Yinbi Cryptocurrency:
Introducing a censorship-resistant cryptocurrency
and cross-border payment wallet

Yinbi Global Alliance LLC
Yin.bi

Background and overview

In the early days of Bitcoin, proponents often claimed that it would be untouchable by governments who might want to control or suppress it. In fact, this was seen by many as one of its primary selling points. For example, the original Slashdot post introducing Bitcoin noted that "[t]he community is hopeful the currency will remain outside the reach of any government."[1]

However, existing cryptocurrencies provide no assurance that they can withstand government efforts to restrict their use. It is a relatively trivial matter for a state adversary to block Bitcoin or any other cryptocurrency's network traffic, either in whole or in part, if it chose to do so. This is a major blindspot in the development of cryptocurrencies to date, and one that Yinbi aims to address.

Existing cryptocurrencies are easily blockable by governments

Most, if not all, cryptocurrencies have some vulnerability that governments can exploit to block their traffic.

Bitcoin provides a useful case study for illustrating this point, not just because it is one of the oldest and most well-known cryptocurrencies, but also because many cryptocurrencies have modeled their transactions after the one described in the initial Bitcoin paper, and therefore suffer from the same flaw.[2]

Bitcoin traffic can be easily identified because the hash of the owner's signature is included in plain text when broadcasting the transaction (illustrated in Figure 1). A government could therefore easily block all transactions by implementing a network block of all transaction broadcasts or, perhaps more likely, block a subset of users from broadcasting transactions, essentially freezing their funds and accounts.

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

[2] See LiteCoin, for example: https://litecoin.com/

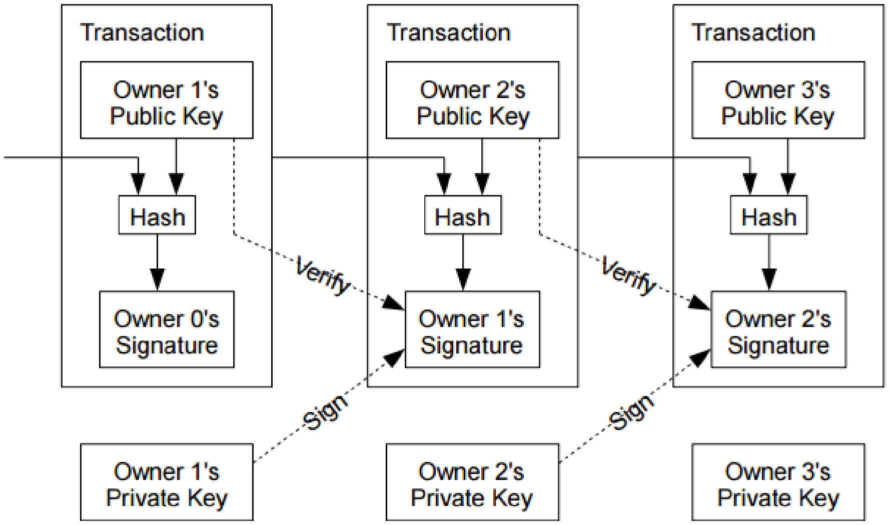


Figure 1. Bitcoin transaction diagram from original Bitcoin paper[3]

Suppose, for example, that Wikileaks has a Bitcoin address for receiving donations. A state adversary wishing to interfere with Wikileaks' operations could block all transactions going to or from this Bitcoin address at the network layer, preventing users from donating to Wikileaks with Bitcoin. Moreover, the state could identify users attempting to donate to Wikileaks and block transactions to and from those Bitcoin addresses, essentially freezing the assets of anyone attempting to donate.

This concern is not merely hypothetical. As the cryptocurrency market has grown, so too has the effort to monitor, regulate, and block the use of and access to these coins. Within "open" democracies such as the U.S., regulatory efforts have increased dramatically in the past year, while more restrictive countries such as China[4] and Russia[5] have moved to censor or ban outright the use of cryptocurrencies.

[3] See https://bitcoin.org/bitcoin.pdf

[4] See https://www.scmp.com/business/banking-finance/article/2132009/china-stamp-out-cryptocurrency-trading-completely-ban

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

Yinbi will provide a censorship-resistant alternative

To address this fundamental vulnerability, Yinbi aims to provide the most censorship- and blocking-resistant cryptocurrency in the market, coupled in the future with a blocking-resistant, decentralized cryptocurrency-to-cryptocurrency exchange.

The initial Yinbi roadmap includes the following products/features:

1. YNB, a token powered by the Stellar network[6] and leveraging our partnership with Lantern[7].
2. A blocking-resistant wallet for sending and receiving YNB payments.
3. A blocking-resistant exchange, similarly leveraging anti-censorship technology developed by Lantern.

These products will have several attractive characteristics over other cryptocurrencies currently available:

1. **Blocking resistance leveraging Lantern's anti-censorship techniques:**

   Yinbi will utilize a number of strategies to evade censors, discussed in depth in the "Blocking Resistance: Technology and design elements" section below.

2. **Unrestricted international transfers**

   Many fiat currencies cannot be freely sent or exchanged across borders because governments often tightly control currency exchanges and international transfers. Restrictions on exchanges and transfers can prevent citizens' from investing or spending money abroad, which poses challenges for citizens wishing to emigrate, seek health care or education abroad, or even vacation overseas. In extreme cases, such as when a country is experiencing

[6] See https://www.stellar.org/

[7] See https://getlantern.org/

hyperinflation, currency exchange is entirely forbidden, causing citizens wealth to erode as the local currency's value drops relative to others and preventing them from obtaining goods and services that might be scarce within their home country.

Yinbi will have no such restriction and will allow instant international payment and transfer, aided by its blocking resistance strategies.

3. **High-speed, low-cost transactions leveraging the Stellar network and consensus protocol**

Many widely recognized cryptocurrencies suffer from slow transaction times due to high block creation times. Bitcoin's block time is notoriously long at around 10 minutes[8], but even a more performant cryptocurrency like Ethereum has a block time of around 15 seconds[9].

Cross-border fiat currency transactions take much longer. Even in countries without substantial restrictions, international payments can often take up to five business days and are quite costly, making them impractical for smaller payments.[10] In countries with greater restrictions, they can take even longer, cost more, or be prohibited entirely.

As a Stellar token, YNB transactions are processed very quickly, typically taking only a few seconds (with estimates ranging from less than one to at most five seconds[11]), and YNB will be able to scale horizontally to billions of users without impacting transaction times. Unlike many virtual currencies, including Bitcoin, this makes it viable as a true medium of exchange at scale, and not just as a store of value.

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

[9] Estimated from https://www.etherchain.org/charts/blockTime as of August 27, 2018.

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

[11] See https://www.abitgreedy.com/transaction-speed/; other reports claim transaction speeds between one and three seconds: https://www.lumenauts.com/blog/how-many-transactions-per-second-can-stellar-process and https://www.mobilecoin.com/whitepaper-en.pdf

> In addition, Stellar's consensus mechanism allows for parallel processing of transactions of smaller amounts without high fees, making it practical for payments and transactions of all sizes.

Blocking resistance: Technology and design elements

Identifying existing cryptocurrency traffic

Traffic for existing cryptocurrencies can be easily identified. Bitcoin traffic, for example, can be identified by running Wireshark alongside the standard Bitcoin wallet[12] and using Wireshark's Bitcoin display filters[13] to flag all Bitcoin traffic (Figure 2). While there is a Bitcoin standard for encrypting traffic between peers[14], it is not adopted in practice.[15]

Currencies focused on user anonymity fare no better than Bitcoin in this regard. While they make it challenging for network observers to identify the sender and receiver of transactions, they do nothing to protect against network observers attempting to block their traffic. Taking Monero as an example, simple analysis of the downloadable binary (or the source code itself[16]) reveals its bootstrapping IP addresses (Figure 3). Monitoring Monero traffic in Wireshark confirms that these IP addresses are used when running Monero, likely by Monero wallets to join the network (Figure 4). A censoring government attempting to control the use of Monero within its borders need only automate the process of identifying these IP addresses within the Monero binary or source code, and then disrupt traffic destined for those addresses, for example by dropping network packets or issuing TCP resets to TCP connections to those IPs.

Hardcoded IPs are not the only vulnerability that censors can exploit to

[12] Available at https://bitcoin.org

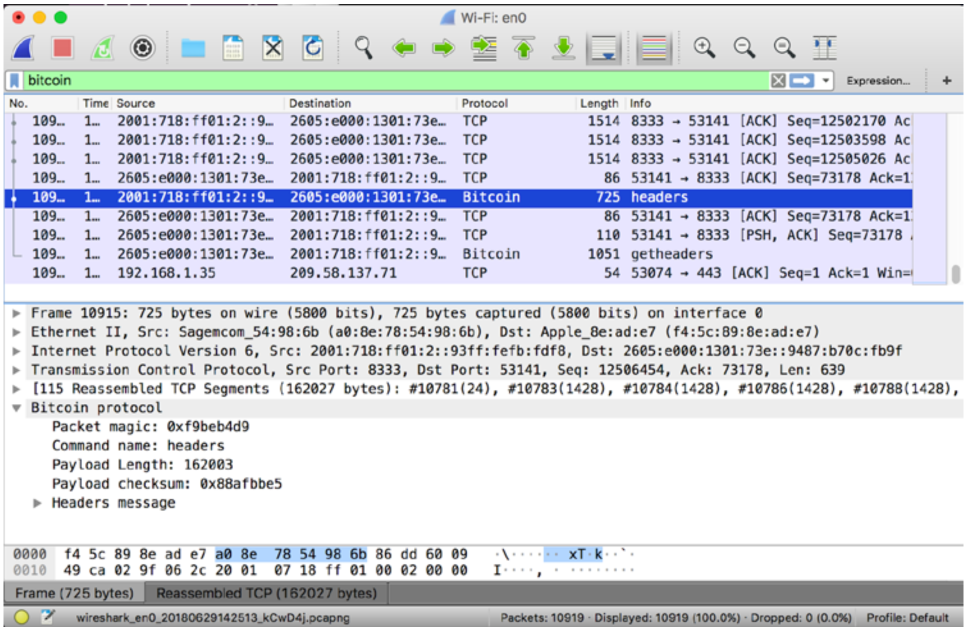
[13] See https://www.wireshark.org/docs/dfref/b/bitcoin.html

[14] See BIP-151 at https://github.com/bitcoin/bips/blob/master/bip-0151.mediawiki

[15] BIP-151 is not implemented at https://github.com/bitcoin/bitcoin/blob/master/doc/bips.md

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

block Monero. Monero also uses fixed ports for P2P traffic (port 18080) and for RPC traffic (18081) by default (Figure 5). While users can configure a custom listening port, users almost always rely on default ports, so censors would be able to block Monero traffic simply by blocking those ports.



No.	Time	Source	Destination	Protocol	Length	Info
109…	1…	2001:718:ff01:2::9…	2605:e000:1301:73e…	TCP	1514	8333 → 53141 [ACK] Seq=12502170 Ac
109…	1…	2001:718:ff01:2::9…	2605:e000:1301:73e…	TCP	1514	8333 → 53141 [ACK] Seq=12503598 Ac
109…	1…	2001:718:ff01:2::9…	2605:e000:1301:73e…	TCP	1514	8333 → 53141 [ACK] Seq=12505026 Ac
109…	1…	2605:e000:1301:73e…	2001:718:ff01:2::9…	TCP	86	53141 → 8333 [ACK] Seq=73178 Ack=1
109…	1…	2001:718:ff01:2::9…	2605:e000:1301:73e…	Bitcoin	725	headers
109…	1…	2605:e000:1301:73e…	2001:718:ff01:2::9…	TCP	86	53141 → 8333 [ACK] Seq=73178 Ack=1
109…	1…	2605:e000:1301:73e…	2001:718:ff01:2::9…	TCP	110	53141 → 8333 [PSH, ACK] Seq=73178
109…	1…	2605:e000:1301:73e…	2001:718:ff01:2::9…	Bitcoin	1051	getheaders
109…	1…	192.168.1.35	209.58.137.71	TCP	54	53074 → 443 [ACK] Seq=1 Ack=1 Win=

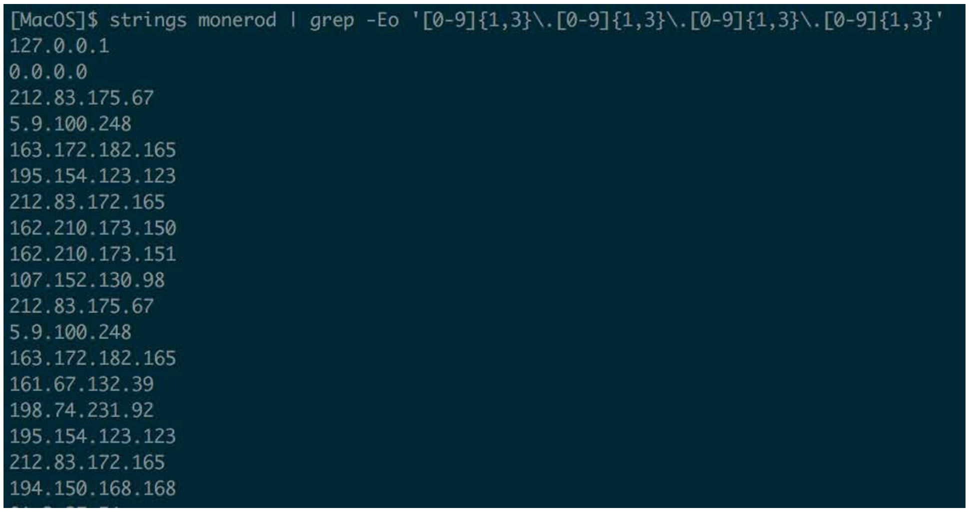
```
▶ Frame 10915: 725 bytes on wire (5800 bits), 725 bytes captured (5800 bits) on interface 0
▶ Ethernet II, Src: Sagemcom_54:98:6b (a0:8e:78:54:98:6b), Dst: Apple_8e:ad:e7 (f4:5c:89:8e:ad:e7)
▶ Internet Protocol Version 6, Src: 2001:718:ff01:2::93ff:fefb:fdf8, Dst: 2605:e000:1301:73e::9487:b70c:fb9f
▶ Transmission Control Protocol, Src Port: 8333, Dst Port: 53141, Seq: 12506454, Ack: 73178, Len: 639
▶ [115 Reassembled TCP Segments (162027 bytes): #10781(24), #10783(1428), #10784(1428), #10786(1428), #10788(1428),
▼ Bitcoin protocol
    Packet magic: 0xf9beb4d9
    Command name: headers
    Payload Length: 162003
    Payload checksum: 0x88afbbe5
  ▶ Headers message

0000  f4 5c 89 8e ad e7 a0 8e  78 54 98 6b 86 dd 60 09   ·\······ xT·k··`·
0010  49 ca 02 9f 06 2c 20 01  07 18 ff 01 00 02 00 00   I····, · ········
```

Frame (725 bytes) | Reassembled TCP (162027 bytes)

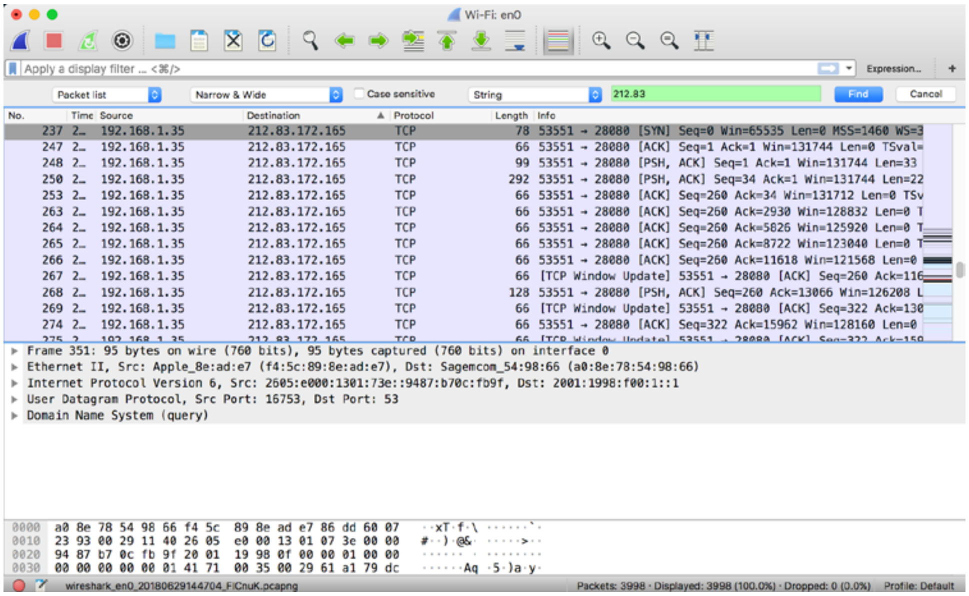
wireshark_en0_20180629142513_kCwD4j.pcapng   Packets: 10919 · Displayed: 10919 (100.0%) · Dropped: 0 (0.0%)   Profile: Default

Figure 2. Bitcoin traffic identified in Wireshark



```
[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
```

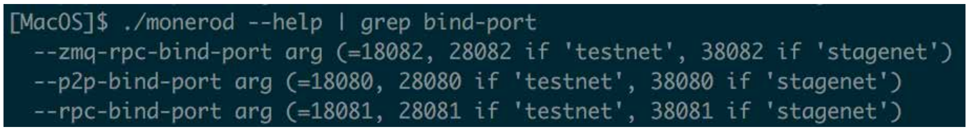
Figure 3. IP addresses embedded in the Monero binary



```
No.   Time Source          Destination      ▲ Protocol  Length Info
  237 2…  192.168.1.35     212.83.172.165     TCP           78 53551 → 28080 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=3
  247 2…  192.168.1.35     212.83.172.165     TCP           66 53551 → 28080 [ACK] Seq=1 Ack=1 Win=131744 Len=0 TSval=
  248 2…  192.168.1.35     212.83.172.165     TCP           99 53551 → 28080 [PSH, ACK] Seq=1 Ack=1 Win=131744 Len=33
  250 2…  192.168.1.35     212.83.172.165     TCP          292 53551 → 28080 [PSH, ACK] Seq=34 Ack=1 Win=131744 Len=22
  253 2…  192.168.1.35     212.83.172.165     TCP           66 53551 → 28080 [ACK] Seq=260 Ack=34 Win=131712 Len=0 TSv
  263 2…  192.168.1.35     212.83.172.165     TCP           66 53551 → 28080 [ACK] Seq=260 Ack=2930 Win=128832 Len=0 T
  264 2…  192.168.1.35     212.83.172.165     TCP           66 53551 → 28080 [ACK] Seq=260 Ack=5826 Win=125920 Len=0 T
  265 2…  192.168.1.35     212.83.172.165     TCP           66 53551 → 28080 [ACK] Seq=260 Ack=8722 Win=123040 Len=0 T
  266 2…  192.168.1.35     212.83.172.165     TCP           66 53551 → 28080 [ACK] Seq=260 Ack=11618 Win=121568 Len=0
  267 2…  192.168.1.35     212.83.172.165     TCP           66 [TCP Window Update] 53551 → 28080 [ACK] Seq=260 Ack=116
  268 2…  192.168.1.35     212.83.172.165     TCP          128 53551 → 28080 [PSH, ACK] Seq=260 Ack=13066 Win=126208 L
  269 2…  192.168.1.35     212.83.172.165     TCP           66 [TCP Window Update] 53551 → 28080 [ACK] Seq=322 Ack=130
  274 2…  192.168.1.35     212.83.172.165     TCP           66 53551 → 28080 [ACK] Seq=322 Ack=15962 Win=128160 Len=0
  275 2…  192.168.1.35     212.83.172.165     TCP           66 [TCP Window Update] 53551 → 28080 [ACK] Seq=322 Ack=159
▶ Frame 351: 95 bytes on wire (760 bits), 95 bytes captured (760 bits) on interface 0
▶ Ethernet II, Src: Apple_8e:ad:e7 (f4:5c:89:8e:ad:e7), Dst: Sagemcom_54:98:66 (a0:8e:78:54:98:66)
▶ Internet Protocol Version 6, Src: 2605:e000:1301:73e::9487:b70c:fb9f, Dst: 2001:1998:f00:1::1
▶ User Datagram Protocol, Src Port: 16753, Dst Port: 53
▶ Domain Name System (query)

0000  a0 8e 78 54 98 66 f4 5c  89 8e ad e7 86 dd 60 07   ··xT·f·\ ······`·
0010  23 93 00 29 11 40 26 05  e0 00 13 01 07 3e 00 00   #··)·@&· ·····>··
0020  94 87 b7 0c fb 9f 20 01  19 98 0f 00 00 01 00 00   ······ · ········
0030  00 00 00 00 00 01 41 71  00 35 00 29 61 a1 79 dc   ······Aq ·5·)a·y·
wireshark_en0_20180629144704_FlCnuK.pcapng      Packets: 3998 · Displayed: 3998 (100.0%) · Dropped: 0 (0.0%)   Profile: Default
```

Figure 4. Monero traffic to hard-coded IP 212.83.172.165 identified in Wireshark



```
[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')
```

Figure 5. Running Monero binary with default ports

The intention here is not to point out flaws in Monero. In fact, Monero is singled out because it is one of the most secure, privacy-preserving currencies. This merely illustrates that even the best designed cryptographic currencies have a critical blindspot that leaves them within reach of governments: namely, that they do not account for the fact that that governments can exert significant control over network traffic. These currencies are only able to exist to the extent that governments around the world permit them to.

VPNs do not provide reliable censorship protection for cryptocurrency traffic

In many countries with internet censorship, users rely on VPNs to access blocked sites. In theory, using a VPN could enable users to thwart censors' efforts to block cryptocurrency traffic as well.

However, VPNs are limited and are generally quite easily blocked relative to Yinbi. They typically lack key features of those tools, such as:

1. *Design defects.* VPN technology was developed to allow remote users and branch offices to securely access corporate applications and other resources.[17] Consequently, VPNs are designed for data security rather than blocking resistance. While modern VPN protocols with correct configuration do offer good security, it is extremely easy to identify and block VPNs using automation.
2. *Protocol diversification.* VPNs use a very limited set of protocols compared to Yinbi, making it easier to identify and block traffic.
3. *Protocol obfuscation via pluggable transports.* Few VPNs if any use pluggable transports[18], as described below, to obfuscate traffic, which also renders traffic more easily identifiable and blockable.
4. *Peer-to-peer systems.* Use of P2P systems can enable users to proxy through trusted peers in a way that can prevent censors from enumerating all access points to the open internet (as discussed in further depth below). VPNs do not make use of P2P.
5. *Trivial node discovery.* Typically a censor can easily enumerate all servers used by a VPN very easily and block their IP addresses, rendering VPNs ineffective. By contrast, Yinbi will implement measures to prevent censors from discovering all internet access points and to dynamically change those access points (such as proxy server IPs) if they become blocked.

Yinbi offers the a greater guarantee of blocking resistance than VPNs, without the inconvenience of running a separate application to access the open internet.

[17] See https://en.wikipedia.org/wiki/Virtual_private_network

[18] There are some VPNs that use ad-hoc obfuscation, but the vast majority do not.

Yinbi blocking resistance strategies

To avoid the pitfalls described above, Yinbi will incorporate censorship-resistance strategies at several levels, with the goals of (1) improving connectivity to the global internet using a number of established censorship circumvention techniques, and (2) reducing reliance on global internet connectivity by carrying more traffic domestically using peer-to-peer technology.

Yinbi will employ a wide range of anti-censorship tools, including some or all of the following, each of which is described in more detail below:

1. Pluggable transports that manipulate traffic in ways that obstruct DPI or use collateral freedom techniques such as domain fronting to increase the cost of blocking traffic
2. A peer-to-peer (P2P) network providing access to information needed by the app to function and facilitating a network of trusted peer nodes
3. A P2P-based trust network that allows only trusted peers to learn each other’s (or proxies’) IP addresses, and thwarting IP enumeration and subsequent IP-blocking attacks.
4. A dynamic network of proxy servers

In addition, Yinbi will continue refining its approach in response to evolving conditions, such as changes in censors’ strategies or the development of new circumvention techniques.

Pluggable transports

First, at the transport layer, Yinbi will use a continually evolving set of “pluggable transports,” each with different censorship resistant properties.[19]

DPI-resistant transports

Censoring governments often deploy DPI to identify network flows they

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

wish to block. Pluggable transports attempt to defeat DPI devices by altering the appearance of network traffic in any fashion that makes DPI approaches more difficult. Pluggable transports can be implemented on top of either TCP or reliable UDP. The Yinbi wallet will be able to use TCP, QUIC, KCP[20], and any other reliable UDP implementation.[21]

Pluggable transports operate above this at the application layer to provide additional censorship-resistant properties. Each transport offers a unique approach designed to make it resistant.

These range from mimicking other common protocols[22] to randomizing packet lengths with high entropy padding along with additional encryption such that DPI devices have no reliable rules for consistently identifying them.[23]

Yinbi will employ a number of these pluggable transports, and will have the ability to dynamically change transports or to utilize new transports as the capabilities of adversaries evolve.

Collateral freedom-based transports

One important class of pluggable transports relies on the principle of “collateral freedom”.[24] Collateral freedom is the idea that one can design a system in such a way that attacking that system would cause significant and undesirable collateral damage. In the the anti-censorship realm, this involves designing tools such that blocking traffic through those tools would be extremely costly and/or politically undesirable to the censoring government.

[20] See https://github.com/xtaci/kcp-go

[21] Reliable UDP alone can provide some moderate degree of censorship resistance simply because DPI devices are generally less sophisticated in their abilities to record the state machines of these less common protocols. For example, simply running TLS 1.3 over KCP could be effective against some adversaries.

[22] See, for example, FTE Proxy https://fteproxy.org/ and Marionette https://github.com/marionette-tg/marionette

[23] See, for example, obfs4 https://github.com/Yawning/obfs4 and Lampshade https://github.com/getlantern/lampshade

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

"Domain-fronting" is one such technique. It takes advantage of the fact that most CDNs route traffic to destination sites according to the HTTP Host header. With HTTPS traffic the Host header is encrypted, making it invisible to censors. If wallet software is able to reach any unblocked IP address on a given CDN that supports the above style of routing, then it can access censored destinations. The only way censors can block domain-fronted traffic is to deploy wholesale IP blocking against the CDN, which would block other uncensored sites served on that CDN. Because this would presumably cause massive disruption to "legitimate" economic or political interests inside the country, censors should be reluctant to take this approach.

Peer-to-peer network

Yinbi will implement a P2P system using a P2P framework such as IPFS.[25] IPFS is a distributed, versioned file system that allows users (IPFS nodes) to request particular content given the cryptographic hash of that content. Pieces of these files — for example, the files for the Yinbi website — would be stored locally on network nodes, and fetched from nearby nodes to satisfy a request for content in a fashion similar to BitTorrent.
This mechanism will enable users of Yinbi to access information stored in the network even in the event of a major network disturbance during which access to the open internet is disrupted. Such information could include data necessary for Yinbi to function, such as wallet configuration data.
It will also provide a means of facilitating the network of trusted nodes described in the next subsection.

Trust network

Yinbi will achieve a high level of censorship resistance by leveraging the vast number of nodes in use as part of the Lantern network as alternate access points.

Yinbi users will designate other nodes in the network as "trusted", e.g. by importing a list of contacts.[26] If a user cannot access the open internet

[25] See https://ipfs.io/

[26] This trust network could also operate along the lines of a system like Kaleidoscope, for example, making use of a user's social network to identify trusted nodes: http://kscope.news.cs.nyu.edu/pub/TR-2008-918.pdf

either directly or via her assigned proxies, she will still be able to access it through her network of trusted peers in the Lantern network, assuming that one or more of those peers has unfettered internet access (because they are located outside of the censored region, have access to an unblocked proxy, etc.).

This federated network approach adds another layer of censorship resistance. In order for censors to block traffic between peers, they would need to enumerate all peers, which in turn requires them to be trusted by other peers in the network. While censors could in theory compromise the network by impersonating trusted peers, that would be extremely challenging and labor intensive at the scale of millions of nodes. Moreover, even if a censor were to compromise the trust network, they would still only act as conduits for encrypted traffic. They would not know the contents of that traffic, nor its destination. At best, they could simply block traffic, at which point Yinbi would automatically route around the network disturbance to use another access point, be it another peer or any other proxied connection.

Yinbi is uniquely positioned among cryptocurrencies to implement a P2P trust network because of the size of its partner Lantern's user base. The greater the size of the potential network of trusted nodes, the better the network should function as an anti-censorship strategy. Currently, Lantern's network comprises over 6 million nodes worldwide, dwarfing the number of nodes available to other cryptocurrencies were they to pursue a similar strategy. For comparison, as of August 23, 2018, Ethereum had approximately 18,000 nodes[27], Bitcoin had under 10,000[28], and Ripple had approximately 800[29] (Figure 6). Yinbi will also leverage this large network to quickly gain widespread circulation of its YNB coin, helping to bolster and stabilize YNB's value.

[27] See https://www.ethernodes.org/network/1

[28] See https://bitnodes.earn.com/

[29] See https://xrpcharts.ripple.com/#/topology

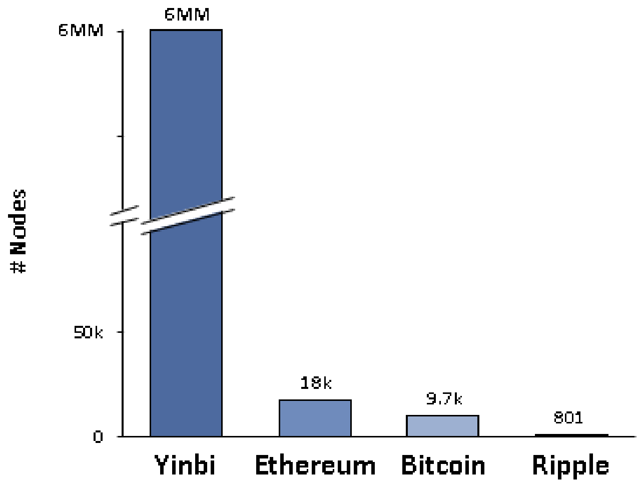


Figure 6. Comparative number of nodes available to Yinbi and other popular cryptocurrencies

Proxy network

Yinbi will use a large and dynamic network of proxy servers to proxy traffic that would otherwise be blocked. Potentially blocked traffic will be routed through users' assigned proxies, with those proxies rotating if and when their IP addresses become blocked by censors.

Network discovery

The "network discovery" problem is a key challenge of anti-censorship tools. The problem, essentially, is that anti-censorship tools must communicate to their users how they should access the network (e.g., by providing IPs of proxy servers or peers in a distributed network) while also attempting to prevent censors from getting that information, which they could use to block network access points (e.g., by enumerating and then blocking proxy IPs).

The problem can be thought of in two parts. First, the tool must decide how to look up network access information. Second, it must actually fetch that information. Normally, a web browser would use DHCP to lookup the IP address of the DNS server (step 1), and then perform DNS lookups on that server (step 2). However, due to DNS poisoning in countries with internet censorship, this is not an option for anti-censorship tools.

Instead, Yinbi will rely on the techniques outlined above to solve these problems. For example, it could fetch proxy server IPs either from trusted peers that store this data or via domain fronting, enabling it to bypass DNS lookup.

Products and roadmap

Yinbi (YNB)

Yinbi will be an asset issued on the Stellar network. A total of 888 billion YNB will be issued, with no additional coins beyond that amount ever to be released. 50% of these coins will be made available initially through a distribution partnership with Lantern. Additional distribution channels may be made available in the future.

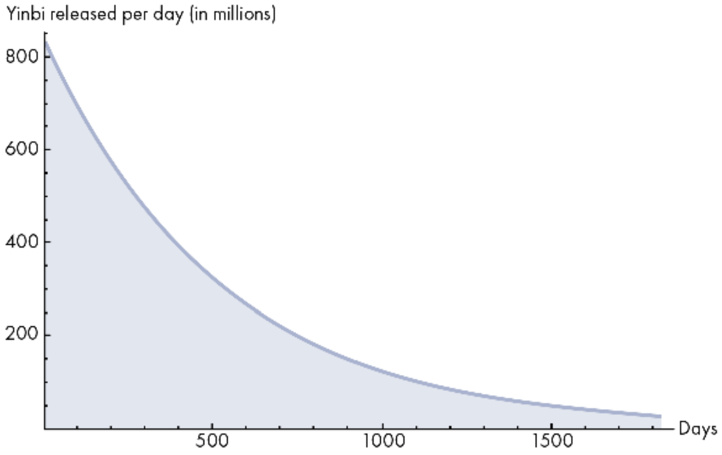
Allocation

%	Participant
50%	Yinbi Community
40%	Founding Team
10%	Future Employees

YNB Distribution

The 50% of YNB to be released to the public will be issued via an ongoing distribution partnership with Lantern. The number of YNB released each day will slowly decrease each day, in a smooth exponential function (Figure 7).

Coins will be released as a giveaway to purchasers of Lantern Pro subscriptions. The coins released on a given day will be divided amongst Lantern users in China who purchased Lantern Pro subscriptions on that day (with a 2-year subscription counted as 2x a 1-year subscription).



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

Figure 7. Yinbi released per day

For example, if 100 YNB were released on a given day, and that day there were eight 1-year Lantern Pro subscriptions and one 2-year Lantern Pro subscriptions purchased[30], then each 1-year account purchaser would receive 10 YNB, and the 2-year account purchaser would receive 20 YNB. Note that a 2-year purchase is more economical than buying two 1-year plans. *(Illustrative example only. Actual daily volume of YNB distributed will start out at 840 million+ and decrease each day according to the formula above).*

	1-Year Account	**2-Year Account**	**Total**
# of accounts purchased*	8	1	9
# YNB per Purchase	10	20	
Total # of YNB Distributed on that day	**80**	**20**	**100**

Yinbi Daily Distribution Example (Illustrative Only)

The distribution will begin in the fourth quarter of 2018, with a precise date to be determined. It will be run on China Standard Time (CST).

[30] "Purchase" can refer to either a direct purchase, a renewal via Lantern, or the redemption of a Lantern Pro code previously acquired from the Lantern bulk purchase portal. (The portal will be released in tandem with the start of the coin distribution.) Note that Yinbi is only available to residents of China.

Yinbi Wallet: Sending and receiving YNB

Yinbi Wallet will enable users to send and receive YNB, and will be released sometime soon after the YNB giveaway has begun.

Yinbi Exchange: Blocking-resistant, decentralized cryptocurrency exchange

The Yinbi Exchange will be a blocking-resistant, decentralized exchange that will enable users to trade cryptocurrencies including YNB, BTC, ETH, and others to be determined and added to over time. It will launch sometime after the Yinbi wallet has been completed.

Additional product details

Platforms

The Yinbi wallet and the Yinbi Exchange will be released on the following platforms initially, possibly with others to follow:

- Android native wallet
- Desktop wallets

Regional availability and language support

The initial release of both products, as well as participation in the YNB giveaway, will be limited to users in China and to the Chinese and English languages. Other regions and language support may be added over time

Team

The Yinbi Global Alliance LLC team has significant experience in the areas of blockchain, P2P, and anti-censorship and blocking resistance technology. The team is comprised of some of the world's most experienced engineers, researchers, and scientists in the P2P, blockchain and censorship-resistance worlds.