

# telehash

*Protocole de distribution P2P sécurisé*

*Gilles Bonhoure - RICM5*

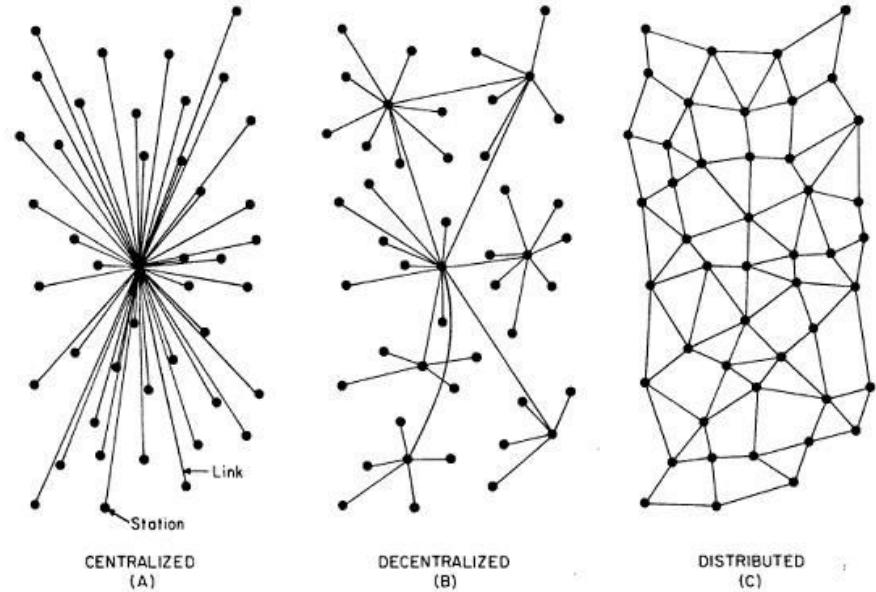
*13 Octobre 2017*

# Sommaire

- ❖ Contexte
- ❖ Telehash
  - Fonctionnement
  - Architecture
- ❖ Solutions
- ❖ Démonstration
- ❖ Conclusion

# Besoins

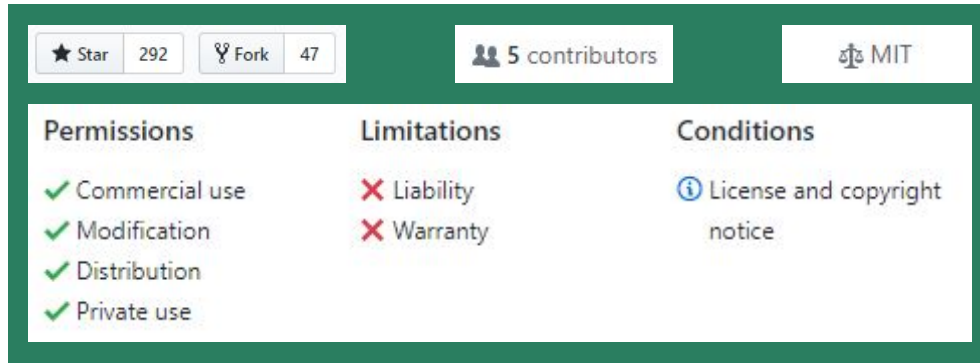
- ❖ Contourner le Cloud
- ❖ Communication directe (P2P)
- ❖ Echanges sécurisés
- ❖ Flexibilité applicative



*medium.com*

# Telehash

- ❖ Créé par Jeremie Miller en 2010
- ❖ Organisation Github
- ❖ Version NodeJs (v3)



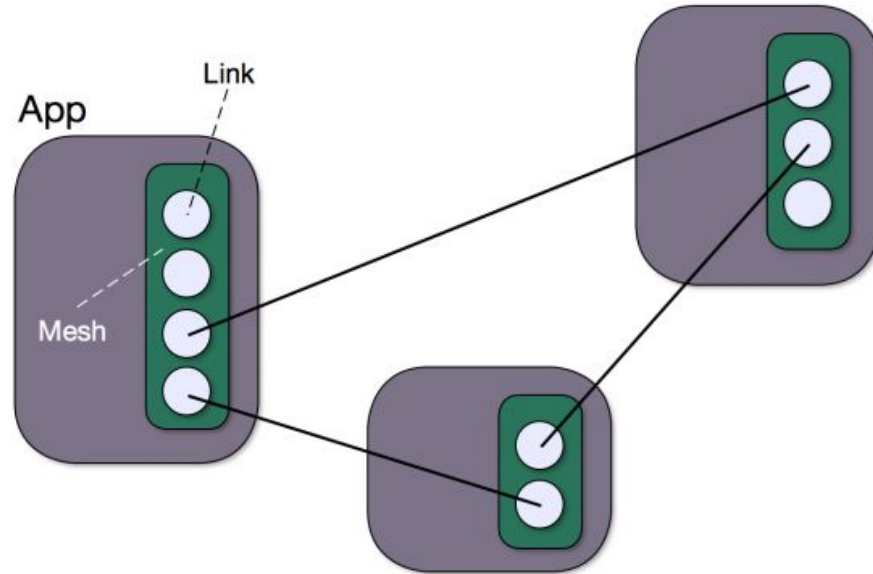
Star 292 Fork 47 5 contributors MIT

Permissions	Limitations	Conditions
✓ Commercial use	✗ Liability	ⓘ License and copyright notice
✓ Modification	✗ Warranty	
✓ Distribution		
✓ Private use		

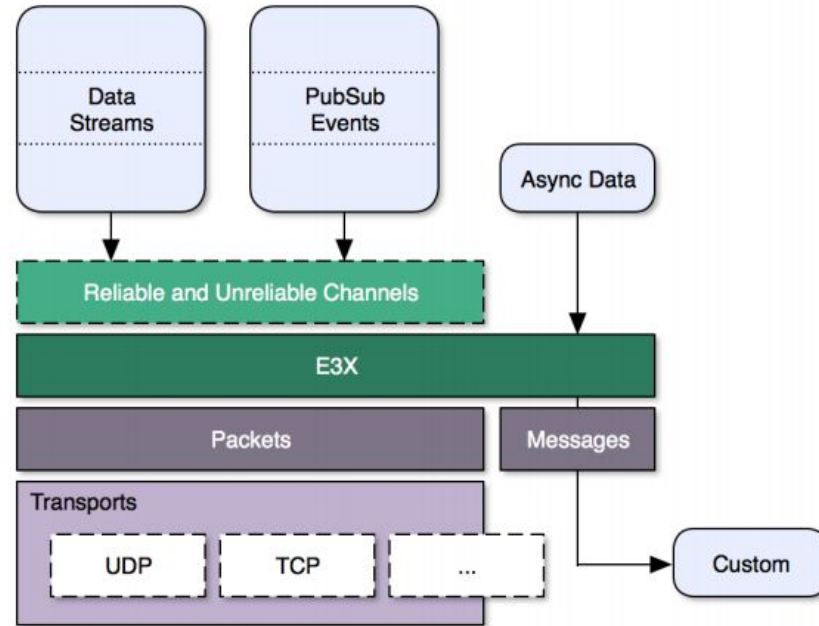


*hacked.com*

# Fonctionnement



# Empilement de couches



# Solutions

- ❖ Identification par Hashname (Kademlia)
- ❖ Clés publiques / privées
- ❖ “Paquets” Json
- ❖ Patterns
  - UDP / TCP
  - HTTP
  - Stream
  - Publish-Subscribe ...

# Démonstration

- ❖ Ping
- ❖ Envoi de messages



# Conclusions

- ❖ Mise en place rapide
- ❖ Stable
- ❖ Réseau performant
- ❖ Multi-applicatif

# Conclusions

- ❖ Pas de mise à jour depuis 2015

	hashname	link	uri	routing	streams	sockets	udp	tcp	http	tls	webrtc	bluetooth
node.js	✓	✓	👤	✓	✓	✓	✓	✓	✓	👤	👤	
browser.js	✓	👤							👤		👤	
c - unix	✓	✓	👤	👤	👤	👤	✓	✓				
c - embedded	✓	✓	👤		👤	👤	👤	👤				
go	✓	✓					✓					
python	✓	👤					👤					

- ❖ Un projet (The Locker Project) avorté ?
- ❖ De nouveaux concurrents ?



**Merci !** 

**Questions ?** 

# Sources

- ❖ <http://telehash.org/> + <http://telehash.org/v3/spec/v3.0.0-stable.pdf>
- ❖ <https://github.com/telehash>
  - <https://github.com/telehash/telehash-js>
- ❖ <https://www.infoq.com/presentations/A-P2P-Digital-Self-with-TeleHash>
- ❖ [https://en.wikipedia.org/wiki/Locker\\_\(software\)](https://en.wikipedia.org/wiki/Locker_(software))
- ❖ <https://en.wikipedia.org/wiki/Peer-to-peer>
- ❖ [https://en.wikipedia.org/wiki/Resilio\\_Sync](https://en.wikipedia.org/wiki/Resilio_Sync)