위스퍼(Whisper)란 무엇이고

어떻게 사용할 수 있을까?

2019. 5. 29 / 장진호

자유로운

생각의 표현

Censorship
검열

Restrictions
제한

대 안?

텔레그램

시그널

근본적인 변화가 필요

Amazon tells Signal's creators to stop using anti-censorship workaround

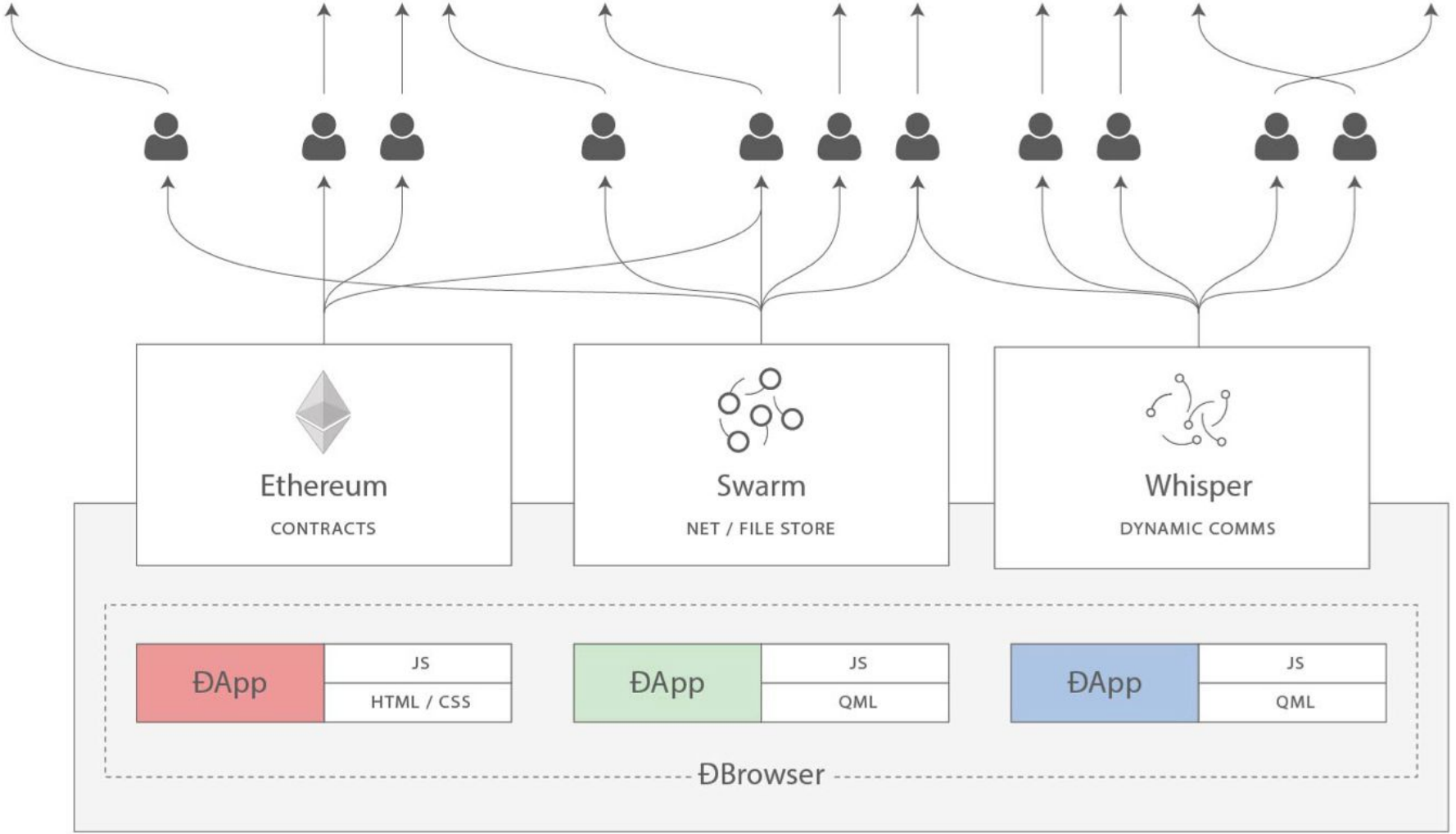
By Adi Robertson | @thedextriarchy | May 1, 2018, 4:10pm EDT

Yandex now censors Telegram.org search results for users in Russia

Meduza 18:43, 27 december 2018

Whisper 위스퍼

댑(DApp)의 상호작용을 위한
커뮤니케이션 프로토콜


Ethereum
CONTRACTS
Swarm
NET / FILE STORE
Whisper
DYNAMIC COMMS
ĐApp
JS
HTML / CSS
ĐApp
JS
QML
ĐApp
JS
QML
ĐBrowser

왜 위스퍼인가?

UDP

0MQ

bitmessage

TeleHash

Tox

High level 프로토콜

폐기잔여시간(Time-to-Live, TTL) 설정 불가

수신인과 발신인에 대한 완벽한 익명성 제공 X

위스퍼의 역사

이더리움 전 CTO, 개빈우드(Gavin Wood)가 이더리움 개발 초기 단계에 댑(DApp) 간의 커뮤니케이션을 돕기 위한 탈중앙 메시징 프로토콜(Decentralized messaging protocol)을 고안

➔ 2014년 10월 12일: Whisper Proposal

➔ 2014년 10월 26일: Whisper Wire Protocol PoC-1

➔ 2015년 8월 20일: Whisper Wire Protocol PoC-2

➔ 현재 Whisper v6(Go Ethereum)이 가장 최신 버전

위스퍼는

1. TCP/IP, UDP, HTTP를 대체하기 위한 플랫폼이 아닙니다.

2. 연결 지향 시스템(Connection-oriented system: 데이터를 보내기 전에 상대편을 확인하고 end-to-end 연결을 유지. 예: TCP)이나 기존처럼 네트워크 End-point 간에 단순히 데이터를 주고 받는 프로토콜이 아닙니다.

3. 대역폭(Bandwidth, 통신량)을 극대화하거나 전송 지연(Latency)을 최소화하여 RTC(Real-time Communication, 실시간 커뮤니케이션)를 구현하는 프로토콜이 아닙니다.

그렇다면 위스퍼는?

1. Dark : 특정 모드(mode)로 설정하면 메시지와 패킷을 추적할 수 없음

2. Low-level : 특정 애플리케이션에 국한되지 않는 범용적 API를 제공하며, API가 DApp에만 노출되고 사용자에게 노출되지 않음

3. Low-bandwidth : 대용량 데이터 전송을 위한 프로토콜이 아님

4. Uncertain-latency : 실시간 커뮤니케이션을 위한 프로토콜이 아님

메시지는 언제 오는가..

위스퍼 설계의 특징

1. P2P 커뮤니케이션 프로토콜

* 메시지를 전파하기 위해 이더리움의 ÐΞVp2p wire protocol 활용

- ÐΞVp2p는 분산 네트워크에서 노드 간 P2P 커뮤니케이션을 돕는 transport-layer 네트워크 프로토콜 모음으로 sub-protocol을 관리하며, 이더리움 외의 블록체인에서도 사용 가능

- 위스퍼는 ÐΞVp2p의 sub-protocol(web3.js shh 패키지)로 통신하며 EVM을 거치지 않음. 즉, 블록체인을 거치지 않아 가스비를 소모하지 않음

위스퍼 설계의 특징

2. 빠르고 효율적인 multi-casting 및 broadcasting

* 멀티캐스트(multi-cast) : 복수의 대상에게 메시지 송신

- 메시지를 보내면 해당 메시지는 네트워크 전체에 전파되며, 의도한 수신인 또는 메시지 주제(Topic)의 공개키(Public Key)를 통해 해당 메시지를 암호화
- 이러한 공개-개인키(public-private key) 암호화 방식때문에 신원 기반 메시징 시스템(Identity based messaging system)으로도 불림. e2e 암호화
- 모든 메시지는 폐기잔여시간(TTL, Time-to-Live)을 가지며, 나에게 의도된 메시지를 수신하더라도 재암호화하여 TTL 내에서 다른 위스퍼 노드에 재전파

위스퍼 설계의 특징

3. Dark 커뮤니케이션 지원

* 특정 모드(Mode)를 활용하면 메시지/패킷을 추적, 조사할 수 없으며 메타데이터를 유출하지 않음

- 클라이언트가 자신에게 전달된 메시지일지라도 TTL 잔여시간 내에서 끊임없이 재전파하기 때문에 송신자와 수신자를 특정하기 어려움

- 메시지의 서명(signature)과 암호화(encryption)여부를 조합하여 어느정도의 데이터를 공개할 것인지 Privacy 수준을 선택할 수 있음

Privacy Level : 내 마음대로 설정하는 보안 수준

JSON 통신

- shh.post({ "topic": t, "payload": p }) - 서명 X, 암호화 X : 익명으로 메시지 전파. 트위터의 대화 주제로 필터링 된 트윗(Tweet)과 유사함

- shh.post({ "from": myIdentity, "topic": t, "payload": p }) - Open 서명, 암호화 X : 일반적인 트윗과 유사함. 특정 인물을 팔로우하는 모든 사람들이 해당 인물이 불특정 다수에게 전파하는 메시지를 확인할 수 있음

* 서명 : 암호화되지 않은 payload에 ECDSA(타원 곡선 디지털 서명 알고리즘) 적용, SHA3-256 해시값

Privacy Level : 내 마음대로 설정하는 보안 수준

- shh.post({ "to": recipient, "topic": t, "payload": p }) - 서명 X, 암호화 O : 암호화된 익명 메시지로, 특정인에게 공유된 익명의 드랍박스 링크와 같음. 메시지는 발신인이 관리하며, 수신인은 누가 보낸 메시지인지 확인할 수 없음

- shh.post({ "from": myIdentity, "to": recipient, "topic": t, "payload": p }) - 비밀(Secret) 서명, 암호화 O : 암호화된 서명 메시지로, 안전한 이메일과 같음. 수신인과 발신인을 제외한 누구도 누가 누구에게 보낸 메시지인지 알 수 없음

Privacy Level : 내 마음대로 설정하는 보안 수준

- shh.post({ "from": myIdentity, "to": recipient, "topic": t, "payload": p, "deniable": d }) - 비밀(Secret) 서명, 암호화 O, 선택적 거부 : 기본적으로 d는 false이며 d가 true이면 메시지 수신자는 메시지 증명 여부를 본인만 알고 있고, 외부로 공개하지 않음

"topic": t , "payload": p >> 메시지 기본 포함 요소

"from": myIdentity >> 서명

"to": recipient >> 암호화

"deniable": d >> 증명 거부 옵션

```
var shh = web3.shh;
var appName = "My silly app!";
var myName = "Gav Would";
var myIdentity = shh.newIdentity();

shh.post({
  "from": myIdentity,
  "topics": [ web3.fromAscii(appName) ],
  "payload": [ web3.fromAscii(myName), web3.fromAscii("What is your name?") ],
  "ttl": 100,
  "priority": 1000
});
```

위스퍼 주요 개념

1. Envelope : Datagram의 Packet과 같은 역할

매개변수 (param)	설명
만료 (expiry)	4 바이트로 의도한 UNIX Time 만료시간 설정
폐기잔여시간 (ttl)	4 바이트로 초 단위의 Time-to-Live 설정
주제 (topic)	4 바이트의 임의 데이터로 배열(array)이 될 수 있음. Index와 같은 개념. 블룸필터 (Bloom filter, 공간 효율성을 높임) 자료구조로 압축되어 전달됨
데이터 (data)	암호화된 **메시지(Payload)**를 포함하며 포함 임의 사이즈의 Byte array
논스 (Nonce)	8 바이트의 임의 데이터, PoW 계산에 활용

위스퍼 주요 개념

2. Messages : envelope의 data를 구성하며 항상 암호화

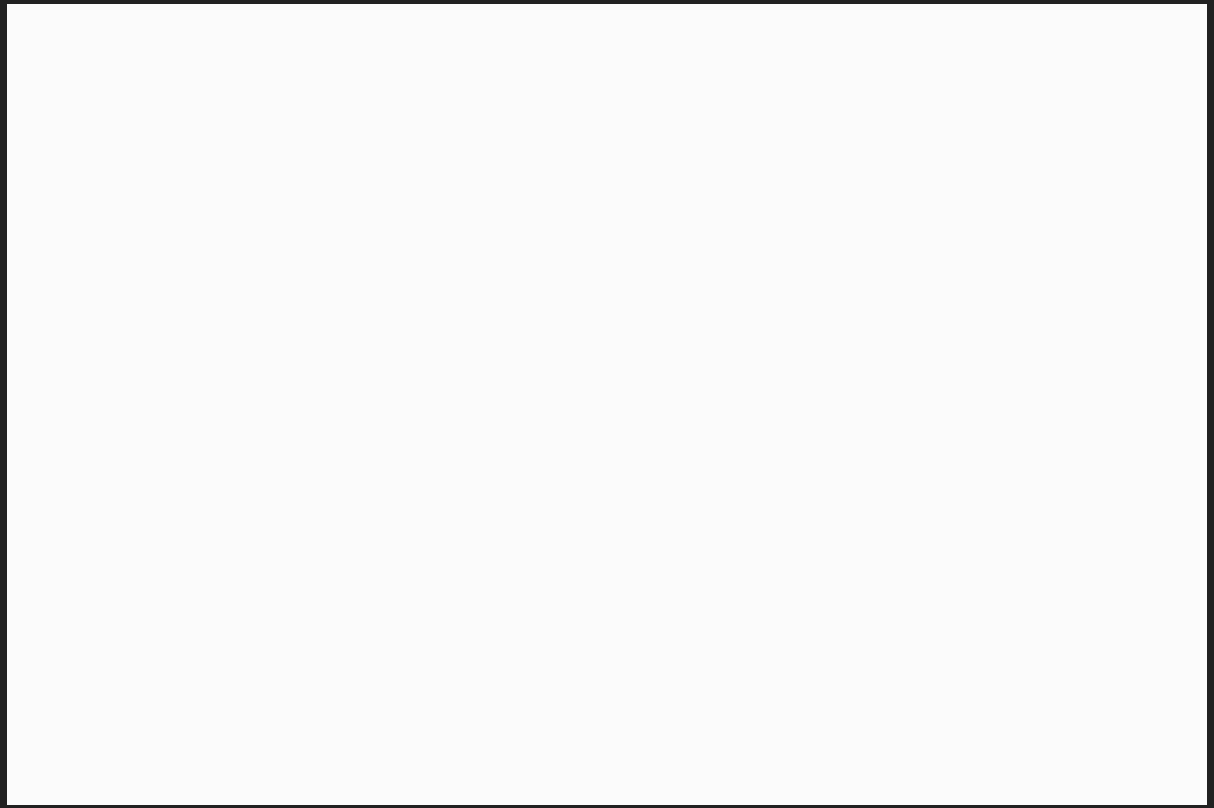
매개변수 (param)	설명
플래그 (flag)	1 바이트로서, 플래그의 Bit 0은 서명 존재 여부 표시. 나머지는 임의의 값
페이로드 (payload)	실제 메시지 컨텐츠를 담고 있음. 수신자의 SECP-256k1 공개키(public key)로 암호화되며, 수신자가 없을 경우 AES-256의 임의의 키로 암호화됨.
서명 (signature)	65 바이트로, 암호화되지 않은 페이로드의 SHA3-256 해시값
보조 필드 (auxiliary field)	최대 4 바이트

위스퍼 주요 개념

3. Topics : 트위터의 해시태그(#)와 같은 개념

- 메시지 발신인 또는 application layer가 설정한 데이터의 SHA3-256 해시값을 구하고, 그 해시값의 왼쪽에서 첫 4바이트로 구성
- 주제의 확장성 및 충돌성 문제를 고려하여 4바이트로 설정
- 노드는 메시지를 받으면 Topic을 확인하고, 가지고 있는 키를 통해 복호화를 시도함. 가지고 있는 키로 복호화에 실패하면 다른 곳으로 전송함

위스퍼 커뮤니케이션 흐름



출처 : https://medium.com/caelumlabs/whisper-shh-bc5416ec0046

PoW를 통한 DDoS 방지

메시지를 보내려면 일을 해라!

- Envelope에 대한 Proof-of-Work를 통해 스팸 메시지 및 네트워크 과부화를 방지하며, 필요한 일의 양은 메시지 크기와 TTL에 비례
- PoW = (2**BestBit) / (size * TTL) : 현재 BestBit[해시값의 선행제로(Leading Zero) 수]를 찾는데까지 걸리는 평균 반복의 수를 메시지 Size와 TTL로 나눔
- 메시지를 전달 받은 노드는 PoW 값이 너무 낮으면 메시지를 거부할 수 있음. 대용량의 메시지(Size)나 긴 TTL은 패널티

왜 위스퍼는 더 안전한가?

- 지속적인 메시지 전파로 메시지 수신자/발신자 특정 어려움. 메시지 전송 중에 수신인과 발신인 ip 등 메타 데이터를 100% 숨길 수 있음

- 메시지 서명 및 검증 (ECDSA)

- 수신인의 SECP-256k1 공개키로 메시지 암호화, 수신인은 개인키로 복호화

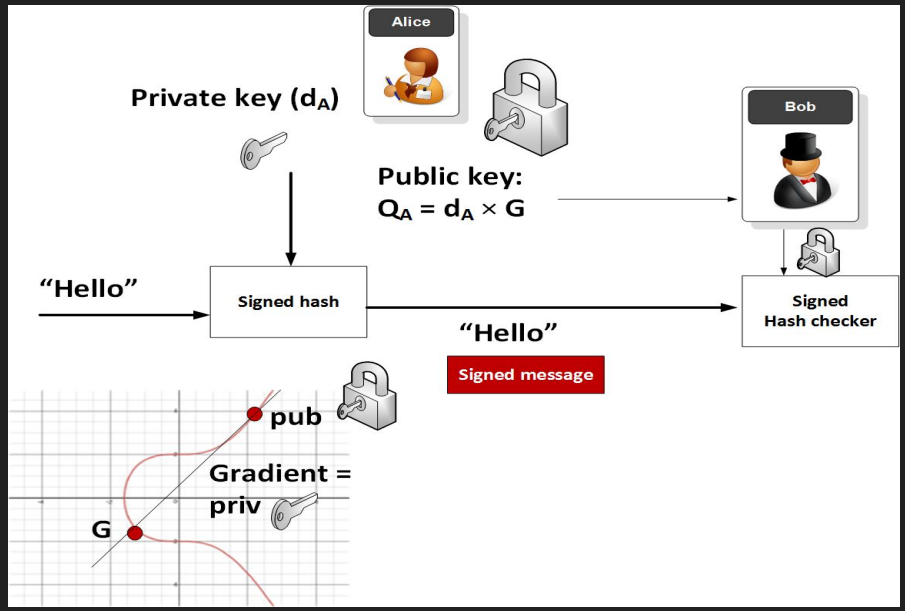


그림 출처 : https://medium.com/caelumlabs/whisper-shh-bc5416ec0046

인생은 실전

어떻게 사용하나?


status


9:41
Chats
Search
Emily
11:17 AM
Thanks Barry. How are things going w...
Parker's Group
11:05 AM
What time are we all meeting later?
2
#introductions
10:30 AM
Welcome to Status!
5
Fiona
10:27 AM
Through privacy and security, empow...
Nelson
9:47 AM
A communication tool to preserve cul....
Football Team
8:59 AM
Is there practice tonight?
#status
8:43 AM
What is the latest with the Sticker Mar...
Robin
7:32 AM
Thanks for the coffee yesterday!
#statusphe
Yesterday
Great work on the
Chats
7
DApps
Wallet
Profile
9:41
Nelson
Today
ey! Great seeing you
esterday
9:12 AM
It was great catching up and glad to see you are using Status
9:37 AM
hat restaurant was so good.
et's go again some time.
9:38 AM
I would love to. Also, how much do I owe you for lunch?
9:38 AM
SENT
was $15
9:39 AM
0.1781005 ETH
~15.08 USD
Sent at 9:40 AM
Confirmed
hanks!
9:41 AM
e a message
2

Michael Shohn 18:34
Almost forgot, access granted!

2 #peoplewithdogs 18 Oct
Alex: I love poodles! 🐕

Michael Shohn 23 Sep
Thanks in advance!

Home Profile

Michael Shohn

interaction anything but social, but technical specifics on how to get on board or participate in a team are I think generally useful, especially if they prevent maintainers from pasting the same response to every PR / issue. 7:30 AM

Sept 23

Michael Shohn
Is there a list of all CC's contact codes on Status? 7:30 AM

Yesterday

Michael Shohn
Can we get #status-security added to the people-ops/status-channels page? 8:00 AM
Let me know 🙏 8:01 AM

You
> Michael Shohn
> Hm, what do you think about http://www.mywebsite.com/? Message bubble max width in public chat is 340px

I ❤️ the website!

Michael Shohn
Do we have abstracted source code contribution guidelines somewhere that could be reused across all sub-projects? Be nice, have tests, follow rules in this doc, etc. that sort of stuff presented in a common language? 8:50 AM

You
Yes, if we can abstract it a little to apply. Talk to @phoebebuffay 9:50 AM

Today

You
👋 Done! Let me need if you need anything else 9:50 AM
Almost forgot, access granted!

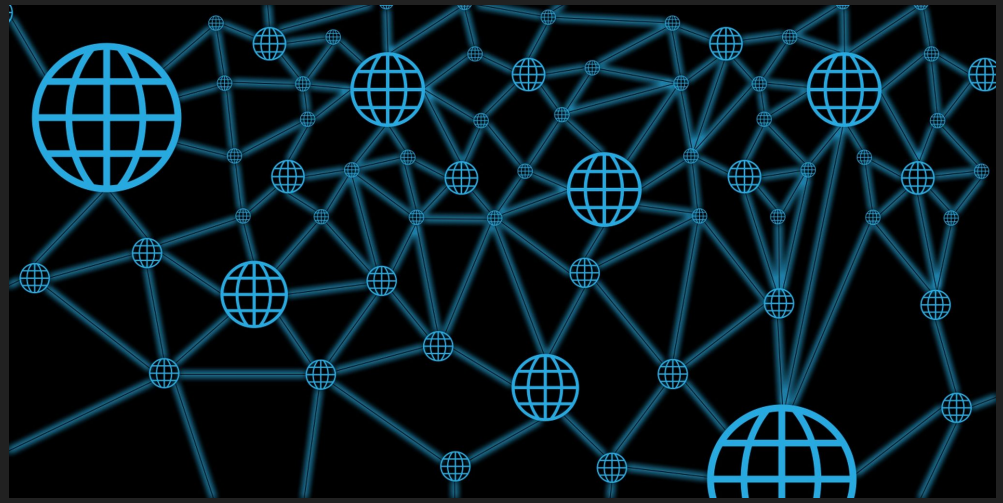
12 ↓

Type a message...

내 메시지!!!

메일서버(Mailserver) 활용

분산화된(Decentralized) 위스퍼 메일 서버를 통해
메시지를 저장하고 다른 노드에 재전파



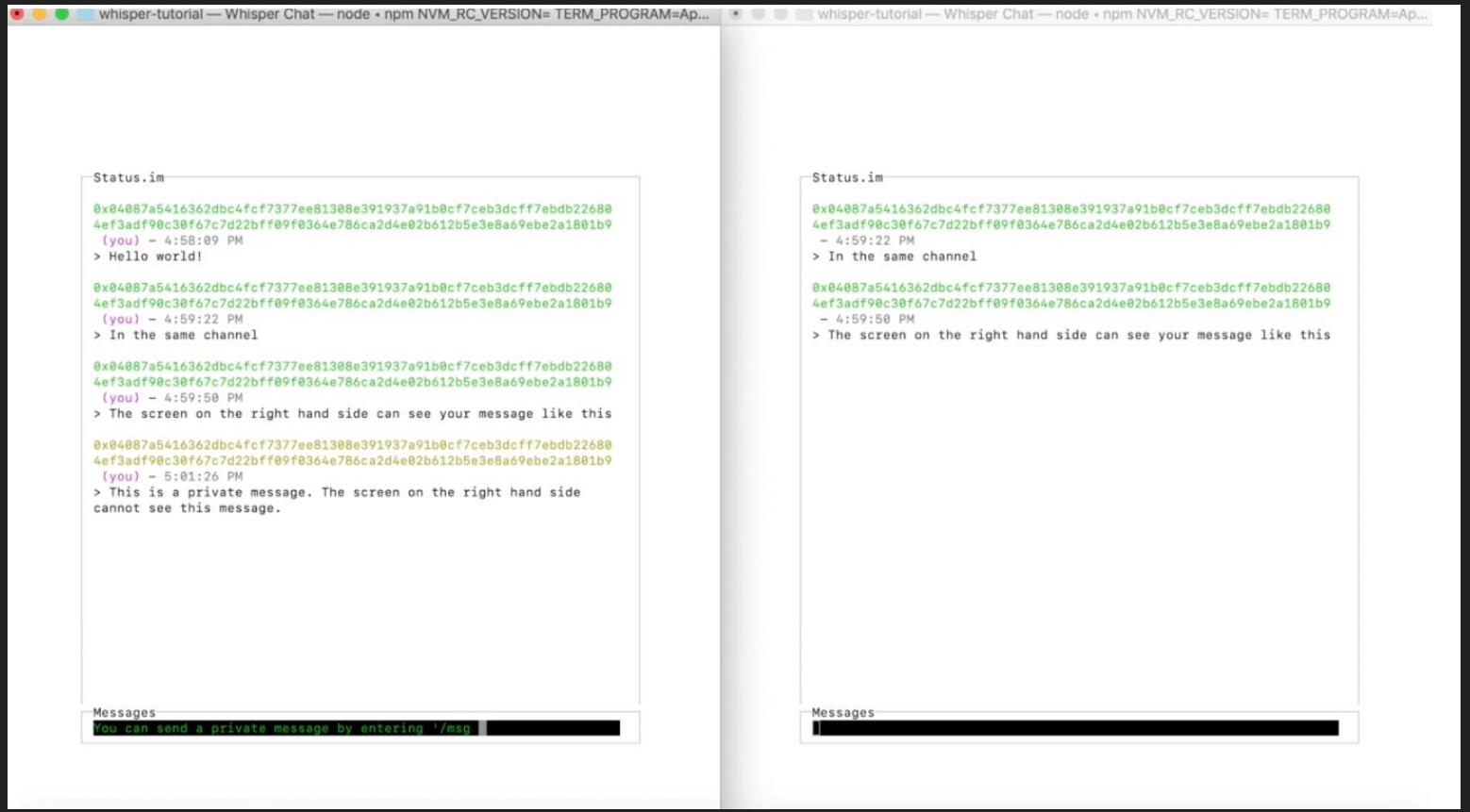
디스크 스토리지 필요 :
한달에 약 600MB
정도의 데이터 공간

소스 코드가 궁금하다면?

스테이터스 앱 : https://github.com/status-im/status-react

스테이터스 Go : https://github.com/status-im/status-go

(메일 서버)

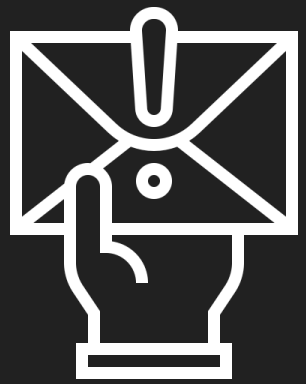


Whisper CLI 튜토리얼 : https://status.im/tutorials/whisper_basic_cli.html

Whisper 튜토리얼 영상으로 따라하기 : https://youtu.be/XgNhY5rRW8E

위스퍼의 한계

- 대규모 데이터 처리 어려움 (복잡한 처리 과정, TTL, 가십 프로토콜)
- 메시지 지연 가능성 (PoW)
- Whisper v2.0 논의 중 (Status, W3F, Validity Labs) >> 확장성 문제 해결



References

David Gabriel Tomuletiu, Whisper - Shh! https://medium.com/caelumlabs/whisper-shh-bc5416ec0046

Ethereum Wiki, Whisper https://github.com/ethereum/wiki/wiki/Whisper

Ethereum Wiki, Whisper overview https://github.com/ethereum/wiki/wiki/Whisper-Overview

Ethereum Wiki, Whisper PoC-2 Whitepaper https://github.com/ethereum/wiki/wiki/Whisper-PoC-2-Protocol-Spec

SigmoiD, Whisper:A pure identity-based messaging system
https://drive.google.com/file/d/1nz8m8P3qn6JYyXSFIwLn3tHbMBa13brG/view?fbclid=IwAR03DfX3HZH7dLs-r4WpgkbI_RPhwtE6pQF-VJY0fAEgS2kMx937UtlZnRg

Go Ethereum, How to Whisper https://github.com/ethereum/wiki/wiki/Whisper-Overview

Status.im, Whisper: Extended Features https://github.com/ethereum/wiki/wiki/Whisper-Overview

Status.im, Whisper in Your CLI https://www.youtube.com/watch?v=XgNhY5rRW8E

Adi Robertson, Amazon tells Signal's creators to stop using anti-censorship workaround
https://www.theverge.com/2018/5/1/17308508/amazon-web-services-signal-domain-fronting-ban-response

Meduza, Yandex now censors Telegram.org search results for users in Russia
https://meduza.io/en/news/2018/12/27/yandex-now-censors-telegram-org-search-results-for-users-in-russia

발표 자료

http://bit.ly/whisperethcon