
VERGE
The most privacy focused cryptocurrency
BLACKPAPER

1.0 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 Bitcoin's 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. Verge is one of the truly decentralized currencies available today due to its standing commitment to building off of the core fundamentals of Bitcoin, while bringing an entirely new layer of anonymity to realization.

2.0 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.

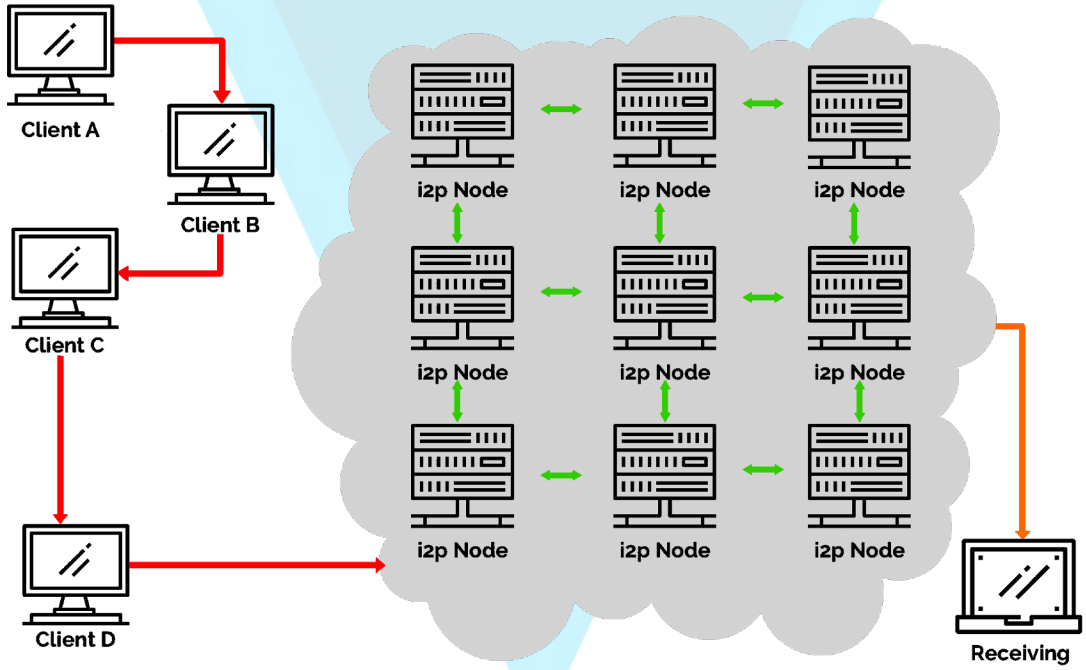
2.1 Tor Integration

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.

3.0 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’s 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’s IP routing. This provides a higher level of reliability and redundancy to the network itself.

Figure 2.1
How an i2p Transaction Occurs



TO NOTE : An i2p node hop occurs every 14 seconds.

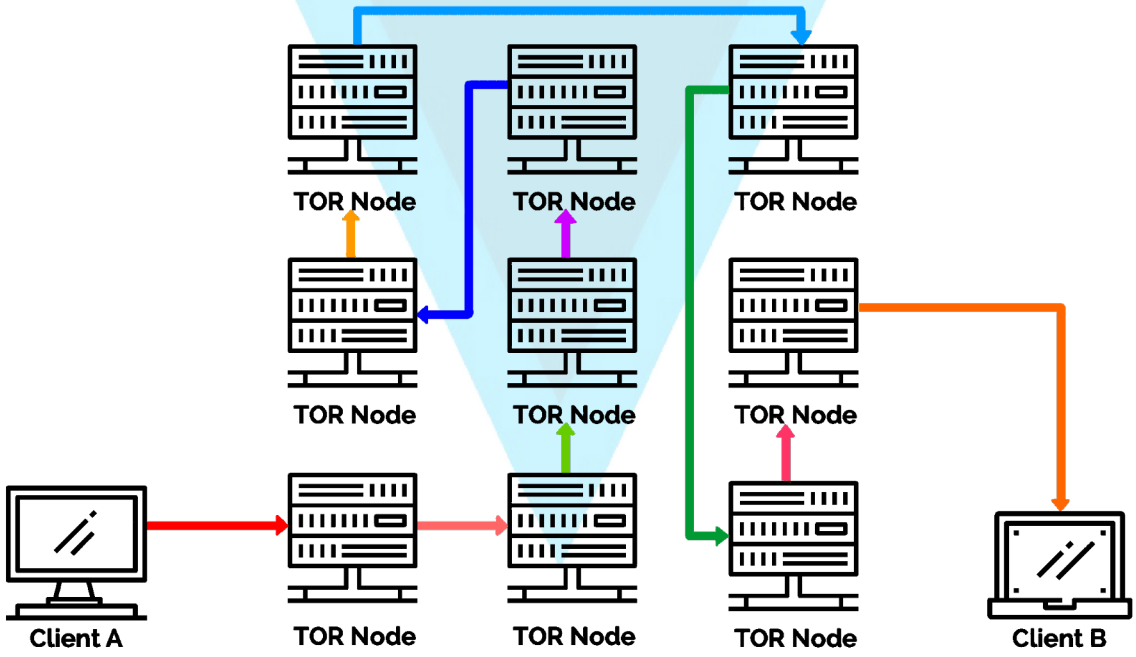
The first time a client wants to contact another client, they make a query against the fully distributed "network database" - a custom structured distributed hash table (DHT) based off the Kademlia algorithm [2]. This is done to find the other client's inbound tunnels efficiently, but subsequent data between them usually includes that information so no further network database lookups are required.

3.1 I2P Integration

I2p is a highly obfuscated tunneling service using ipv6 that anonymizes all Verge 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) [2]. In turn, when a client wants to send Verge 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 DHT's 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 Tor's formation of a single duplex circuit (see figure 1.1).

Figure 1.1
How a TOR Transaction Occurs



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

4.0 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 Verge 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 Verge network could be called “Single-signature transactions” [4], because transfers require only one signature - from the owner of the private key associated with the Verge address. An Electrum transaction, with multi-signature support, requires the signatures of multiple people before the coins can be transferred. Verge then requires multiple different party addresses to be provided in order to do anything with them.

> “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 Transactions
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.

5.0 Multi-Algorithm Support

Verge 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 5 hash functions combined on one blockchain. This results in increased security and a wider range of people and devices that can mine Verge hence equal distribution of Verge is ensured for everyone.

The total supply of Verge is 16.5 Billion coins. What makes Verge stand out from other cryptocurrencies are the 5 Proof-of-Work algorithms that run on its blockchain, namely Scrypt, X17, Lyra2rev2, myr-groestl and blake2s. All 5 algorithms have a 30-second block target block time. The difficulty is influenced only by the algorithm's hash rate. This allows improved security and protection against 51% attacks.

6.0 Android Tor + I2P

Verge sits at the forefront of innovation in the mobile cryptocurrency space. We have pioneered 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 Verge Tor and I2p wallets are built around the premise of anonymity. The wallets have no built-in ability to connect to or broadcast user information over Clearnet. Transactions are completed via Simple Payment Verification (SPV), a technique described in Satoshi Nakamoto's paper that allows for the wallet to verify transactions through proof of inclusion; a method for verifying if a particular transaction is included in a block without downloading the entire block (similar to how an Electrum wallet functions).

SPV allows for nearly instant payment confirmations because it acts as a thin client that only needs to download the block headers, which are drastically smaller than full blocks. The Verge Tor and i2P wallets also have built in security features such as a 4 digit pin code and biometric locking options for an added layer of physical security.

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

7.0 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 Verge 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 Verge). RSK is able to do this by pegging (or matching) its smart token to Verge, so that the value of an RSK token is exactly that of a Verge 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's Verge into a type of reserve where it is locked up and then used to back the RSK token, known as smartXVG. Think of it as putting your Verge 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 Verge, simple smart contracts are taken to a whole new level, with turing-complete smart contract capabilities that will go head-to-head with Ethereum's 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, a scaling solution originally designed for bitcoin that Is currently being tested on Litecoin.

8.0 Future Development: Discord & Telegram P2P

Peer-to-Peer(P2P) transaction support for Telegram and Discord is currently in development, and is slated to be released to the public in the month of August. 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 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, iOS and has a browser accessible web client. Implementing Verge 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 Verge. 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.

Verge is one of the only cyrptocurrencies to already offer P2P solutions for Twitter, Reddit, Internet Relay Chat (IRC), Slack and Steam. These P2P offerings allow users to transfer Verge to anyone on the same social platform as them.

9.0 References

[1] Nakamoto, S. (2009). Bitcoin: A Peer-to-Peer Electronic Cash System. Retrieved from https://bitcoin.org/bitcoin.pdf

[2] I2P: A scalable framework for anonymous communication - I2P. (n.d.). Retrieved from https://geti2p.net/en/docs/how/tech-intro

[3] Multisignature - Bitcoin Wiki. (n.d.). Retrieved August 8, 2017, from https://en.bitcoin.it/wiki/Multisignature

[4] Voegtlin, T. (n.d.). Welcome to the Electrum Documentation! — Electrum 2.5 documentation. Retrieved August 8, 2017, from http://docs.electrum.org/en/latest/

Additional References:

Gribble, S., Brewer, E., Hellerstein, J., & Culler, D. (2000, October 23). Scalable, Distributed Data Structures for Internet Service Construction. Retrieved from https://www.usenix.org/legacy/events/osdi2000/full_papers/gribble/gribble_html/index.html

Anonymity and the Block Chain • IHB News™. (2014, November 18). Retrieved August 08, 2017, from https://ihb.io/2014-11-17/news/anonymity-block-chain-13570

Holden, E. (2017, July 18). An Introduction to Tor vs I2P. Retrieved August 08, 2017, from https://www.ivpn.net/privacy-guides/an-introduction-to-tor-vs-i2p

Distributed hash table. (n.d.). Retrieved August 08, 2017, from http://infoanarchy.org/Distributed_hash_table

Scharr, J. (2013, October 23). What Is Tor - How Does Tor Work - How to Use Tor. Retrieved August 08, 2017, from https://www.tomsguide.com/us/what-is-tor-faq,news-17754.html

Durumeric, Z., Wustrow, E., & Halderman, J. (2013). ZMap: Fast Internet-Wide Scanning and its Security Applications. Retrieved from https://zmap.io/paper.pdf

Voegtlin, T. (2015). Simple Payment Verification — Electrum 2.5 documentation. Retrieved from http://docs.electrum.org/en/latest/spv.html

SPV, Simplified Payment Verification - Bitcoin Glossary. (2017). Retrieved from https://bitcoin.org/en/glossary/simplified-payment-verification

https://atlas.torproject.org/#search/flag:authority

http://torstatus.blutmagie.de/

10.0 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

The Author

CryptoRekt

O.G Verge Development Team

Sunerok

Gfranko

CryptoRekt

Contributors

Core Marketing Team

@Spookykid
@CryptoRekt
@gfranko
@Crypto_K1NG
@JtheLizzard
@lucklight
@Cryptonator92
@feyziozsahin
@Slemicek
@Trilla6six6
@Dabbie USA
@Cyrus7at
@Thehunter9 Netherlands
@GGWeLost
@Jeanralphio69
@Crypth
@deheerlen
@Twomanytimes
@ScagFX
@TraderNILW

Github Contributors

Sunerok
Gfranko
CryptoRekt
Mkinney
badbrainIRC
Grinfax
Swat69
NeosStore
Koenwoortman
Hellokarma
Kirillseva
Fuzzbawls
Buzztiaan
Spiralmann666
stshort
alcy0ne
chisustation
ShapeShifter499
Infernoman
pallas1
bearsylla
2Dai
31percent
Racoooon
ceasarpolar
enewnanwebdev
giovanni1186
labelmeagod

Contact Info

Twitter Telegram Slack Facebook IRC Reddit Steam Verge Discord BitCoinTalk Radio Station