Yinbi Cryptocurrency:

Introducing a censorship resistant cryptocurrency

Yinbi Wallet: Local and crossborder unrestricted and private payment client

Yinshi: A blocking-resistant, peer to peer marketplace and exchange

Yinbi Global Alliance Foundation

Yin.bi

Background and Overview

In the early days of Bitcoin, proponents often claimed that it would be untouchable by adversaries who might want to control or suppress it. In fact, this was seen by many as one of its primary selling points.

However, existing cryptocurrencies provide no assurance that they can withstand 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

Most, if not all, cryptocurrencies have some vulnerability that adversaries 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.[1]

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). An adversary 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 LiteCoin, for example: https://litecoin.com/

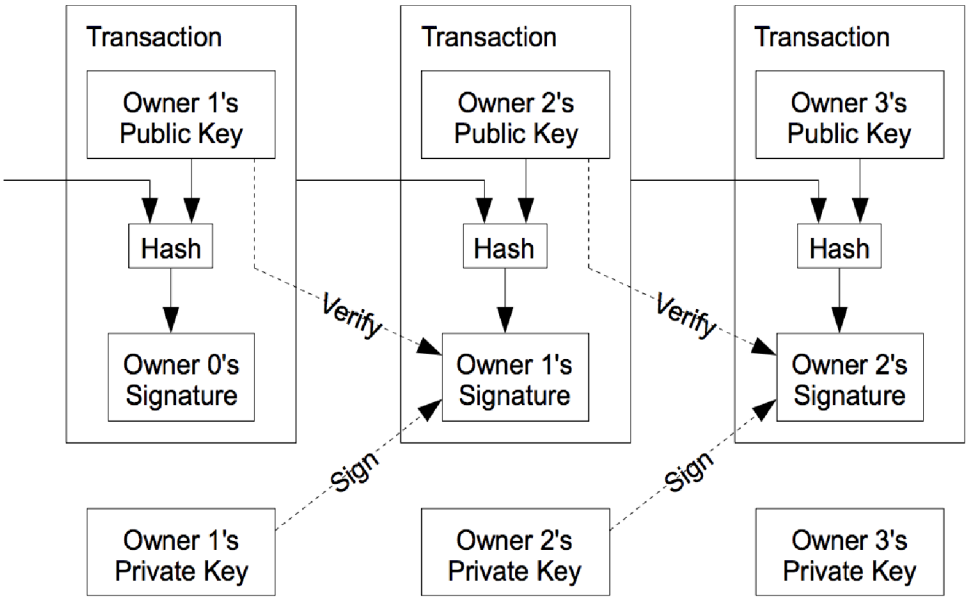

Figure 1. Bitcoin transaction diagram from original Bitcoin paper[2]

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 last few years, while more restrictive places have moved to censor or ban outright the use of cryptocurrencies, exchanges and mining.

[2] https://bitcoin.org/bitcoin.pdf

Yinbi will Provide a Censorship-resistant and Private Alternative

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

The initial Yinbi roadmap includes the following products/features:

1. YINBI, a token powered by the Stellar network[3] and leveraging the Lantern network[4];
2. A blockingresistant client for sending and receiving YINBI payments;
3. Yinshi: Blocking-resistant, peer to peer marketplace and exchange
4. Privacy Preserving technology to anonymize the sender, receiver and amount of transactions

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. **Anonymous uncensored payment**
   a. Many digital wallets impose a strict real name policy and censor payments. The account holder is required to upload a photo of themselves with any ID card and to verify their phone number and bank account, each of which are real name verified already. They could easily add users to a blacklist. Yinbi Wallet does not

[3] https://www.stellar.org/
[4] https://getlantern.org/

require any real name ID, phone number, or email address. Furthermore, Yinbi uses privacy preserving technology to assure users can pay with confidence that their transaction data is not only uncensorable but also private.

b. Many digital wallets impose strict censorship on transactions. For example, video games need to go through approval before they can be released to the public or imported, and many games fail to obtain approval. For example, popular games such as Fortnite and PlayerUnknown's Battlegrounds (PUBG) were banned in some regions.

c. Nearly all categories of merchant are subject to this approval. Many books, websites, newspapers, and other media outlets are unable to collect payment. Yinbi Wallet has no such restrictions, and could allow blacklisted users to purchase goods and services from merchants with Yinbi accounts.

3. **Unrestricted international transfers**

Many fiat currencies cannot be freely sent or exchanged across borders because adversaries 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 some regions, banks are required to ensure that transactions meet certain requirements, for example that they do not exceed the annual purchase limit of $50,000 worth of local currency per person. Citizens could have their account suspended for the remainder of the year if they violate these limits[5]. In extreme cases, such as when a region is experiencing hyperinflation, currency exchange is entirely forbidden, causing their 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 in that region.

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

[5] https://www.ft.com/content/b69166fa-ee01-11e7-b220-857e26d1aca4

4. **Privacy protections for transactions.**

   A ring signature[6] is a type of digital signature that can be performed by any member of a group of users that each have keys. A message signed with a ring signature is endorsed by someone in a particular group of people. However, which member of the group signed the message should be impossible to deduce: One of the security properties of a ring signature is that it should be computationally infeasible to determine which of the group members' keys was used to produce the signature.

   A stealth address is a privacy enhancing technology for protecting the privacy of receivers of cryptocurrencies. Stealth addresses require the sender to create a random, one time address for every transaction on behalf of the recipient so that different payments made to the same payee are unlinkable.[7]

   Confidential Transactions[8] is a cryptographic tool to keep the amounts transferred visible only to participants in the transaction (and those they designate).

5. **Highspeed, 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[9], or in congested times much longer, but even a more performant cryptocurrency like Ethereum has a block time of around 15 seconds[10].

---

[6] https://en.wikipedia.org/wiki/Ring_signature

[7] https://hackernoon.com/blockchain-privacy-enhancing-technology-series-stealth-address-i-c8a3eb4e4e43

[8] https://people.xiph.org/~greg/confidential_values.txt

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

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

Crossborder 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.[11] In countries with greater restrictions, they can take even longer, cost more, or be prohibited entirely.

As a Stellar token, YINBI transactions are processed very quickly, typically taking only a few seconds (with estimates ranging from less than one to at most five seconds[12]), and YINBI 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.

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 client[13] and using Wireshark's

[11] https://smartasset.com/checking-account/how-long-does-a-wire-transfer-take
[12] 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-proces_s and https://www.mobilecoin.com/whitepaper-en.pdf
[13] https://bitcoin.org

Bitcoin display filters[14] to flag all Bitcoin traffic (Figure 2). While there is a Bitcoin standard for encrypting traffic between peers[15], it is not adopted in practice.[16]

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 censors attempting to block their traffic. Taking Monero as an example, simple analysis of the downloadable binary (or the source code itself[17]) 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 clients to join the network (Figure 4). An adversary 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 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.

[14] https://www.wireshark.org/docs/dfref/b/bitcoin.html
[15] See BIP-151 at https://github.com/bitcoin/bips/blob/master/bip-0151.mediawiki
[16] BIP-151 is not implemented at https://github.com/bitcoin/bitcoin/blob/master/doc/bips.md
[17] https://github.com/monero-project/monero/blob/master/src/p2p/net_node.inl#L388

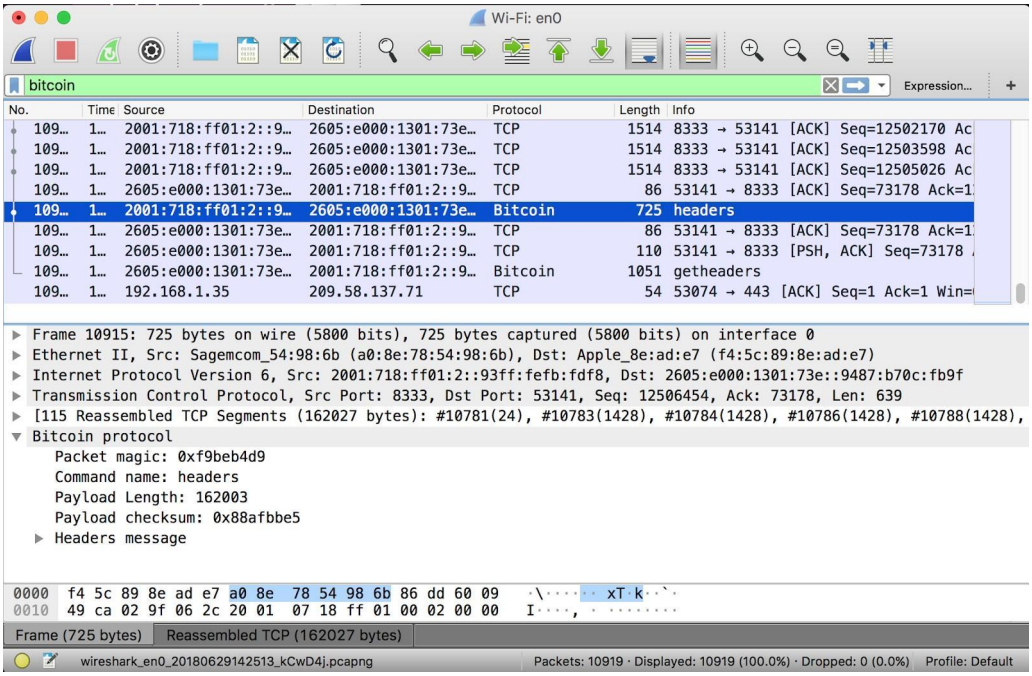

Figure 2. Bitcoin traffic identified in Wireshark

```
[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

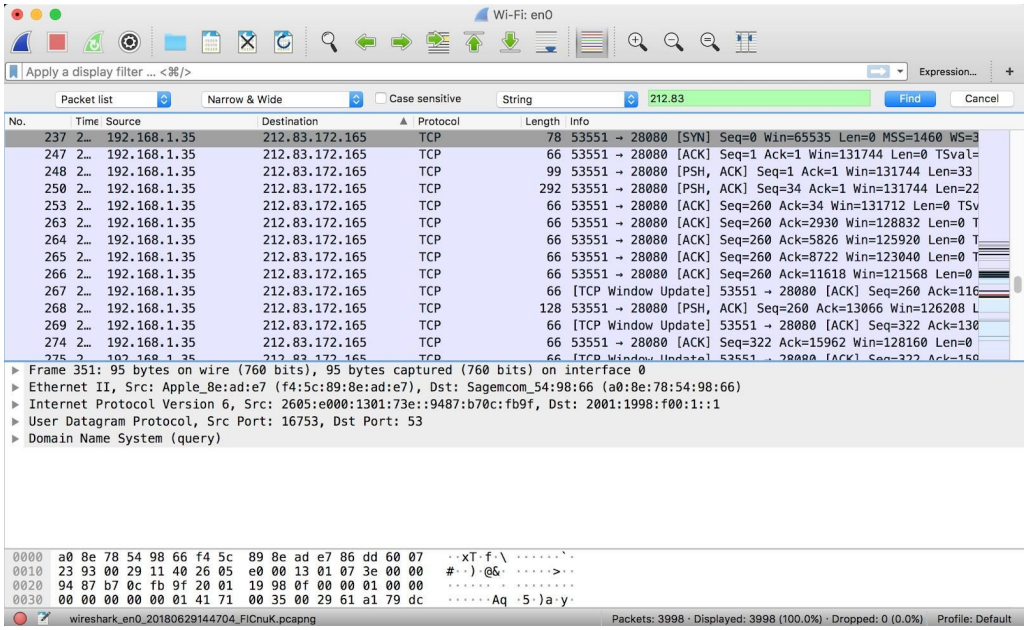

Figure 4. Monero traffic to hard-coded IP 212.83.172.165 identified in Wireshark

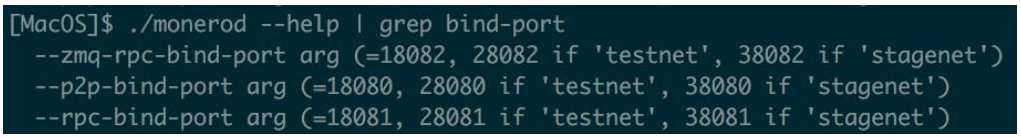

Figure 5. Running Monero binary with default ports

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 adversaries: namely, that they do not account for the fact that adversaries can exert significant control over network traffic. These currencies are only able to exist to the extent that adversaries around the world permit them to.

VPNs Provide no Reliable Censorship Protection for Cryptocurrency Transactions

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.[18] 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[19], as described below, to obfuscate traffic, which also renders traffic more easily identifiable and blockable.

4. No 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

[18] See https://en.wikipedia.org/wiki/Virtual_private_network
[19] There are some VPNs that use ad-hoc obfuscation, but the vast majority do not.

and to dynamically change those access points (such as proxy server IPs) if they become blocked.

6. No anonymity on the blockchain. Even though a VPN could obfuscate IP addresses broadcasting the transaction, the data stored in the blockchain will be mostly in plaintext. This could allow the censor to discover and link real world identities with the transaction and subsequently use force or intimidation to stop transactions. By contrast, Yinbi will not only prevent censors from discovering users' IP addresses as mentioned above, but will also store the blockchain in a privacy preserving way, preventing censors from blocking transactions based on sender or receiver addresses or the amount transferred.

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

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, providing greater access to the open internet and thwarting IP enumeration and subsequent IPblocking 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.[20]

DPI-resistant transports

Censoring adversaries often deploy DPI to identify network flows they 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 client will be able to use TCP, QUIC, KCP[29], and any other reliable UDP implementation.[21]

[20] https://www.torproject.org/docs/pluggable-transports.html.en and https://www.pluggabletransports.info/
[29] https://github.com/xtaci/kcp-g_o
[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.

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 randomize 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 anti censorship realm, this involves designing tools such that blocking traffic through those tools would be extremely costly and/or politically undesirable.

"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 client 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

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

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, 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 client 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 either directly or via her assigned proxies,

[25] 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

he/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 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 YINBI coin, helping to bolster and stabilize YINBI's value.

[27] https://www.ethernodes.org/network/1
[28] https://bitnodes.earn.com/
[29] https://xrpcharts.ripple.com/#/topology

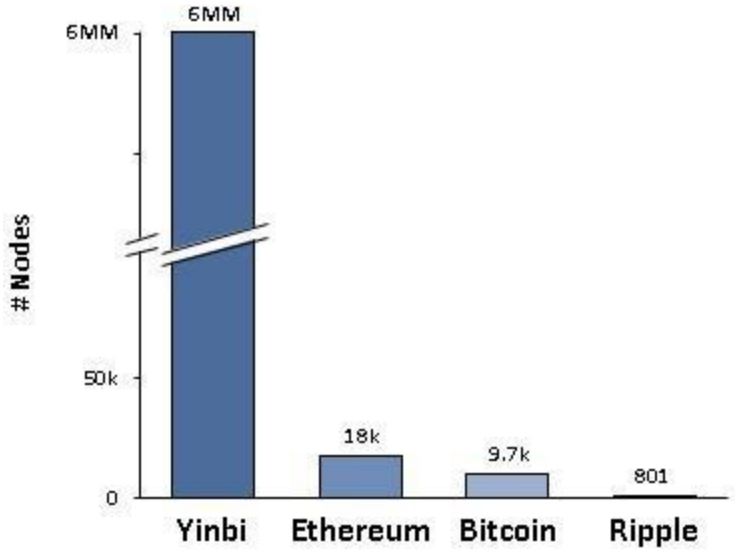

Figure 6. Comparative number of nodes available to Yinbi and other popular cryptocurrencies

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 (YINBI)

Yinbi will be an asset issued on the Stellar network. A total of 888 billion YINBI will be issued, with no additional coins beyond that amount ever to be released. YINBI will be distributed to the Yinbi community and used to reward Lantern users, Yinshi users and YINBI holders.

Yinbi Wallet: Sending and Receiving YINBI

Yinbi Client will enable users to send and receive YINBI, and will be released sometime soon after the YINBI community giveaway has begun. The wallet will be censorship resistant.

Yinshi: Blocking-resistant, peer to peer and exchange

Yinshi is a blocking resistant peer to peer international C2C marketplace that allows users to trade virtual goods using YINBI, BTC, USDT and more. It will enable users to trade cryptocurrencies including YINBI, BTC, USDT, ETH, and also allow users to use fiat digital wallets to trade cryptocurrency peer to peer. YINBI will act as the medium of exchange among

all other currencies, assets and digital goods. It will implement the same blocking resistant and privacy preserving technologies mentioned in the previous sections.

Additional Product Details

Regional availability and language support

The initial release of these products, as well as participation in the YINBI 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. (We do not currently plan to support use in the U.S.)

Team

The Yinbi Global Alliance Foundation has significant experience in the areas of blockchain, cryptocurrency, 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.

Language

The whitepaper has been translated into Chinese solely for the information and convenience of Chinese speakers. However, the English version of the whitepaper shall be controlling in all respects, and all versions hereof in any other language shall be for accommodation only and shall not be binding upon the parties hereto. In the event of any inconsistency between the English version and the Chinese version, the English version shall control.