出代理: 看名字可能不太好理解，其实差不多可以称之为多重代理。

类似于 Tor 的代理

数据包伪装: 类似于 Shadowsocks-rss 的混淆，另外对于 mKCP 的数据包也可伪装，伪装常见流量，令识别更困难

WebSocket 协议: 可以 PaaS 平台搭建 V2Ray，通过 WebSocket 代理。

也可以通过它使用 CDN 中转，抗封锁效果更好

Mux: 多路复用，进一步提高科学上网的并发性能”

“VMess 协议的特征是在目前常见协议中最弱的。即如果你认为 VMess 具有某个特征，那么在 ss/ssr/其它协议中一定存在同样或更强的特征；反之则不然。”

“关于 TLS 混淆，V2Ray 用的是真 TLS，即完全符合 TLS 协议；Shadowsocks 的 obfs 和 ShadowsocksR 的 TLS 混淆用的均为假 TLS，即只模拟了部分 TLS 协议。真 TLS 的优势是服务器端防探测，第三方用任意的 TLS 数据包探测，V2Ray 都能做出合理的响应，而假 TLS 则带有明显的特征。真 TLS 会有首次连接时进行一个两次通信(2-rtt)的握手，比起假 TLS 略慢，但之后的连接中，由于使用了缓存，握手不会有性能差异。”

## 2. V2Ray 的缺点

- (1) 配置复杂
- (2) 产业链不成熟

### (三) Project V 官网与交流群

官网: <https://www.v2ray.com/>

公告: <https://t.me/v2msg>

吹水: <https://t.me/joinchat/AAAAAEIYaH-hjDDZS716jg>

使用: <https://t.me/projectv2ray>

开发: <https://t.me/joinchat/DNcazUMxm77Jt0LQuwiGAQ>

推特: <https://twitter.com/projectv2ray>

Telegram 讨论组规则见: [https://www.v2ray.com/chapter\\_00/tg.html](https://www.v2ray.com/chapter_00/tg.html)

### (四) V2Ray 获取渠道

Github Release: [github.com/v2ray/v2ray-core](https://github.com/v2ray/v2ray-core)

IPFS: [/ipfs/QmdtMuAhEUPFX9NQiGhRj2zhS1oEA76SXNDnZRHqivjMwR](https://ipfs.io/ipfs/QmdtMuAhEUPFX9NQiGhRj2zhS1oEA76SXNDnZRHqivjMwR)

IPFS 分流: <https://v2ray.com/download>

### (五) 小结

V2Ray 可能是目前最具前景的翻墙手段，但它对于那些没有 Linux 基础或者 VPS 使用经验的入门者难度相对较高。如果你看完本节、Project V 官网和白话文教程后仍然一头雾水，建议先阅读 HyperApp 的相关教程，借助 HyperApp 部署 V2Ray。

HyperApp 是 iOS 平台上一个基于 SSH 和 Docker 的自动化部署工具，允许用户在图形化界面下将应用一键部署到 VSP 上，详见 HyperApp 用户文档：<https://www.hyperapp.fun>。

注：Project V 与 V2Ray 的关系：V2Ray 升级到 3.0 后正式扩展为 Project V，除了 V2Ray 本身之外，Project V 包含所有 V2Ray 的周边产品，包括客户端、配置工具等。

## 二、如何使用 V2Ray

### (一) 服务器端

#### 1. 购买 V2Ray 节点

经营 V2Ray 的服务商正在不断涌现，但目前的数量较为有限，产业规模尚不及 Shadowsocks 及其衍生协议。以下 V2Ray 服务商信息引自 [Project V 官网 - 一些推广](#)（最后一次访问于 2019 年 2 月 1 日）：

#### BabyDriver

支持 V2Ray 的 VPN 服务。优惠码：bcb518

#### 喵帕斯

V2Ray 小范围内测中。

#### 蓝岸

基于 V2Ray 的网络加速服务。优惠码：v2ray

#### 多数派

基于 V2RAY 的全新的网络加速服务

#### V2rayPro

基于 V2Ray 的网络加速服务。专属优惠码：v2ray.com

#### vProxy

由 V2Ray 驱动的网络加速器。专属优惠码：v2ray.cool

#### 栖息地

对内小众的 V2ray 优质网络加速服务。邀请码：V2RAY

NicoNode

支持 V2Ray 的网络加速改善服务。专属促销代码：V2RAYNOW

V2Net

## 2. 租用 VPS 自建 V2Ray

### (1) VPS 简介

VPS 是 Virtual Private Server 的缩写，中文名称是虚拟专用服务器，指将一台服务器分区成多个虚拟专享服务器的服务。本文主要介绍将 VPS 用作代理服务器用于翻墙，此外 VPS 还具有搭建博客、私人云盘等诸多用途。

常见的 VPS 厂商有：GCP (Google Cloud Platform, 提供为期一年、价值\$300的免费试用)、AWS、Vultr、Linode、Bandwagon、DigitalOcean 等。

VPS 的选择和入门教程可参考：

- [HyperApp 用户文档 - 各云厂商使用教程](#)
- [HyperApp 用户文档 - 爱国软件 - 科学上网综述](#)
- [HostAdvice: 2018最佳VPS主机公司](#)

\*Bandwagon 等 VPS 厂商现已支持使用支付宝付款，安全起见还是建议使用 PayPal 等不受国内直接监管的支付手段作为付款方式。

购买 VPS 后建议先测试能否在国内直接连接这台 VPS，为此你需要一个 SSH 客户端。如果你使用 Linux 或 macOS 操作系统，你可以直接使用系统自带的“终端”应用；如果你使用 Windows，你需要下载 SSH 客户端应用，常见的有 Xshell、PuTTY、KiTTY、MobaXterm、mRemoteNG、Bitvise SSH 客户端（更多参见：[维基百科 - SSH 客户端比较](#)）；在 iOS 设备上可以使用 SSH 客户端 Terminus 来操作 VPS。

以“终端”应用为例，先关闭 VPN 或 Shadowsocks 等代理工具，在“终端”中输入以下字符后回车：

```
ping 你的 VPS IP #例如 00.00.00.00
```

注：“#”后的内容是注释，不会作为命令代码运行，下同

如果能接收数据则证明能够直连，之后可按下“Control+C”来中止这一进程。如果不能直连则说明该 IP 可能已被 GFW 屏蔽，建议将其注销另租一台。

## (2) 常用 Linux 命令

### ① 远程登录 Linux 主机 / VPS

远程登录和操作 VPS 同样需要用到 SSH 客户端应用。以“终端”为例，下同。

输入以下字符后回车：

```
ssh root@你的 VPS IP #例如 00.00.00.00
```

初次登陆可能需要在 (yes/no) 选项下输入“yes”，然后输入你的 VPS 登录密码（VPS 网页中获取），需要注意的是此时输入的密码在应用界面下并不可见，输入完毕后回车，如果密码无误即可成功登录。

### ② 退出登陆

输入“exit”后回车

### ③ 使用 cd 前往指定目录

输入 cd + 目录，例如：

```
cd /etc/v2ray/
```

需要退出 cd 时输入“cd”后回车即可。

### ④ 使用 vim 或 vi 修改配置文件

以 V2Ray 为例，输入“vim config.json”进入 vim 界面。vim 界面下不能直接编辑配置文件，但可以通过连击“D”键删除光标所在行。如需修改或插入内容，需要依次按“esc”、“I”和“Enter”键进入可编辑的“Insert”模式（底部会出现 Insert 字样），之后你可以之后修改，或者将所有内容删除后粘贴已经在其他编辑器中写好的配置信息，完成后按“esc”键退出“Insert”模式。输入“:w”后回车以保存，输入“:q”回车退出，也可以输入“:wq”回车一步到位。

## (3) 如何部署 V2Ray 服务器端

如果你选择使用 HyperApp 搭建 V2Ray，请参考：

[HyperApp 用户手册 - 爱国软件 - V2Ray](#)

如果在 Linux 下部署，请参考以下教程：

- [Project V - 下载安装](#)

- [Project V - 新手上路](#)

- [V2Ray 白话文教程](#)

### ① 使用 SSH 登录 VPS，输入：

```
ssh root@00.00.00.00 #你的服务器 IP
```

## ② 修改时间

使用 Vmess 协议必须保证本地和服务端的时间差不超过一分钟，因此需要修改 VPS 的系统时间：

```
rm -rf /etc/localtime #先删除默认的时区设置
ln -s /usr/share/zoneinfo/Asia/Shanghai /etc/localtime #替换上海作为默认
```

或者使用“date --set”：

```
sudo date --set="2018-01-01 00:00:00"
```

查看时间：

```
date -R
```

## ③ 使用 Linux 脚本安装 V2Ray（更新 v2ray-core 时同样使用此脚本）

```
bash <(curl -L -s https://install.direct/go.sh)
```

此部分请参考：[Project V - 下载安装](#)

运行 `service v2ray start` 来启动 V2Ray 进程，使用 `service v2ray start | stop | status | reload | restart | force-reload` 控制 V2Ray 的运行

## ④ 编辑配置文件

```
cd /etc/v2ray/
vim config.json
```

参考上文 vim 的用法编辑你的配置文件，输入“:wq”回车来保存和退出。

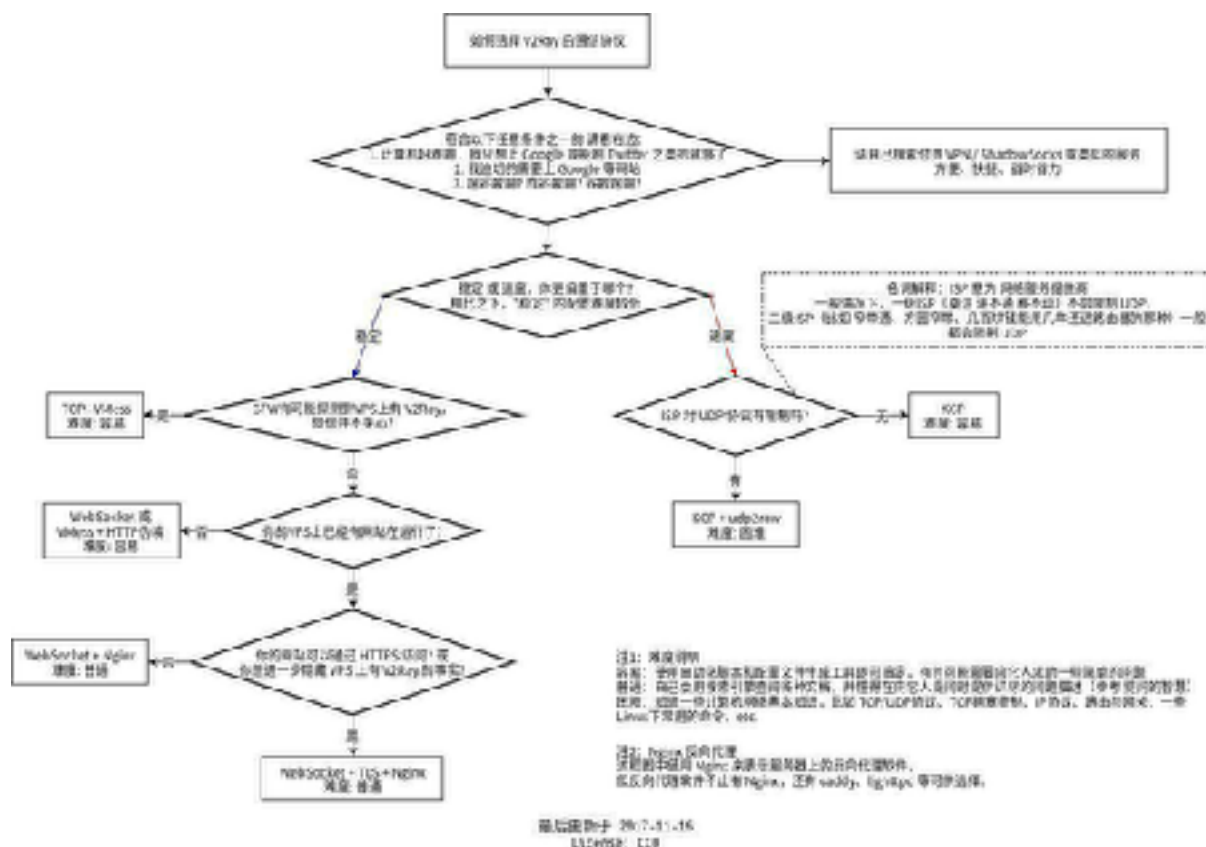
## ⑤ 重启 V2Ray 并查看是否正常运行

```
systemctl restart v2ray
systemctl status v2ray
```

如果显示红色的 failed 表明你的配置有误，V2Ray 无法正常运营。V2Ray 本身提供了检查功能，输入：

```
usr/bin/v2ray/v2ray -test -config /etc/v2ray/config.json
```

来检测 config.json 是否有误。



[https://raw.githubusercontent.com/KiriKira/vTemplate/master/How\\_To\\_Choose.jpg](https://raw.githubusercontent.com/KiriKira/vTemplate/master/How_To_Choose.jpg)

关于 V2Ray 的模式选择，可以参考上图。Vmess 裸奔的难度最低，可参考 [Project V - 新手上路](#)。（事实上 Vmess 协议本身的强度已经足够了，如果担心 VPS 的 IP 被 GFW 屏蔽可以购买 CDN 加速服务隐藏真实 IP，具体方法请自行搜索）

TCP + TLS 可以参考 [白话文教程 - TLS](#)。使用 TLS 需要域名和 SSL 证书，域名可以从 [Freenom](#) 免费获取，或者从 [Namecheap](#) 购买廉价域名；SSL 证书可由 acme.sh、Caddy、Nginx、certbot 等应用自动注册，详见 [VINGA: 免费获取个人专属顶级域名](#)、[白话文教程 - TLS](#)（购买域名后需要添加一个 A 记录指向 VPS 的 IP，之后若 ping 域名可以 ping 通且显示 VPS 的真实 IP 则表明域名已经解析成功）。WS+TLS+Web 可能是目前最好的模式，但难度也相对较高，新手可以借助 HyperApp 来辅助搭建。

关于 V2Ray 使用教程的选择，建议先看懂 [Project V 官网](#) 和 [白话文教程](#)，如有需要再搭配其他博客上的教程和配置模板。对于后者，编者建议认准同一份教程，因为不同作者采用的方法和使用配置文件之间存在差异，对新手而言同时参考多份教程可能会使你的思路越来越混乱。

如果在配置过程遇到问题，建议先自行搜索相关信息，在 Github 上查看 [v2ray-core](#) 已有的 [Issue](#)，或者在 Telegram 群组 [Project V \(使用与反馈\)](#) 中搜索英文关键



字查看聊天记录中的类似问题。如果问题仍未解决，可以在该群组中提问，或者参照模板在 Github 上提交 issue。

相关工具：

- [V2Ray 配置生成器](#)

其他教程：

- [KIRIKIRA.MOE](#)

- [Kiri | 五分钟入门V2Ray](#)

- [Kiri | 链式代理与透明代理：V2Ray 的进阶用法](#)

★ [YEARLINY | V2Ray完全使用教程](#)

- [IVY SEEDS - 科学爱国 - V2Ray](#)

- [abccit: 安装 V2Ray 配置 WebSocket+Nginx+TLS](#)

- [科学上网翻墙教程：搭建V2Ray翻墙](#)

★ [YouTube | 刘伟教程：零基础手把手教你搭建V2ray翻墙Linux/Windows/MacOS/安卓/苹果](#)（如果你是 VPS 和 Linux 新手，可以在 YouTube 上搜索、观看相对直观的视频教程来加深了解）

关于 V2Ray 的常见问题可以在私聊模式下向 Telegram bot [Kiray](#) (a V2Ray FQA bot by Kiri, username: @kiraybot) 提问，该 bot 目前收录了 36 个问题（最后一次访问于 2018 年 5 月 29 日），可以以 Q&A 的形式呈现答案。请勿在群组中使用该 bot，以免刷屏给其他成员造成困扰。

## （二）客户端

V2Ray 客户端

macOS: [V2RayX](#)、[V2RayU](#)、[V2RayC](#)、[ClashX](#)

iOS: [Kitsunebi](#)、[Kitsunebi Lite](#)、[i2Ray](#)、[Shadowrocket](#)、[Pepi](#)、[Quantumult](#)

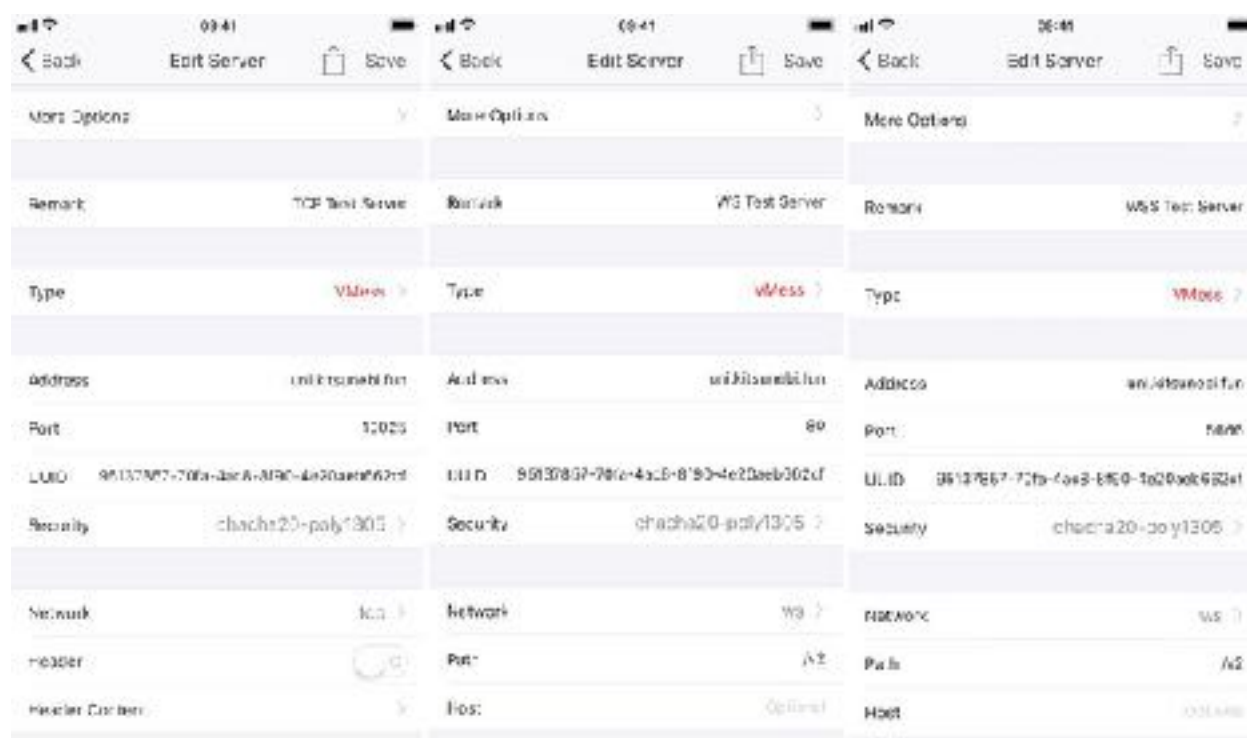
Android: [BifrostV](#) (PlayStore)、[V2RayNG](#) (PlayStore) 等

Windows: [V2RayW](#)、[V2RayN](#)、[V2RayS](#) 等

★ 参见：[Project V - 神一样的工具](#)（最后一次访问于 2019 年 2 月 10 日）

\* iOS 客户端 Kitsunebi 和 i2Ray 均使用了 V2Ray Core

如果你使用 Kitsunebi，可以根据你对服务器端配置，参考 Kitsunebi 内置测试服务器的 TCP、WS、WSS、H2 和 KCP 五种模式的节点信息来填写添加。其他平台的图形化客户端的配置方法与之基本相同。



以 Project V 官网上“新手上路”教程为例，在客户端添加节点信息时，协议类型 (Type) 选择“Vmess”，地址 (Address) 填写自己 VPS 的 IP 或域名，端口 (Port) 填“10086”，UUID 与服务器端保持一致，加密方式 (Security) 填“chacha20-poly1305”，传输协议 (Network) 选择“tcp”。

### 三、捐助支持 Project V

#### Project V 捐助支持

比特币 (BTC): [15dQnC9yvX6JJXaFkP9MiRYvJS3FvsqvKW](https://www.blockchain.com/transaction/15dQnC9yvX6JJXaFkP9MiRYvJS3FvsqvKW)

比特现金 (BCH): [1NNRgpWYD8UX1bkckCEoD6HHpaw98onxa](https://www.blockchain.com/transaction/1NNRgpWYD8UX1bkckCEoD6HHpaw98onxa)

以太坊 (ETH): [0x196b695ce3b44c4bd16fe43981bcc908a6a09c2e](https://www.etherscan.io/tx/0x196b695ce3b44c4bd16fe43981bcc908a6a09c2e)

莱特币 (LTC): [LVdeH2HkCgGRs8ZEpan7fkAEEPbiJ4McoR](https://www.blockchain.com/transaction/LVdeH2HkCgGRs8ZEpan7fkAEEPbiJ4McoR)

门罗币 (XMR):

48kA4NyLRCWQvB7U2A77G66Z25uWbyzmoZSYjxJfrMR1J4dRFW6fWFLDn3wirAqP8y  
SnR4rnvoXWxfkNFhrK5ZxY1WyBqKg

EOS: 0x196b695ce3b44c4bd16fe43981bcc908a6a09c2e

嫩模币 (OMG): 0x196b695ce3b44c4bd16fe43981bcc908a6a09c2e

贡献你的 CPU

## 第六节 Shadowsocks

Shadowsocks，简称 ss，既指基于 Socks5 代理方式的加密传输协议，也指实现 Shadowsocks 协议的各种传输包，是中国大陆最为流行的翻墙工具之一。

### 一、Shadowsocks 发展简史

Shadowsocks 是 clowwindy 开发的翻墙软件，经推广后因过于火爆引起了公安的关注，作者 clowwindy 被警方约谈后迫于压力于 2015 年 8 月 22 日在 Github 上删除了 Shadowsocks 项目的全部代码并停止开发。

破娃酱 (breakwa11) 接手开发了 ShdowsocksR（简称 SSR）分支，在原版 Shdowsocks 基础上提高了安全性并加入了混淆。2017 年 7 月 27 日，breakwa11 遭到自称“ESU.TV”的不明身份人士的人身攻击，对方宣称如果不停止开发 SSR 将公开更多包含个人隐私的资料。breakwa11 称遭对方人肉的是无关人士，为了防止对方继续伤害无关人士将删除 SSR 在 GitHub 上的所有代码、停止维护 ShadowsocksR 项目并解散相关 Telegram 交流群组。之后 Akkariiin 宣布接手 SSR 项目并在此基础上开发 ShadowsocksRR 分支。其他较为知名的 Shadowsocks 分支还有 Shadowsocks-libev，ShadowsocksR-python，Shadowsocks-python，Shadowsocks-go，libQtShadowsocks 等。

### 二、Shadowsocks 与 VPN 的区别

Shadowsocks 与 VPN 都被用于翻墙，常有人把 Shadowsocks 与 VPN 混为一谈，但事实上两者并不是一回事——Shadowsocks 是加密版的 Socks，而前文中已经提到 Socks 是与 VPN、HTTP 相并列的代理模式。此外 Shadowsocks 与 VPN 的区别还在于：

## （一）设计目的

Shadowsocks 的初衷就是突破网络封锁，而 VPN 原本的用途是保障恶劣网络环境下的通信安全。因此 VPN 在世界范围内被广泛使用，而只有在中国大陆、伊朗、土耳其等存在严格网络管制的地区被用于突破网络封锁。

## （二）代理模式

Shadowsocks 可以实现智能分流，即访问被 GFW 屏蔽的网址时由代理服务器转发数据，访问墙内网址时直连；也可开启全局代理，让所有的流量都走代理；此外用户可以自行修改 Shadowsocks 的配置文件，根据自身需要添加规则，实现屏蔽广告等功能。VPN 默认全局代理，即开启后所有流量都会被传输到海外服务器，只有极少数 VPN 服务提供智能分流功能。

## （三）流量特征

VPN 的流量特征很明显，GFW 已经实现对 PPTP、IPSec、L2TP 等 VPN 协议的精准识别，因而完全可以在党代会、两会、六四等具有政治敏感性的时间点上屏蔽所有 VPN 流量。就 Shadowsocks 而言，其流量特征明显弱于 VPN，GFW 仍可以通过机器学习加以识别。目前基本可以精准识别原版 Shadowsocks 协议，不过后续演化的 Shadowsocks 的流量特征会随着加密协议和混淆协议组合的不同而呈现不同的样态，GFW 尚无能力探测和屏蔽所有的 Shadowsocks 流量，目前主要采取批量封杀服务器 IP 段这样盲目粗暴的方法来对付 Shadowsocks。

## （四）直观体验

1. Shadowsocks 的连接速度快于 VPN
2. Shadowsocks 的稳定性优于 VPN  
Shadowsocks 连接以后基本不会出现断线，VPN 在网络质量不佳的情况下很容易出现断线。在长时间待机后唤醒的场景下，Shadowsocks 还能保持连接状态，VPN 基本会断线，需用户手动打开开关重连。
3. Shadowsocks 可实现智能分流，可以无缝突破 GFW 的封锁快速访问国际互联网。  
VPN 默认全局代理，在使用微信等墙内服务时网速会明显变慢。
4. Shadowsocks 的 iOS 客户端大多支持隐藏 VPN 图标的功能（iOS 平台上的 Shadowsocks 客户端应用调用了 Network Extension 接口，在连接 Shadowsocks 后顶栏也会显示“VPN”图标），可以避免你在分享手机截图或在人多眼杂的场所连接 Shadowsocks 时显示 VPN 图标。VPN 应用基本不提供隐藏 VPN 图标的功能。

## 三、如何使用 Shadowsocks

Shadowsocks 分为服务器端和客户端两部分，像 Shadowrocket 这样的 Shadowsocks 客户端本身只是一个空壳，必须手动导入 Shadowsocks 的服务器节点信息后才能连接使用。就这点而言 Shadowsocks 和 VPN 很不一样，VPN 软件基本采用客户端应用内置服务的模式，用户下载 VPN 客户端并购买服务后打开 VPN 开关就可连接。

## （一）服务器端

获取 Shadowsocks 节点的方式主要有以下几种：

1. 购买 Shadowsocks 服务商（也称“机场”、“梯子商”）提供的服务
2. 使用他人自建或购买后共享的 Shadowsocks 节点
3. 租用 VPS 自建 Shadowsocks

### 1. 购买商业服务


购买现成 Shadowsocks 服务的好处在于 Shadowsocks 服务商往往提供十几条到几十条不等的线路，在服务器所在国的选择上更多样，万一有线路被封也有回旋余地。同时 Shadowsocks 服务商持续提供技术保障，保证网速；其议价能力较强，在更换代理服务器上更有效率。此外部分厂商会提供 BGP 线路，即在连接境外代理服务器先连国内的中继服务器作中转，有利于规避 GFW 的封锁。

Shadowsocks 服务商有 [喵帕斯](#)、[rixCloud](#)、[RfcNetwork](#)、[熊猫翻滚](#) 等（请自行 Google 获取更多厂商信息及服务评价）。笔者不推荐从个人卖家处购买 Shadowsocks 服务，更不要从在 QQ 群、Telegram 群聊中兜售服务的个人卖家处购买服务，以免上当受骗。

参见 [聪聪：SS/SSR 简介 - 介绍](#)

### 2. 使用共享节点

使用共享节点的最大好处是几乎零成本，但弊端也显而易见——众多用户使用同一个节点势必导致低网速，使用体验不佳；同时也容易招致 GFW 的封杀，必须更换新的节点，稳定性无法保证。

Telegram 上有 [V2ray,SSR 节点最新发布](#)、[360 互联网安全中心](#) 等发布共享 Shadowsocks、V2Ray 节点信息的频道。更多关于提供共享 Shadowsocks 节点的渠道请自行搜索。

以 V2ray,SSR节点最新发布  提供的 SSR 节点为例，复制 URL “ssr://xxxx……xxx”后打开 Shadowsocks 客户端即可自动导入节点信息。

更多共享节点：

“免费 SS 账号分享（能不能用，能用多久我就不确定了）

<https://free-ss.site>

<https://ss.freess.org>

<https://doub.io/sszhfx>

<https://us.ishadowx.net>

[https://tool.ssrshare.us/tool/free\\_ssr](https://tool.ssrshare.us/tool/free_ssr)

SSR 免费节点订阅地址(PS：至于节点能不能用我就知道了，别人分享的)

<https://github.com/ImLaoD/sub/raw/master/ssrshare.com>

[https://github.com/ImLaoD/sub/raw/master/v2ray\\_ssrshare.com](https://github.com/ImLaoD/sub/raw/master/v2ray_ssrshare.com)

<https://yzzz.ml/freessr>

”

—— 聪聪：SS/SSR 简介 - 介绍

### 3. 租用 VPS 自建 Shadowsocks

“自建和购买商业服务对比有什么优势？

最主要的优势是隐私和安全，如果你看下上面 Shadowsocks 的日志，你就知道服务商可以知道你的所有浏览历史的，如果你访问了不支持 HTTPS 的网站，那么请求内容也可能被监控（比如密码信息）。

另外是质量和成本，很多商家是使用和上面同样的机器但是卖给几百个人，你应该能明白了。成本方面没有免费试用的话1个人用可能会有点贵，但如果和朋友家人一起用就超值了，比如使用 \$2.5/月的 Vultr，每月500G 流量够很多人用的。”

—— Hyperapp 用户文档 - 手把手爱国教程

网络上可以检索到大量的 Shadowsocks(R) 一键安装脚本。如果你不会使用 Linux 系统，可以借助 iOS 平台上的 HyperApp 应用在图形用户界面下配置安装各类 Shadowsocks 的服务端。

参见：

★ HyperApp 用户文档 - 爱国软件 - SSR

由 HyperApp 用户上传的视频教程：[YouTube | 五分钟快速建立vpn，可全程手机操作，方便快捷的一款强大软件hyperapp之ssr教程](#)（需翻墙）

## （二）客户端

### 1. 客户端的选择

#### （1）iOS

##### Shadowrocket

物美价廉的 Shadowsocks 客户端，俗称“小火箭”，支持 Shadowsocks、ShadowsocksR、Vmess 等多个协议。美区售价 \$ 2.99（CNY ¥18），中国区已下架。

##### Quantumult

新生代 Shadowsocks 客户端，TF 版支持 Vmess 协议。美区售价 \$ 4.99（CNY ¥30）中国区已下架。

参见：

[落格博客：谈谈 Shadowrocket 和 Quantumult](#)

##### Patatso 2

##### Patatso Lite

中国区已下架。轻量版的 Patatso，能满足基本的使用需求，不支持 Vmess。

##### Surge 3

美区售价 \$ 49.99（¥ 328）

不建议普通用户购买 Surge。Surge 除去 Shadowsocks 客户端外还有开发者调试工具的面向，如果你没有这方面的需求则大可选择相对便宜的应用。（注：Surge 不支持 ShadowsocksR 协议）

iOS 3 Pro Personal License \$ 49.99（Surge 官网）

#### （2）macOS

##### ShadowsocksX-NG-R

##### ShadowsocksX-NG

##### Surge for Mac

Standard License ( 1 device ) \$ 49.99

Pro License ( 3 devices ) \$ 69.99

Mega License ( 5 devices ) \$ 99.99

★更多 Shadowsocks 客户端参见 [聪聪：SS/SSR 简介 - 客户端](#)

## 2. 客户端的使用

Shadowsocks 客户端的使用方法基本相同——添加节点信息 > 选择协议类型（例如 Shadowsocks、ShadowsocksR、Socks5 等），填写主机 IP、端口、密码、加密方式、混淆协议及标签等。部分 Shadowsocks 服务商支持像客户端应用一键导入节点信息。

Shadowsocks 服务商往往会提供客户端的使用教程。

参见：

- [少数派：Shadowrocket 入门使用教程 | archive](#) 此教程写作时间较早，仍可作参考。

## 第七节 其他翻墙手段概要与评析

### 一、翻墙手段一览

1. VPN (包括 pptp, l2tp, sstp, ipsec, anyconnect, IKEv2, Open VPN 协议)
2. Lantern (蓝灯)
3. Psiphon (赛风)
4. GAE (包括 GoAgent, xx-net, GoProxy)
5. Shadowsocks
6. ShadowsocksR
7. Hosts
10. 自由门
11. VPN Gate
12. 无界
13. V2Ray
14. 浏览器翻墙插件
15. 翻墙浏览器
16. 路由器透明代理
17. 浏览器一键包
18. 萤火虫代理
19. SSH
20. Meek + Tor
21. 肉翻



- 22. 在线网页代理
- 24. obfs4
- 25. GFWPress

上述内容参考了 ShadowsocksR 开发者 breakwa11 在其 Telegram 频道（现名“ShadowsocksR已停止更新”）发布的科学上网方式占有率调查统计结果。

## 二、对部分翻墙手段的评析

### （一）VPN

与 V2Ray 和 Shadowsocks 相比，VPN 固然显得逊色，但操作简单不失为其优点——用户只需下载客户端一键连接即可，便于入门者上手。GFW 已经可以有效识别、封杀各类 VPN 协议，但也不是那么绝对，因为 VPN 本身也在进化，比如知名 VPN 厂商 Golden Frog 开发的 VyprVPN。

VyprVPN 的特色在于其专有的 Chameleon（变色龙）协议（仅限高级账户，暂不支持 iOS），原理是在 OpenVPN 协议的基础上加入混淆以对抗深度包检测 (DPI) 技术，使其 VPN 服务在中国、伊朗、土耳其等存在网络封锁的地区能够正常使用。除 VyprVPN 外，ExpressVPN 和 PUREVPN 也是网络排名较为靠前的 VPN，这三款 VPN 的客户端都覆盖全平台。

### 其他推荐 VPN 服务

“推荐以下这些 VPN 服务，它们都不在美国境内、都使用加密，并且接受 Bitcoin 付款，支持 OpenVPN 而且采用不记录用户活动的政策：

AirVPN，位于意大利，162 台服务器；AzireVPN，瑞典，5 台服务器；Cryptostorm，冰岛，18 台服务器；EarthVPN，北塞浦路斯，432 台服务器；ExpressVPN，维京群岛，145 台服务器；FrootVPN，瑞典，27 台服务器；hide.me，马来西亚，88 台服务器；IVPN.net，直布罗陀，21 台服务器；Mullvad VPN，瑞典，168 台服务器；NordVPN.com，巴拿马，475 台服务器；OVPN.com，瑞典，39 台服务器；Perfect-Privacy.com，巴拿马，41 台服务器；ProtonVPN.com，瑞士，112 台服务器；Proxy.sh，塞舌尔，300 台服务器，Trust.Zone，塞舌尔，48 台服务器；VPNTunnel.com，塞舌尔，80 台服务器。

⚠️ 挑选 VPN 提供商的标准：在美国境外或其它五眼联盟以外的国家营运；避免挑选以英国和美国为基地的服务商；支持 OpenVPN 软件；接受比特币、现

金、借记卡或现金卡等付款方式；注册帐号时不会要求提供个人信息，只需填写用户名、密码与电子邮件即可。

另外一个标准是 warrant canary，这是有些组织公布一份文件来声明他们在一段特定期间内，并未接到任何秘密的官方命令。如果这份文件未能及时定期更新，那么用户可以假设该组织可能收到了不可公开的秘密传票，此时应该停止使用他们提供的网络服务。

你可以在[这里](#)看到拥有 warrant canary 的公司和组织；在[这里](#)查看 Bruce Sneyer 对权证的批评以及针对 warrant 的法律案例。”

——[iYouPort | 安全手册：这里是你需要的几乎所有安全上网工具；以及为什么建议不要使用以美国为基地的网络服务](#)

注：推荐 VPN 处的超链接为本书编者所加。

参见：[iYouPort | 安全手册：这里是你需要的几乎所有安全上网工具；以及为什么建议不要使用以美国为基地的网络服务](#)

## （二）自由门、无界网络

自由门和无界网络是目前世界范围内较为流行的翻墙软件，二者都有法轮功背景，且都没有开源。

## （三）Lantern 蓝灯

Lantern 是一款开源的翻墙软件，支持 Android、Windows、macOS 和 Linux 平台，iOS 版也在开发中。最新版（4.0版）的 Lantern 提供付费专业版和免费版两种版本，其中免费版有每月 500 MB 的免费高速流量，超出流量上限后仍可翻墙，但会被限速。

Lantern 打开客户端即可连网，很好上手；速度和稳定性都优于 Psiphon，适合对翻墙上网需求不高、无力驾驭 Shadowsocks 又不想购买付费 VPN 的新手用户。关键词“Lantern”已被墙内的百度、必应等搜索引擎封杀，你可以[免翻墙通过搭建在 Github 上的蓝灯官方论坛](#)获取最新版客户端的下载地址。

## （四）Psiphon 赛风

Psiphon 是由加拿大多伦多大学公民实验室开发的开源免费翻墙软件，最新的 Psiphon 3 综合使用了 VPN、SSH、HTTP 和 Socks 代理技术，支持 Android、Windows 和 iOS 平台。VOA 与 BBC 中文网都将 Psiphon 作为其推荐的翻墙方式。值得一提的是 2017 年 10 月初 GFW 为迎接即将到来的中共“十九大”进行了升级，使得当时刚发布的最新版 Psiphon 与 Lantern 失效，而在此期间 Shadowsocks（包括已停更数月的 ShadowsocksR）与 V2Ray 都安然无恙，可见前二者的抗封锁能力不及基于 Socks 的代理软件。

## （五）翻墙浏览器与浏览器插件

翻墙浏览器与浏览器插件的局限性显而易见——它们只能在浏览器层面解决翻墙上网问题，面对 Twitter、Telegram 客户端这样的软件就无能为力了。此外，就获取 Google Chrome 浏览器的翻墙插件而言，仍需解决先有鸡还是先有蛋的问题——用户必须先翻墙才能登录插件商店下载插件。

## （六）Tor + Meek

Tor 浏览器是 Tor (The Onion Route, 洋葱路由器) 项目的旗舰产品，使用多重代理来实现匿名并支持访问暗网，支持 Windows、macOS、Linux、Unix、BSD、Android 和 iOS 平台。早期的 Tor 因其流量特征太过明显，很快就被中国的 GFW 封杀。新版的 Tor 浏览器加入了 Meek 流量混淆插件，通过将 Tor 流量伪装成访问 Microsoft Azure 和 Amazon 云服务的正常流量来绕过 GFW，使中国用户得以将 Tor+Meek 这一组合用于翻墙用途。不过使用 Meek 后浏览网页往往会卡顿，用户体验不佳。

关于 Tor+Meek 的使用方法，建议阅读编程随想撰写的 [“如何翻墙”系列：扫盲 TOR Browser 7.5——关于 meek 插件的配置、优化、原理](#)

## （七）Outline

「Outline is an open source project created by Jigsaw to provide a safer way for news organizations and journalists to access the internet.」

Outline 是由 Google 旗下的 Jigsaw 开发的旨在为新闻组织和记者提供安全访问互联网方式的开源项目。Outline 基于 Shadowsocks，其实质相当于在自己的服务器自建 Shadowsocks 服务。相比于购买 VPN 或 Shadowsocks (R) 服务，Outline 提供的这种方式使用户享有更高的自主性，基本杜绝了服务商泄露用户信息的隐患。部署 Outline

所需的操作基本在图形用户界面下进行，不过对于长期习惯使用 VPN 的人而言，Outline 的学习成本仍然较高。

Outline 的使用步骤大致是：注册并订购 DigitalOcean 的虚拟主机 (VPS) 服务，在 VPS 上安装 Outline 的服务端，然后在 Outline 客户端输入来自服务端的 ss 链接就能建立连接。

Outline 没有像 ShadowsocksR 和 Shadowsock-libev 分支那样加入混淆插件，而主要通过屏蔽恶意端口扫描、服务器不保留互联网流量任何日志等方式来保证安全性与稳定性。此外 Outline 尚不支持智能分流，只有全局代理模式。

Outline Manager (服务器端) 支持的操作系统——Linux、Windows、macOS

Outline 客户端支持的操作系统——Android、Chrome OS、Windows、iOS、macOS

Outline 官网：<https://getoutline.org/en/home>

Outline 搭建与使用教程：[Outline搭建与使用教程-来自与Google合作的工具](#) (仅供参考)

[科学上网翻墙教程：搭建Outline翻墙 | YouTube 视频教程](#)

## (八) Project Fi

「[Project Fi](#) 是 Google 旗下的移动虚拟运营商 (MVNO)，通过 T-Mobile 和 Sprint 的 Wi-Fi 和蜂窝移动网络向美国以及超过120个国家的漫游用户提供语音及数据服务。」

Google 通过与各国电信运营商合作提供 Project Fi 服务，使用户出国后无需购买当地 SIM 卡就可直接使用所在国的数据服务。[Project Fi 产生的所有连接数据会经过 VPN 加密](#)，因此在中国大陆等网络封锁的地区可以实现无缝“翻墙”。使用 Project Fi 服务翻墙的门槛很低，可以推荐给短暂来华访问的外国友人使用。

Project Fi 最初只适用于 Google Pixel 和 Nexus 系列手机，以及各型支持蜂窝移动网络功能的平板电脑 (包括 iPad)，现已[扩展至支持 iPhone、三星和一加手机](#)。用户可在 [Project Fi 官网](#) 登录 Google 账号后输入所在地区的邮政编码以检验 Project Fi 是否支持该地区。

参见：[Using Project Fi in China: Say goodbye to VPNs](#)

## 三、通用翻墙手段难易度汇总

- 1、使用命令行自建 V2Ray
- 2、使用 HyperApp 自建 V2Ray
- 3、使用 HyperApp 自建 Shadowsocks
- 4、购买 V2Ray/Shadowsocks 服务或使用分享的免费节点
- 5、VPN、Lantern 等客户端一键翻墙

## 第三章 加密即时通讯应用

### 第八节 加密通讯应用概论

- 一、什么是端对端加密
- 二、常见即时通讯应用的加密方式
- 三、值得推荐的端对端加密 IM

### 第九节 Telegram 使用指南

- 一、Telegram 简介
- 二、Telegram 客户端
- 三、注册
  - (一) 号码选择
  - (二) 注册前提
    1. 使用内置代理
    2. 获取内置代理
  - (三) 注册步骤
- 四、安全性设置
  - (一) 隐私设置
    1. 黑名单
    2. 显示在线情况
    3. 语音通话权限
    4. 群组权限
  - (二) 安全设置
    1. 本地密码与生物验证
    2. 两步验证
    3. 当前在线
  - (三) 自动销毁机制
  - (四) 通讯录
    1. 通讯录的功能
    2. 同步通讯录
    3. 使用通讯录进行备注
  - (五) 私密模式下的链接预览
- 五、其他设置
  - (一) 个人信息设置
    1. 姓名
    2. 头像
    3. 签名
    4. 更换号码
    5. 用户名

6. 退出登录

7. 小结

(二) 数据与存储

(三) 外观

(四) 语言

## 六、基础功能

(一) 普通模式

1. 发送消息类型

2. 编辑

3. 删除

4. 回复

5. 转发

(二) 私密模式

(三) Saved Messages

(四) 群聊

1. 创建群组

2. 私有群组与公共群组

3. 普通群组与超级群组

(五) 频道

(六) 机器人

(七) 贴纸

1. 获取贴纸

2. 发送贴纸

3. 分享贴纸

(八) GIF

1. 发送 GIF

2. 保存 GIF

3. GIF 搜索引擎

(九) Telegraph

(十) Instant View

## 第八节 加密通讯应用概论

### 一、什么是端对端加密

“端到端加密 (End-to-end encryption, E2EE) 是一个只有参与通讯的用户可以读取信息的通信系统。总的来说，它可以防止潜在的窃听者——包括电信供应商、互联网服务供应商甚至是该通讯系统的提供者——获取能够用以解密通讯的密钥。此类系统被设计为可以防止潜在的监视或篡改企图，因为没有密钥的第三方难以破译系统中传输或储存的数据。举例来说，使用端到端加密的通讯提供商，将无法将其客户的通讯数据提供给当局。”

—— [维基百科 - 端对端加密](#)

### 二、常见即时通讯应用的加密方式

包括微信 (WeChat) 在内的所有主流即时通讯 (Instant Messaging, IM) 软件都会对信息加密，但显然微信并不支持端对端加密。在支持端对端加密的 IM 软件当中，加密模式可分为默认端对端加密 (always end-to-end encrypted) 和选择性端对端加密两种。前者的代表有 WhatsApp 和 Apple 的 iMessage，采用后者的应用有 Telegram、Facebook Messenger 和 Google Allo 等。

Telegram 因为没有默认启用端对端加密而受到批评，而事实上用户通讯数据的安全性不只取决于加密方式，还取决于 IM 软件运营者是否将用户数据上传在云服务器上。WhatsApp 虽然默认开启端对端加密，但仍会将用户的通讯数据存储和备份到自己的云端服务器上，以便将其同步到该用户的其他设备上；Apple 也在 iOS 11.4 中加入了与前者相似的 Messages in iCloud 功能 (可自行选择开关)。这种模式充其量只能保护传输过程中的信息安全，而存储在云端服务器上的用户数据在政府情报部门和黑客面前实际上很脆弱的，端对端加密的保护在传输完成后已然失效。而 Telegram 同时提供了普通模式和私密模式两种模式，普通模式下用户的聊天记录会被存储到云端服务器以便备份和同步；在私密模式下，Telegram 服务器只负责转发信息，本身并不存储任何信息，通讯只建立在两台终端设备之间，不会同步到同一用户其他设备的 Telegram 客户端上。云端不存储信息的端对端加密模式排除了政府和黑客通过云端攫取用户信息的可能，无疑更能保护用户的通讯安全。

参见 Telegram 创始人、CEO Pavel Durov 撰写的 [Why Isn't Telegram End-to-End Encrypted by Default?](#)



### 三、值得推荐的端到端加密 IM

- [Telegram Messenger](#)
- [Signal](#)
- [Wire](#)
- [Riot.im](#)

参见：

- [一天世界 | 聊天软件安全图例 v1.2](#) (2017-07-19)
- [Solidot | 腾讯的QQ和微信被指毫无隐私](#) (2016-10-22)

“国际特赦组织的“通讯隐私排名”以1至100分计对科技公司进行了排名，基于它们在下列5方面的表现：认识到用户在隐私和言论自由方面所面临之网上威胁；默认启用端到端加密；让用户知道其权利所面临之风险，以及其提供之加密强度；披露政府要求公司提供的用户数据之详情，以及其应对方式；公布加密系统的技术细节。中国的腾讯公司因对通讯隐私采取的措施最少及最不透明而得零分垫底，其次是黑莓和快拍(Snapchat)，分别得到20及26分。尽管微软制定了强有力的人权保护政策，它在Skype上依然采取了薄弱的加密方式，因此仅得40分，排名倒数第4。这些公司中无一对用户通讯提供端到端加密。仅有3家公司在对通讯软件默认启用端到端加密方面得满分，即苹果、连我(Line)以及Viber。”

- [Solidot | 微信有隐私吗?](#) (2018-01-08)

“国际特赦组织对流行通讯应用的隐私保护进行了排名，腾讯的QQ和微信没有得到一分，以零分垫底，被认为毫无隐私。在公开场合，腾讯则坚称它的服务是有隐私的，但拒绝披露更多详情，比如加密细节之类的。”

## 第九节 Telegram 使用指南

其他 Telegram 教程：

★ [resistance M: 请帮助你的朋友使用 Telegram](#) (2018-06-22)

★ [Telegram 新手指南](#) (Telegram 频道)

- [推墙技术部: Telegram 简明教程 \(适合异议者\)](#) (2017-09-22)

- [電報安全使用方案: Telegram 简明教程 \(适合反共者\)](#) (2017-05-19)

### 一、Telegram 简介

Telegram 是一款专注于速度和安全性的即时通讯应用，它快速、简单且免费。用户可以同时所有设备上使用 Telegram，消息可以在任意数量的手机、平板电脑或计算机上无缝同步。使用 Telegram，用户可以发送任何类型的消息、照片、视频和文件（文档，zip，mp3 等），以及为最多 200,000 人创建频道或群组，以便向无限的受众群体进行广播。用户可以写入手机通讯录，并按用户名查找人员。因此，Telegram 就像短信和电子邮件相结合，可以满足所有个人或业务通信需求。此外，Telegram 还支持端到端加密的语音通话。

#### Q: What is Telegram? What do I do here?

Telegram is a messaging app with a focus on speed and security, it's super-fast, simple and free. You can use Telegram on all your devices **at the same time** — your messages sync seamlessly across any number of your phones, tablets or computers. With Telegram, you can send messages, photos, videos and **files** of any type (doc, zip, mp3, etc), as well as create groups for up to **200,000** people or **channels** for broadcasting to **unlimited** audiences. You can write to your phone contacts and find people by their **usernames**. As a result, Telegram is like SMS and email combined — and can take care of all your personal or business messaging needs. In addition to this, we support **end-to-end encrypted voice calls**.

参见：

- Telegram 官网：<https://telegram.org>

★ Telegram FQA：<https://telegram.org/faq>

★ [少数派 | Telegram——真正定义即时通讯 | archive](#)

- [少数派 | Telegram - 替补 iMsg 的不二之选](#) (编者注：“iMsg”是 iMessage 的简写)

## 二、Telegram 客户端

Telegram 提供全平台客户端，包括 Android、iOS、Windows Phone、macOS、macOS/Windows/Linux Desktop 版以及网页版。

推荐使用从 App Store、Google Play 以及 Telegram 官网等正规渠道下载的官方客户端以规避潜在风险，不建议使用第三方客户端（已有币用、butterfly.im（蝴蝶 IM）、Teleplus（v5.4.2 之前版本）等多款 Telegram 第三方客户端被曝上传用户信息，详见 Telegram 频道 [PSA-安全公告专栏](#)）。

Telegram 官方表示现有的第三方 Telegram 客户端竞争力不足，无法对 Telegram 官方客户端构成挑战，因此让自家团队另行开发了面向 iOS 和 Android 平台的 Telegram X 客户端来跟原有的客户端竞争和验证新功能。iOS 版 Telegram X 以及 5.0 及后续版本的 Telegram 使用 Swift 语言重写，速度比混用 Objective-C 和 Swift 的旧版 Telegram 更快，耗电量更低。

Telegram 群组中流传的 Telegram X 安装包及类似客户端文件很有可能被植入了后门，切勿安装使用。

## 三、注册

### （一）号码选择

如果你已经肉翻（指常住中国境外，已经入籍或取得绿卡），并且并不畏惧或反感所在国政府实施或可能实施的大规模监控项目，这种情况下尽可使用自己日常使用的手机号码注册 Telegram。

如果你对匿名性有要求或者居住在中国大陆地区，建议使用 Google Voice 等虚拟号码/VoIP 注册 Telegram 以尽可能保证匿名性，获取方法见本书第三节。在中国内地使用虚拟号码的原因在于中国政府在 2015 年“709 案”后屏蔽了 Telegram，而此前维权律师群体曾广泛使用 Telegram，有理由相信 Telegram 最迟在此时开始受到中国强力部门的关注。由于中国大陆对手机号码采取实名制，国安、公安机关可以通过批量注册自己的 Telegram 帐号后导入全国的手机号码和对应个人身份信息的方法，借助中国大陆 +86 的实名制手机号码实现对大陆用户注册的 Telegram 帐号的“实名制”。

此外由于 2017 年以来中国政府部门在微信等墙内平台对“区块链”相关话题的管制，中国“币圈人士”大量涌入 Telegram，此类人士使用 +86 开头的中国大陆手机号码注册

的账号普遍存在强行拉人入群、大量发送 spam 信息等滥用行为，使 Telegram 官方不得不限制 +86 号码新注册的 Telegram 账号主动发起聊天，这成为了使用虚拟号码/境外号码注册 Telegram 的新理由。

你也可以使用短期出境时购买的临时电话卡或者在淘宝等电商平台购买的境外电话卡（例如 CMHK）注册 Telegram，需要注意的是你必须保证该账号在至少一台设备上时刻在线，否则你在失去该号码后将因无法接收验证短信而无法登录，实际也就失去了该账号的控制。

## （二）注册前提

Telegram 在中国大陆地区被 GFW 屏蔽，除了极少数情况下可以实现直连外，通常需要使用 V2Ray、Shadowsocks、VPN 等代理工具才能访问。

除此之外，用户可以直接使用 Telegram 客户端应用内置的代理，包括 Socks5 和 MTProto 两种代理方式，后者是 Telegram 自主研发的专用网络传输协议。

### 1. 使用内置代理

如果是初次注册，在未使用代理工具的情况下，输入手机号码点击发送验证短信数秒后会跳出使用内置代理的窗口，用户选择代理方式，输入代理的服务器 IP、端口、用户名和密码后即可使用代理。

如果已经登录账号进入应用界面，具体设置方法是 Settings > Data and Storage > Use Proxy 一项中选择“SOCKS5”或“MTPROTO”填入代理服务器节点信息；或者直接点击代理链接。

以 Project V 之前提供的 SOCKS5 代理 <tg://socks?server=51.15.125.253&port=7777&user=telegram&pass=tgpassword> 为例，在 Telegram 中点击该链接就可完成添加；如手动输入信息，可照 Server: 51.15.125.253, Port: 7777, Username: telegram, Password: tgpassword 填写。

### 2. 获取内置代理

与获取 V2Ray、Shadowsocks 节点相似，获取 Telegram 内置代理的方式也可以分为自建和获取现成的代理两种。

你可以在租用的 VPS 上搭建自己的 Telegram 专用代理，相关教程可以参考：

- <https://github.com/TelegramMessenger/MTPProxy>

- MTPProxy: 专为Telegram打造的代理工具-荒岛

Telegram 专用代理可以在 V2ray,SSR节点最新发布🚀🚀🚀🚀🚀、MTProxy 等频道获取。

### (三) 注册步骤

输入你的手机号码，Telegram 会自动向你发送短信验证码，输入短信验证码就可完成注册，进入应用界面。

与微信的账号（手机号/QQ号/微信号）+密码，必要时发送短信验证码的登录模式不同，Telegram 每次登录时都会采用短信验证码；如果你额外开启了两步验证（two-step verification），那么输入验证码后还要再输入两步验证密码。

\*根据 GDPR，如果你的 IP 位于欧盟国家或者英国，你必须年满 16 周岁才能注册 Telegram。

## 四、隐私与安全设置

### (一) 隐私设置

Settings > Privacy and Security

#### 1. 黑名单 (Blocked Users)

此处可以添加/查看被屏蔽拉黑的用户

#### 2. 显示在线情况 (Last Seen)

默认设置下，你的联系人可以看到你的在线情况，可分为四种类型：

- ① 不久前在线 (last seen recently)
- ② 一星期前在线 (last seen within a week)
- ③ 一个月前在线 (last seen within a month)
- ④ 长时间未上线 (last seen a long time ago)

用户可以在隐私与安全设置中选择向哪些人展示你的真实在线情况，可供选择的对象有所有人 (Everybody)、我的联系人 (My Contacts) 和任何人都不可见 (Nobody)，

此外还可以自行设置白名单（即 Always Share With）选项，只向该名单上的用户展示你的真实在线状况。

### 3. 语音通话权限 (Voice Call)

Telegram 在 2017 年提供了语音通话功能，而隐私与安全设置中的 Voice Call 选项可以让你选择谁有权和你进行，可选择的有所有人 (Everybody)、我的联系人 (My Contacts) 和任何人都不 (Nobody)，另外你可以自行设置语音通话权限的黑名单 (Never Allow) 和白名单 (Always Allow)。

PEER-TO-PEER 选项是对通话时数据模式的选择，P2P 模式指通话数据直接两台设备间传输，非 P2P 模式下通话数据会由 Telegram 的服务器进行中转以免直接暴露你的 IP 地址，从而保护用户的隐私与安全，但该模式会降低通话质量。你可以选择对所有人 (Everybody)、我的联系人 (My Contacts) 和任何人都不 (Nobody) 通话时使用 PEER-TO-PEER 模式。

iOS 客户端上的 iOS Call Integration 是指将 IM 应用的语音通话接入 Apple 的 CallKit 框架，开启该选项后来自 Telegram 的语音通话会像普通来电一样在锁定屏幕上显示，通话会被存储在系统的通话记录中；如果你开启了 iCloud 同步，这些通话记录会被上传到 Apple 的 iCloud 云服务器上。

### 4. 群组权限 (Groups)

群组权限指你可以选择那些用户有权将你加入新的群聊，可选择的只有所有人 (Everybody) 与我的联系人 (My Contacts)，此外你可以设置自己的黑名单 (Never Allow) 和白名单 (Always Allow)。

## (二) 安全设置

### 1. 本地密码和生物验证 (Passcode & Touch ID)

你可以对 Telegram 客户端设置独立的解锁密码，之后每次需要解锁才能进入该客户端。如果你的设备配备了 Face ID、Touch ID 或者其他生物识别传感器，你可以使用生物验证来代替数字密码解锁客户端。

### 2. 两步验证 (Two-Step Verification)

设置两步验证后，每次你重新登录 Telegram 账号时，在输入，你还需要额外输入自己设置的密码才能完成登录。

在登录认证中加入两步验证是对单纯短信验证风险漏洞的填补——政府情报部门和黑客等潜在攻击者在获知你用于注册 Telegram 的手机号码后可以通过 SS7 攻击劫持验证短信的方式来获取验证码，进而登入你的 Telegram 帐号并读取该帐号上的所有消息。因此，编者建议所有 Telegram 用户开启两步验证。

参见：[Solidot | SS7攻击绕过WhatsApp和Telegram加密](#)



两步验证是指用户重新登录 Telegram 账号时，在输入 Telegram 发送到其他已登陆设备上的验证码或者 SMS 短信验证码（没有已登录设备的情况下）后，还需额外输入设置的密码才能登录账号。

设置两步验证的方式非常简单，在 Settings > Privacy and Security > Two-Step Verification 中设置密码，然后添加密保邮箱（以便在遗忘两步验证密码后还能重新找回账号），然后在验证邮件中确认即可。

### 3. 当前在线 (Active Sessions)

用户可以在此处查看本帐号当前登录了多少台设备，所使用的 Telegram 客户端版本、设备的 IP 地址和位置，以及设备运行的操作系统版本。

#### (三) 自动销毁机制 (If Away For)

Telegram 设置了帐号自动销毁，长时间未登录达到设置期限后 Telegram 会自动注销你的帐号以及该帐号之前产生的所有数据，以此保证用户数据不会泄露。Telegram 的默认期限是 6 个月，此外有 1 个月、3 个月、6 个月和 12 个月可选。

#### (四) 通讯录 (Contact)

##### 1. 通讯录的功能

对 Telegram 开启通讯录权限后，之后通讯录中的联系人新注册了 Telegram 后，你将会收到“xxx joined Telegram”的通知；所有已经注册联系人都会显示与你的通讯录记录相一致的身份信息，不再显示该用户自己设置的姓名。

##### 2. 同步通讯录

在默认设置下 Telegram 会把你的通讯录上传到云端并同步，在新版本中 Telegram 为遵守欧盟的 GDPR 推出了新的隐私与安全权限，允许用户选择是否同步同步通讯录，并提供了删除已同步通讯录的选项 (Delete Synced Contacts)。

##### 3. 使用通讯录进行备注

Telegram 没有提供对联系人进行备注的功能，但你可以借助通讯录，将 Telegram 联系人的姓名和手机号码存入自己的通讯录，从而间接实现对 Telegram 联系人身份信息进行自定义的功能。如果你关闭了 Telegram 的通讯录权限，你仍可编辑制作仅适用于 Telegram 的通讯录。

#### (五) 私密模式下的链接预览

你可以选择是否在私密模式中开启链接预览，此项也是为符合 GDPR 而推出的新权限。链接预览 (link preview) 由 Telegram 的服务器生成，但 Telegram 不会存储链接数据。

### 五、其他设置

#### (一) 个人信息设置

##### 1. 姓名



姓和名是注册时需要填写的信息，登录后随时可以在设置中更改姓名。你设置的姓名会对向

## 2. 头像

Telegram 会自动生成由你的姓、名首字母组成的图片作为头像，你可以在设置中上传图片更换头像。需要注意的是 Telegram 会默认保留曾经使用过的所有头像，所有人都可以点击进入你的头像后通过划动来查看你的曾用头像。你如果不希望别人看到你的历史头像，需要在设置中手动删除。

## 3. 签名

bio 是供选填的个性签名和自我介绍。

## 4. 更换号码

你可以在 Change Number 中更换注册 Telegram 的手机号码。需要注意的是如果他人自己的 (Telegram) 通讯录里存储了你的手机号码，当你使用 Change Number 更换号码后他可以看到更新后的号码。

如果你怀疑自己的 Telegram 账号被怀有恶意的第三方知悉需要更换号码的，或者原先使用中国内地 +86 开头的号码注册需要更换外国号码的，不要在原账号使用更换号码 (Change Number) 功能，而应弃用该账号或者登录 Telegram 网站手动注销，然后使用新的号码另行注册一个 Telegram 账号。

## 5. 用户名

你可以设置一个 Username (用户名) 来方便别人找到你。在 Telegram 中对方可以直接通过“@你的用户名” (例如 @username) 来搜索到你的帐号；Telegram 还会为你生成一个“https://t.me/username”的链接，以便你将自己的 Telegram 帐号直接分享到 Twitter、Facebook 等其他社交平台。所有人都可以通过你的 username 找到你，但他们不会看到你的手机号码，除非你自己选择了“Share My Contact”。

## 6. 退出登录

点击“Log Out”来退出当前帐号

## 7. 小结

如果你对匿名性要求较高，建议随机填写姓名信息，不填写 bio 或填入无关信息，不要在 Telegram 上使用与其他社交/即时通讯帐号相同的姓名、用户名、昵称、个性

签名和头像，以免对方可以通过关联确定的你的真实身份；除非你有意公开自己在网络上的虚拟身份。

## (二) 数据与存储 (Data and Storage)

Telegram 默认将所有信息存储在云端，每次进入应用 Telegram 都会自动从云端同步数据，相比微信和 QQ 的存储占用会从刚下载时的 100 MB + 逐渐膨胀至 1 GB +，Telegram 几乎不占用本地存储空间（其不足可能是会耗费更多流量）。

在 Settings > Data and Storage 中，你可以查看 Telegram 的存储 (Storage) 与网络 (Network) 使用情况，选择自动下载 (Auto-Download Media) 的媒体类型（默认自动下载图片，视频、文件、语音消息、视频消息需要手动点击下载），是否自动下载还可以根据上网方式（无线网络/蜂窝移动数据网络）。此外你可以选择是否将新收到的图片自动保存到本地、是否保存经 Telegram 编辑过的图片和是否自动播放 GIF。

## (三) 外观 (Appearance)

在外观设置中，你可以选择字体大小、聊天背景（除 Telegram 提供的背景图片外，用户可以通过相册上传自己的图片作背景）、是否自动启用黑夜主题 (Auto-Night Theme) 以及色彩模式（有 Day Classic（经典模式）、Day（接近于 iMessage，只有 Day 模式下会出现 Accent Color 选项供用户自定义主题颜色）、Night Blue（暗蓝色调的黑夜模式）、Night（黑夜模式）四种模式可选）。

## (四) 语言 (Language)

Settings > Language

“Telegram 客户端，官方支持中文语言”

Telegram 客户的版本要求：

iOS 客户端  $\geq$  5.0.16

Android 客户端  $\geq$  5.0

macOS 客户端  $\geq$  4.8

Windows/macOS/Linux Desktop 客户端  $\geq$  1.5

Telegram 客户端下载地址：<https://congcong0806.github.io/2019/01/08/Telegram>

Telegram 客户端内直接点击链接更改语言：

英文: <tg://setlanguage?lang=en>  
简体中文: <tg://setlanguage?lang=zh-hans-raw>  
简体中文(聪聪): <https://t.me/setlanguage/zhcncc>  
简体中文(@zh\_CN 版): <tg://setlanguage?lang=classic-zh-cn>  
简体中文(langCN): <tg://setlanguage?lang=zhlangcn>  
繁体中文(香港): <tg://setlanguage?lang=zh-hant-raw>  
繁体中文(台湾): <tg://setlanguage?lang=taiwan>  
”

——[印象笔记 | 科技 NEWS 606](#)

## 六、基础功能

### (一) 普通聊天模式

普通聊天模式并未开启端对端加密，所有的聊天记录都会被存储到 Telegram 云端。

#### 1. 发送消息类型

Telegram 支持发送文字消息、表情贴纸 (Stickers)、GIF、视频、文件，并支持发起语音通话。

对于文字消息，你可以通过右键或快捷键自定义字体格式，可选择粗体或斜体，支持在文字中植入网页链接。

对于在 Telegram 中发送的链接，Telegram 会根据链接网页类型提供相应的页面预览，如链接支持 Instant View 快速预览功能（例如 Telegraph），Telegram 会提供网页标题、首段文字摘录和第一张图片，并在下方生成“Instant View”按钮；对于一般的网页链接，Telegram 会提供标题、文字摘录和首张图片的预览；微信公众号推文等少数的网页链接完全不支持预览，只能以链接形式呈现。

在 Telegram 发送图片时，发送点击图片可以进入图片编辑模式，提供画笔、马赛克等简单的图片标注功能。如果需要发送的图片数量大于等于 2 张，你可以选择单张发送图片，也可以选择将数张图片拼成图集后一次性发送。如果你担心图片被压缩后质量下降，，可以选择以文件形式发送图片 (Send as a file)，对方收到后需要下载解压后查看。

你可以发送任何形式的文件，单个文件大小不能超过 1.5 GB。

## 2. 编辑 (Edit)

Telegram 允许用户在消息发送后 48 小时内编辑修改已发送的消息，编辑过的文字仍会留在原处。（微信的“编辑功能”只是“撤回”的增强版，即在消息撤回后将该消息自动粘贴到你的输入栏中以供修改）

## 3. 删除 (Delete)

Telegram 没有微信那样的撤回机制，只提供删除功能。在一对一对话中，你在“Delete”时可以选择同时为自己和对方删除还是仅对自己删除，前者相当于“撤回”，支持在发送后 48 小时内删除已发送消息，后者相当于删除自己的聊天记录，不及于对方（此选项也会导致后续无法为对方删除消息，因此选择时需慎重）。在群聊中，“删除”的效力是“delete for everyone”，可以等同于“撤回”。

## 4. 回复 (Reply)

无论是一对一还是在群聊中，你都可以选中他人发送的消息后选择“Reply”（回复），之后你发送的回复会附上对方之前的消息，使得聊天时的回复更有针对性。

## 5. 转发 (Forward Message)

你可以选中他人发送的消息后选择“Forward Message”，将该消息转发到各处。被转发的消息上注有“Forward from xxx（原作者的名字）”。

### （二）私密聊天模式

在 chats 界面点击右上角的新建按钮（如果你关闭了 Telegram 的通讯录权限将无法新建对话，Telegram X 和 Desktop 版本不受此限），选择 New Secret Chat 来新建私密聊天；或者在联系人的名片页点击“Start Secret Chat”。之后 Telegram 会向对方发送私密聊天请求 (secret chat request)，只有对方同意进入后双方才能交换端对端加密 (end-to-end encrypted) 密钥，进入私密聊天模式。进入私密聊天模式后，在 chats 主界面上该联系人的姓名为绿色，姓名左侧有绿锁标记。

私密聊天受限于创建该对话的设备，产生的聊天记录不会上传存储到 Telegram 云端，也不会同步到你的其他设备上。

私聊聊天模式中不允许使用转发功能 (don't allow forwarding)，同时可以设置消息自毁计时器 (self-destruct timer, 相当于阅后即焚)，可供选择的时间有 1 - 15 秒、30 秒、1 分钟、1 小时、1 天和 1 周，你也可以选择“Off”，即不开启。

### (三) Saved Messages

向 Saved Messages 发送消息就是用户自己跟自己对话，你可以把 Saved Messages 当成自己的私人网盘来使用。

### (四) 群聊

#### 1. 创建群组

你可以在新建消息中选择“New Group”来创建群组，最初必须有两人以上才能创建成功。如果你关闭了通讯录权限，你将无法在 Telegram iOS 客户端中新建群组，但是 Telegram X 和 Desktop 版不受限制。如果你暂无联系人，可以将自己创建的 Bot（机器人）拉入群组。

Telegram 群组有私有群组与公共群组、普通群组和超级群组之分。

#### 2. 私有群组与公共群组

私有群组与公开群组的差别在于公开性，私有群组的邀请链接的形式是“t.me/joinchat/”，而公开群组的链接的形式是“t.me”的短链接；打开私有群组的邀请链接后，必须入群 (Join) 才能查看消息，而打开公开群组的链接后即便不入群也可以查看历史消息。

关于区分私有与公开群组，Project V 的几个 Telegram 交流群就是很好的例子——私有群组 Project V 吹水群“小微姐姐的日常”的链接是 <https://t.me/joinchat/AAAAAEIYaH-hjDDZS716jg>，公开群组“Project V（使用与反馈）”的链接是 <https://t.me/projectv2ray>。

公开群组提供 Copy Link 的功能，即群聊中每位成员发送的消息都有对应的链接，选中一则消息后选择“Copy Link”以获取链接。

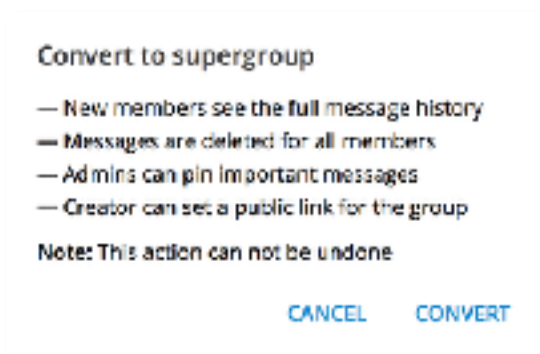
#### 3. 普通群组与超级群组

普通群组与超级群组的差别在于人数与功能，和是否为私有/公开群组之间没有必然联系（例如“紫薇姐姐的日常”既是私有群，也是超级群）。

普通群组的人数上限为 200 人，任何人都可以邀请新成员并编辑群名和群头像。超级群组 (Supergroup) 的人数上限高达 200,000 人，并拥有一些普通群组所不具备的功能。

超级群组为用户提供个性化的通知权限，你可以设置为群中有人提到你（即“@”）或者回复 (Reply) 你的消息时才通知你。超级群组的创建者可以授权给管理员来协助管理（机器人同样可以拥有管理员权限），管理员可以在群中置顶消息 (Pinned Messages)。

普通群组可以升级到超级群组，但该操作不可逆。



参见：★ [聪聪 | Telegram 群组、频道、机器人 - 汇总分享 - 群组 Group](#)

## （五）频道

Telegram Channel (频道) 的使用模式与用 Telegram 聊天高度相似，差别只在于只有频道所有者（或者说创建者 (creator)）及其授权的管理员 (Admin) 有权发布消息，其他关注频道的用户只有只读权限。

频道和群聊一样分为公开群组和私有群组，二者的差别和群聊基本一致。公开频道提供的 Copy Post Link 功能类似公开群组的 Copy Link 功能，可以直接以链接形式分享该消息。

频道可以发挥公告板的作用，可以像微信公众号平台那样使用。频道的推送完全没有次数和内容的限制（Telegram 官方只审查煽动使用暴力的内容，并对 Apple 设备

屏蔽传播色情内容的频道)，自由度远高于微信公众号。频道也可以当作微信朋友圈使用，你可以借助 like bot 等机器人转发消息来实现类似点赞或者评论功能。

少数由 Telegram 官方创建的 Channel 有蓝色八角形、白色对勾的认证标识（如 Telegram、[Durov's Channel](#)、[Telegram News](#)、[Gamee](#)）。

参见：★ [聪聪 | Telegram 群组、频道、机器人 - 汇总分享 - 频道 Channel](#)

## （六）机器人 (bot)

bot 是 Telegram 上的机器人账户，通常具有 AI 属性并可充当自动化工具，进而扩展 Telegram 的功能。bot 近似于微信小程序，例如 @like 可以为消息提供类似点赞功能，@PullBot 可以发起群投票，@tgcjoincaptchabot 可以对入群者进行 reCAPTCHA 验证。Telegram 开放了 bot 的 API，用户可以根据自身需要开发自己的 bot。

名称右侧有蓝色八角形、内有白色对勾图标的 bot 是由 Telegram 官方出品或经 Telegram 官方认证的 bot，相对安全可靠。

常见 Bot 列表：

- @BotFather 官方认证。创建和管理机器人
- @IFTTT 官方认证。IFTTT的官方机器人，可以连接各类 IFTTT 服务。
- @GmailBot 官方认证。Gmail 客户端
- @telegraph 官方认证。发送、管理 Telegram 文章及查看统计数据
- @gamee 官方认证。游戏平台
- @get\_id\_bot 获取你的 Telegram Chat ID（一串数字）
- @bing/@pic/@gif: Bing / Yandex / Giphy 图片搜索，可用于贴纸斗图
- @AirPollution\_bot: 空气污染指数，数据来源为 aqicn.org
- @QRCodeRoBot 二维码识别
- @TextEmojiBot: 颜文字
- @GithubBot: GitHub Commit 和 Issue 更新提醒
- @like 提供类似点赞按钮
- @vote 发起投票
- @PullBot 发起投票
- @zh\_groups\_bot TGCN-群组频道狗🐶 TGCN-群组索引计划机器人
- @AntiServiceMessageBot 自动删除入群、退群通知

参见：

★ [聪聪 | Telegram 群组、频道、机器人 - 汇总分享 - 机器人 Bot](#)

## (七) 贴纸 (Stickers)

Telegram 的 Stickers (贴纸) 功能类似于微信的表情包。在“表情包”上，Telegram 与微信的差别在于区分了 Stickers 和 GIF，Sticker 是静态的图片，GIF 是动图，不像微信表情包那样动静混杂。得益于 Telegram 的开发性和中国用户的努力，熊本熊、脆皮鸚鵡、小肥柴等热门表情都有了 Telegram Stickers 版本。

### 1. 获取贴纸

点击他人发送的单张贴纸就可查看整套贴纸，点击下方的“Add Stickers”就可将它保存到自己的贴纸库。Telegram Stickers 同样存储在云端，一经添加会自动同步到你的所有设备上。

你也可以借助 Stickers Pack bot 来制作自己的贴纸包。教程参见：[懒\(烂\)办法制作 Telegram Sticker Pack](#)

### 2. 发送贴纸

你可以直接在自己的贴纸库中选取贴纸，也可以输入 emoji 表情后选择该 emoji 映射的贴纸，因为每张贴纸都有与之对应的 emoji 表情。

### 3. 分享贴纸

点击已保存在贴纸库中的贴纸包时会显示“Share Stickers”的按钮，点按后会生成形如“<https://t.me/addstickers/example>”的贴纸分享链接。

部分 Telegram 贴纸链接：

Great Minds <https://t.me/addstickers/TelegramGreatMinds>

ssr's daily <https://t.me/addstickers/ssrstickers>

ssr's daily 2 <https://t.me/addstickers/ssrsdaily2>

科学常用表情包 <https://t.me/addstickers/yaffs64>

熊本熊污 <https://t.me/addstickers/xiongbenxiongwu>

💰 <https://t.me/addstickers/PowerEmoji>

Docomo by Suisr [https://t.me/addstickers/suisr\\_docomo](https://t.me/addstickers/suisr_docomo)

cute call <https://t.me/addstickers/cutecall>

ARU Full Part2 <https://t.me/addstickers/arup2>

可爱不过老子 <https://t.me/addstickers/keaibuguolaozi>

茄 <https://t.me/addstickers/karen321>



Tom基本法 <https://t.me/addstickers/tombasiclaw>  
behnam(wild boy) <https://t.me/addstickers/behnambbbbmmmm>  
这只 Gayhub 到处咬东西 <https://t.me/addstickers/PeeGayhub>  
Suddenly <https://t.me/addstickers/Suddenly2x>  
中老年表情包 <https://t.me/addstickers/oldaged>  
我想静静 <https://t.me/addstickers/PeterCxy>  
Subway's WeChat Collection <https://t.me/addstickers/myfavoritewechatstickers>  
Windy's Pack <https://t.me/addstickers/Windyspack>  
张德帅 <https://t.me/addstickers/changmz>  
Jony Ive [https://t.me/addstickers/Jonathan\\_Ive](https://t.me/addstickers/Jonathan_Ive)  
rw-Style <https://t.me/addstickers/rwStyle>  
白白在吃啥 <https://t.me/addstickers/BacBacsDiet>  
KOGENU @Nekosticker <https://t.me/addstickers/nekostickerpack498>  
Big Emoji <https://t.me/addstickers/PowerEmoji>  
The Elder and HK journalist <https://t.me/addstickers/TheElderPart2>  
Excited <https://t.me/addstickers/excited>  
蛤蛤 <https://t.me/addstickers/hahajiecao>  
TheElder <https://t.me/addstickers/TheElder>  
清真表情包 <https://t.me/addstickers/PowerEmoji>  
Bazinga <https://t.me/addstickers/Analytics2>  
变态熊猫-RW <https://t.me/addstickers/biantaiPanda>  
ugly triple <https://t.me/addstickers/uglytriple>  
你懂我意思吧 [https://t.me/addstickers/do\\_you\\_know\\_what\\_I\\_mean](https://t.me/addstickers/do_you_know_what_I_mean)  
过两招-rw <https://t.me/addstickers/Guoliangzhao>  
Kizuna Ai  [https://t.me/addstickers/Kizuna\\_Ai\\_San](https://t.me/addstickers/Kizuna_Ai_San)  
HailTheJudge <https://t.me/addstickers/HailTheJudge>

## (八) GIF

Telegram 会将 GIF 转码成 MPEG 4 格式，在相同画质下至多可节省 95% 的存储占用空间，使你能够在 Telegram 上以比以往快 20 倍的速度下载 GIF。得益于开发者的优化，Telegram 可以同时流畅播放几十个 GIF。

### 1. 发送 GIF

GIF 按钮与贴纸按钮并列，点击后可以查看你自己的 GIF 图库。

### 2. 保存 GIF

以 iOS 为例，点按 GIF 查看大图，再点按右下方的“+”就能将此 GIF 保存到自己的 GIF 栏中。

### 3. GIF 搜索引擎

Telegram 内置了 GIF 动态搜索功能，你可以在输入栏中输入“@gif 关键词”（例如“@gif cat”）来搜索相关的 GIF。

#### （九）Telegraph

Telegraph 是 Telegram 提供的匿名博客服务，你可以通过 Telegram 中的 Telegraph bot (@telegraph) 或者在浏览器中输入“telegra.ph”来使用它。Telegraph 的匿名体现在它只根据浏览器缓存来识别作者，Telegraph 文章刚发布时还可重新编辑，一旦浏览器缓存被清除后就不可再编辑，同时无法溯源到原作者。

Telegraph 支持大小标题、粗体/斜体文字、图片、网页链接和视频链接，对链接没有任何限制。

如果你需要在 Telegram 群组中发送长段文字，可以考虑使用 Telegraph 链接或 pastebin 类工具，以免占据过多屏幕空间对他人造成影响。

Telegraph 支持下文会提到的 Instant View 功能。

#### （十）Instant View

Instant View 是 Telegram 内置的网页快速浏览功能。支持 Instant View 功能的网页链接（例如：Telegraph、BBC）会在标题、摘要和图片下方会显示“Instant View”按钮，点击后即进入 Instant View 模式，网页文章会被渲染成类似阅读模式的风格，用户可选择文字背景颜色和字体大小等。Instant View 的意义在于可以极大缩短 Telegram 内置浏览器或跳转外部浏览器加载、打开链接的时间，同时为用户提供了良好的阅读体验，用户可以把 Telegram 当作阅读器来使用。

## 第四章 个人信息保护指南

### 第十节 个人信息保护指南

- 一、系统安全防护
- 二、数据安全保护
- 三、隐私权限限制
- 四、加密邮箱
- 五、浏览器
- 六、Tor 浏览器
- 七、搜索引擎
- 八、密码管理
- 九、输入法
- 十、智能家居
- 十一、多设备策略

### 第十一节 社交媒体使用建议

- 一、账号管理
- 二、身份隔离
- 三、言论边界

## 第十节 个人信息保护指南

### 一、系统安全防护

#### (一) 尽可能不使用国产操作系统

常见的桌面操作系统均非国产操作系统，此处略过。

建议国产 Android 手机用户，通过刷机使用 LineageOS 等接近原生系统的第三方 ROM。使用中国厂商定制的安卓 ROM 最大潜在风险在于越权收集用户信息和为中国政府提供后门监控用户，此外还有阉割原生 Android 的功能、推送海量垃圾广告和信息（以 MIUI 为代表）、推送 Android 官方安全补丁不及时等诸多缺点。

在移动操作系统对隐私保护孰优孰劣的问题上，Android 系统得益于其开放的特性，使有相应能力的用户可以全面地掌控各应用程序的权限和活动，但是其学习成本较高，只适用于极客群体。iOS 的优点在于沙盒运行机制及严格的 App Store 审核规则，从源头上遏制了恶意应用程序和流氓软件的滋生；但其封闭的系统特性和不明确

的隐私权限设置使得用户无法知晓应用程序在后台对个人信息的调用活动，确实存在硬伤；但对于小白级用户而言，iOS 至少可以在简捷易用的前提下保证相对的安全。



华为账号更新通知

图片来自推特用户“郭元庆”(@qq196837) [原推链接](#)

参见：

- [The “Dicision” app in Huawei P20 was found to continuously collect your location and send the data to hicloud.com, the Huawei Cloud \(2018-10-03\)](#)

推主 [Elliot Alderson \(@fs0c131y\)](#) 发布了系列推文，揭露华为 P20 手机预置的“Decision”应用持续收集用户的定位并将数据传送到 [hicloud.com](#)，即华为云的服务器上。

- 华为手机系统被曝自动删除从国际互联网下载的文件，旧版系统可能不受影响 (2019.01)

<https://twitter.com/yxw860510/status/1084962096121434113>

[https://twitter.com/8\\_9\\_6\\_4/status/1084130766030663680](https://twitter.com/8_9_6_4/status/1084130766030663680)

<https://twitter.com/servalcandle/status/1087692589044617217?s=21>

<https://twitter.com/servalcandle/status/1087709643730604032?s=21>

- [Solidot | 一加的氧 OS 会跟踪用户的所有活动 \(2017-10-10\)](#)

“深圳万普拉斯科技有限公司为其一加智能手机开发的 Android 定制版本 OxygenOS 内置了跟踪分析功能，会跟踪用户在应用中的所有活动，相关数据会被发送到域名 [open.oneplus.net](#)，一加收集的数据并不匿名，包含了用户设备

的详细信息。用户没有办法禁用，但可以通过 adb 移除名为 OnePlus Device Manager 的跟踪应用。”

- [新京报网 | 百度系两款APP未经提示开启隐私权限 | archive](#)

- [iOS Security - Apple](#)

安卓手机刷机教程参见：

★ [ch: 手机刷机Why&How](#) (2018-03-12)

## (二) 及时更新最新版系统

如果是大版本迭代前可以先观望一段时间，以防新系统不稳定带来麻烦。

## (三) 病毒防护

运行 iOS、macOS 和 Linux 操作系统的设备因其系统特性几乎不会感染病毒，无需用户自己动手查杀病毒。

就 iOS 设备而言，不建议从第三方应用市场（例如 PP 助手、爱思助手等）下载破解版应用。如果不具备相应的技术能力，不要盲目“越狱”。

就 Windows PC 而言，微软提供的 Windows Defender 软件基本可以满足日常的安全保护需要（Windows Defender 可运行在 Windows XP 及更高的版本上，并内置于 Windows Vista 及后续版本），你也可以选择 [Avira](#)（俗称“小红伞”）、[Norton Security](#) 等国外杀毒软件或者 [火绒安全软件](#) 等口碑较好的国产安全防护软件。

360 安全卫士、腾讯电脑管家和百度卫士是国产毒瘤软件的代表，以窃取用户信息、捆绑安装全家桶（如 360 安全浏览器、360 手机管家等）、占据大量内存加重卡顿见长，建议尽早将其删除。

参见：

- [Solidot | 你的百度云管家报毒了吗？](#) (2017-02-06)

## 二、数据安全保护

## （一）定时备份

建议定期使用外置移动硬盘备份电脑、手机中的数据。

## （二）硬盘加密

你可以给电脑硬盘加密来进一步增强数据安全性。macOS 和 Windows 操作系统均内置了硬盘加密工具。在 macOS 下你可以开启“文件保险箱 (FileVault)” (设置 > 安全性与隐私 > 文件保险箱)，在 Windows 下你可以打开 BitLocker。

开源的硬盘加密软件 [VeraCrypt](#) 可用于在文件中创建虚拟加密硬盘或加密分区，在 Windows 系统下还支持在开机前授权全盘加密。

教程参见：

★ [有关密码学的科普内容 | Veracrypt的基本操作](#)

- [编程随想 | 如何用“磁盘加密”对抗警方的【取证软件】和【刑讯逼供】，兼谈数据删除技巧 \(2019-02-14\)](#)

## （三）文件加密

对于文件和邮件文本内容都可以采用 PGP (Pretty Good Privacy) 协议加密，PGP 分为公钥和私钥，使用公钥给文件加密，再用私钥解密；此外 PGP 还支持给文件添加加密的数字签名以验证真伪。使用 PGP 需要使用的软件是 [GnuPG](#) (GNU Privacy Guard, GPG)，支持 Windows, macOS, RISC OS, Android, Linux 系统。

## （四）销毁数据

数据一旦在写入磁盘，此后无论是删除文件还是格式化磁盘，理论上都可以使用技术手段恢复此数据。对此可以选择多次抹掉硬盘数据以防止文件被恢复。

8. 如果选取了 Mac OS 扩展（日志式，加密），若要防止已抹掉的文件被恢复，请点按“安全性选项”，使用滑块来选取覆盖已抹掉数据的次数，然后点按“好”。

覆盖数据三次即符合美国能源部关于安全抹掉磁性介质的标准。覆盖数据七次即符合美国国防部的 5220-22-M 标准。

9. 点按“抹掉”，然后点按“完成”。

参见 [Apple Support | 在 Mac 上使用“磁盘工具”抹掉宗卷](#)

对于曾经存储过重要信息的废弃机械硬盘、固态硬盘或闪存条，不要将其随意丢弃，可以考虑用外力将在物理上彻底破坏后再丢弃。

对于淘汰或者损坏的手机，若打算将其挂到二手平台上出售，建议先将其恢复出厂设置。如果是废弃的 iPhone 手机，可以按照官网的指示进行相关操作，然后将其交给苹果做拆解处理。

### 三、隐私权限限制

除了不开启定位就无法使用的地图类应用外，建议一律关闭定位和通讯录权限。

对于微信、QQ、微博、贴吧、知乎、淘宝、天猫、闲鱼、京东等国产应用，建议在平时关闭调用相机和麦克风权限。

如果你对应用开启了相册权限，理论上该应用可以扫描你的整个相册。如果间歇性开启相册权限，其效果与经常性开启并无二致。如果你对于隐私保护要求较高，建议彻底关闭微信、新浪微博等国产软件的相册权限。新版 iOS 系统已经在相册权限上对读取和写入权限做了区分，但社交类软件的读写权限通常是合二为一的，关闭相册权限的同时意味着你无法将微博上的图片保存到相册中，对此你可以使用抓图应用通过网页链接抓取图片，或者在浏览器中打开链接后直接保存。如果你觉得这些额外步骤过于繁琐影响生活质量，可以考虑同时使用两部手机或更多部设备，在专门的手机上对国产软件开放相机、相册等隐私权限。

参见：

- [Solidot | 小米华为被发现悄悄给予应用过多权限 \(2018-02-12\)](#)

“[新京报的调查发现](#)，华为、小米应用商店下载的应用默认开启了多个敏感权限。在华为、小米、OPPO、vivo 的内置应用商店下载 APP 时，天猫、携程、58同城、优酷、今日头条、爱奇艺、赶集网七款 APP 在华为和小米应用商店下载时未经明示提醒就默认开启了定位或其他敏感权限，而在 OPPO 和 vivo 应用商店下载时则基本都对其权限进行了明示提醒。以天猫为例，在小米手机安装后，默认开启了定位、相机、录音权限；在华为手机安装后，默认开启了定位、相机、读取通话记录权限；OPPO 手机安装后，未开启任何权限；vivo 手机安装后，明示提醒并开启了定位权限。其它应用有类似情况。一位开发者称，应用市场一般执行最低权限策略，除非权限是刚需，比如读取通讯录是为了实现加通讯录好友。至于 APP 具体能够开启哪些权限，要看应用商店的审

核要求。如果应用商店觉得你索取的权限出于正当目的，就可以上架，至于默认开启权限的功能，只能是与应用商店有关。”

- Solidot | 京东金融 APP 被发现会收集用户银行 APP 截图 (2018-02-16)

- Telegram 频道 荔枝木 - <https://t.me/lycheewood/5454> (2018-02-16)

“今天京东金融截图的事情闹得沸沸扬扬，不乏有些用户鼓吹转移到 iOS 系统下就没有这些问题。

真的如此吗？我觉得可以参考一下这篇文章：[https://weibo.com/ttarticle/p/show?id=2309404340311663991197#\\_0](https://weibo.com/ttarticle/p/show?id=2309404340311663991197#_0)

iPhone 给应用后台 15min 保持的时间里微信会私自访问相册你知道吗？——你当然不会知道，因为 iOS 没有“每次访问相册权限”都提醒的功能，所以这一现象只有在重置后的 iOS 系统上，当微信认为自己已经被授权而偷偷访问的时候会被发现。既然相册可以被静默访问，其它权限同理，比如联系人。

再比如说 iOS 的某些应用同样会在 WiFi 开关的时候后台向服务端发送设备和网络信息——而且这还是在关闭了后台刷新并结束进程之后。

在这些方面 Android 得益于更开放的系统环境，得以用一些 tweak & hack 来拦截，而 iOS 很遗憾就只能抓瞎了，所以我认为 iOS 隐私保护更好很可能是个伪命题。”

- Telegram 频道 每日消费电子观察 - [https://t.me/CE\\_Observe/7537](https://t.me/CE_Observe/7537) (2018-02-16)

“我觉得这篇文章想表达的意思是：作为用户，应当理解在 iOS、Android 或其他系统上，授予应用每一项权限都意味着什么，这项权限如果被滥用到极致可以收集哪些隐私；看清应用温馨提示的借口，不要盲目给予它们不必要的权限。

而不要只是见到某 App 的某个行为被曝光了就短时间内抵制某某公司。

BTW：为什么我反对甚至痛恨二维码的推广普及？

因为使用二维码就必然会使用摄像头；能使用摄像头了，你觉得流氓们会规矩地只在你扫二维码的时候才调用摄像头吗？”

- 少数派 | 如何才能阻止下一个京东金融「偷」走你的照片？ (2019-02-19)



## 四、加密邮箱

使用国产的 163、126、yeah、QQ、新浪、搜狐邮箱服务必然伴随在中国政府对电邮内容的监视。因此无论使用电子邮件本身，还是使用邮箱注册 Twitter 等网络账号，都建议使用 Gmail 等国外邮件服务。此外在传输敏感信息时，可以考虑使用支持端对端加密的邮箱服务以保证安全。

端对端加密匿名邮箱有 [ProtonMail](#)、[Tutanota](#)、[Disroot.org](#)、[Mailfence](#)、[Mailbox.org](#)、[Runbox](#)，此外 [ZeroNet](#) 等去中心化网络也有相应的端对端加密邮箱服务。

值得注意的是“端对端加密”只适用于相同邮箱服务的账户之间，如果你用 ProtonMail 向 Gamil 用户发送加密邮件，你还需要通过其他通讯渠道向对方提供解锁邮件的私钥。

参见：[hatecpc: #2 匿名邮箱:protonmail](#)

### #“零收件箱”策略

对于高度敏感的邮件往来，可以使用“零收件箱”策略，即双方阅读邮件后即时删除邮件。这样一来，即便公安无论使用技术手段还是强迫当事人交出邮箱密码而控制了邮箱，最终仍然无法获取定“罪”证据。

## 五、浏览器

### (一) 浏览器的选择

推荐使用 Safari（仅限苹果设备）、Chrome、Firefox，以及来自独立开发者/开发商的浏览器应用，如对匿名性要求较高可以使用 Tor 浏览器。

不建议使用国产安卓手机厂商系统内置的浏览器，以及 BAT 出品的百度浏览器、QQ浏览器、UC浏览器等，理由同样是存在植入后门监视用户的可能。以小米 MIUI 国内版浏览器为例，该浏览器直接屏蔽了 Github 的网址，在信息封锁上比 GFW 更进一步。

参见：

- [公司安全部门通知：“百度浏览器过度收集用户隐私信息，请在任何情况下都避免使用”](#)（2016-03-18）

- [MIUI论坛 | miui自带浏览器7000+拦截网址曝光，厉害了](#)

## （二）浏览器的使用

使用浏览器时可以使用隐私模式（也称“无痕浏览”），即不保留历史记录，以免受到网站追踪。

尽可能使用 HTTPS (Hypertext Transfer Protocol Secure, 超文本传输安全协议) 的连接网页。HTTPS 经 HTTP (HyperText Transfer Protocol, 超文本传输协议) 进行通信，并使用 TLS/SSL 对传输数据进行加密，它的 URL 以“https://”作为开头，浏览器往往在其 URL 前显示锁的图形，可凭此对 HTTPS 和不加密的 HTTP 进行区分。不要在 HTTP 连接的网页中输入账号、卡号和密码等敏感信息，这些数据一旦被黑客拦截会直接以明文形式呈现，进而可能造成信息泄露、财产损失等严重后果。

## 六、Tor 浏览器

VPN 等传统代理工具只提供一层代理，如果与 VPN 的连接因意外断开，你的真实公网 IP 就会暴露并被网络服务提供商 (ISP) 记录。Tor 浏览器的多重代理则有助于降低前者发生的风险，同时保障上网的匿名性和安全性。

Tor 浏览器的使用门槛比 VPN、Shadowsocks 等代理工具更高，其带来的安全性提升建立在牺牲一定效率的基础上。编者建议在网络上积极发表政治观点的指导级受众使用 Tor 浏览器，以访问国际互联网为主要需求、平时只浏览资讯不发言讨论的参考级用户可根据自身需求来判断是否使用 Tor。

### （一）Tor 的原理

“Tor（英语：The Onion Router，洋葱路由器）是实现匿名通信的自由软件。Tor 是第二代洋葱路由的一种实现，用户通过 Tor 可以在因特网上进行匿名交流。

#### 匿名外连

Tor 用户在本机运行一个洋葱代理服务器 (onion proxy)，这个代理周期性地与其他 Tor 交流，从而在 Tor 网络中构成虚电路 (virtual circuit)。Tor 是在 5 层协议栈中的应用层进行加密（也就是按照‘onion’的模式）。而它之所以被称为 onion，是因为它的结构就跟洋葱相同，你只能看出它的外表，而想要看到核心，就必须把它层层剥开。即每个路由器间的传输都经过点对点密钥 (symmetric key) 来加密，形成有层次的结构。它中间所经过的各节点，都

好像洋葱的一层皮，把客户端包在里面，算是保护信息来源的一种方式，这样在洋葱路由器之间可以保持通讯安全。同时对于客户端，洋葱代理服务器又作为 SOCKS 接口。一些应用程序就可以将 Tor 作为代理服务器，网络通讯就可以通过 Tor 的虚拟环路来进行。

进入 Tor 网络后，加密信息在路由器间层层传递，最后到达“出口节点”（exit node），明文数据从这个节点直接发往原来的目的地。对于目的地主机而言，是从“出口节点”发来信息。要注意的是明文信息即使在 Tor 网络中是加密的，离开 Tor 后仍然是明文的。维基解密创始人便声称其公开的某些文件是截获于 Tor 的出口节。

## 隐藏服务

Tor 不仅可以提供客户端的匿名访问，Tor 还可以提供服务器的匿名。通过使用 Tor 网络，用户可以维护位置不可知的服务器。这些服务器所构成的网络被称为“Tor Hidden Services”，信息界又称为暗网，一般的互联网则被相应地称为明网。因为在明网里，客户端和服务端彼此知道对方的真实 IP 地址，而在暗网里双方互不知 IP 地址。若服务端能做到不记录用户使用信息，以及客户端能做到任何时刻都不输入真实个人数据，则通过 Tor 隐藏服务可以达成上网的完全匿名性。

如果要访问 Tor 隐藏服务，客户端必须安装 Tor 浏览器，在搭载 Android 操作系统的手机或平板电脑上，则必须安装 Orfox。

在 Tor 浏览器里面，于地址栏输入 Tor 隐藏网络特有的顶级域名 .onion，可以访问 Tor 隐藏服务（暗网）。Tor 浏览器可以识别 .onion 域名，并自动路由到隐藏的服务。然后，隐藏的服务将请求交由标准的服务器软件进行处理，这个服务器软件应该预先进行配置，从而只侦听非公开的接口。

Tor 隐藏服务（暗网）有个另外的好处，由于不需要公开的 IP 地址，服务就可以躲在防火墙和 NAT 背后。但如果这个服务还可以通过一般的互联网（明网）来访问，那也会受到相关连的攻击，这样就没有真正的隐藏起来。”

——[Tor - 维基百科](#)

参见：

- [Tor 官网](#)

- [securityinabox | Tor Browser for Windows - 网络匿名及审查规避](#)

## (二) Tor 的入门级使用

### 1. 获取 Tor 浏览器

Tor 的官网已被 GFW 封锁，你首先需要有一个可用的代理工具来访问 Tor 官网并下载适用的 Tor 浏览器。

### 2. Tor 网络设置

初次打开 Tor 浏览器时应用会先要求用户进行 Tor 网络设置，对于身处中国大陆的用户应该勾选“我所在的国家对 Tor 进行了封锁”，之后选择“内置网桥”，目前有“obfs4”、“obfs3”和“meek-azure”三种网桥可选。

如果你没有连接代理，可以选择中国可用的 meek-azure 网桥（即把 Tor 混淆成访问微软 Azure 云服务的流量）实现仅限于 Tor 的“单重代理”。然而使用 meek-azure 网桥确实可以连接，但网页的加载时间太过漫长，不论是与用普通浏览器直连访问墙内网站还是使用代理访问墙外网站的体验均相差甚远，所以不推荐这种使用方式。在双重代理部分使用的“obfs4”网桥的速度要比 meek 快不少。



### 3. 使用双重代理

#### 原因1

因为 Tor 的影响力很大，GFW 对 Tor 进行重点封杀。全球大多数的 Tor 中继节点都被 GFW 列入“IP 黑名单”。所以天朝的网友，如果单独使用 Tor，很难联网成功。这种情况下，就需要使用双重代理。

#### 原因2

所有的软件都可能存在缺陷（Tor 也不例外）。如果你仅仅使用 Tor，万一 Tor 出现安全漏洞并且被攻击者利用，那么攻击者就有可能对你进行逆向追溯（说不定能追溯出你的真实公网 IP）。

而如果使用多重代理，即使出现上述风险，攻击者也只能追踪到 Tor 的前置代理，而不会直接追踪到你本人。这样一来，风险大大降低。

### 原因3

前面提到，全球的 Tor 网络中可能会有陷阱节点。虽然你可以利用俺刚才介绍的方法，排除危险国家/地区的节点，但并不能确保万无一失。

比如说你碰到某个极小概率事件——你使用的线路上，碰巧三个节点都是陷阱——这种情况下，你的真实公网 IP 会暴露。

但如果你用了双重代理，即使碰到这种小概率事件，只会暴露你使用的前置代理服务器的 IP，而【不会暴露】你的本人的公网 IP。

——编程随想：“如何翻墙”系列：关于 Tor 的常见问题解答

如果利用已有的代理工具+Tor 实现双重代理（如 VPN+Tor、Shadowsocks+Tor、V2Ray+Tor），你需要在“内置网桥”选项中选择“obfs4”网桥，然后勾选“使用代理访问互联网”。接下来你需要填写自己的代理信息，包括代理类型（SOCKS 4、SOCKS 5、HTTP / HTTPS）、地址、端口、用户名和密码（可选）。

如果选择“SOCKS 5”作为代理类型，则“地址”栏填写本地 Socks5 监听地址 (Local Socks5 Address)，通常为“127.0.0.1”（可以在 Shadowsocks、V2Ray 客户端查看，下同），“端口”栏填写本地 Socks5 监听端口 (Local Socks5 Port)，如“1080”。

如果选择“HTTP / HTTPS”作为代理类型，则“地址”栏填写本地 HTTP 监听地址 (Local Http Address)，仍为“127.0.0.1”，“端口”栏填写本地 HTTP 监听端口 (Local Http Port)。



参见：

★ [有关密码学的科普内容 | Proxy over Tor](#)

## 七、搜索引擎

百度以竞价广告和诈骗信息著称，已是公认的业界毒瘤，建议有能力的读者早日弃用；搜狗、360搜索、必应国内版等搜索引擎也是信息封锁政策的执行者，同样建议有能力者弃用。

国外的搜索引擎，在搜索内容质量上 Google 是首选。如果你对 Google 搜集用户数据的行径和监控资本主义的商业模式表示担心，可以使用承诺不监控、不记录用户搜索内容的 [DuckDuckGo](#) 和 [StartPage](#) 等作为替代品，值得一提的是 StartPage 提供 Google 的搜索结果，体验较佳。DuckDuckGo 和 StartPage 同样被中国 GFW 封锁，需翻墙后使用。

在墙内你还可以尝试使用未被 GFW 封杀的、更小众的国外搜索引擎，比如来自俄罗斯的 [Yandex](#)。

参见：[百度替代指南，帮你用上更好的搜索引擎](#)（原文来自「eBooksPlan」：[百度替代指南，帮你用上更好的搜索引擎](#)）

参见：

- [麦琪：百度为作恶而生](#)
- [Solidot | 百度代理商被指强推信息流广告](#) (2017-09-25)
- [【麻辣总局】“嫩滑”体验之百度与谷歌](#) (2018-08-08)
- [Solidot | 百度再度被指混淆广告投放和合法结果](#) (2018-12-11)
- [新闻实验室 | 搜索引擎百度已死](#) (2019-01-22)
- [方可成 | 我为什么要写《搜索引擎百度已死》](#) (2019-01-23)
- [端传媒 | 洛德：在“被豢养”的互联网世界，批评百度时我们忽略了什么？](#) (2019-01-25)

### ★ [对百度的争议 - 维基百科](#) 目录

- 1 [域名劫持和软件流氓化](#)
  - 1.1 [域名劫持](#)
  - 1.2 [软件强制捆绑安装](#)
  - 1.3 [旗下软件站植入恶意代码](#)
  - 1.4 [手机应用超范围申请权限](#)
- 2 [百度推广相关争议](#)
  - 2.1 [影响网民使用的竞价排名](#)
    - 2.1.1 [竞价除名丑闻](#)

- 2.1.2 央视曝光百度竞价排名事件
- 2.1.3 魏则西事件
- 2.1.4 推广赌博网站事件
- 2.1.5 百度搜索洋酒回收遭遇诈骗
- 2.1.6 假冒NARS中国大陆官网事件
- 2.1.7 假冒苹果官方售后维修店事件
- 2.1.8 新华社曝光百度竞价排名事件
- 2.1.9 “复大医院”广告事件
- 2.1.10 “上海美国领事”广告泛滥
- 2.1.11 高仿签证网站广告事件
- 2.1.12 用户搜索“QQ邮箱”出现盗号网站推广
- 2.2 是否为广告内容的争议
- 2.3 移动端、网页端推广“双标准”问题
- 3 侵犯版权
- 4 涉嫌侵犯隐私
- 5 内容审查
- 6 百度贴吧相关争议
  - 6.1 2009年被互联网整风行动谴责与曝光
  - 6.2 爆吧事件
  - 6.3 2009年高校贴吧禁言事件
  - 6.4 2012年百度员工收受贿赂付费删帖
  - 6.5 被净网2014行动谴责与曝光
  - 6.6 盗版网络原创文学问题
  - 6.7 “卖吧”事件
    - 6.7.1 2015年舰队collection吧吧主被调换事件
    - 6.7.2 2015年Minecraft吧空降吧主事件
    - 6.7.3 2016年血友病吧事件
    - 6.7.4 学科类贴吧被卖事件
  - 6.8 守望先锋吧被封禁事件
  - 6.9 恶搞事件
    - 6.9.1 2010年X来自未来事件
    - 6.9.2 2011年龅牙哥事件
  - 6.10 戒赌吧被封
- 7 色情内容
- 8 百度文库侵权事件
- 9 百度百科相关争议
  - 9.1 开放性争议
  - 9.2 版权争议
  - 9.3 破坏恶搞
- 10 行业纠纷
  - 10.1 奇虎360与百度争斗事件

- 10.2 “作业帮”纠纷
  - 10.2.1 引起不良学习习惯
  - 10.2.2 涉嫌抄袭学霸君界面
  - 10.2.3 陷害小猿搜题事件
- 10.3 与今日头条的纠纷

## 11 百度其他争议

- 11.1 伪造民意 建党节虚假“献花”
- 11.2 ImageNet图像识别挑战赛作弊
- 11.3 用户体验总监因演讲内容不当被撤职
- 11.4 与王志安的纠纷
- 11.5 百度没有文化一文事件
- 11.6 百家号的自家内容过多

## 八、密码管理

### （一）密码设置

使用大小写字母、数字、符号随机组合成的长密码，如果担心自己记不住可将其记在实体纸张上或者密码管理器中。

不要使用 123456、qwerty 等简单密码或者 admin 等默认密码，不要将自己的姓名拼音、出生日期用作密码。

对不同的账号设置不同的密码，不要重复使用同一密码以免其中一家网站的数据库遭遇黑客攻击“脱库”后导致其他账号随之一并泄漏、扩大损失。

### （二）密码管理器

使用密码管理器的好处在于用户只要记住密码管理器自身的主密码，就可以在需要时由密码管理器应用自动填充你的各类网络账户的复杂密码，免去了自己记忆密码的麻烦，也有利于减少在公共场所输入密码时被他人旁窥窃取密码的可能性。如果你的设备配备了 Touch ID、Face ID 等生物识别传感器，在使用密码管理器无疑会更加便利。

常见的密码管理器应用有 1Password、KeePass、LastPass 等，作为 iCloud 服务组成部分的 iCloud Key Chain（钥匙串）也发挥着密码管理器的作用。

切勿使用盗版、破解版密码管理器应用。



## 九、输入法

输入法应用为了扩大词库，通常会将用户的个人词库上传到服务器。对中国政府来说获取本国互联网企业存储在境内服务器上的数据易如反掌，而有些国内厂商在用户信息上传过程中的加密环节出了纰漏，增加了用户隐私被黑客劫取的风险。

在输入法的选择上应同样遵循尽量不用国产软件的原则，建议尽量使用系统原生输入法或由知名国外厂商开发的输入法：

iPhone/iPad：苹果原生输入法、Gboard

Mac：苹果原生输入法、鼠鬚管 Squirrel

Android 手机：Gboard

Windows PC：微软原生输入法、小狼毫 Weasel

\* Gboard 是 Google 为 Android / iOS 设备开发的输入法应用，特色是支持滑行输入、支持内置的 Google 搜索引擎。Gboard 未上架中国区 App Store，可在其他国家/地区的商店获取。

\*常见国产输入法：搜狗输入法、科大讯飞输入法、百度输入法、QQ输入法、各大国产手机厂商预置的输入法……

\*“鼠鬚管”和“小狼毫”分别是开源输入法软件“RIME / 中州韻输入法引擎”的 macOS 和 Windows 发行版。

参见：

- [Solidot | 搜狗输入法收集用户隐私信息，未屏蔽爬虫](#) (2013-06-05)
- [Solidot | 流行虚拟键盘应用泄漏 3100 万用户信息](#) (2017-12-06)
- [Solidot | 一加的“Badword”过滤主要影响中国用户](#) (2018-01-29)
- [Solidot | 百度手机输入法被发现会调用录音功能](#) (2018-07-02)

## 十、智能家居

安全性：none > Apple > Google、Amazon 等国际厂商 > 小米、阿里等国产厂商

对于像 Amazon Echo 这样搭载智能语音助手、能够控制智能家居设备的智能音箱，能不用尽量不用。

参见：

★ [Solidot | 亚马逊证实 Alexa 记录了私人对话然后发送给随机联络人](#)

- [Solidot | 黑客能利用缔奇扫地机器人监视屋主](#)

## 十一、多设备策略

如果你对信息安全性要求很高，并且具有相应的经济条件，建议同时使用两部或更多部手机。日常使用时，在一部手机上安装支付宝、微信、QQ、新浪微博等国产应用，不要存储任何政治敏感性文件；另一部安装翻墙软件和 Twitter、Facebook、Instagram、Telegram、WhatsApp 等国外应用，不要安装任何国产社交、通讯应用，以防中国政府借助国产应用内植入的后门监视手机用户。

此外，多设备策略可以应对可能发生的警察强制查手机的情况。新疆警察使用手持设备在街头拦截路人检查手机是否存有“暴恐”内容已成常态，手机扫描仪等相关图片在 2017 年就已流传在微博、推特等平台上。2017 年下半年以来 Telegram 中文圈流传着北京、苏州等地的警察在地铁口强制扫描路人手机内容，内地新疆化趋势正在路上。虽然警察强查手机侵犯隐私于法无据，但在这个取消国家主席任期限制的宪法修正案都能毫无阻力地通过的魔幻国度，没有什么是不可能的，还是小心为妙吧。

警察扫描手机内容并非虚言，在技术上完全可以实现，参见：

- [Reuters | At Beijing security fair, an arms race for surveillance tech](#)

- [Solidot | 中国公司展示能破解 iOS 系统的扫描仪](#)

本节末尾附上编程随想“如何隐藏你的踪迹，避免跨省追捕”系列博文的链接，以供参考：

[如何隐藏你的踪迹，避免跨省追捕\[0\]：为啥要写此文？](#)

[如何隐藏你的踪迹，避免跨省追捕\[1\]：网络方面的防范](#)

[如何隐藏你的踪迹，避免跨省追捕\[2\]：个人软件的防范](#)

[如何隐藏你的踪迹，避免跨省追捕\[3\]：操作系统的防范](#)

[如何隐藏你的踪迹，避免跨省追捕\[4\]：通讯工具的防范](#)

[如何隐藏你的踪迹，避免跨省追捕\[5\]：用多重代理隐匿公网IP](#)

[如何隐藏你的踪迹，避免跨省追捕\[6\]：用虚拟机隐匿公网IP（原理介绍）](#)

[如何隐藏你的踪迹，避免跨省追捕\[7\]：用虚拟机隐匿公网IP（配置图解）](#)

[如何隐藏你的踪迹，避免跨省追捕\[8\]：如何搭配“多重代理”和“多虚拟机”](#)

[如何隐藏你的踪迹，避免跨省追捕\[9\]：从【时间角度】谈谈社会工程学的防范](#)

[如何隐藏你的踪迹，避免跨省追捕\[10\]：从【身份隔离】谈谈社会工程学的防范](#)

## 第十一节 墙外社交媒体使用建议

本节预设的受众限于居住在中国大陆、希望在网络空间积极表达政治见解的异议人士，并非在所有情况下都适用，特此说明。

### 一、账号管理

使用 Gmail、iCloud（非云上贵州）等国外电子邮箱或者端对端加密的匿名电子邮箱注册墙外社交媒体账号，不要使用 163、126、qq 邮箱等国内电子邮箱账号注册墙外社交媒体。

不要使用中国大陆 +86 开头的手机号码注册墙外社交媒体或者将该号码与社交账号相绑定。

使用复杂密码。

开启双重验证两步验证（Two-Factor Authentication, 2FA），首选基于验证器应用的 2FA 或者使用 U2F (Universal 2nd Factor)，谨慎使用基于 SMS 短信的 2FA。

从事高风险活动的人士建议运行虚拟机后使用 Tor 浏览器完成注册。

### 二、身份隔离

注册 Twitter 等墙外社交媒体时建议使用新的虚拟身份，同时与墙内的社交/即时通讯平台使用的身份相隔离。

换言之，不要在 Facebook、Instagram、Twitter、WhatsApp、Facebook Messenger、Telegram、Line、Reddit、Quora 等墙外平台使用与墙内的微信、微信朋友圈、QQ、QQ空间、新浪微博、贴吧、知乎、豆瓣、虎扑、bilibili、天涯、简书等平台相同的用户名、昵称、头像和签名。

不要将相同的联系方式，如电子邮箱、即时通讯软件账号（微信、QQ、Telegram 等）以备注、个人资料或博文等形式公布同时公布在墙外和墙内社交平台上，以防中国政府部门或者居心不良之人通过墙外与墙内社交软件账号之间的关联，利用已经过实名制认证的墙内社交软件来确定用户的真实身份。

不要在墙外平台上发送可能泄露自己真实身份的信息，比如公开自己的姓名、学号、学校、专业、工作地点、常住城市。

不要发送露脸的自拍照，带有易于判断具体位置的地标的照片，未对姓名、身份证号、出发地、目的地、座位等关键信息打马的火车票、高铁票、飞机票的照片，未对卡号、安全码等关键信息打马的银行卡的照片。发送自己拍摄照片前建议去除照片的 EXIF (Exchangeable image file format, 可交换图像文件格式)，后者包含了照片的属性信息和拍摄数据，包括拍摄设备、拍摄时间和拍摄地点定位等信息。iOS 用户可以使用 Shortcuts 捷径“[Clear Photo Exif Info](#)”去除 exif 信息，Android 用户可以从 Google PlayStore 下载 [Photo Metadata Remover - Clear Exif Metadata](#)。方便起见你也可以在相册中对截屏后发送原照片的截图。

不要在社交平台分享你的定位信息，不论是你的居住地点、工作地点还是旅行时访问的地点。

不要将网易云音乐等墙内服务的超链接转发到墙外社交平台，因为有些链接中可能包含了墙内平台用户的个人信息，网警因而可以顺藤摸瓜。

如果需要发表风险较高的言论，如“辱包”（讽刺中共领导人习近平）言论、呼吁颠覆中共政权的言论，建议使用该社交账号时全程使用 Tor 浏览器，或者在虚拟机中使用 Tor。

不要在墙外社交媒体使用自己在墙内社交媒体的较为明显习惯性用语。

如果自行检查时发现有身份泄露的风险后建议立即放弃当前帐号（删除旧账号发布的所有内容后注销该账号），然后另行注册新账号。不要通过修改用户名、昵称和头像等信息继续使用该账号，如果你已经被定位，后续的修改是无济于事的。

### 三、言论边界

“互联网不是法外之地”，不要发表任何涉及儿童色彩、种族歧视、仇恨言论等在文明国家公认为不法的言论，违反后果包括但不限于被平台封号、承担法律责任、被人肉搜索。

建议中文圈的推特用户浏览支纳维基上的“兔杂”词条和支纳维基、恶俗维基上被“出道”（指户籍等个人信息被公开）的反面教材的事迹。

参见：

- [RFA | 大陆掀起「推特强拆」风暴 数百推友被删号](#) (2018-12-12)
- [纽约时报中文网 | 网络审查再升级：中国推特用户遭政府盘查或拘留](#) (2019-01-11)

## 第五章 信息难民自救指南

### 第十二节 404 信息保存

#### 一、网页存档

(一) archive.is

(二) archive.org

#### 二、截图

(一) 网页截图/长截图

1. 移动端

2. 桌面端

(二) 截图拼接

#### 三、页面存储

#### 四、Telegraph

#### 五、区块链

### 第十三节 404 信息获取

#### 一、中国数字时代

#### 二、端点星

#### 三、其他渠道

## 第十二节 404 信息保存

中国网民在 GFW 内的微信、微博等平台上发布的涉及敏感事件和话题（如 2017 年的红黄蓝幼儿园事件、北京清退“低端人口”事件等）的内容往往会被管理者以“多人举报”、“违反《网络安全法》”等借口删除，即人们常说的“404”。本节内容旨在介绍几种在敏感信息被“404”将之保存下来以便二次传播的方法。

### 一、网页存档

在使用网页存档工具保存网页的优势在于可以基本保持网页的原貌，主要用以保存微信公众号文章以及财新网等墙内媒体的新闻报道。

## (一) archive.is

archive.is 是一个私人资助的数字时间囊网站，提供抓取网页内容的服务。archive.is 还拥有 archive.li、archive.fo 等多个不同的域名，支持以“archive.today.xxx”的短链接形式转发分享。该网站已被 GFW 屏蔽。



## (二) archive.org

archive.org 是一个非营利性的数字图书馆组织，同样提供网页存档服务，它的中文名称是“互联网档案馆”。虽然它的 archive.is 的域名很相像，两者在网页抓取方式上存在差别。

## 二、截图

长截图工具主要用于保存微博等难以直接存档的社交媒体内容，或者用以获取墙外媒体资讯分享到墙内，例如香港端传媒的客户端自身支持将文章导出为长图的功能，以使用户转发传播。

### (一) 网页截图/长截图

#### 1. 移动端

iOS 平台上的长截图应用有 Picsew 和 Tailor，另外图片标注应用 iMark（我的标记）与智能剪贴板应用 Pin 也提供网页截图的功能。Android 平台上的知名长截图应用有 PPIICC。

## 2. 桌面端

利用 Chrome 开发者工具进行网页长截图（Chrome 版本要求：59 或更高版本）

macOS:

Command + Option + I

① 截取整个网页的内容

Command + Shift + P

输入命令：Capture full size screenshot

②（模拟移动设备）截取手机版网页长图

Command + Shift + M

点击右上方的扩展按钮选择“Capture full size screenshot”

Windows:

① Control + Option + F12

截取整个网页的内容

② Control + Shift + P

输入命令：Capture full size screenshot

参见 [少数派：利用 Chrome 原生工具进行网页长截图 | 一日一技 archive](#)

macOS 平台上的截图应用 Xnip 也支持长截图。

## （二）截图拼接

对于过长的截图，长截图工具可能无法一次性抓取，此时可以采取分页截图后再拼接的方法。iMark 提供最高支持 9 张图片的拼图功能，其生成的长图能保持高清不留痕迹，值得推荐；如果分页截图超过 9 张，还可以在生成的长图的基础上继续拼接。

## 三、页面存储

在 Windows 和 macOS 这样的桌面级操作系统上，可以利用浏览器提供“页面存储”功能将相关网页存储到本地。其缺点是最终得到的是一个文件，难以直接分享。（使用 macOS 的 Safari 浏览器存储的网页归档文件类型为“.webarchive”，在 Windows 上可用 IE 等浏览器打开该类文件）



在移动设备上可以将网页导出为 pdf 或 epub 文件，缺点同上。

#### 四、Telegraph

Telegraph 是由加密即时通讯应用 Telegram 提供的匿名博客服务，用户可以将涉及敏感话题的网页内容转录到 Telegraph 后加以转发分享。

#### 五、区块链

将区块链用于首见于 2018 年 4 月的北大岳昕事件，有网友将她的公开信写入了以太坊 ETH 的交易信息，使之就此长存于区块链。

你也可以选择 Steemit、Matters 等以区块链作为底层技术的平台存储信息。

参见：

- 为众人抱薪者，必将铭刻于区块链上
- 某天，当你像北大岳昕一样无助时，请把你的话说给区块链（含教程）

### 第十三节 404 信息获取

#### 一、中国数字时代

“中国数字时代（英语：China Digital Times；缩写：CDT）是一个英语、中文双语的新闻网站，创办人及现任总编辑为萧强，2004年创办英文版，2009年创办中文版，致力于聚合“中国的社会与政治新闻，和它在世界上的新兴的角色”有关的报道和评论。网站由加州大学伯克利分校的新闻研究生院师生创办，现由加州大学伯克利分校信息学院“逆权力实验室”（Counter-Power Lab）提供技术支持和反封锁软件的开发。网站的中文内容来自对自媒体和防火长城外网站时政类内容的系统采集分类，编辑推荐和部分原创性报道；英文部分包括新闻聚合和翻译的内容。”——中国数字时代 - 维基百科

中国数字时代会实时转载墙内热点议题相关的文章，包括但不限于已经被删除的内容，不失为了解中国网络舆论的一个窗口。中国数字时代已经被 GFW 屏蔽，在中国大陆需要翻墙才能访问。

除了 [中国数字时代](#) 网站外，你也可以通过关注 Telegram 频道 [中国数字时代消息推送](#) 接收资讯。



## 二、[端点星计划](#)

「Terminus 端点星计划，是在 GitHub 开放平台搭建的一个站点，用于备份微信、微博等平台被删文章。」

端点星已先后被微信和 GFW 屏蔽，在中国大陆需要翻墙才能访问。

参见：[如何协作参与端点星计划](#)

## 三、其他渠道

相关网站：[自由微博](#)、[自由微信](#)、[墙与书](#)

## 四、搜索引擎

在 Google 等不受中共审查的搜索引擎中搜索被删文章、帖子的标题或关键词查找他人的转载和备份。

参见：[数字移民 | 如何找回被删除的网页/新闻](#) (2018-10-14)

## 第六章 番外

### 第十四讲 去中心化网络

- 一、ZeroNet
- 二、Mastodon
- 三、Steemit
- 四、IPFS
- 五、Matters
- 六、其他

### 第十五讲 加密数字货币

- 一、加密数字钱包
- 二、如何获取比特币

## 第十四讲 去中心化网络

墙外的 Facebook、Instagram、Twitter 和墙内的微信、微博、豆瓣、知乎、贴吧等社交平台都是典型的中心化网络的产物。用户的数据统一存储在中心服务器上，全操于平台服务商之手，因此网信办等公权力机关可以肆无忌惮地删帖销号，或者通过恶法和行政命令要求腾讯、新浪等运营者自我审查，制造白色恐怖；Facebook 可以藉此分析用户习惯、精准投送广告和其他信息，将自己掌握的海量用户数据变现。2018 年 Facebook 用户数据泄露丑闻被曝光后人们逐渐开始对 Facebook 等互联网巨头主导的监控资本主义 (Surveillance Capitalism) 商业模式和传统的中心化网络有所警醒。

参见：

- [Solidot | Facebook 付费给青少年安装它的 VPN 应用收集隐私，曝光之后宣布将关闭](#)
- [The Verge | Apple blocks Facebook from running its internal iOS apps](#)

与中心化网络相对应的去中心化网络不再需要高度集中的中心服务器，每一个去中心化网络的参与者都自动成为该网络中的一个节点，数据将分布存放在参与网络的每一台设备，从而避免了对数据享有绝对控制权的网络巨头滥用支配地位的可能。

去中心化网络能够弥补中心化网络的若干弊病，有利于保障用户的隐私权与信息自决权，但它目前仍不够完善，现存的多个去中心化社交媒体的规模都无法与 Facebook 和 Twitter 相匹敌，在短期内显然无法全面取代中心化网络。编者对去中心化网络所知十分有限，在此仅提供相关名词和摘自维基百科的解释，仅供读者参考。

## 一、ZeroNet

“ZeroNet，中文被译为“零网”，是一个以对等网络用户为基础构成的类互联网的分布式网络。ZeroNet 的总部位于匈牙利的布达佩斯。ZeroNet 默认不提供匿名保护，但用户可以使用 Tor 来隐藏 IP 地址以达到匿名效果。此软件自带的 Tor 网络在中国大陆被封禁，用户可能需要前置 VPN 才能正常下载初始配置文件。

ZeroNet 使用了比特币加密技术和 BitTorrent 网络协议。现时该平台上托管了很多热门网站，而邮件客户端、文件管理器和新闻客户端等专有功能也为 ZeroNet 的生态系统增加了价值。”

—— [ZeroNet - 维基百科](#)

参见：

- [ZeroNet 官网](#)
- [ZeroNet 工作原理](#)
- [如何使用 Tor 实现匿名](#)

## 二、Mastodon

“Mastodon（官方中文译“万象”，网民又称“长毛象”）是一个免费开源的去中心化的分布式微博客社交网络。它的用户界面和操作方式跟推特类似，但是整个网络并非由单一机构运作，却是由多个由不同运营者独立运作的服务器以联邦方式交换数据而组成的去中心化社交网络。每个 Mastodon 的运营站点被称为“实体（Instance）”，用户可到任何开放登记的实体登记，任何一个实体上

的用户可以与其他实体上的用户沟通。用户在推特中发布的内容称为“推文”，而在 Mastodon 中发布的内容则称为“啾文 (Toot)”，用户可以调整隐私设置限制啾文被其他人或实体读取或查看。Mastodon 吉祥物是一个棕色或灰色的长鼻目，描绘成正在使用平板电脑或智能手机。

此服务试图通过定位成独立运作的小型社区，而不是由上而下的审查。如同 Twitter，Mastodon 支持用户间直接、私密的消息，但与 Twitter 张贴的“推文”不同，Mastodon 的“啾文”可以是：对用户、用户的追踪者私密，对特定实体、或通过实体网络公开。联邦式的 Mastodon 实体组成联邦世界。”

—— [Mastodon - 维基百科](#)

参见：

- [Mastodon 项目官网](#)

- [长毛象中文站](#)

长毛象中文站维护者 [海啾督](#) 的 [一张图看懂长毛象项目](#)

\* Instance 也译为“实例”，编者注



### 三、Steemit

[Steemit](#) 是一个基于 Steem 区块链为内容发布者提供奖励的博客和社交网站。用户可以通过发布、发现和评论来获得 Steem 区块链提供的 Steem 和 Steem Dollars 两种可交易的代币。运行 Steemit 的 Steemit, Inc. 是一家设在纽约，总部位于弗吉尼亚州的私人公司。

Steemit 的亮点在于发布在该平台上的内容会被存储在区块链中，理论上可以永久保存（同时一经发布后就无法删除）；作者可以根据读者的“点赞”数量来获得相应的代币奖励。（V2Ray 项目已将其官方博客迁移到了 Steemit 上—— <https://steemit.com/@v2ray>）

目前获取 Steemit 帐号的方式主要有免费注册、使用比特币等加密数字货币付费购买和从已有帐号者手中购买帐号。免费注册 Steemit 帐号这种方式对中国大陆的用户不是很友好，往往申请就石沉大海杳无音讯。如果你只是想要一个帐号来给别人的文章点赞帮她/他创收，用支付宝从已有帐号者那里买一个倒也无妨；如果你想将 Steemit 作为发布原创内容的博客平台，编者建议通过 <https://anon.steem.network> 支持加密数字货币的方式购买一个 Steemit 帐号，以保证帐号的相对匿名性和自身安全。

参见：[Steemit 注册页面](#)

#### 四、IPFS

星际文件系统（InterPlanetary File System，缩写 IPFS）是一个旨在创建持久且分布式存储和共享文件的网络传输协议。它是一种内容可寻址的对等超媒体分发协议。在 IPFS 网络中的节点将构成一个分布式文件系统。它是一个开放源代码项目，自 2014 年开始由 Protocol Labs 在开源社区的帮助下发展。其最初由 Juan Benet 设计。

IPFS 是一个对等的分布式文件系统，它尝试为所有计算设备连接同一个文件系统。在某些方面，IPFS 类似于万维网，但它也可以被视作一个独立的 BitTorrent 群、在同一个 Git 仓库中交换对象。换种说法，IPFS 提供了一个高吞吐量、按内容寻址的块存储模型，及与内容相关超链接。这形成了一个广义的 Merkle 有向无环图（DAG）。IPFS 结合了分布式散列表、鼓励块交换和一个自我认证的名字空间。IPFS 没有单点故障，并且节点不需要相互信任。分布式内容传递可以节约带宽，和防止 HTTP 方案可能遇到的 DDoS 攻击。

该文件系统可以通过多种方式访问，包括 FUSE 与 HTTP。将本地文件添加到 IPFS 文件系统可使其面向全世界可用。文件表示基于其哈希，因此有利于缓存。文件的分发采用一个基于 BitTorrent 的协议。其他查看内容的用户也有助于将内容提供给网络上的其他人。IPFS 有一个称为 IPNS 的名称服务，它是一个基于 PKI 的全局名字空间，用于构筑信任链，这与其他 NS 兼容，并可以映射 DNS、.onion、.bit 等到 IPNS。

—— [星际文件系统 - 维基百科](#)

相比于中心化网络下的 Google Drive、Dropbox 等网盘，基于 P2P 的 IPFS 更难以 GFW 所封杀，V2Ray 就已开始使用 IPFS 来分发安装包和客户端应用：

目前对于文件分享，P2P 的一个主流方案是 IPFS。和 BT 类似，IPFS 没有中心服务器，你可以连接到其它的 IPFS 节点来下载所指定的文件。文件名（或目录名）就是一个字符串，有了这个字符串，你就可以下载到 V2Ray 的安装包。

—— [v2ray: 尝试使用 IPFS 来分发 V2Ray 安装包](#)

原理与使用方法参见 [IPFS 官网](#)

## 五、Matters

[Matters](#) 是端传媒前总编辑張潔平（Annie Zhang Jie Ping）离职后创办的内容生态系统。Matters 以区块链作为底层技术，以去中心化方式连接社群，以 IPFS 存储信息，鼓励用户创造优质内容并予以回报，目前尚在内测中。

参见：

- [Matters Lab: 社交媒體的另一種可能：Arendt的桌子](#) (2018-04-02)
- [Matters Lab: Matters 項目草案：重塑內容價值鏈](#) (2018-05-31)
- [Matters Lab: 給Matters朋友們的一封信：向星際啟航](#) (2018-11-09)

## 六、其他

“[diaspora](#) 基于三大核心哲学：去中心化、自由和隐私。它希望能引起大家关切由中心所控制社交网站下的隐私问题，所以可以让用户自行架设服务器（或称“pod”）来控制内容，而各个服务器可以再自行互动分享动态更新、照片或其它的资料。

[Friendica](#) 强调在隐私控制上的仔细设置，它是一个容易安装在服务器上的软件，以期待尽可能出现更多其它的社交网络联邦。Friendica 用户可以从 Facebook, Twitter, Diaspora, GNU social, App.net, Pump.io 等等多项社交网络服务来整合其联系人的名单到自己的社交时间流。

[GNU social](#) 的功能有点类似推特，但希望能为微博客社群，提供更开放、互相扶持的分散式沟通功能。企业或个人可以自行安装 GNU social 在自家机器上，以控管自己的服务与资料数据。著名的公共网站如： [quitter.se](#) 和 [gnusocial.no.](#)”

## 第十五讲 加密数字货币

编者对于加密数字货币所知有限，只能帮助入门者解决从无到有的问题，币圈玩家请忽视本讲内容。

### 一、加密数字钱包

Blockchain是业界领先的数字货币软件平台，提供在线数字货币钱包服务。由平台在线托管数字货币的优点在于用户只需要记住自己的比特币地址和密钥就可登录管理，无需下载高达数百 GB 的完整交易列表而使电脑本地磁盘不堪重负。

为了确保资产安全，Blockchain 提供了多重安全验证机制（层级数可由用户决定），除了钱包 ID 和密码外，每次登录时都需要登录验证邮箱在验证邮件中点击确认链接；此外用户还可以选择加入两步验证、关联手机号和备份恢复字串等方式增强账户的安全性。

建议使用端对端加密的匿名邮箱作为 Blockchain 的验证邮箱，不要使用国内邮箱

关于两步验证 (2FA)，你需要在移动设备上安装 Google Authenticator 或类似应用（请从 App Store、Google Play 等官方应用商店搜索下载），对相应网站进行关联设置。之后每次登录时你在输入密码后需要额外填写 2FA 应用实时显示的 6 位数验证码，该验证码会在设定的时间间隔内自动更新。

参考教程：

Velaciela: 比特币钱包安全指南 (2018)

### 二、如何获取比特币

#### （一）交易平台



提供两个加密数字货币交易平台，仅供参考。

LocalBitcoins：线下/线上交易比特币

CoinCola：线下交易 BTC、ETH、BCH、USDT 等货币。

不推荐使用国内的交易平台。

## （二）购买流程

——以在 LocalBitcoins 购买比特币为例

1. 买家可以根据卖家所在地区、标价、最低/最高购买额度、支付方式（支付宝、微信支付、国内银行卡转账、PayPal……）等标准筛选卖家
2. 确定卖家后输入需要购买的比特币金额，开始交易
3. 按照卖家的要求付款
4. 卖家确认收到款项后释放比特币，由平台暂时托管
5. 稍后平台会将比特币转移到你的账户上
- \*6. 你可以将其比特币转移到自己的数字货币钱包中（需要支付一定手续费）

\*使用支付宝、国内银行卡转账等支付手段进行比特币交易会被中国政府监控，请谨慎使用这类交易手段，不要进行大额交易。

\*编者在自学加密数字货币的过程中从 Project V 官网处获益良多，特此向小薇姐姐表示感谢🙏。

## 附录

### 推荐阅读

Security in-a-box 数据安全工具及策略 (中文版) (网页)

数字安全实用手册 (网页, 内含三部 pdf 电子书)

人权捍卫者的数据安全与隐私 (电子书)

公民实验室: 如何绕过互联网审查 (电子书)

Citizen Lab: EVERYONE'S GUIDE TO BY-PASSING INTERNET CENSORSHIP

privacytools.io (网页)

Electronic Frontier Foundation 电子前哨基金会 (网站)

数字移民 (网站)

https://medium.com/@iyouport (博客)

https://steemit.com/@iyouport (博客)

有关密码学的科普内容 (博客)

【编程随想】收藏的电子书清单 (多个学科, 含下载链接) (网页)

## 鸣谢

(按首字母顺序排序)

Baye

编程随想

破娃酱

clowwindy

聪聪 (印象笔记 | 科技 NEWS)

Cryptoboy404

iYouPort

Telegram Messenger

PSA-安全公告专栏

泡泡

Shadowrocket News

Solidot

Telegram 新手指南

Victoria Raymond

网络公民安全指南

信息极权社会的生存手册 (已删号)