Element Protocol: The Completely Anonymous, Untraceable, Decentralized, Realtime, Peer-to-Peer Communication Protocol

Caleb Marshall
January 6th, 2019
anythingtechpro@gmail.com
https://www.element-protocol.com

Abstract. A communication protocol that is designed for complete anonymity, privacy, and security that is capable of communicating at realtime speeds using a light weight, blockchain-less, peer-to-peer network. Peers can communicate through the network without the use of specialized routing nodes in order to securely transfer the data. Messages are double encrypted as they are relayed to other nodes, the encrypted data is only relevant to those with the cryptographically secure key pair(s). There are no limitations to how many participants can use a single key pair to communicate across the network.

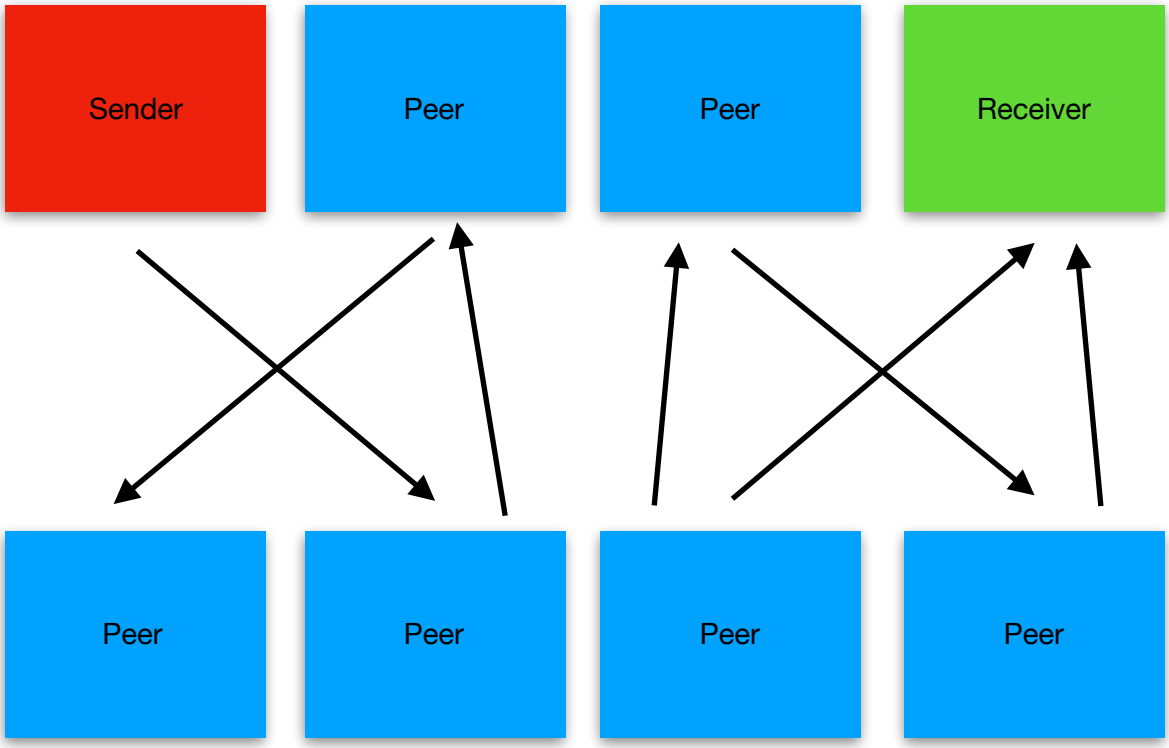
1. Introduction

As the internet continues to evolve, innovating and achieving new heights that were never believed to be possible before. Privacy has become more and more relevant in society. Government organizations take advantage of these privacy issues by exploiting them to achieve desired surveillance over the internet and its users. Many solutions to these issues have popped up in the past such as (but not limited to), TOR, I2P, BitTorrent, BitMessage, and cryptocurrency technology like Bitcoin, Ethereum, Monero etc… But most of these "privacy centric" anonymous communication protocols have many weakness; for example with TOR and I2P there is always a way to draw a line between Point A. and Point B. In the data routing process, other issues like for example with Bitmessage which uses a "proof-of-work like mechanism" to process data communication…

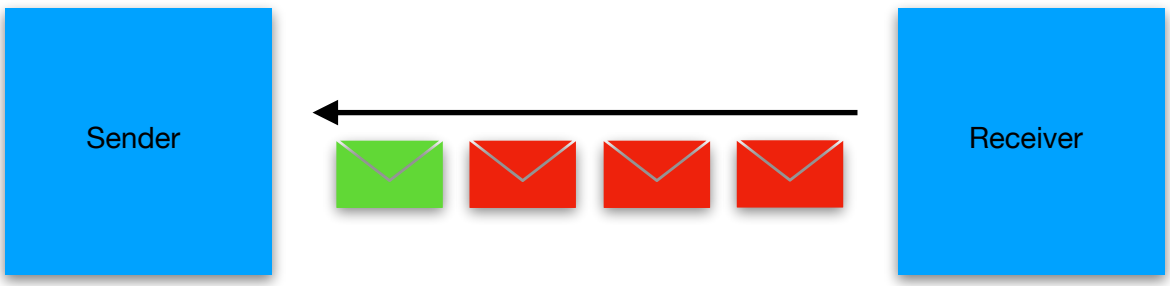
2. Communication

The peer-to-peer network consists of a network of peers that act as relay nodes, no other peer in the network has more authority, all peers have the same authority over the routing process. When a message is sent, it is broadcasted to the peers in which the sender is connected to. The message is continuously passed through the

network until a receiver(s) recognize they have the key pair(s) to decrypt the data, the receiver will never announces that they've received the data to anyone except for the sender, in this case the receiver will



send a reply message notifying the sender that they've received their message and to not bother resending it again (depending on the variant of the sub-protocol used). In order to prevent a message from being received more than once, each message is marked with a timestamp in which it was originally sent at. The timestamp indicates when the message expires and is dropped by the peers in the network, to ensure all peers eventually drop the message, peers validate each timestamp within a range of a minute since they were originally sent, if they exceed a minute then they are considered expired and will be dropped by the network. Each node that has received a message stores a hash checksum of the message and its contents so that if the message arrives more than once, it will be checked and if the message has been queued already, then it will no longer be processed. The checksum of the message will be removed from the queue when the message expires.



3. Sub-Protocols

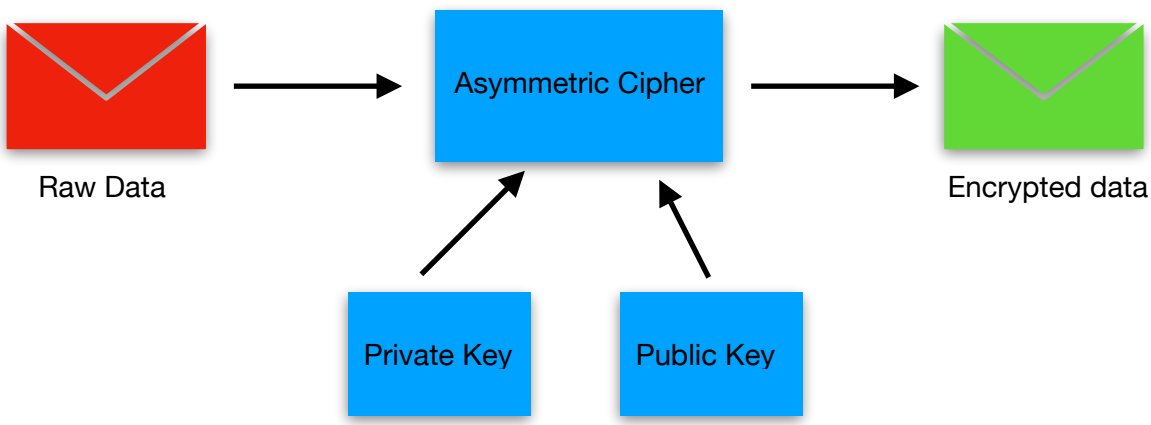
The sub-protocols consist of a high level protocol that handles the processing of data received by the network, for example a TCP and/or UDP like sub-protocol would be implemented in order to handle that type of stream based data communication. Another concept would be to implement some sort of micro-transaction based cryptocurrency which uses the network as its peer-to-peer network for sending/receiving, verifying transactions. Commercial services can also be built upon the network to implement their own custom sub-protocol for encrypted instant messaging, emails, social media, video streaming, etc…

4. Incentive

In order to establish a functioning distributed network, It will require nodes that are willing to route messages to other nodes until the message expires and is dropped… By convention, for any node to receive and/or send data, they will need to participate in the network by routing not only their own data, but any other data they receive. This ensures all peers have the incentive to participate.

5. Privacy

Messages are encrypted with a cryptographically secure asymmetric key pair, anyone with the key pair(s) can intercept and decrypt data that is being broadcasted through the network. The network works similar to that of UDP multicast, you can be anywhere with no association to where you are whatsoever and have the ability to send and/or receive data from/to another peer with the established key pair(s). Messages do not have any kind of association to their sender(s) or receiver(s), they are encrypted with the key pair(s) and a signature of the message is paired along with the message for the receiver to effortlessly determine if the message received has been encrypted with one of their known key pairs, the public key which was used to sign the message signature is not provided, as both the public key and private key are confidential, bound to only the few who have the key pair(s).



6. Conclusion

In this paper we have proposed a system that routes data between a peer-to-peer network to anonymize both senders and receivers allowing them to communicate with complete anonymity in realtime without the limitations of conventional communication protocols as referred to above. The protocol will create a new decentralized, privacy centric internet of its own. As more and more software integrates with the network, it will become more anonymous and untraceable, faster data transfer speeds, etc…

7. References

- Michael J. Fischer, Nancy A. Lynch, Michael S. Paterson, “Impossibility of Distributed Consensus with One Faulty Process”, 1985.
- Satoshi Nakamoto, “Bitcoin”, 2008.
- Adrian Yanes, “Privacy and Anonymity”.
- Peter L. Dordal, “An Introduction to Computer Networks”, 2018.