ETHEREUM MASTERNODE

Your Most Secure Private Coin

WHITEPAPER

Website: https://www.ethereummasternode.info Telegram: t.me/joinemn
Twitter: https://twitter.com/emn_node

Ethereum is an open-source, public, blockchain-based distributed computing platform featuring smart contract (scripting) functionality. It provides a decentralized Turing-complete virtual machine, the Ethereum Virtual Machine (EVM), which can execute scripts using an international network of public nodes. Ethereum also provides a cryptocurrency token called "ether", which can be transferred between accounts and used to compensate participant nodes for computations performed. "Gas", an internal transaction pricing mechanism, is used to mitigate spam and allocate resources on the network

The core innovation behind Ethereum is its decentralized structure. Unlike traditional fiat currencies, Ethereum has no central control, no central repository of information, no central management, and no central point of failure. However, one of the challenges facing Ethereum is that most of the actual e-services and e-businesses built around the Ethereum ecosystem are centralized. Due to the centralized nature of the current system, e-commerce is ran by individuals in specific locations that utilize vulnerable computer systems that are susceptible to legal entanglements. Ethereum Masternode is one of the truly decentralized currencies available today due to its standing commitment to building off of the core fundamentals of Ethereum, while bringing an entirely new layer of anonymity to realization.

1. Tor Integration

Tor, derived from an acronym for the original software project name. The Onion Router is an IP obfuscation service which enables anonymous communication across a layered circuit based network. Tor directs internet traffic through a free worldwide volunteer overlay network consisting of more than seven thousand relays to conceal a user's location and usage from anyone conducting network surveillance or traffic analysis. The layers of encrypted address information used to anonymize data packets sent through Tor are reminiscent of an onion, hence the name. That way, a data packet's path through the Tor network cannot be fully traced. Tor's use is intended to protect the personal privacy of users, as well as their freedom and ability to conduct

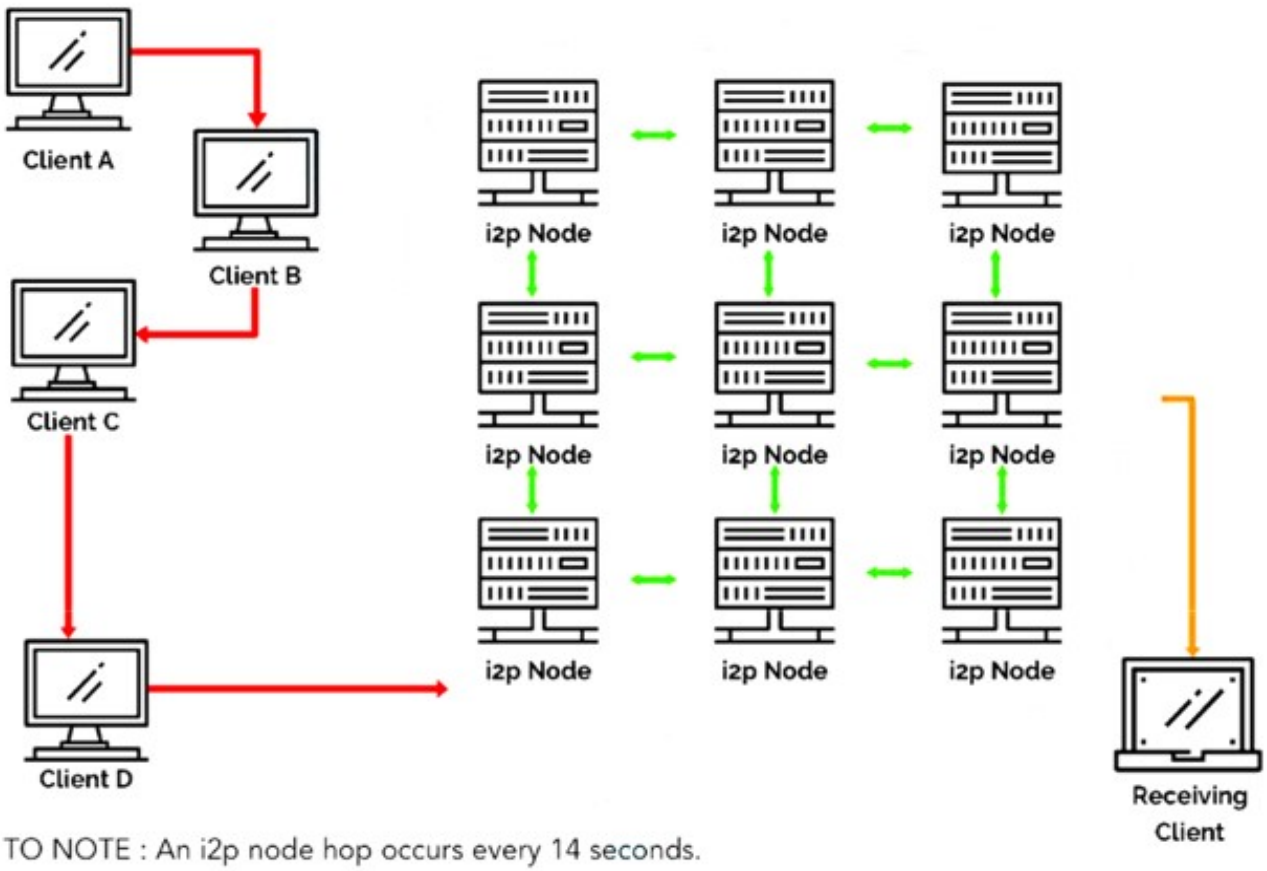
confidential communication by keeping their Internet activities from being monitored.

Onion routing is implemented by encryption in the application layer of a communication protocol stack, nested like the layers of an onion. Tor encrypts the data, including the next node destination IP, multiple times and sends it through a virtual circuit comprising successive, randomly selected Tor relays. Each relay decrypts only enough of the data packet wrapper to know which relay the data came from, and which relay to send it to next. The relay then rewraps the package in a new wrapper and sends it on. The Final relay decrypts the innermost layer of encryption and sends the original data to its destination without revealing, or even knowing, the source IP address.

Because the routing of communication is partly concealed at every hop in the Tor circuit, this method eliminates any single point at which the communicating peers can be determined through network surveillance that relies upon knowing its source and destination

2. I2P Integration

I2p was originally built to provide hidden services which allow people to host servers at unknown locations. I2p provides many of the same benefits that Tor does. Both allow anonymous access to online content, make use of a P2P-style routing structure, and both operate using layered encryption. However, I2p was designed to be a network within the internet, (see figure 2.1) with traffic staying contained in its borders. I2P performs packet based routing as opposed to Tor circuit based routing. This provides the benefit of permitting I2p to dynamically route around congestion and service interruptions in a manner similar to the internet? IP routing. This provides a higher level of reliability and redundancy to the network itself.

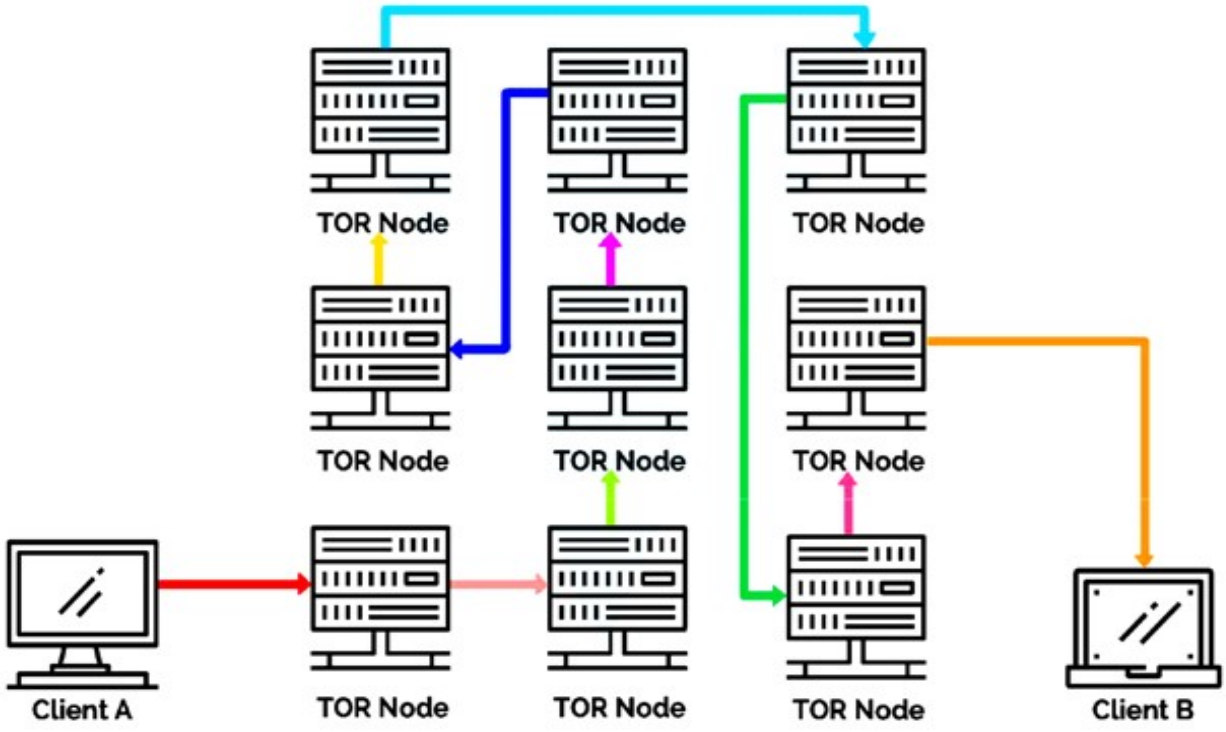


The first time a client wants to contact another client, they make a query against the fully distributed "network database" -a custom structured distributed hash table (DHT) based off the Kademlia algorithm. This is done to find the other client's inbound tunnels efficiently, but subsequent data between them usually includes that information so no further network database lookups are required.

I2p is a highly obfuscated tunneling service using ipv6 that anonymizes all Ethereum Masternode (EMN) data being sent over the network. Each client application has their i2P "router" build several inbound and outbound "tunnels" - a sequence of peers that pass data in one direction (to and from the client, respectively). In turn, when a client wants to send EMN data to another client, the application passes the message through one of their outbound tunnels

targeting one of the other client's inbound tunnels, eventually reaching the destination.

Rather than relying on a centralized set of directory servers, like Tor, I2p uses two distributed hash tables to coordinate the state of the network. Distributed hash tables or DHTs are a distributed and often decentralized mechanism for associating hash values with content. The primary advantage to DHTs are their scalability. A successful decentralized P2P network requires good scalability of its services to ensure the size of content or transaction sharing can continue to grow as required. Additionally I2P does not rely on a trusted directory service to get route information. Instead, network routes are formed and constantly updated dynamically, with each router constantly evaluating other routers. Lastly, I2p establishes two independent simplex tunnels for traffic to traverse the network to and from each host as opposed to Tors formation of a single duplex circuit (see figure 1.1).



TO NOTE: A TOR node hop occurs every 10 minutes.

3. Electrum

Electrum's strength is speed and simplicity, with low resource usage. It uses secure remote servers that handle the most complicated parts of the EMN network and also allows users to recover their wallets with a secret seed phrase. Additionally, Electrum offers a simple and easy to use cold storage solution. This allows users to store all or part of their coins in an offline manner. Moreover, Electrum is one of the only wallets to provide native Tor and i2P support. By integrating Electrum with Tor and i2P, one can achieve anonymity while using the desktop/mobile wallet. Both IP address and transaction information is secured and does not leak to the connecting servers; increasing user privacy.

Electrum enables multi-signature support, which requires more than one key to authorize a Electrum transaction. Standard transactions on the EMN network could be called Single-signature transactions, because transfers require only one signature - from the owner of the private key associated with the EMN address. An Electrum transaction, with multi-signature support, requires the signatures of multiple people before the coins can be transferred. EMN then requires multiple different party addresses to be provided in order to do anything with them.

Here is an example:

One Electrum wallet is on your primary computer, the other on your smart phone - the coins cannot be spent without a signature from both devices. Thus, an attacker must gain access to both devices in order to steal your coins.

Key Features of an Electrum Wallet

Deterministic Key Generation

If you lose your wallet, you can recover it from its seed. You are protected from your own mistakes

Instant On

The client does not download the blockchain, it requests blockchain information from a server. No delays, always up-to-date.

Locally signed Transact ions

Your private keys are not shared with the server. You do not have to trust the server with your coins.

Freedom and Privacy

The Electrum server does not store user accounts. You can also export your private keys, meaning YOU own your address.

4. Supply & Circulation

The total supply of EMN is 15 Million coins. The ICO price is 0.02$ per EMN. Remember if all 20% will not sold in the ICO, the remaining coin will be burned. To see more, check our roadmap.

Website: https://www.ethereummasternode.info Telegram: t.me/joinemn
Twitter: https://twitter.com/emn_node

5. Android Tor + I2P

Ethereum Masternode fully innovation in the mobile cryptocurrency space. We will pioneer and developed two very unique and first of their kind android wallets. One of which operates exclusively on The Onion Router Network (Tor) and the other operating exclusively on The Invisible Internet Project (I2P). The EMN Tor and I2p wallets will build around the premise of anonymity. The wallets have no built-in ability to connect to or broadcast user information over Clear net. Transactions are completed via Simple Payment

Verification (SPV), a technique described in Vitalik paper that supports for the wallet to verify transactions through proof of work; a method for verifying if a single transaction is included in a block without downloading the entire block (similar to how an Electrum wallet functions).

SPV supports for closely instant payment confirmations because it acts as a thin client that only needs to download the block headers, which are very smaller than full blocks. The EMN Tor and i2P wallets also will build in security features such as a 4 digit pin code and biometric locking options for an added layer of physical security and also planning for eye scanning option.

Additionally, the EMN Tor and i2P wallets are able to handle P2P QR code scan transactions with instant verification. Clients will be able to also import QR codes from paper wallets to pull balances from cold storage if required.

6. P2P Platform-Integrated Portals

Peer-to-Peer (P2P) transaction Follows for Telegram, Discord and Twitter will support Ethereum Masternode, Slack and Steam integrations are currently in development, and is slated to be released to the public in the month of January. Telegram is a free cloud-based instant messaging service that supports Android, iOS, Windows Phone, Windows NT, macOS and Linux. Telegram uses a symmetric encryption scheme called MTProto. The protocol was developed by Nikolai Durov and other developers at Telegram. Discord is a proprietary freeware VoIP application that has widespread adoption in the crypto community. Like Telegram, Discord has support on Windows, macOS, Android, iOS and has a browser accessible web client. Implementing EMN P2P capabilities on these platforms allows users to send and receive funds on the fly, no matter where they are (regardless if they have an actual wallet installed or not).

P2P is an online innovation that allows users to transfer coins via the internet or mobile device. To do this, consumers use an online application, or in

this case a bot to designate the amount of coins to be transferred. The recipient is designated by just their username and once the transfer has been initiated by the sender, the recipient then receives a notification to use the online bot. that he has received a payment at a newly established deposit address. The user is then allowed to tweet or message the bot with a simple command such as! Withdraw and is then prompted with a set of instructions on how to receive their newly acquired EMN. This service does not require any additional information past the amount you want to send and who to send to. No privacy information such as IP addressing, location, name is retained during this process. Your personal identity outside of initiating the transaction remains completely anonymous.

Ethereum Masternode is one and only coin that makes offer P2P solutions for Telegram, Discord, Twitter and Internet Relay Chat (IRC) with Reddit, Slack and Steam support coming at a future date. These P2P offerings allow users to transfer EMN to anyone on the same social platform as them.

7. What is a Key Agreement?

A Key agreement scheme is a procedure by which two or more parties agree upon a value from which they can subsequently derive one or more keys for use in symmetric encryption. Neither party completely determines the key value on their own. Instead, they both contribute to the final key value and most important, anyone who observes the exchanges between the two parties cannot tell what the final result will be. It is important to note that in their basic form, key-agreement schemes are anonymous, they do not tell either party the identity of the other party.

8. Future Development: RSK Smart Contracts

Rootstock, or commonly referred to as RSK, is a two-way pegged sidechain that grafts smart contract functionality onto the EMN network. It also introduces an off-chain protocol for near-instant payments. RSK is an independent blockchain that does not have its own token, it instead relies on existing tokens (such as EMN). RSK is able to do this by pegging (or matching) its smart token to EMN, so that the value of an RSK token is exactly that of a EMN token. Users have the capabilities to freely move their tokens back and forth between the two chains.

A smart contract works by placing a user. Ethereum Masternode into a type of reserve where it is locked up and then used to back the RSK token, known as smartEMN. Think of it as putting your EMN into a checking account and then using the RSK network to spend that money. It is important to note that simple contracts have been in place for Bitcoin which allow users to create contracts, like mutlisig, that requires two or more users to sign off on a payment before it can be released. With the implementation of RSK on EMN, simple smart contracts are taken to a whole new level, with turing-complete smart contract capabilities that will go head-to-head with Ethereum current offerings.

Another added benefit of RSK is its ability to scale. RSK currently achieves 400 payment transactions per second, which is a huge progressive leap when compared to our current standing transaction rate; around 100 per second. The RSK development team has stated that the eventual goal is to push the bar even higher with future goals to support 2,000 transactions per second using a second layer technology called Lumino. As stated in the LCTP whitepaper, the Lumino Network is an off-chain payment system that relies on a protocol known as the Lumino Transaction Compression Protocol. The LTCP can be compared to the Lightning Network.

9. Contributors

As an open source project we find it very important to thank our contributors who have given us a helping hand in order for us to get to where we are today. To that we say Thank you

Core Marketing Team

@Spookykid @Crypt oRekt @gfranko @DJ_Erock23 @Crypt o_K1NG @Jt heLizzard @lucklight @Crypt onat or92 @feyziozsahin @Slem icek