Verge: An Anonymity-Centric Crypto-Currency

Sunerok
CryptoRekt
Buk-Lee

Abstract: A Crypto-Currency based on the Bitcoin blockchain, the creation of Satoshi Nakamoto, with multiple anonymity-Centric network adaptations known as Tor and i2p. Included are other improvements such Multi-algorithm mining capabilities as well as Blackhole Technology, for IP-obfuscation which through Electrum transaction simplification; allows for instant transaction confirmations without a centralized authority. While people race to encrypt their transactions, we should ask ourselves a question.. What good are encrypted transactions when they are still stored in a blockchain database with immutable timestamps, while the users ip addresses are also timestamped and broadcast across the network? Verge will ensure that all transactions are fully secure and truly anonymous.

1.0 Introduction

Centralized fiat currencies lay the foundation for a financial market structure that consists of all transactions being routed to one central exchange with no other competing market, where the supply can be artificially inflated. With this in mind, Verge was conceived in order to provide a form of decentralized currency to eliminate the problem of having one centralized location where transactions are processed. Verge solves this problem by limiting its total supply to be created, and providing a multitude of various transactional options which provide not only a rich opportunistic environment for transactions via multiple platforms; but doing so with the additional benefits of anonymity-centric transactional applications such as Tor, i2P and Electrum.

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 block-chain to handle varying degrees of large transactions. With increased demand comes increased transactional waiting periods, and this has resulted in an increased demand for 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 run by individuals in specific locations that utilize vulnerable computer systems, which are susceptible to legal entanglements. Verge is one of the only 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 fruition.

2.0 Tor Network

To protect users against traffic analysis, which is a form of network surveillance that threatens personal freedom, privacy, and confidential transactional activities, the users transactional traffic is routed through a number of global servers. Each of these servers removes the information of the previous server to the extent that the last exit node server ends up being unaware as to where the network originated from. As a result, Verge users can comfortably send and receive transactions of Verge over the internet with the assurance that the currency trail is virtually untraceable; the receiving end of the transaction and any watchful parties will not be able to link the transactions made to the original sending IP address. Figure 1.1 below illustrates how a Tor transaction occurs.

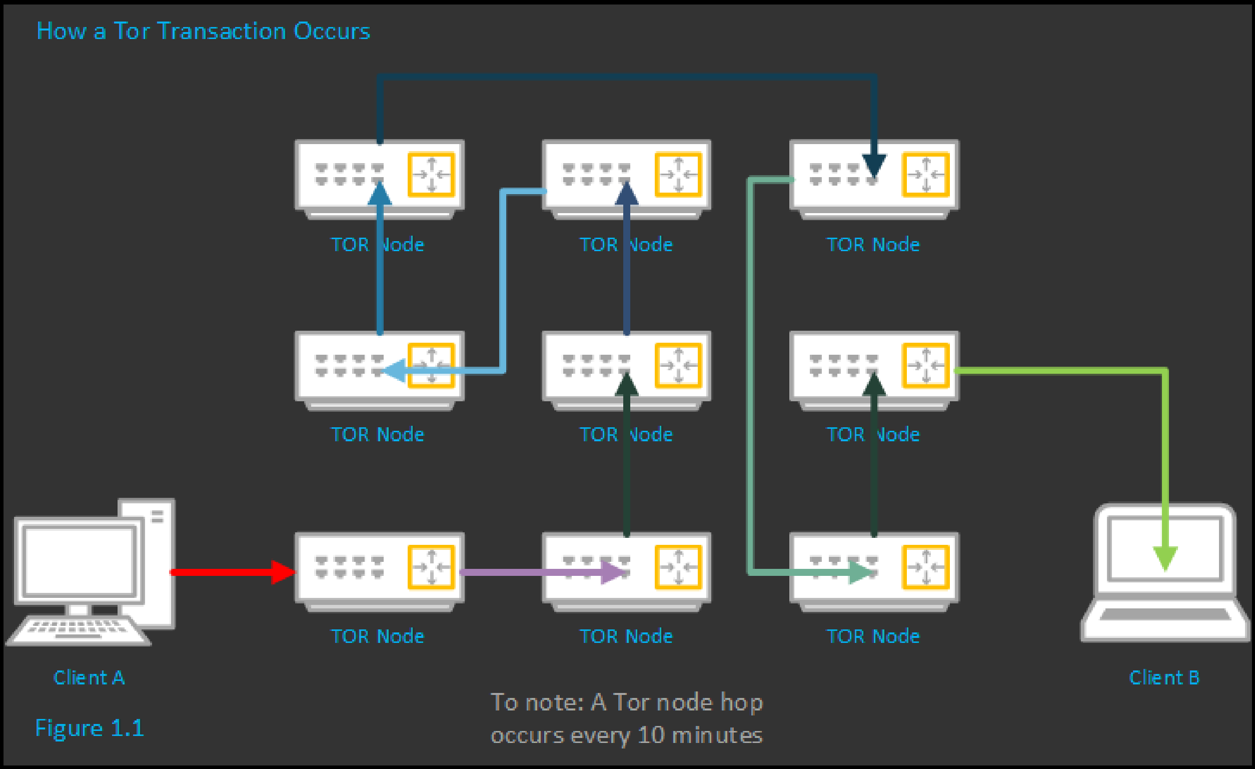

Figure 1.1

To note: A Tor node hop occurs every 10 minutes

By utilizing the Tor Network, Verge will achieve the following:

- **Anonymous Payments:** Verge payments are completely anonymous and untraceable by attackers, government agencies or anyone else for that matter.
- **Fast Confirmation Times:** Verge provides accelerated transaction times, meaning you can send and receive funds almost instantly, without the slow confirmation times of Bitcoin.

3.0 i2P Network

A highly obfuscated tunneling service using ipv6 anonymizes all Verge data that is 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 client passes that message through one of their outbound tunnels targeting one of the other client's inbound tunnels, eventually reaching the destination. Every participant in the network chooses the length of these tunnels, and in doing so, makes a tradeoff between anonymity, latency, and throughput according to their own needs.

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.

When Alice wants to send a message to Bob, she first does a lookup in the netDb to find Bob's leaseSet, giving her his current inbound tunnel gateways. She then picks one of her outbound tunnels and sends the data through it with instructions for the outbound tunnel's endpoint to forward the message onto one of Bob's inbound tunnel gateways. When the outbound tunnel endpoint receives those instructions, it forwards the data as requested, and when Bob's inbound tunnel gateway receives it, it is forwarded through the tunnel to Bob's router. If Alice wants Bob to be able to respond to the data, she needs to transmit her own destination explicitly as part of the data itself. This can be done by introducing a higher-level layer, which is done in the streaming library. Alice may also cut down on the response time by bundling her most recent LeaseSet with the message so that Bob doesn't need to do a netDb lookup for it when he wants to reply, but this is optional [2]. See figure 2.1 for an example.

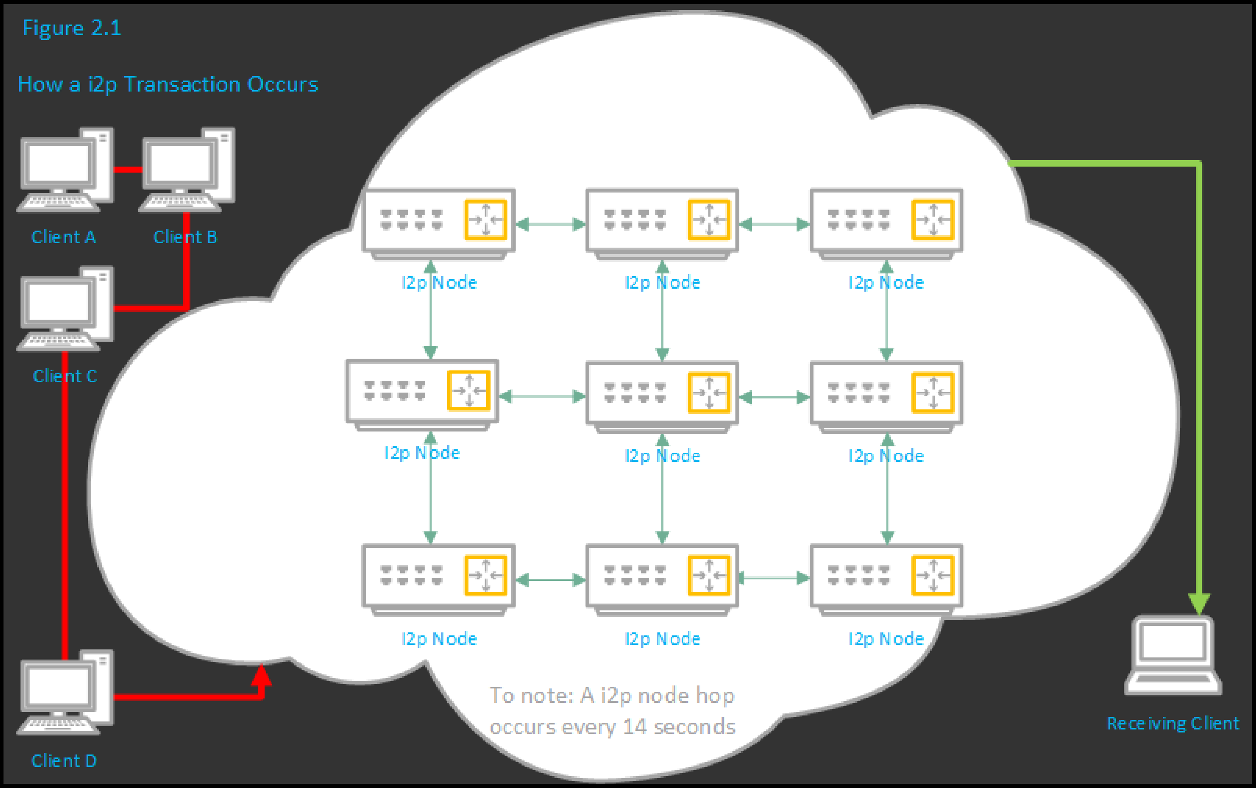

Figure 2.1

How a i2p Transaction Occurs

To note: A i2p node hop occurs every 14 seconds

While the tunnels themselves have layered encryption to prevent unauthorized disclosure to peers inside the network (as the transport layer itself does to prevent unauthorized disclosure to peers outside the network), it is necessary to add an additional end-to-end layer of encryption to hide the message from the outbound tunnel endpoint and the inbound tunnel gateway. This "garlic encryption" lets Alice's router wrap up multiple messages into a single "garlic message", encrypted to a particular public key so that intermediary peers cannot determine either how many messages are within the garlic, what those messages say, or where those individual cloves are destined. For typical end-to-end communication between Alice and Bob, the garlic will be encrypted to the public key published in Bob's leaseSet, allowing the message to be encrypted without giving out the public key to Bob's own router [2].

A bare minimum set of cryptographic primitives are combined together to provide i2P's layered defenses against a variety of adversaries. At the lowest level, inter-router communication is protected by a transport layer security known as Secure Semireliable UDP (SSU) [2]. SSU functions by encrypting each packet with AES256/CBC with both an explicit IV and MAC (HMAC-MD5-128), after agreeing upon an ephemeral session key through a 2048-bit Diffie-Hellman exchange and station-to-station authentication with the other router's DSA key.

Additionally, each network message has their own hash for local integrity checking. Tunnel messages passed over the transports have their own layered AES256/CBC encryption with an explicit IV and verified at the tunnel endpoint with an additional SHA256 hash. Various other messages are passed along inside "garlic messages", which are encrypted with ElGamal/AES+SessionTags [2].

4.0 Verge-Electrum Clients + Servers

Verge-Electrum's focus is speed and simplicity, with low resource usage. It uses remote servers that handle the most complicated parts of the Verge system, and it allows you to recover your wallet from a secret phrase. Additionally, Verge-Electrum offers a simple and easy to use cold storage solution. This allows users to store part of their funds in an offline manner. Moreover, Verge-Electrum is one of the only wallets to provide native Tor and i2p support. By integrating Verge-Electrum with Tor and i2p, one can achieve anonymity while using the desktop wallet; IP addressing information as well as transactional information won't leak to the servers that the client is connecting too.

Verge-Electrum enables multi-signature support, which requires more than one key to authorize a Verge-Electurm 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. A Verge-Electrum transaction with multi-signature support require the signatures of multiple people before the funds can be transferred. The idea is that Verge becomes "encumbered" by providing addresses of multiple parties thus requiring cooperation of those parties in order to do anything with them. Here is an example:

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

Key features of the Verge-Electrum wallet to note:

- **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 that information from a server. No delays, always up-to-date.
- **Transactions are signed locally:** Your private keys are not shared with the server. You do not have to trust the server with your money.
- **Freedom and Privacy:** The Verge Electrum server does not store user accounts. You are not tied to a particular server, and the server does not need to know you. As a matter of fact, the Verge and i2P Electrum servers do not even get an ip address from the client. You can also export your private keys, meaning YOU own your address.
- **No scripts:** Electrum does not download any script. A compromised server cannot send you arbitrary code and steal your bitcoins.

5.0 Multi-Algo 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 and equal distribution of Verge is ensured.

The total supply of Verge is 16.5 Billion. 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 since a wider range of hardware is required in order to take over 51% of the blocks and control the blockchain.

6.0 Conclusion

This paper introduces various concepts and anonymity implementations designed to improve upon the core fundamental concepts that bitcoin first introduced back in 2009. With multiple anonymity-Centric network adaptations known as Tor and i2p, Multi-algorithm mining capabilities and Blackhole technology, which through Electrum transaction simplification; allows for instant transaction confirmations without a centralized authority. While people race to encrypt their transactions, we should ask ourselves a question: What good are encrypted transactions when they are still stored in a blockchain database with immutable timestamps, while the users ip addresses are also broadcasted with timestamps across the network? Verge will ensure that all transactions are fully secure and truly anonymous.

7.0 References

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

[2] I2P: “A Scalable Framework for Anonymous Communication - I2P”
<https://geti2p.net/en/docs/how/tech-intro>

[3] Multisignature. (n.d.).
<https://en.bitcoin.it/wiki/Multisignature>, (2017)

[4] Electrum Documentation. " *Welcome to the Electrum 2.5 Documentation.*”
<http://docs.electrum.org/en/latest/>