A Secure Decentralised Messaging Application Utilising the Whisper Protocol

Seán Durban
Tuesday 17th April 2018

Motivation

- Web 3.0 - decentralised web
- Global surveillance
- Current applications
- Improvement of traffic analysis

Design Goals

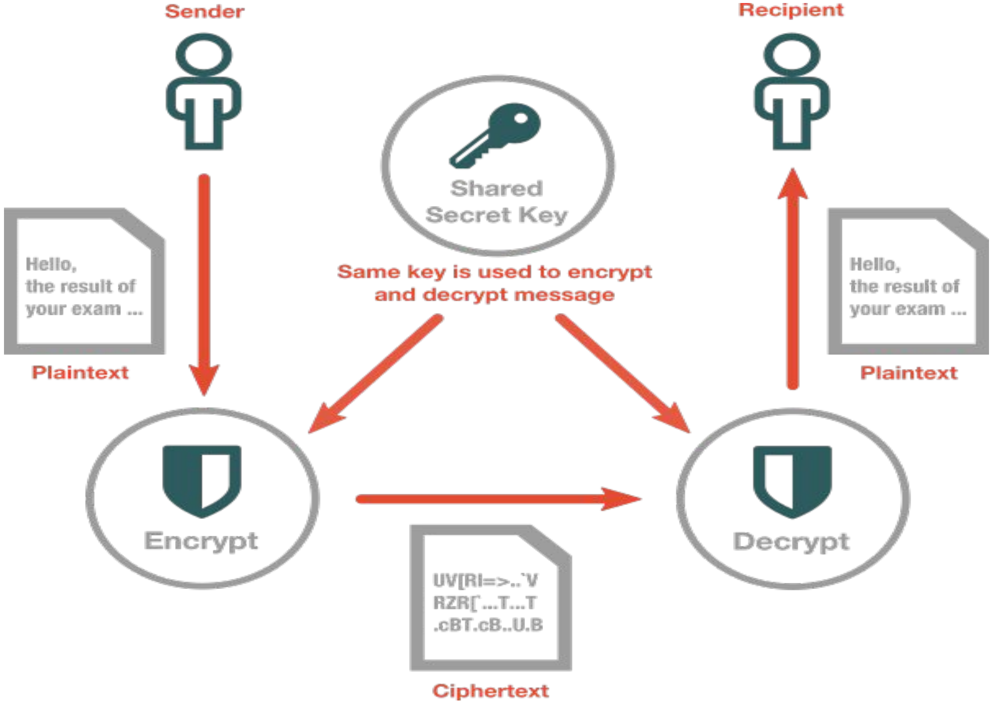
***A secure decentralised messaging application utilising the Whisper protocol*.**

With the following features:

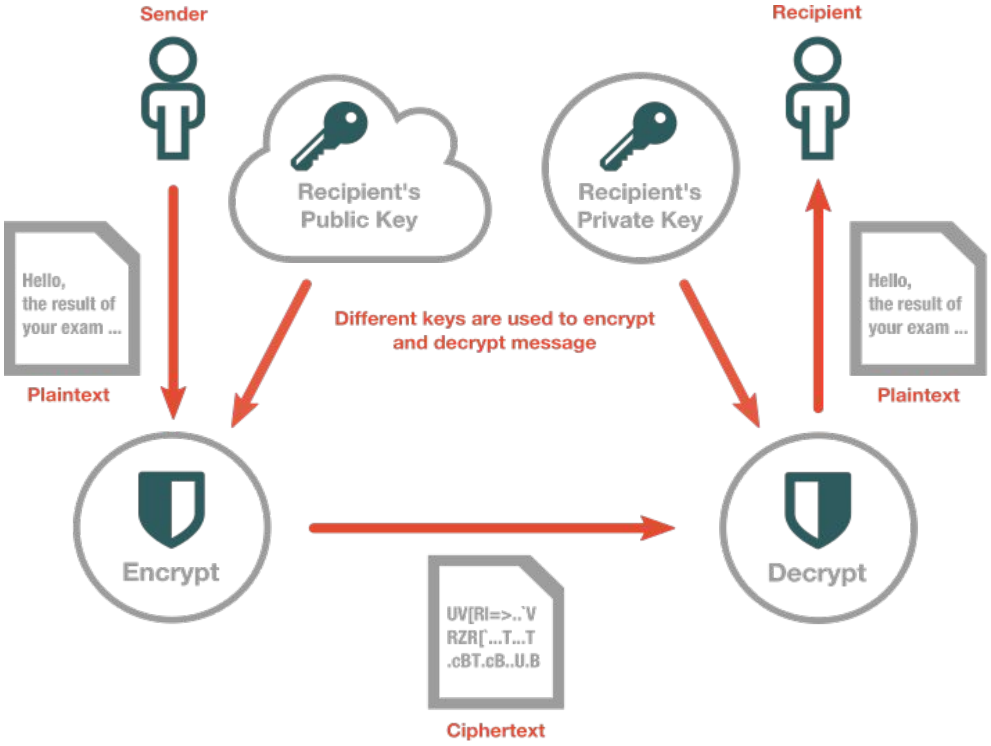
- Intuitive UI with the ability to engage in direct or group messaging
- Preserves backward and forward secrecy
- Spam prevention
- Maintains anonymity and leaks no compromising metadata (Achieves *Darkness*)

Background

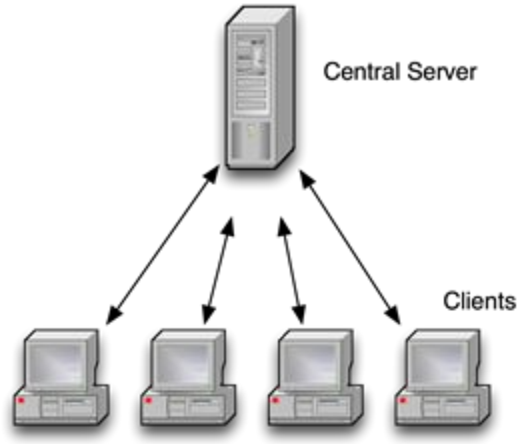
Symmetric Encryption


Sender
Recipient
Shared Secret Key
Same key is used to encrypt and decrypt message
Hello, the result of your exam ...
Plaintext
Hello, the result of your exam ...
Plaintext
Encrypt
Decrypt
UV[RI=>..`V RZR[`...T...T .cBT.cB..U.B
Ciphertext

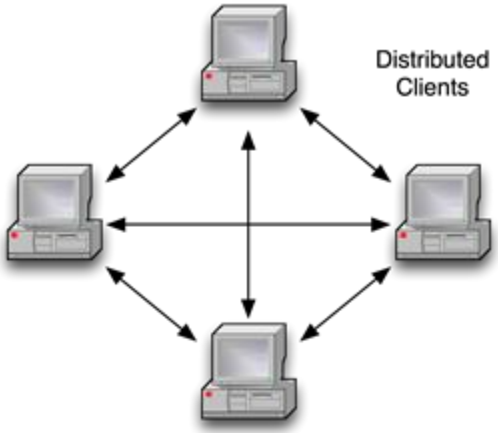
Asymmetric Encryption



Networks



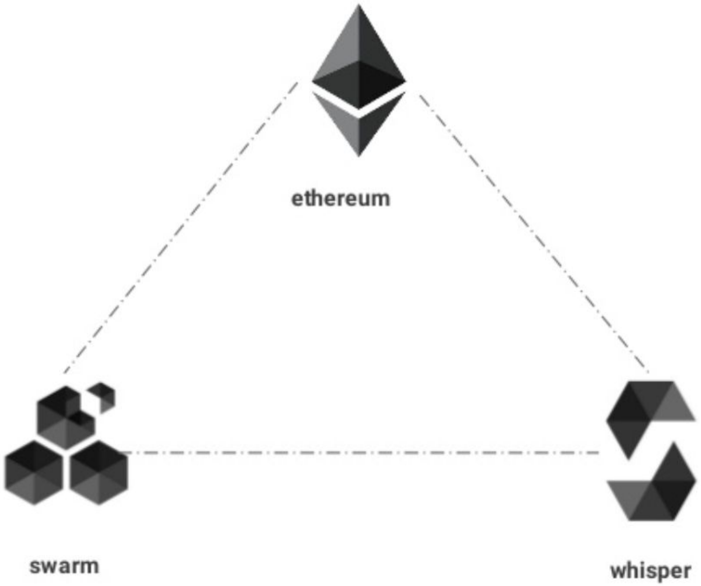
Client / Server



Peer to Peer

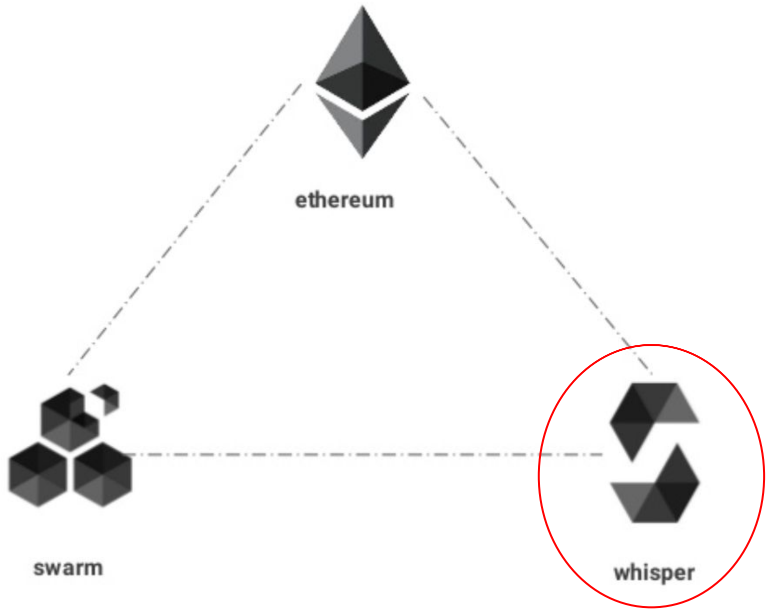
Ethereum

- Decentralised Blockchain platform
- Build and use decentralised applications (Dapps)
- Three major components
  1. Ethereum - Blockchain and distributed consensus
  2. Swarm - Distributed storage
  3. Whisper - Decentralised messaging



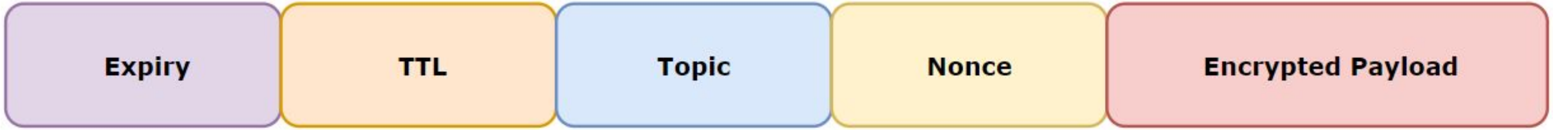
Whisper

- Sub-protocol of Ethereum
- Peer-to-Peer
- Low-level API
- Not endpoint oriented
- User-configurable level of darkness



Envelopes & Messages

- Envelopes are data packets send between Whisper nodes



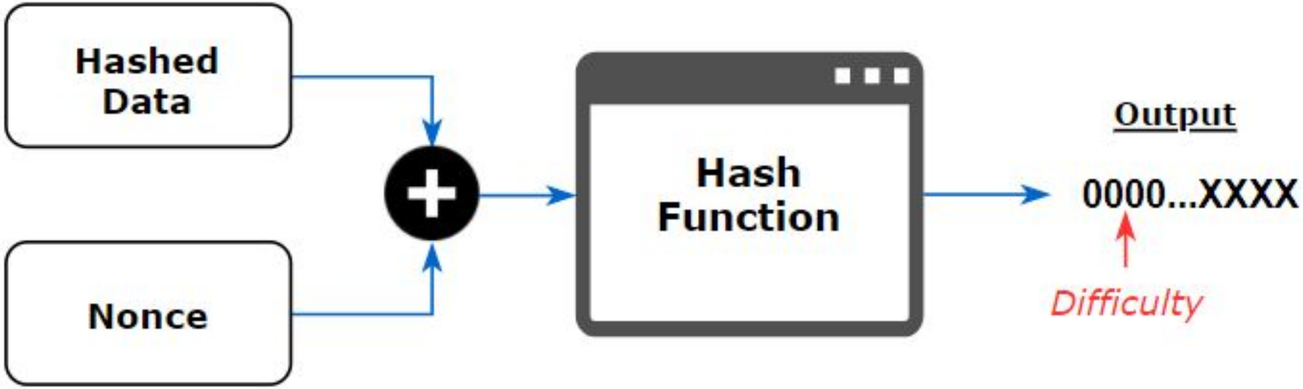
Expiry	TTL	Topic	Nonce	Encrypted Payload

- Messages are an Envelope’s payload in plaintext
- All messages must be encrypted either symmetrically or asymmetrically

Proof Of Work (PoW)

- A prover demonstrating to a verifier that they have performed a certain amount of computational work in a specified interval of time.
- Whisper PoW:

$$2^{\text{Difficulty}} / (\text{TTL} * \text{Message Size})$$



Topics

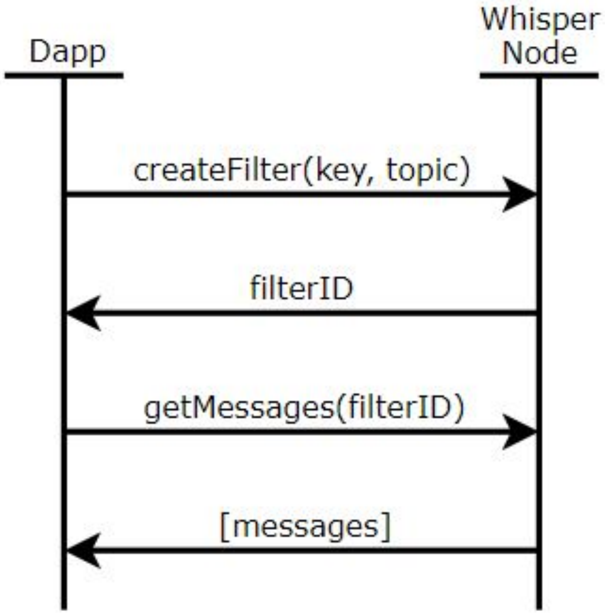
- 4 bytes of arbitrary data (>2 billion unique topics)
- Included in all envelopes as an identifier
- Probabilistic hint to encryption key used
- Partial topics

Example topic: 0xffddaa11

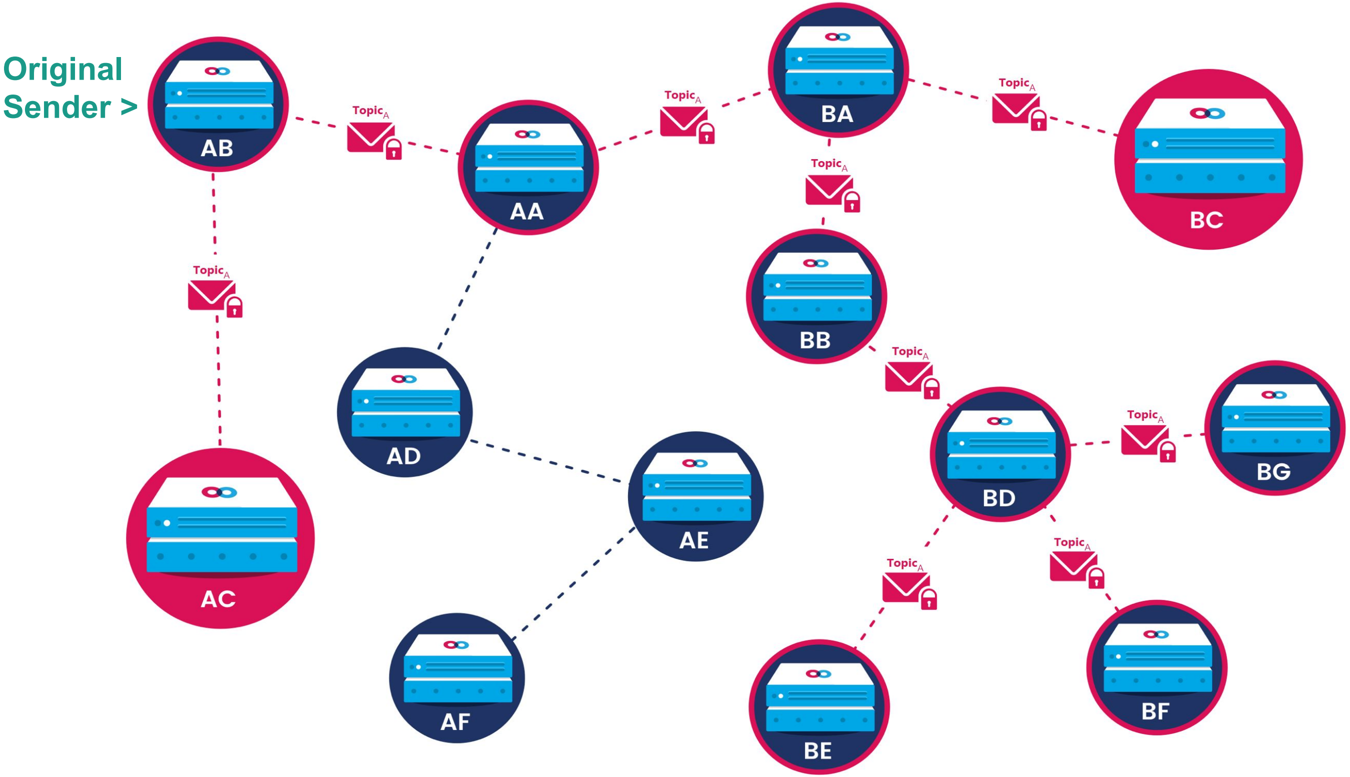
Partial topic (2 bytes): 0xffddXXXX

Filters

- Indicates if node should attempt to decrypt incoming envelope
- Contains a key and conditions (topics, minimum PoW)
- Created by Dapps, handled by node
- Share filters with peers
- Bloom filters



Whisper Example



Darkness

"A truly dark system is one that is utterly uncompromising in information leakage from metadata."

- Padding in messages
- Maintaining constant level of noise
- Plausible deniability from topic collisions
- Overall increased difficulty of traffic analysis

My Application

Design Goals

A secure decentralised messaging application (Dapp) utilising the Whisper protocol.

The following features were delivered:

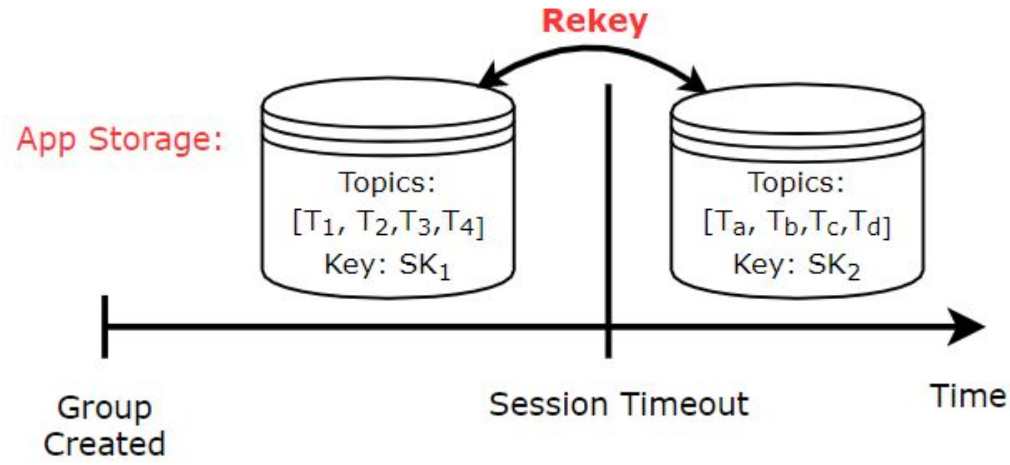
- An intuitive UI with the ability to engage in direct or group messaging ✓
- Preserves backward and forward secrecy ✓
- Spam prevention ✓
- Maintains anonymity and leaks no compromising metadata (Achieves *Darkness*) ✓
- Send files ✓

Spam Prevention

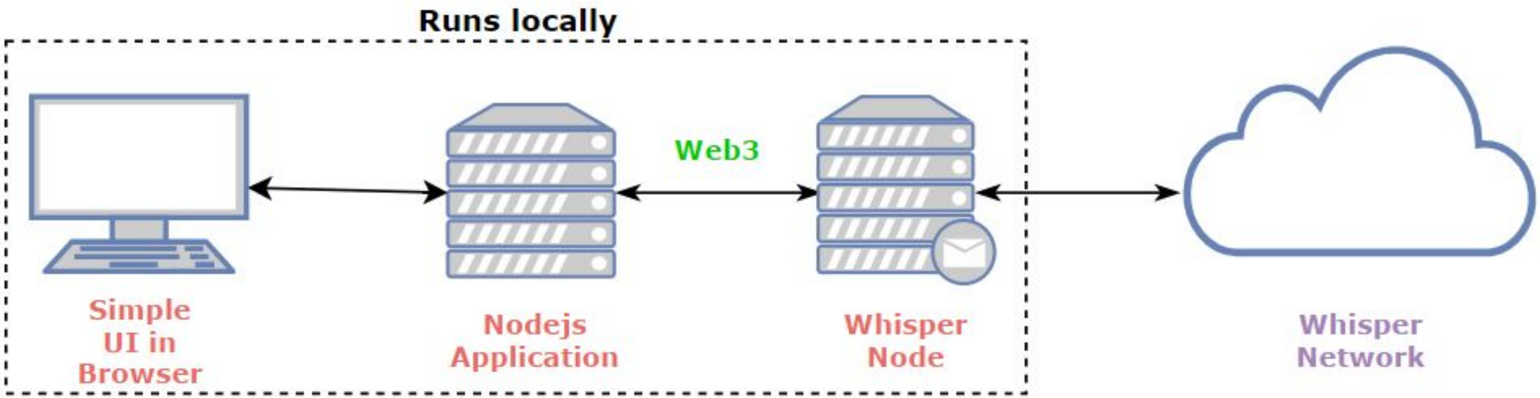
- PoW inherently hinders spam
- Controls network traffic
- User configurable
- PoW condition in filter

Demo Keywords

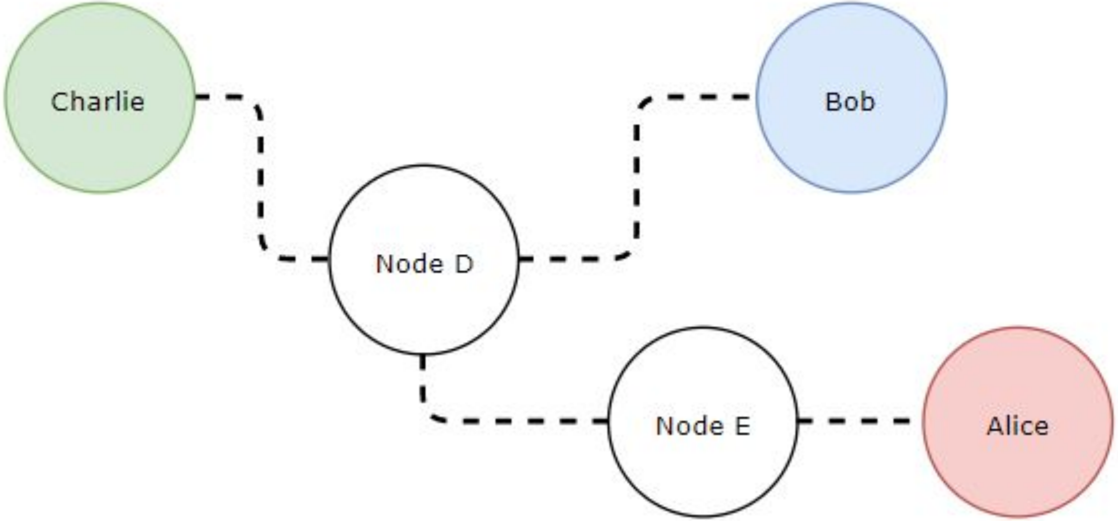
- Group Channel : A messaging group. One shared key, topic per member
- Group Controller : The user who initiated the group and acts as group admin
- Rekey : New topics and session key are generated and used for the group channel
- Session : The period of time when a group channel uses a certain set of topics and some key (time in between rekeys). When a session time out a Rekey occurs



Application Structure



Demo Network Diagram



Demo Objectives

The demo will show the following steps:

1. Create a group channel (both direct and multiple members)
2. Sending and receiving messages
3. An automatic session timeout and Rekey
4. Display forward/backward secrecy by adding and removing members
5. Sending a small file
6. Dealing with spam

Demo Video

Conclusions

Application Limitations

1. Production networks
2. Node failure
3. Centralised group controller
4. Limited testing

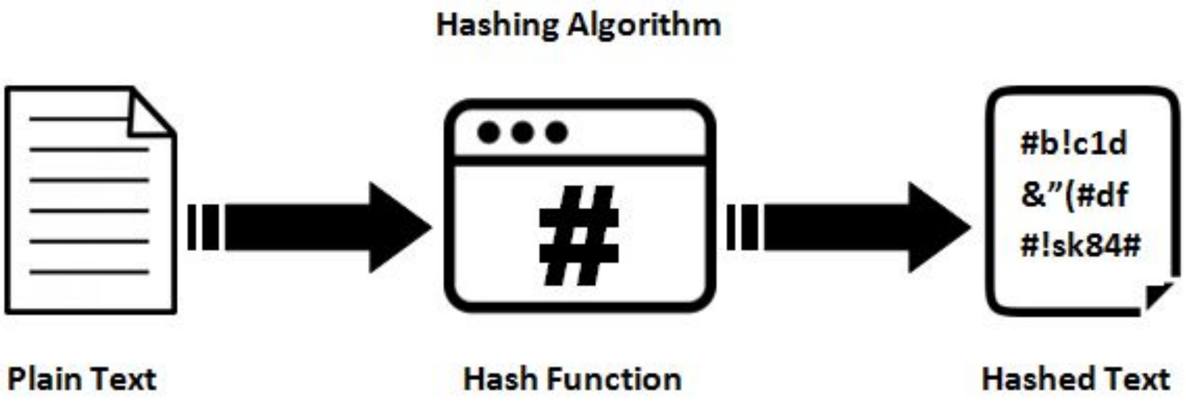
Application Improvements

1. Perfect forwarding via mail server feature in V6
2. Proposed change to a different network to resolve adoption issue
3. Other darkness features

Thank you for listening!

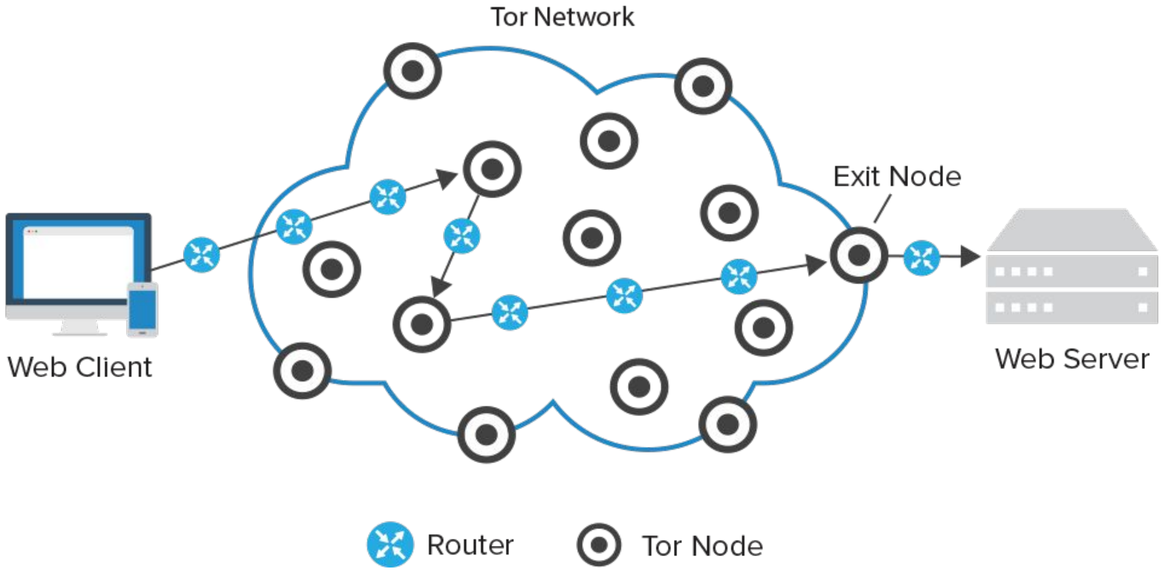
Questions?

Cryptographic Hashing



Anonymity Network

- Blocks tracking or tracing of user's identity on the internet
- Moves traffic through large network of volunteer servers
- Performing traffic analysis and network surveillance more difficult


Tor Network
Exit Node
Web Client
Web Server
Router
Tor Node