Ethereum Secure

Whitepaper

1. Introduction

Bitcoin was developed and released in 2009 in response to an inherent flaw in the way transactions were processed on the Internet. In his whitepaper, Nakamoto explains that Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model?[1]. Since its original inception in 2009, Bitcoin has been rapidly adopted into today?s modern marketplaces. A primary issue with Bitcoins rapid adoption is the increase of demand on the original blockchain to handle varying degrees of large transactions. With increased demand comes increased transactional waiting periods, and this has resulted in higher transactional fees in attempts to try and speed-up transaction confirmation times.

The core innovation behind Bitcoin is its decentralized structure. Unlike traditional fiat currencies, Bitcoin has no central control, no central repository of information, no central management, and no central point of failure. However, one of the challenges facing Bitcoin is that most of the actual e-services and e-businesses built around the Bitcoin 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 Secure is one of the truly decentralized currencies available today due to its standing commitment to building off of the core fundamentals of Bitcoin and Ethereum, while bringing an entirely new layer of anonymity to realization.

For most of written history, transactions have been private and fairly anonymous. The information of a transaction was only disclosed to the sender and the recipient. Recently, the large majority of financial transactions have become facilitated by technology, making it increasingly difficult to maintain financial privacy. The most common methods of payment (e.g. credit/debit card, ApplePay, etc.) result in all the information of a transaction being stored digitally. While there are immense benefits that come with these transaction methodologies, it should not preclude the utility of financial privacy for the average consumer.

Considering how often breaches occur within large financial institutions resulting in significant leaks of personal and financial information, it is clear there is a need for financial privacy options. Furthermore, various financial institutions have been caught selling customer data, as well as blocking legal transactions with no valid legal basis.

Ethereum Secure (ETHSecure) - is the resolution of transaction privacy which uses advanced privacy technology in which all the data are split, encrypted, archived and distributed across our MultiDecentralized Private Blockchains. This means payments are published on a public blockchain, but the sender, recipient and other transactional metadata remain unidentifiable.

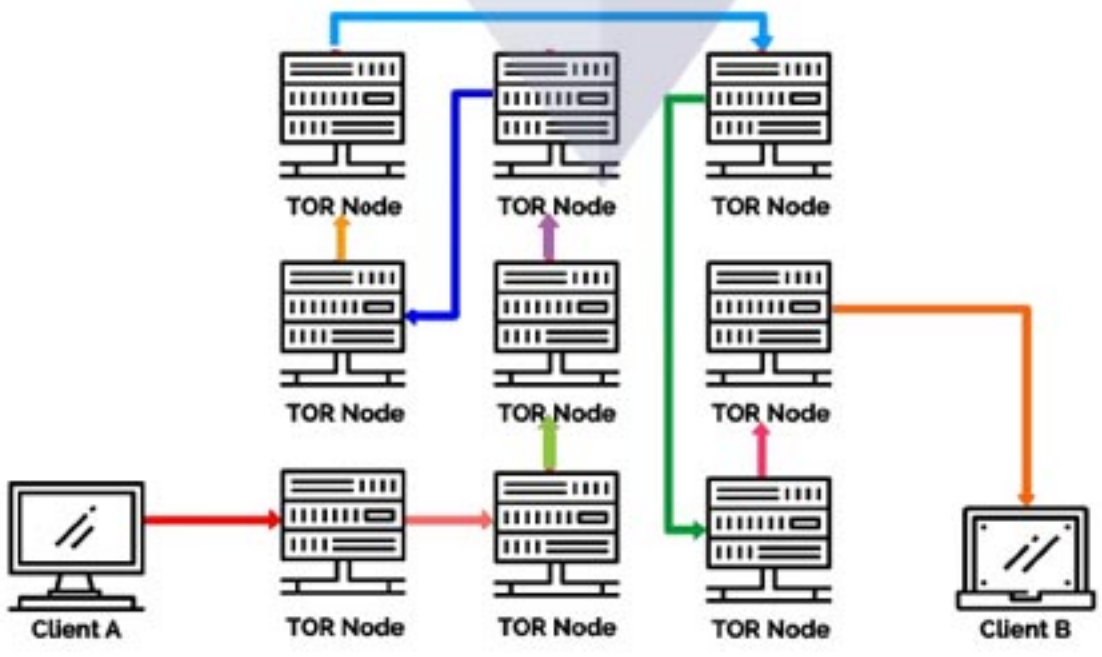
2. The Onion Router Integration (TOR)

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 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.

How The Onion Router Integration Occur

Figure 1.0



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

3. Multi-Algorithm Support

Ethereum Secure is a multi-algorithm cryptocurrency that is designed to enable people with different types of mining devices to have equal access to earning coins. It is one of the only cryptocurrencies to support the latest hash functions technology combined on one blockchain. This results in increased security and a wider range of people and devices that can mine ETHSecure hence equal distribution of ETHSecure is ensured for everyone.

The total supply of Ethereum Secure is 21 Million coins and this gave us assurance of fast growing. What makes ETHSecure stand out from other cryptocurrencies are the Proof-of-Work algorithms that run on its blockchain. All 5 algorithms have a 20-second block target block time. The difficulty is influenced only by the algorithms hash rate. This allows improved security and protection against attacks.

4. P2P Platform-Integrated Portals

Peer-to-Peer (P2P) transaction support for Telegram and Twitter is supported by ETHSecure and Steam integrations are currently in development. Telegram is a free cloud-based instant messaging service that supports Android, iOS, Windows Phone, Windows NT, macOSand Linux. Telegram uses a symmetric encryption scheme called MTProto. The protocol was developed by Nikolai Durov and other developers at Telegram and is based on 256-bit symmetric AES encryption, RSA 2048 encryption and Diffie?Hellman key exchange. Discord is a proprietary freeware VoIP application that has widespread adoption in the crypto community. Like Telegram, Discord has support on Windows, macOS, Android, iOSand has a browser accessible web client. Implementing ETHSecure 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 technology 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 ETHSecure.
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 Secure is one of the only cryptocurrencies to already offer P2P solutions for Telegram, Twitter and Internet Relay Chat (IRC) with Reddit, and Steam support coming at a future date. These P2P offerings allow users to transfer ETHSecure to anyone on the same social platform as them.

5. ETHSecure Specter Protocol

Specter Protocol makes it possible to choose between a public or private ledger. Through this new system, users who value transparency and accountability, e.g. merchants, have the option to have transactions viewable on the blockchain. On the other hand, it also provides an option to those who prefer transactions to vanish entirely. Spectre Protocol allows for complete anonymity to be maintained while providing a safe and secure method of sending and receiving ETHSecure coins without transactions being traceable on a publicly accessible ledger. The update includes stealth Addressing and the latest Tor+SSL integration that will take our core QT users off of clearnet, and migrate them to exclusively operate on the latest Tor network. Also included are the capabilities to designate which ledger a user wishes to transact across, public or private. With elegant simplicity, the Wraith Protocol update will enable users to toggle a switch within the Core QT wallet that allows them to transact via stealth addressing with an additional layer of IP obfuscation through the Tor Network.

6. Atomic Swaps Of ETHSecure

Atomic swaps, aka atomic cross-chain trading, allows for interoperability between ETHSecure and all other cryptocurrencies in circulation with Atomic swap capabilities enabled. An Atomic swap works in the same way users would send funds to one another by allowing users to cross-trade different cryptocurrencies without relying on centralized parties. ETHSecure will be implementing BIP65 Check Lock Time Verify (CLTV) otherwise known as Hash Time-Locked Contract. (HTLC). HTLC is a class of payments that use hash-locks and time-locks that require the receiver of a payment to acknowledge receiving the payment prior to a deadline by generating cryptographic proof of payment or forfeit the ability to claim the payment, returning it to the payer. For example, both parties submit their individual transactions to the appropriate blockchain. User A sends ETHSecure on the ETHSecure blockchain, and user B sends ETH on the Ethereum blockchain. The recipient can only claim this transaction by revealing a secret hash (proof of payment). This results in both transactions being linked to one another, despite them taking place across two different blockchains. If the recipient does not reveal their secret hash - the payment is then forfeit and returned to the payer.

Ethereum Secure users will be able to leverage Atomic Swaps while transacting across the Tor network via Specter Protocol, thereby maintaining IP obfuscation and personal identity integrity while sending and receiving ETHSecure through cross-chain transactions. Furthermore, this implementation not only allows for cross-chain transactions but it also paves the way for future implementations such as the Lightning Network, which will allow for automatic execution of cross-chain transactions and trading.

7. Free Initial Coin Offering

Ethereum Secure (ETHSecure) is distributing ETHSecure tokens freely to all our community members that participate in the small task given on our website and contribute as stated on the website would be receiving 500 ETHSecure token freely and both referral programs included on the website. However, the team decided to give tokens out freely on view of community matters first.

Please be aware that Ethereum Secure is not offering Pre-sale, Private Sale and ICO sale.

8. ETHSecure Distribution

75%
Free Initial Coin Offering

12%
Founders & Core Team

6%
Operations

4%
Promotion/Marketing

3%
Partnerships

Total Supply: 21,000,000

8.1 EthsecurenDebit Card

Instant payment with the power ofMultiDecentralized connection with mobile eWallet and decentralized exchange, the debit card gives users the ability to withdraw money at any ATM worldwide through the use of our MultiDecentralized blockchain technology.

9. The Team Ethereum Secure

William
Founder & CEO

Adam
Chief Technology Officer

Ava
Sales Director

Henry
Marketing Coordinator

Lily
Community Manager

Alexander
Market Analyst

James
Technical Architect

Logan
Web Developer

Albie
Web Developer

Mason
Web Developer

Elsie
Accounts Support

Frederick
Head of Accounts

10. Roadmap


June - September 2018
Development
Legal Setup
November 15th - 25th, 2018
Launch dashboard
Token Listed On:
Idex
Kucoin
HitBtc
Binance
December 24th, 2018
Mainnet Launch
Establish contract with advertisers
Quarter 2 - 3, 2019
Core Wallet 3.0 Release
Launch of ETHSecure Credit Card
Febuary - May 2018
Team Formed
Idea & Researches
Adopted Blockchain Technology
October 2018
Publish Smart Contract Address
Registration Portal Open
Free Initial Coin Offering
Token distribution to all participants
Quarter 1, 2019
Launch GitHub For Open Source
Launch IOS & Android App
Quarter 4, 2019
New website
Merchandise Online Store
Desktop Wallet

11. Contact

Website:
https://ethereumsecure.org

Telegram:
https://t.me/ethereumsecure

Twitter:
https://twitter.com/EthereumSecure

Youtube:
https://www.youtube.com/channel/UC5ayrvR9vjQYCi9QO5XDcHw

Reddit:
https://www.reddit.com/user/ethereumsecure

Medium:
https://medium.com/@ethereumsecure

You can also reach us on:
support@ethereumsecure.org