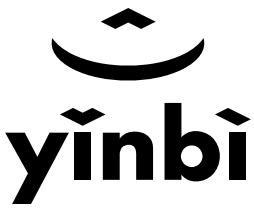


隐币加密货币:
无封锁无金融限制的加密货币
跨境转账支付钱包

Yinbi Global Alliance LLC
Yin.bi

背景与概览

在比特币早期，支持者经常宣称，比特币无法被那些想要控制或压制它的政府染指。事实上，这是比特币主要的亮点之一。例如，最早引入比特币的Slashdot帖子指出：“这个社区希望，比特币将不受任何政府控制。”[1]

然而，现有的加密货币无法确保它们能经受政府的限制。某个国家想要完全或部分封锁比特币或任何加密货币的网络流量，不是什么难事。这是迄今加密货币发展中的一个主要盲区，而隐币将致力于解决这个问题。

政府可轻易封锁现有加密货币

大多数（甚至是全部）加密货币都有一些弱点，政府可以利用这些弱点封锁其流量。

让我们以比特币作为案例来说明这一点。这不仅因为它是最早最知名的加密货币之一，而且因为许多加密货币的交易机制都沿袭最初的比特币设计，也继承了同样的缺陷。[2]

比特币流量可以很容易识别，因为在广播交易时，所有者签名包含在明文中（如图1所示）。政府通过封锁广播交易的流量，就能轻松阻止所有交易。政府还可以根据流量分析阻止一部分用户广播他们的交易，本质上冻结他们的资金和账户。

假设维基解密有一个用于接收捐赠的比特币地址。希望干扰维基解密运营的国家可以在网络层面阻止来自或去向该比特币地址的交易，防止用户使用比特币向维基解密捐款。这些国家还可以识别试图捐赠给

1 见 https://news.slashdot.org/story/10/07/11/1747245/bitcoin-releases-version-03

2 比如莱特币：https://litecoin.com/

维基解密的用户并阻止与这些比特币地址之间的交易，冻结任何试图捐赠的人的资产。

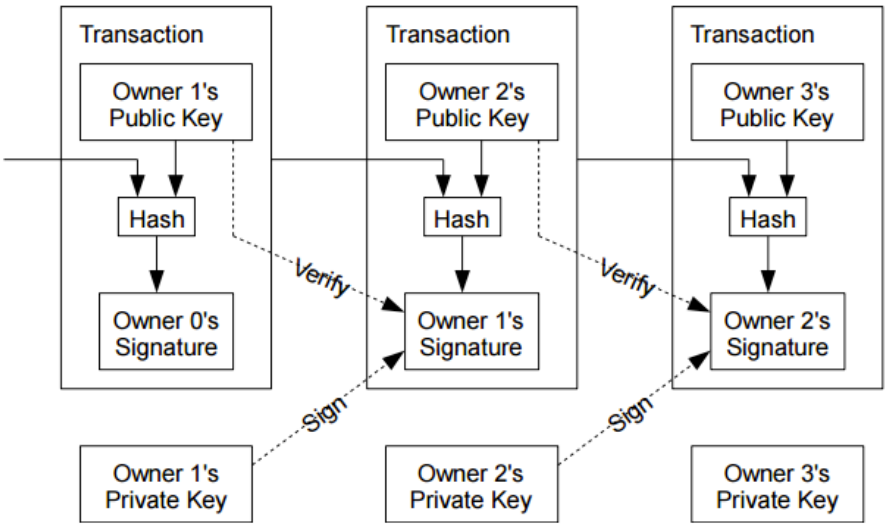


图1.比特币交易图解，选自比特币白皮书[3]

这种担心并非仅仅是理论上的。随着加密货币市场的增长，监控、管理和阻止这些货币的使用和访问的努力也在增加。在美国这样的“开放”民主国家中，监管在过去一年中急剧增加，而中国[4]和俄罗斯[5]等更具限制性的国家已经开始审查或禁止使用加密货币 。

隐币是抗审查的加密货币

为了解决这一根本性弱点，隐币旨在提供市场上最抗封锁审查的加密货币，并在未来创建抗封锁去中心化的币币交易平台 。

隐币的第一阶段计划包含如下产品／功能:

3 https://bitcoin.org/bitcoin.pdf

4 https://www.scmp.com/tech/enterprises/article/2161014/china-block-more-120-offshore-crypto-currency-exchanges-crackdown

5 https://www.theregister.co.uk/2017/10/10/russia_to_ban_cryptocurrency_exchanges/

1. 隐币（YNB），是由恒星币网络提供支持的代币[6], 网络上与Lantern合作[7]。
2. 抗封锁的钱包用于支持隐币（YNB）收付款；
3. 利用Lantern反审查技术建立抗封锁的币币兑换平台。

与目前可用的其他加密货币相比，这些产品具有以下优势：

1. 利用Lantern的反审查技术抗封锁

隐币将利用一系列策略来规避封锁，详见“抗封锁：技术和设计元素”一节。

2. 无限制的国际转账

许多法币不能自由地交换或跨境支付，因为政府通常严格控制货币兑换和国际转账。限制兑换和转账导致公民无法在境外投资或消费，这使得移民、医疗、留学，甚至海外度假都变得困难。在极端情况下，如当一个国家正在经历恶性通货膨胀时，货币兑换可能被完全禁止，当地货币的价值相对于其他货币的价值急剧下降，财富缩水，并致使法币持有者无法获得本国可能稀缺的货物和服务。

隐币将没有这样的限制，并将利用其抗封锁技术，支持即时的国际支付和转账。

3. 利用恒星币的网络和共识协议进行高速低成本的交易

许多广泛认可的加密货币需要较长的时间创建区块，导致交易时间颇为缓慢。众所周知，比特币的区块创建时间大约为

6 https://www.stellar.org/

7 https://getlantern.org/

10分钟[8],即便像以太坊这样性能更高的加密货币也需要大约15秒的时间[9]。

跨境的法币交易需要更长时间。即使在没有跨境支付限制的国家，国际支付通常也需要长达五个工作日，并且费用很高，这使得小额支付非常不切实际的[10]。 在有金融限制的国家，它们可能需要更长时间，更多花费，甚至完全被禁止。

作为一款恒星币代币，隐币（YNB）交易处理速度非常快，通常只需几秒钟（估计不到一秒，至多五秒[11]）。隐币将能够支持数十亿用户，而不会影响交易处理时间。与包括比特币在内的许多虚拟货币不同，这使得隐币能成为真正的大规模交易媒介，而不仅仅是一种储存财富的方法。
此外，恒星币的共识机制允许其以低廉的成本并行处理较小金额的交易，从而使其适用于各种规模的支付和交易。

抗封锁：技术和设计元素

识别现有加密货币交易流量

现有加密货币的流量可以被轻松识别。例如，在比特币客户端上运行Wireshark并使用[12]其比特币显示过滤器[13]，就能标记所有比特币流量（图2）。虽然有用于加密客户端之间流量的比特币标准[14]，但并未实际采用。[15]

8 https://bitinfocharts.com/comparison/bitcoin-confirmationtime.html

9 2018年8月27日根据 https://www.etherchain.org/charts/blockTime 推算。

10 https://smartasset.com/checking-account/how-long-does-a-wire-transfer-take

11 https://www.abitgreedy.com/transaction-speed/; 其他报告估计交易时间1-3秒: https://www.lumenauts.com/blog/how-many-transactions-per-second-can-stellar-process 和 https://www.mobilecoin.com/whitepaper-en.pdf

12 https://bitcoin.org

13 https://www.wireshark.org/docs/dfref/b/bitcoin.html

14 见 BIP-151 https://github.com/bitcoin/bips/blob/master/bip-0151.mediawiki

15 BIP-151 并未执行 https://github.com/bitcoin/bitcoin/blob/master/doc/bips.md

在这方面，专注于用户匿名的货币并不比比特币好。虽然它们使交易的发送者和接收者难以被网络审查者识别，但他们没有采取任何措施来阻止试图封锁其流量的网络审查者。以门罗币（Monero）为例，对其可执行文件（或源代码本身[16]）的简单分析可发现其内置的IP地址（图3）。在Wireshark中监控门罗币流量可以确认，客户端在加入网络（图4）时确实使用了这些IP地址。试图在其境内控制门罗币使用的政府只需要自动扫描可执行文件或源代码，找到这些IP地址，然后通过丢包或者TCP连接重置等手段封锁这些地址。

内置固定IP并不是门罗币容易封锁的唯一弱点。默认情况下，门罗币还为P2P流量（端口18080）和RPC流量（端口18081）使用固定端口（图5）。虽然这些端口号可以自定义，但绝大部分用户都使用默认端口，因此审查者只需阻止这些端口便可阻止门罗币流量。

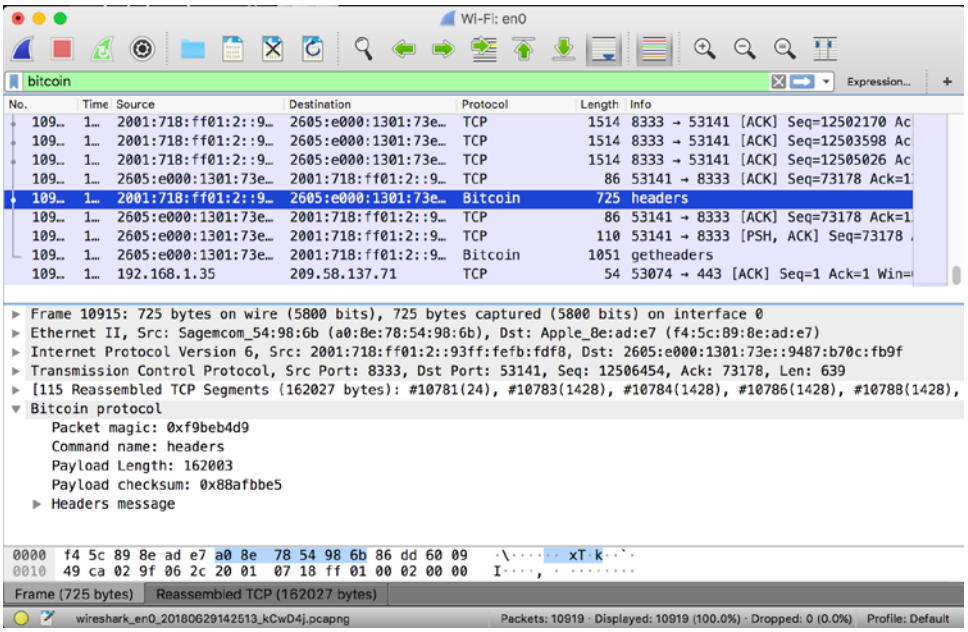


图2. Wireshark识别比特币流量

16 https://github.com/monero-project/monero/blob/master/src/p2p/net_node.inl#L388

```
[MacOS]$ strings monerod | grep -Eo '[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}'
127.0.0.1
0.0.0.0
212.83.175.67
5.9.100.248
163.172.182.165
195.154.123.123
212.83.172.165
162.210.173.150
162.210.173.151
107.152.130.98
212.83.175.67
5.9.100.248
163.172.182.165
161.67.132.39
198.74.231.92
195.154.123.123
212.83.172.165
194.150.168.168
```

图3. 门罗币二进制代码中包含的IP地址

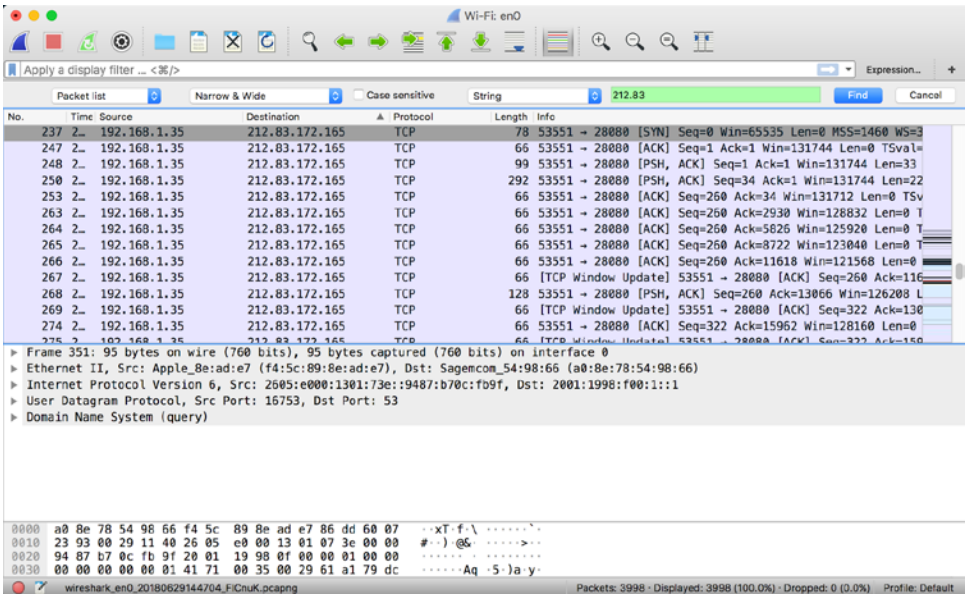


图4. Wireshark识别到门罗币到内置IP 212.83.172.165的流量

```
[MacOS]$ ./monerod --help | grep bind-port
  --zmq-rpc-bind-port arg (=18082, 28082 if 'testnet', 38082 if 'stagenet')
  --p2p-bind-port arg (=18080, 28080 if 'testnet', 38080 if 'stagenet')
  --rpc-bind-port arg (=18081, 28081 if 'testnet', 38081 if 'stagenet')
```

图5: 通过默认端口运行门罗币

前文的目的不是为了指出门罗币的缺陷。事实上，门罗币被点出是因为它是最安全、最保护隐私的货币之一。这说明即使是设计最好的加密货币也有一个关键的盲点，使它们仍然受到政府影响：它们没有考虑到政府可以大规模地控制网络流量。这些货币能存在是因为政府还未对货币网络进行封锁。

VPN不能为加密货币交易提供可靠的反审查保护

在许多有互联网审查的国家/地区，用户依靠VPN来访问被封锁的网站。理论上，使用VPN可以使用户避开审查者对加密货币流量的封锁。

然而，VPN有很大局限性，相对于隐币通常很容易被封锁。它们通常缺少这些关键功能，例如：

1. 设计缺陷：VPN技术的开发是为了使远程用户和分支机构安全地访问企业应用程序和其他资源[17]。因此，VPN的设计是为了数据安全而不是抗封锁。虽然配置得当的现代VPN协议确实提供了良好的安全性，但自动化识别和封锁VPN非常容易 。
2. 协议多样性: 与隐币相比，VPN使用的协议非常有限，从而更容易被识别和封锁流量。
3. 通过pluggable transports进行协议混淆：很少有VPN使用pluggable transports来混淆流量[18], 这也会使流量更容

17 https://en.wikipedia.org/wiki/Virtual_private_network

18 有些VPN使用业余的流量混淆方案, 但是大部分没有使用。

易识别和封锁。

4. 无点对点(P2P)系统：使用P2P系统可以使用户通过可信节点代理流量，以防止审查者枚举所有开放的代理节点（以下将进一步深入讨论），而VPN不使用P2P。
5. 节点容易被发现：通常，审查者可以轻易地枚举VPN使用的所有服务器并封锁其IP地址，从而使VPN无效。相比之下，隐币将采取措施防止审查者发现所有互联网接入点，并在这些接入点被封锁时动态更改这些接入点（如代理服务器IP）。

隐币提供了比VPN更好的抗封锁保证，而无需运行单独的代理软件。

隐币抗封锁策略

为了避免上述缺陷，隐币将在多个层面上采用抗审查策略，目标是（1）使用一系列已有的审查规避技术改善与全球互联网的连接，以及（2）通过使用点对点技术在国内传输更多流量，减少对全球互联网连接的依赖。

隐币将灵活采用以下所有或部分的反审查工具：

1. Pluggable transports，混淆流量以阻碍深度包检测 (DPI)，或使用诸如域前置(Domain Fronting)等依附的自由（collateral freedom）技术增加封锁流量成本。
2. 点对点（P2P）网络，应用藉此访问所需的信息并建立可信节点之间的网络。
3. 基于P2P的信任网络，仅允许受信任的节点了解彼此的（或其代理的）IP地址，提供更好的网络访问，阻止IP地址枚举和与之相关的IP封锁。
4. 动态的代理服务器网络。

此外，隐币将继续完善技术以应对不断变化的条件，例如审查策略的

变化或新规避技术的发展。

Pluggable transports

首先，在传输层，隐币将使用一组不断发展的“Pluggable transports”，每一种都具有不同的抗审查特性。[19]

抗深度包检测（DPI）的传输

政府审查经常部署深度包检测（DPI）来识别他们希望封锁的网络流量。Pluggable transports通过改变网络流量特征，使得深度包检测更难实施。Pluggable transports可以在TCP或可靠的UDP之上实现。隐币客户端将能够使用TCP、QUIC、KCP[20]，和任何其他可靠的UDP协议[21]

Pluggable transports在应用层之上运行，以提供额外的抗审查特性。每个Pluggable transport都有不同设计，来防止流量分析。

这些方法包括模仿其他常见协议[22]，随机数据包长度并加密等，使得深度包检测（DPI）设备没有可靠的规则来识别它们 。[23]

隐币将使用许多种Pluggable transports，并且随着攻击者能力的发展，能够动态地改变或利用新的传输方式。

---

19 https://www.torproject.org/docs/pluggable-transports.html.en and https://www.pluggable-transports.info/

20 https://github.com/xtaci/kcp-go

21 因为深度包检测设备的状态机对非常见数据包检测不太熟悉，可靠的UDP协议能抗部分审查。比如使用KCP来传输TLS 1.3协议对某些政府很有效。

22 比如 FTE Proxy https://fteproxy.org/ 和 Marionette https://github.com/marionette-tg/marionette

23 比如 obfs4 https://github.com/Yawning/obfs4 和Lampshade https://github.com/getlantern/lampshade

依附的自由

一类重要的pluggable transports依赖于“依附的自由”[24]原则。依附的自由是指设计一个系统，攻击该系统会造成重大和不良的附带损害。在反审查领域，这样的设计使得封锁流量对于审查政府来说代价高昂和/或得不偿失。

域前置(domain fronting)就是这样一种技术。大多数CDN根据HTTP头字段将流量路由到目标站点。使用HTTPS流量时，HTTP头字段被加密，对审查者不可见。如果客户端软件能够访问CDN任何未封锁的IP地址，就可以访问被封锁的目标地址。审查机构阻止域前置流量的唯一方法是封锁CDN所有的IP，而这将封锁在该CDN上的所有站点，包括审查机构不打算审查的站点。因为这可能会对该国“合法”的经济或政治利益造成大规模破坏，因此审查机构不愿采取这种做法。

点对点网络

隐币将使用IPFS[25] 等P2P框架实现P2P系统。IPFS是一个分布式版本化文件系统。用户（IPFS节点）给出需要文件的加密哈希来请求特定内容。这些文件，例如隐币网站的文件，将分成片断，存储到本地或其他的IPFS节点，并按需用类似于BitTorrent的方式从附近的节点获取。

通过这种机制，即使互联网出口被干扰或阻断，隐币的用户仍能够访问存储在网络中的信息。此类信息可包括隐币运行所需的数据，例如客户端配置。它还将提供促进可信节点网络的方法，详见下一小节。

24 https://www.teamupturn.org/static/files/CollateralFreedom.pdf

25 https://ipfs.io/

信任网络

通过利用Lantern网络的大量节点作为备用接入点，隐币可以达到高度的抗封锁。

隐币用户可指定网络中的某些节点为“可信”，例如通过导入联系人列表。[26] 如果用户无法直接或通过其指定的代理访问开放的互联网，但在Lantern的P2P信任网络中尚有一个或多个节点未被封锁（因为他们在审查区域之外，或者可以访问未封锁的代理等），他/她仍然可以通过Lantern网络中的可信任节点访问互联网。

这种分散网络的方法增加了抗审查能力。审查机构若要阻止客户端之间的流量，需要穷举所有客户端。但审查者只有被其他客户端信任才能穷举。虽然审查机构理论上可以通过冒充受信任的客户端来破坏网络，但在数百万个节点中，这将极具挑战，费时费力。此外，即使审查机构破坏了信任网络，他们仍然只能作为加密流量的渠道。他们不会知道该流量的内容，也不知道其目的地。充其量，它们可以简单地封锁流量，而此时隐币将自动路由，避免网络干扰以使用其他接入点，通过其他客户端或任何其他代理连接。

由于其合作伙伴Lantern的用户群巨大，隐币可以实现可信网络，在加密货币中具有独特的地位。潜在的可信节点网络的规模越大，网络作为反审查策略的作用就越好。目前，Lantern的网络在全球范围内拥有超过600万个节点，即便其它加密货币采用类似的策略，他们的可用的节点数量也相形见绌。相比之下，截至2018年8月23日，以太坊有大约18,000个节点[27]，比特币有10,000个以下[28], 而Ripple大约有800

26 信任网络可以由 Kaleidoscope 来组建，使用用户的社交网络来建立可信节点: http://kscope.news.cs.nyu.edu/pub/TR-2008-918.pdf

27 https://www.ethernodes.org/network/1

28 https://bitnodes.earn.com/

个[29]（图6）。 隐币还将利用这个大型网络快速推动其隐币的广泛流通，从而支持和稳定隐币的价值。

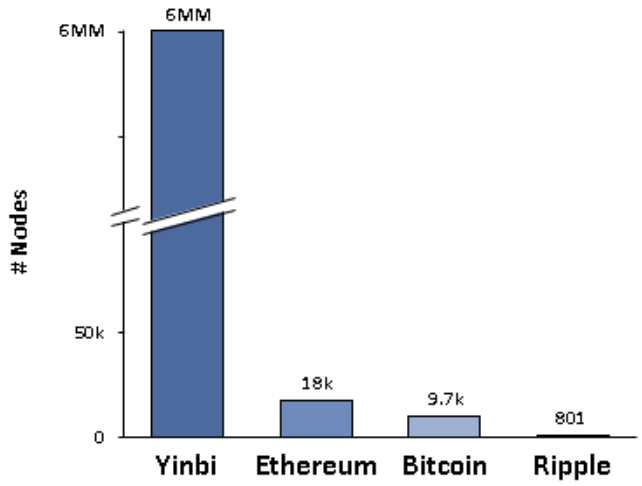


图6. 隐币和其他主流的加密货币可用节点的数量比较

代理网络

隐币将使用一个庞大的动态代理服务器网络来代理被封锁流量。当某些代理的IP地址被审查者封锁时，代理会自动轮换。

网络节点渗透

“网络节点渗透”问题是反审查工具的关键挑战。本质上，反审查工具必须告诉客户端如何访问网络（例如，通过在分布式网络中提供代理服务器或其他节点信息）。与此同时，反审查工具又必须阻止审查者获取接入点信息（防止其通过枚举封锁代理IP）。

这个问题可以分两部分来看。首先，该工具必须决定如何查找网络访问信息，其次再实际获取该信息。通常，Web浏览器将使用DHCP来获取DNS服务器的IP地址（步骤1），然后在DNS服务器上查找域名

29 https://xrpcharts.ripple.com/#/topology

（步骤2）。但是，由于审查国家的DNS被污染，该方案并不是反审查工具的选择。

相反，隐币将依靠前述的技术来解决这些问题。例如，它可以从其他可信客户端或者域前置获取代理服务器IP，从而防止DNS污染。

产品与路线图

隐币（YNB）

隐币是恒星币网络(Stellar Network)上发行的资产。发行总额为8880亿的YNB，不会超额发行。隐币中的50％最初将通过与Lantern合作进行分配。将来可能会提供额外的分配渠道。

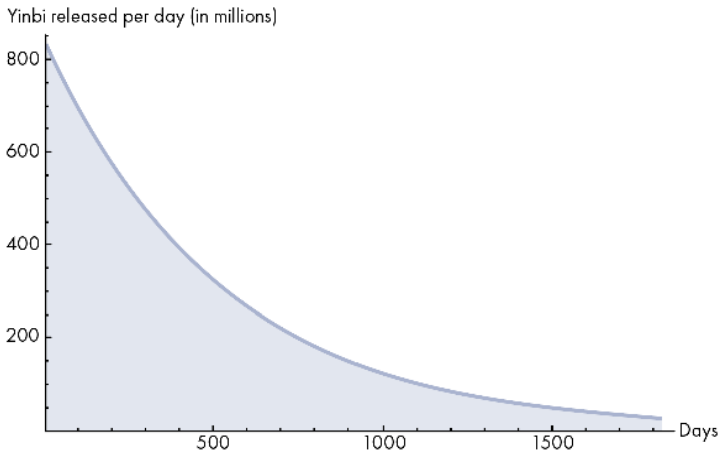
分配

%	参与方
50%	隐币社群
40%	创始团队
10%	未来员工

YNB分配

50％的YNB将向公众发行，并通过与Lantern的持续合作进行发行。每天释放的YNB数量将以平滑的指数函数逐天缓慢减少 。

隐币将发送给Lantern专业版用户，根据每天来自中国的Lantern专业版购买数量，在中国购买者之间进行分配（2年用户的隐币配额是1年用户的2倍） 见图7。



$$13875\left(1-\frac{1}{\sqrt[365]{2}}\right)2^{5-\frac{n}{365}}$$

图7:隐币每天发放的数量

例如，如果在某天发布100个YNB，当天来自中国的购买[30]是8个1年的Lantern专业版和1个2年的Lantern专业版，那么每个1年的帐户购买者将获得10个YNB，而2年账户购买者将获得20 YNB。（仅作为说明性示例。分配的YNB的首日交易量将从840万开始，并且根据上述公式每天减少）。

	1年用户	2年用户	总计
购买量*	8	1	9
隐币配额	10	20	
当日隐币发行总量	**80**	**20**	**100**

示例说明隐币每日分配情况

30 “购买”包括直接在应用内购买/续订，也包括在应用内激活Lantern专业版激活码。Lantern专业版激活码可从第三方代理或Lantern批量购买接口购买（该接口将随着与隐币发行同步。）若使用激活码，隐币的发放以用户在应用内激活Lantern专业版激活码当日参与分配，而非激活码生成/购买日期。Yinbi仅适用于中国居民。

隐币将于2018年第四季度开始发型，具体日期待定。将在中国标准时间（CST）运行。

隐币客户端:收付YNB

隐币客户端将允许用户发送和接收YNB，并将在YNB发行开始后不久发布。

隐币交易所:抗封锁去中心化的加密货币交易所

隐币交易所将是一个抗封锁去中心化的交易所，用户将能够交易包括YNB、BTC、ETH及其它随后添加的加密货币币种。隐币客户端发布之后，隐币交易所将随后到来。

其他产品细节

操作系统

隐币客户端和交易所将首先发布以下版本，其他版本待定:

- 安卓版
- 电脑版

发放区域和支持的语言

两款产品首发以及YNB赠送，仅限于中国用户，支持语言为中文和英文。随着时间的推移，可能会添加其他区域和语言支持。

团队

隐币全球联盟 (Yinbi Global Alliance LLC) 团队在区块链、P2P、反审查和抗封锁技术方面拥有丰富的经验。该团队由P2P、区块链和反审查领域的一些世界上最有经验的工程师、研究人员和科学家组成。