Agenda
–

1. Waku Introduction
2. Waku Demo
3. Need for flexible rate limit
4. Economics

1. Waku Introduction
–

Waku is:

- A suite of messaging protocols
- Meant for delivering a message from A->B
- Or A->B/C/D
- In a privacy-preserving way
- Without relying on a central entity
- Generalized for any use case
- Permissionless for everyone

1. Waku Introduction
–

Problems already solved by Waku:

1 Latency

- ✅ Limit msg size (150 kB)
- ✅ Tradeoff D and bandwidth
- ✅ <1 sec

2 Rate limiting

- ✅ Anonymous rate limit using RLN
- ✅ Peer scoring, kick bad peers

3 Offline nodes

- ✅ Store protocol
- ✅ Store sync

4 Resource-restricted devices

- ✅ Light protocols (filter/light-push/peer exchange)
- ✅ Onchain merkle trees (Lazy IMT)

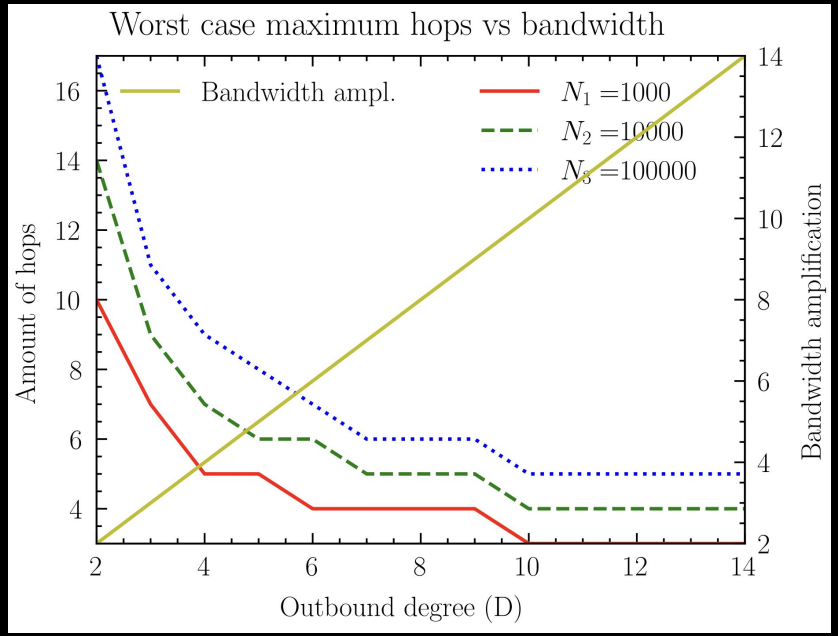
5 Scalability

- ✅ Shard the network

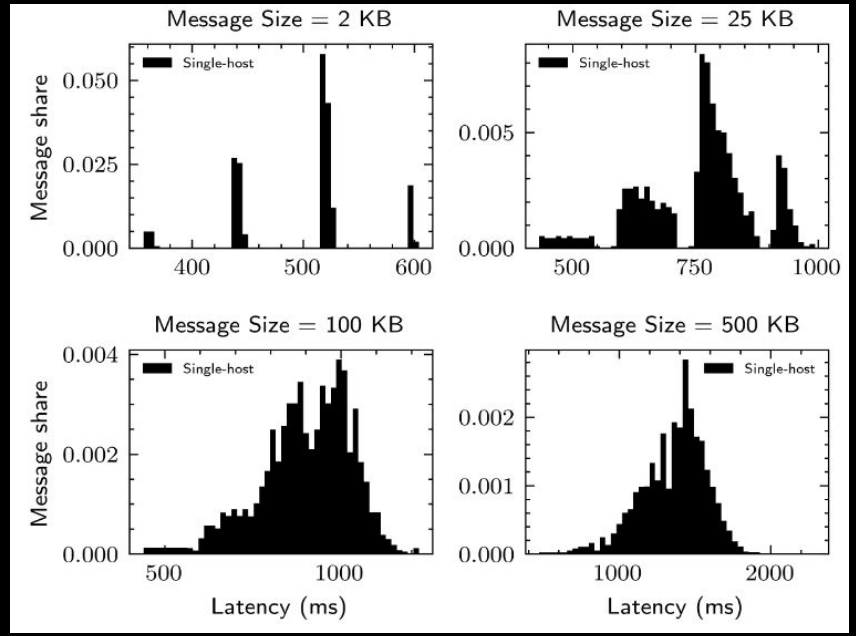
1. Waku Introduction
–

1 Latency

- 95% of messages <1 second to all peers



Theory



Simulations

1. Waku Introduction
–

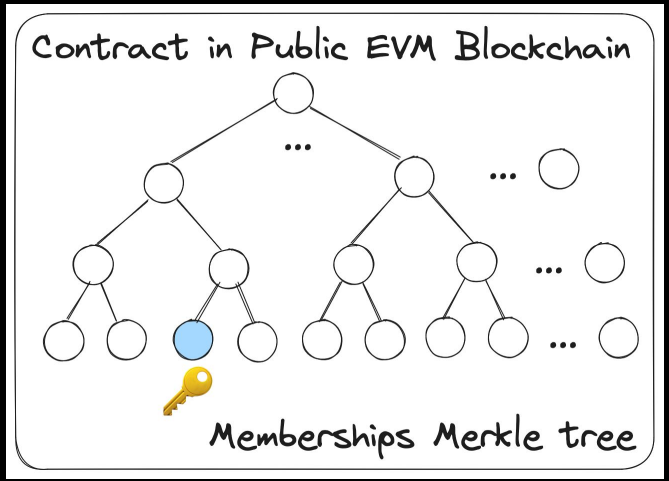
2 Rate limiting I

- Uses Rate Limiting Nullifiers (RLN)
- Rate limits users. Example: 100 messages per hour.
- Does so in a privacy preserving way using zero knowledge proofs.
- Allows to act upon rate exceeded. Eg slash.
- By PSE (Ethereum Foundation)

1. Waku Introduction
–

2 Rate limiting II

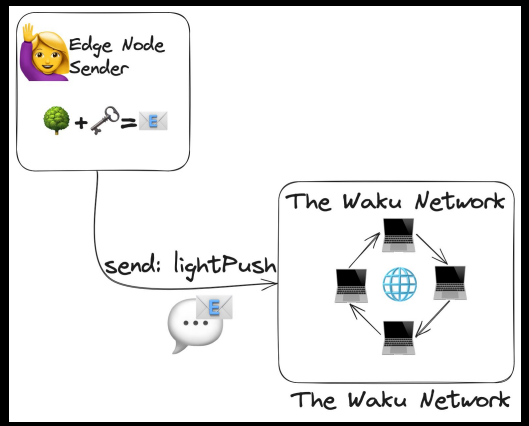
- 🌳 Membership set stored as a Merkle tree onchain.
- 🔑 Anyone can register its public key aka commitment.



1. Waku Introduction
–

2 Rate limiting III

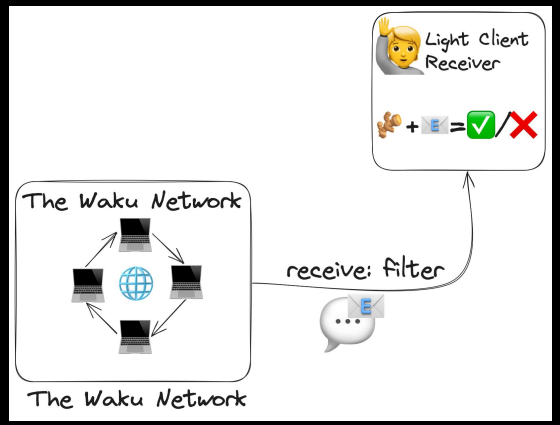
- 🔑 With the private key
- 🌳 And the Merkle proof
- 📧 The user generates a “stamp” (aka zk proof)
- 💬 That attached to the message, it makes it valid in the network



1. Waku Introduction
–

2 Rate limiting IV

- 🫚 With the root anyone can check if the message:
  - ✅ Is valid
  - ❌ Or invalid



3 Offline nodes

- Nodes can go offline. Eg sw update.
- Store protocol allows to fetch past messages.
- Store sync allows to synchronize store messages.
- RBSR based (Range-based set reconciliation)

1. Waku Introduction
–

4 Resource-restricted devices I

- Not all nodes can participate in relaying messages. Eg phone.
- Light protocols:
  - 👉💬🙋‍♂️ Light-push: To send
  - 🙋‍♂️👉💬 Filter: To receive

4 Resource-restricted devices II

- Latest feature:
  - Onchain Merkle trees
  - Reduces friction for edge nodes
  - Can generate proofs without syncing the tree locally
  - Contract provides gas free Merkle proofs/root.
  - With some reasonable gas increase in insertion.
  - RLN 🤝 Light protocols

5 Scalability

- Network splitted in multiple shards.
- 8 for The Waku Network.
- 1 shard = 1 pubsub topic

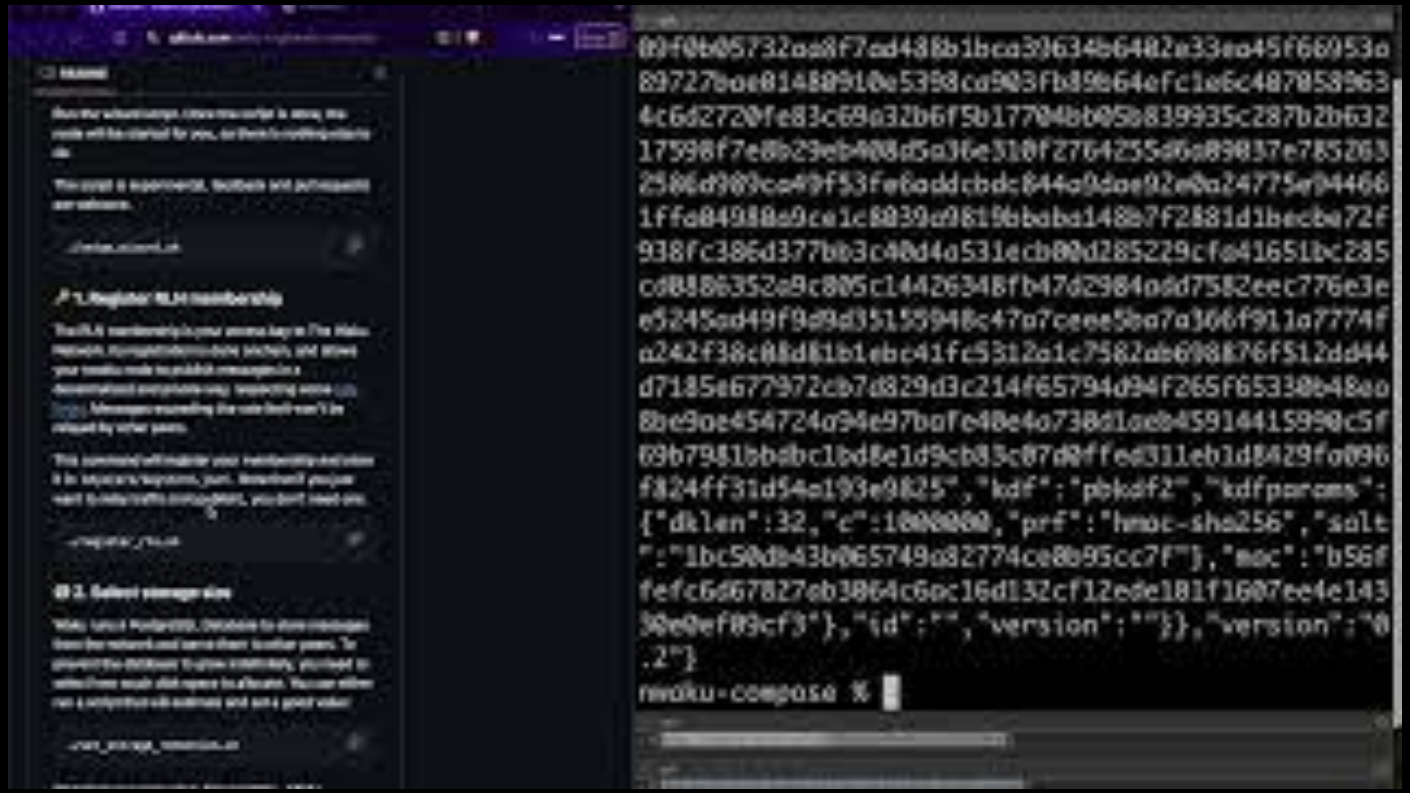
1. Waku Demo

Demo - https://github.com/waku-org/nwaku-compose

1. Waku Demo

–

Demo



https://youtu.be/NSpAtin9O18

1. Waku Demo

–

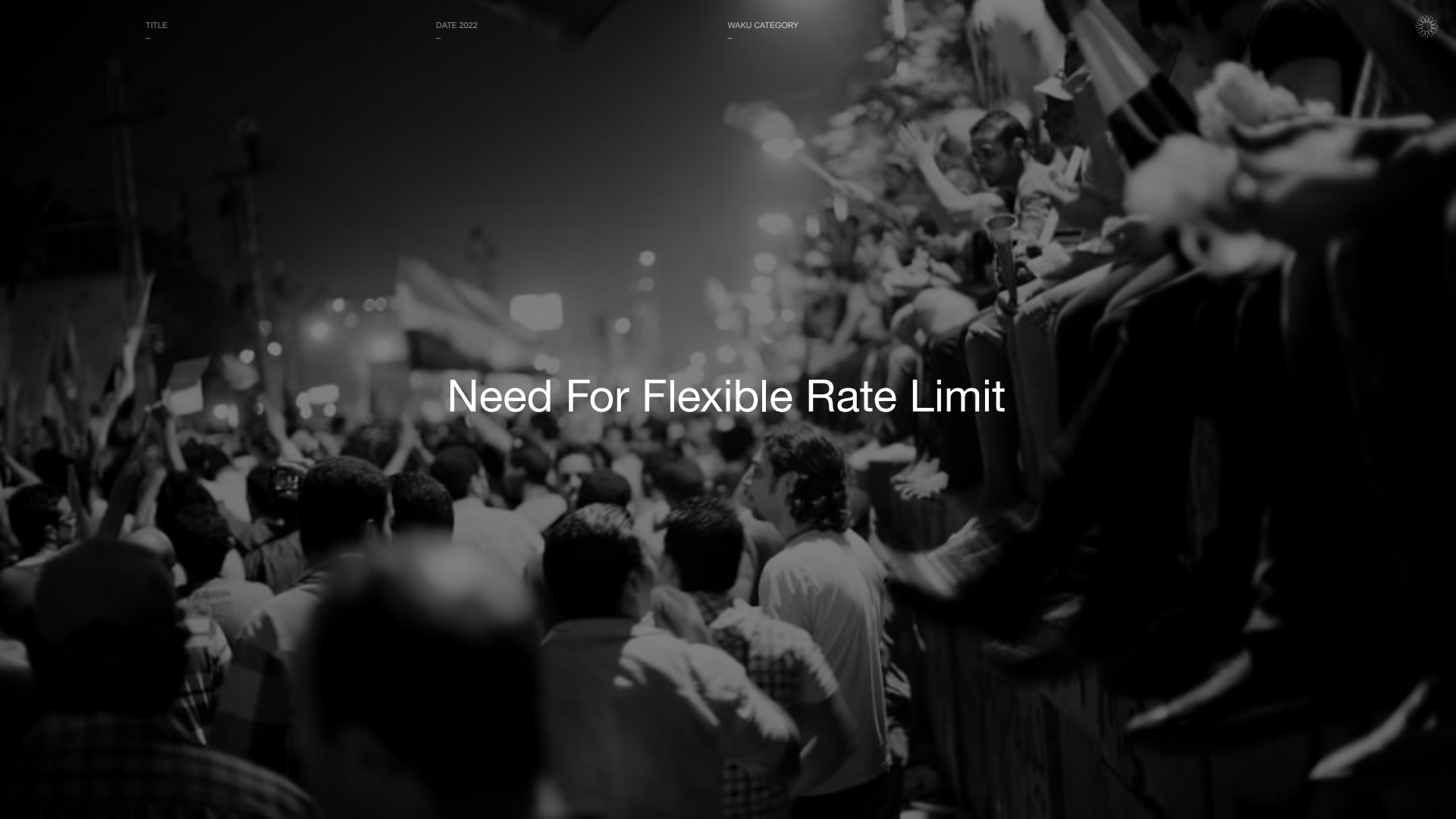
Demo under the hood

- Runs full node
- Relays traffic in the network
- Stores past messages
- With RLN membership registered
- Allowed to use the network up to rate limit
- Messages not linked to any identity nor IP
- Sovereign, no trust required
- Decentralized, no single point of control

TITLE
–

DATE 2022
–

WAKU CATEGORY
–



Need For Flexible Rate Limit

Flexible Rate Limit

–

RLN v1

- 1 message per epoch
- Smallest practical epoch: 1 second
- -> 1 msg per second

5KB msg

1k users

- > ~5MBps steady traffic

Flexible Rate Limit

–

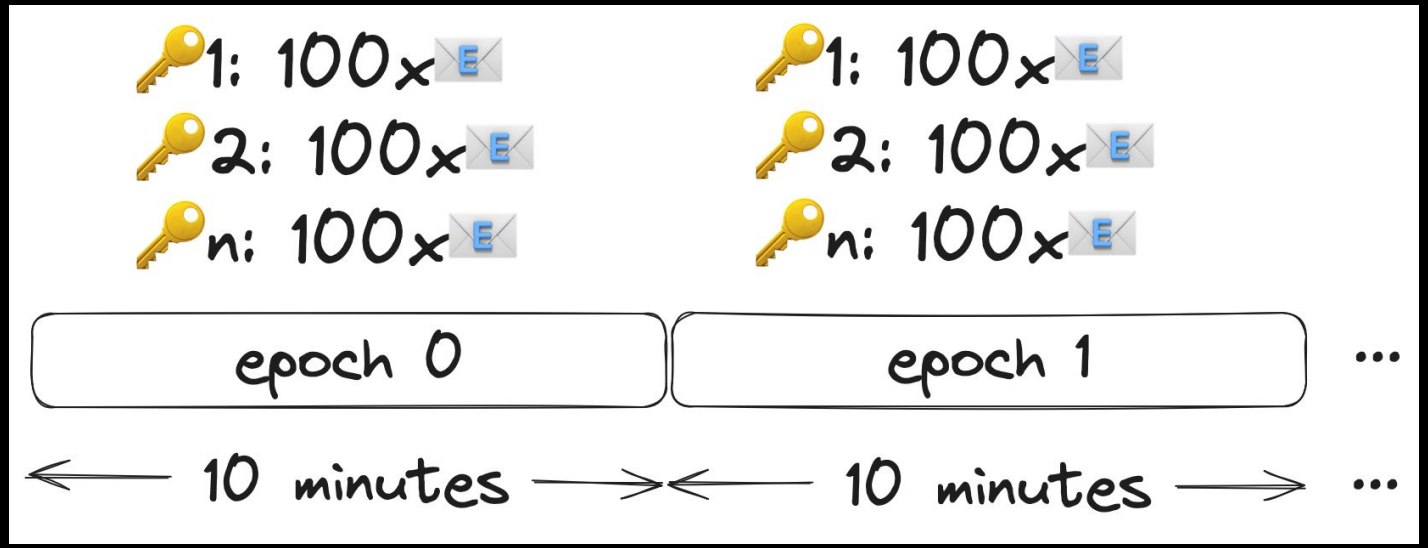
RLN v2

- N messages per epoch
- 20-600 msgs per 10 min
- 160,000 msgs/epoch
- 150KB max message size

More API Token like

Flexible Rate Limit

–



Flexible Rate Limit

–

RLN v2

10 min epoch

- 128B nullifier
- 600 msg -> 75KiB/user
- 732 MiB for 10k users

Spike control

Flexible Rate Limit

–

RLN v2

Averages:

- traffic of 266 msg/s
- Message size 4KB
- 6 is average gossipsub D-out degree.
  -> 6 MBps network

0.75 MBps per shard
-> assumes uniform distribution

Economics

Economics

–

6 months membership

- Followed by 1 month grace period

5c per msg per epoch

- 20 msgs/10min: $1
- 600 msgs/10min: $30

~232k gas

- ~$10 mainnet
- ~70c L2

Economics
–

Membership can be extended during grace period

Deposit can be withdrawn after grace period

Caller can override expired memberships

Economics
–

Future:

Longer membership?

Non-linear pricing
- Bulk discount?

Impact on chat protocol

Economics
–

Future: Free membership?

Counter-productive but somewhat necessary

- Stealth commitments
- Paymaster
- Referral

Questions?

–

Franck
https://x.com/fryorcraken

Alvaro
https://x.com/alrevuelta

https://waku.org
https://github.com/waku-org/specs/