Ethereum Whisper

(An Overview)

Vishal Kumar Singh(IIT2015141 Sno. 49)
Shreyansh Gupta(IIM2015001 Sno. 7)
Ayush Agnihotri(IIM2015004 Sno. 8)
Nidheesh Pandey(IIM2015501 Sno. 9)
Abhishek Pasi(ICM2015002 Sno. 1)

What Is Whisper??

- It is a Peer to Peer communication protocol for Distributed Applications(dApps).
- It is designed to deliver DARKNESS (Total anonymity) at high cost.
- Part of Ethereum ecosystem.
- Included by default in Ethereum’s peer-to-peer (P2P) protocol package (go-ethereum/p2p).

Contd.

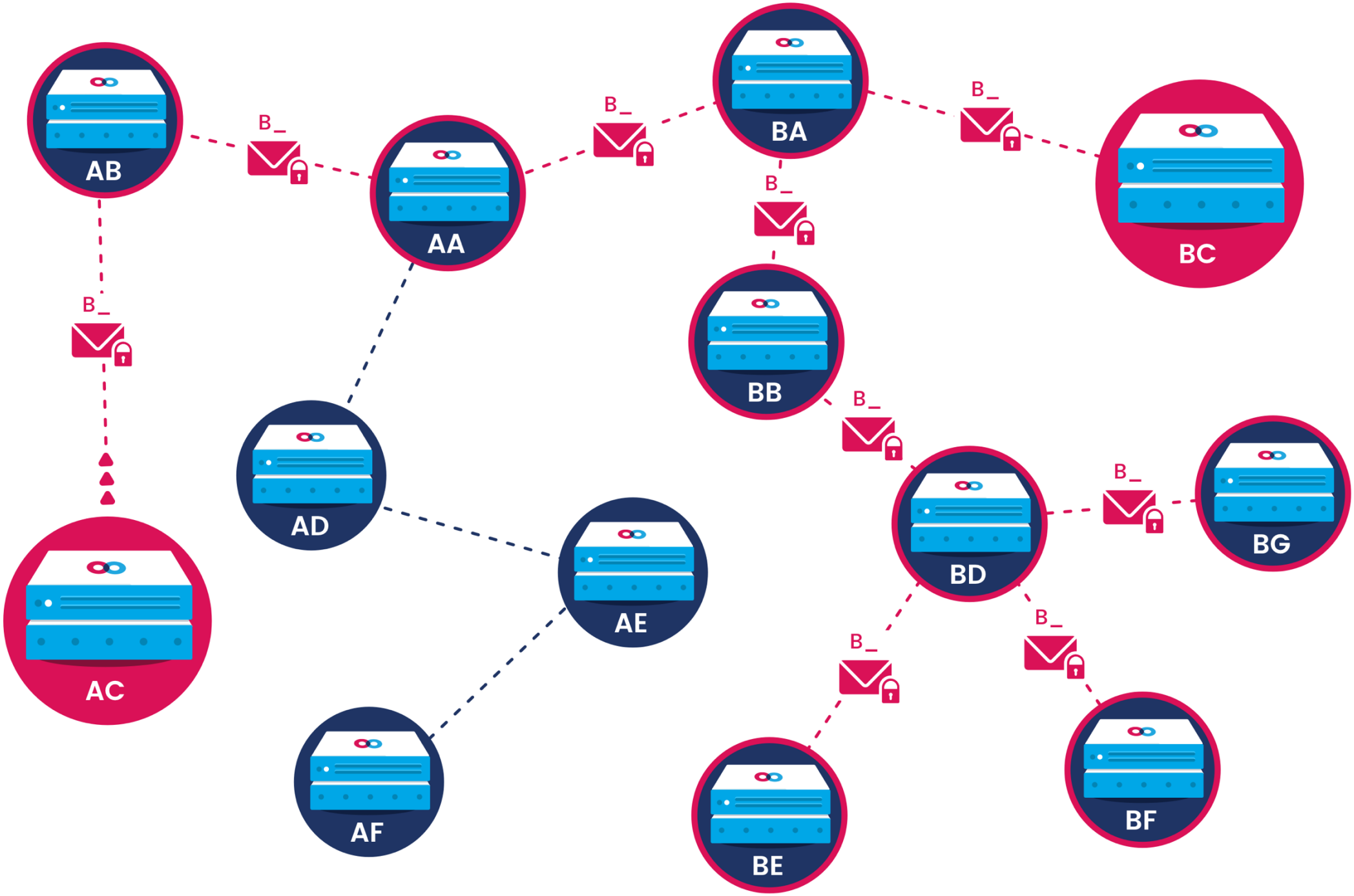
- High cost means high network bandwidth usage, high computational power.
- Tradeoff between level of privacy desired and performance
- Off chain

What is Darkness(Here)??

- No Meta information is leaked.
- Plausible deniability – If a particular message is found on a machine, It cannot be proved that the message was addressed to you.
- We will see how whisper achieves darkness in coming slides.

Principle

- Every message delivered to every node
- Node broadcasts the message to its neighboring nodes, but only recipient has the key to decrypt it.
- All nodes continously forward the message to nearby nodes until the recipient recives it. Then the recipient even forwards it (untraceability)


AB
B_
AA
B_
BA
B_
BC
B_
BB
B_
BD
B_
BG
B_
BF
B_
BE
B_
AF
AE
AD
AC

Message Structure

- TTL – Time to Live. Peers will automatically flush out messages which have exceeded their time to live (max 2 days)
- TOPIC – To Be Discussed Later.
- NONCE – For Proof Of Work to prevent spamming.
- Encrypted Payload – Encrypted message.

Sealing/Proof Of Work

- To prevent a node from spamming the network, whisper uses PoW concept.
- Here, PoW is defined as average number of iterations, required to find the current BestBit i.e the number of leading zero bits in the hash, divided by message size and TTL.
- PoW = (2^BestBit) / (size * TTL)
- Sealing involves hashing contents of the message repeatedly into the smallest possible number via PoW.
- After creating the Envelope, its Nonce should

Priority Based Forwarding

- Priority of the message is decided on following factors -
- Proof of Work(Higher PoW, Higher Priority).
- TTL(Lower the TTL, Higher Priority).
- Message with PoW below a specified threshold is rejected.
- The more work that you perform locally, the faster your message will propagate through the network.

Topic

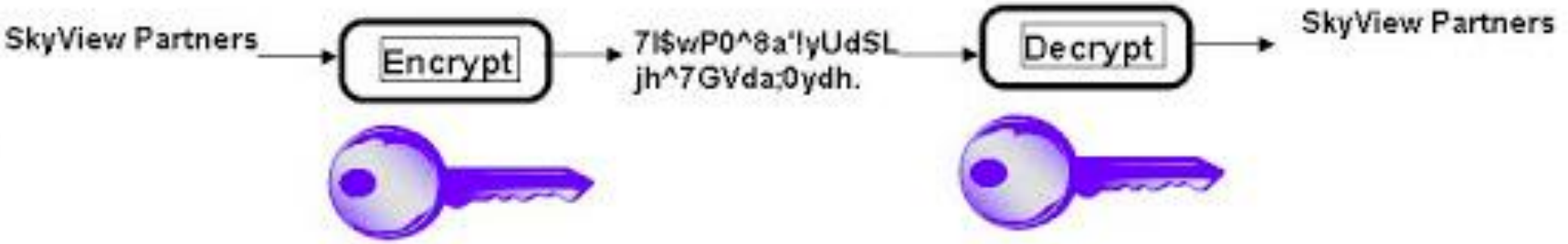
- Heuristics to help node determine whether it worth to decrypt a message or not.
- Every node sets a filter i.e what kind of topics they want to receive.
- Use of Topic Field might reduce darkness, but it reduces latency and processor load.

Types of Encryption

DES
TripleDES
AES
RC5

Symmetric Keys

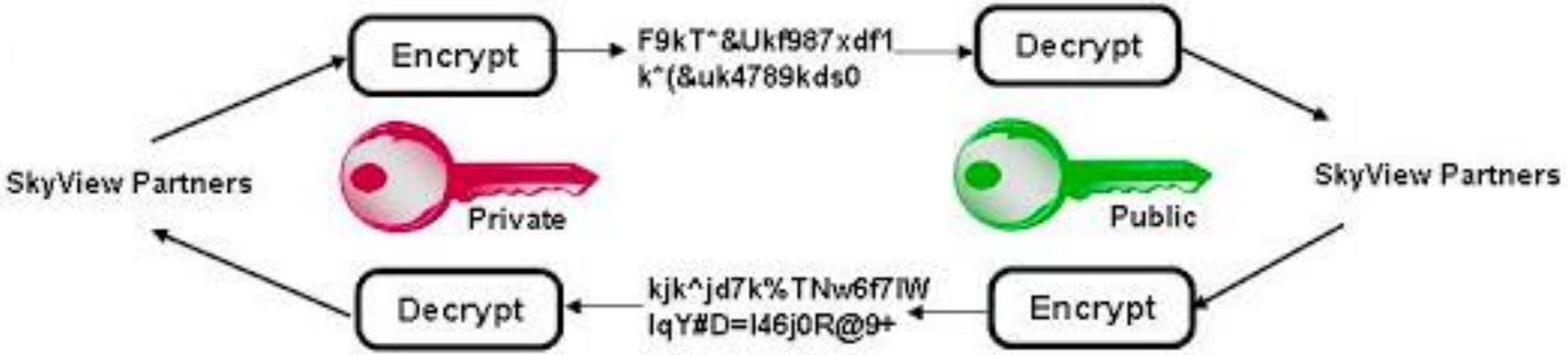
- Encryption and decryption use the **same key**.



RSA
Elliptic Curve

Asymmetric keys

- Encryption and decryption use different keys, a **public key** and a **private key**.

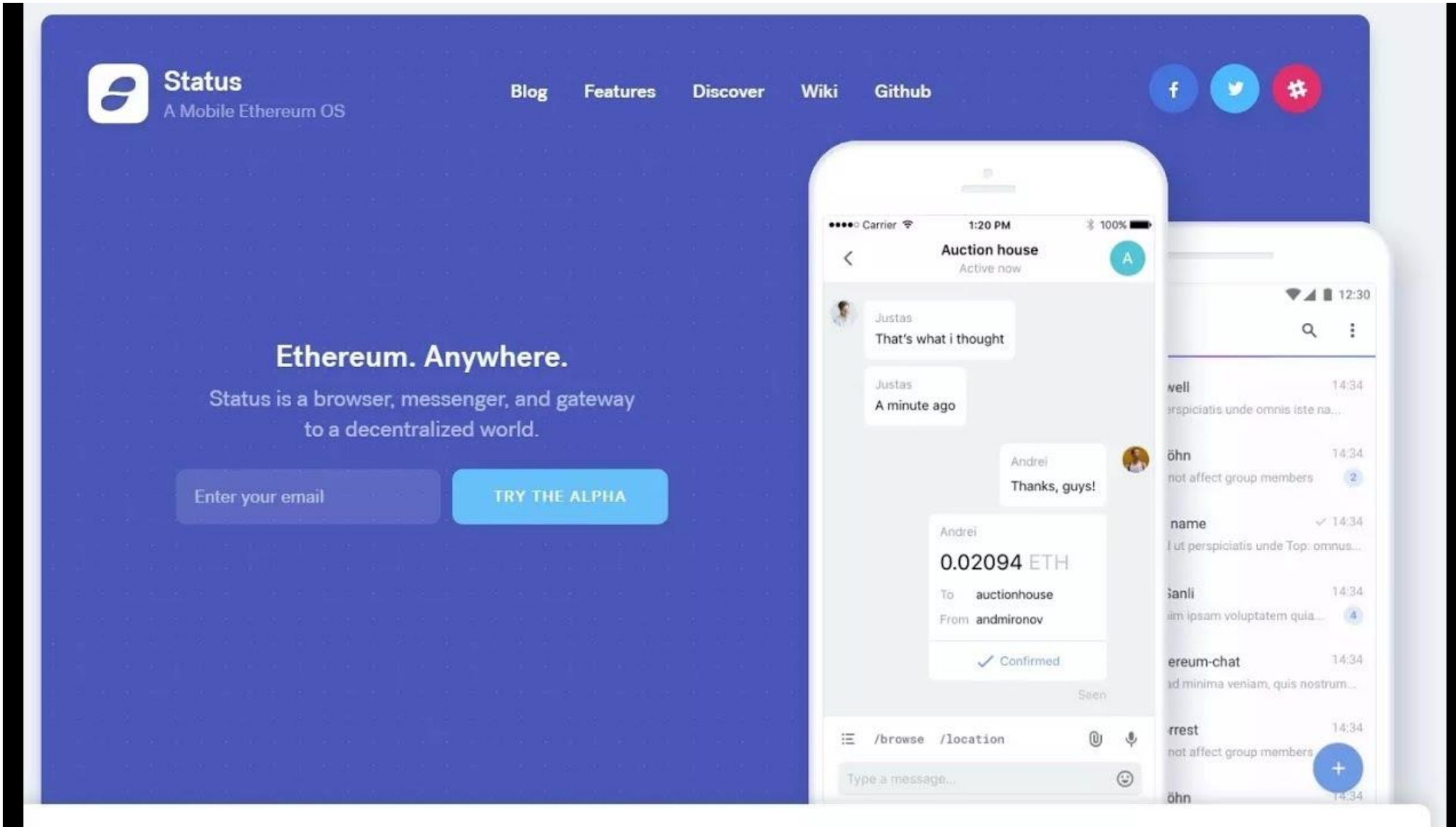


Encryption

- Every Whisper message must be encrypted either symmetrically or asymmetrically.
- Messages could be decrypted by anyone who possesses the corresponding key.
- Every node may possess multiple symmetric and asymmetric keys.
- Upon Envelope receipt, the node should try to decrypt it with each of the keys, depending on Envelope's encryption mode -- symmetric or asymmetric.
- In case of success, decrypted message is

Decryption

- Decryption takes place using a private key, if the message's envelope was encrypted by no more than one sender.
- In such case, the known full message topic is matched to one of the envelope's abridged topics.
- The index is determined and section of the encryption key is decrypted at the beginning of the data segment, so that the final key is retrieved.


Status
A Mobile Ethereum OS
Blog
Features
Discover
Wiki
Github
Ethereum. Anywhere.
Status is a browser, messenger, and gateway to a decentralized world.
Enter your email
TRY THE ALPHA
Carrier
1:20 PM
100%
Auction house
Active now
A
Justas
That's what i thought
Justas
A minute ago
Andrei
Thanks, guys!
Andrei
0.02094 ETH
To auctionhouse
From andmironov
Confirmed
Seen
/browse
/location
Type a message...
12:30
14:34
14:34
2
14:34
4
14:34
14:34
14:34

Conclusion

- Low-bandwidth: Only designed for smaller data transfers.
- Unpredictable latency: Not designed for real-time communication of data.
- Dark (No reliable methods for tracing packets)

Refrences

- https://github.com/ethereum/wiki/wiki/Whisper
- Whisper: Achieving Darkness- Devcon Nov,2017 https://www.youtube.com/watch?v=koZizelOUeI&t=382s
- Decentralized Chat – Siraj Rawal

https://www.youtube.com/watch?v=vVsIHCTGjsE&t=808s