evolving devp2p

Felix Lange (Ethereum Foundation)

Nov 2, 2017

devp2p (2014)

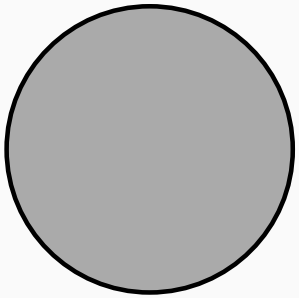
> *libp2p (aka DEVp2p) aims to provide a lightweight abstraction layer that provides these low-level algorithms, protocols and services in a transparent framework without predetermining the eventual transmission-use-cases of the protocols.*
> *– DEVp2p Whitepaper Wiki Page*

- We should probably delete this wiki page ;)

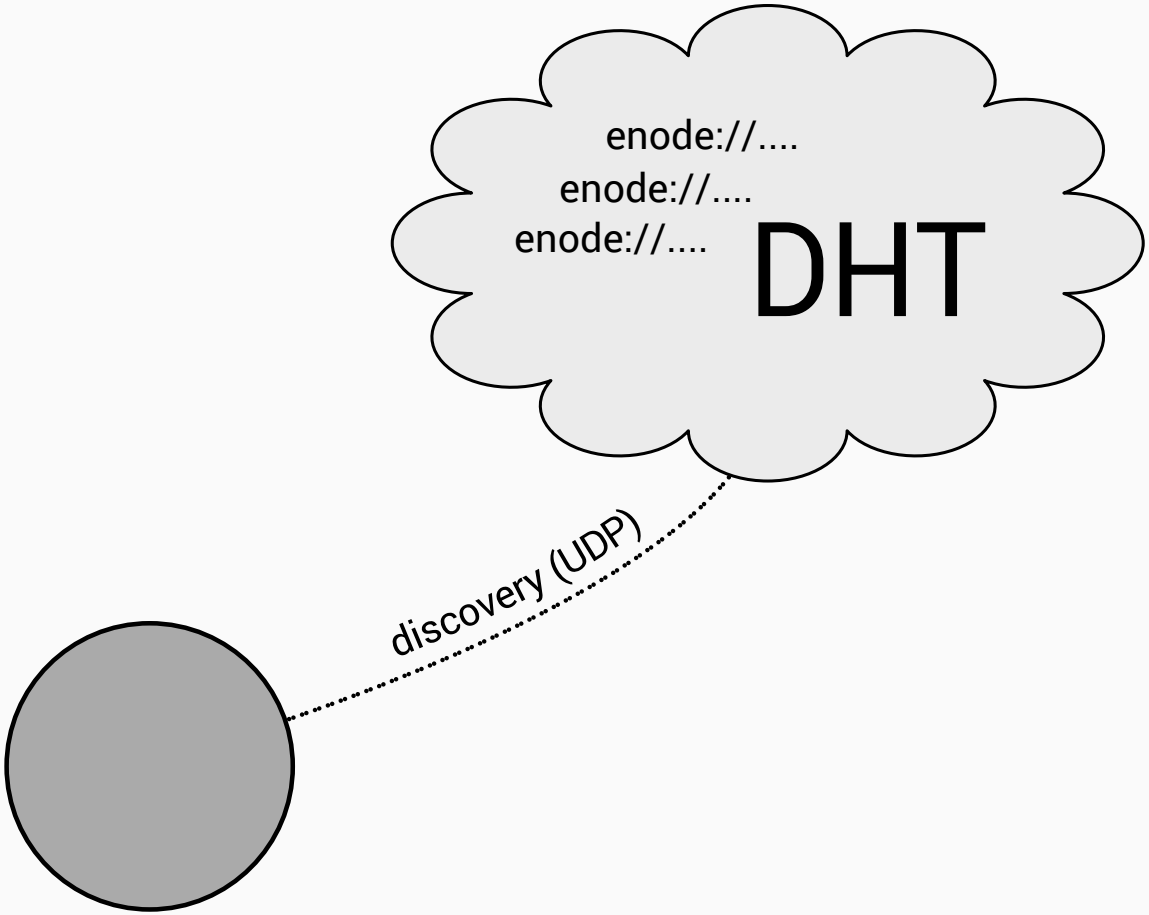
devp2p (2017)

- Part of all known Ethereum implementations
- Very few protocol changes since 2014
- Elements
  - Node Discovery
  - Transport (RLPx)
  - Application Layer (devp2p)

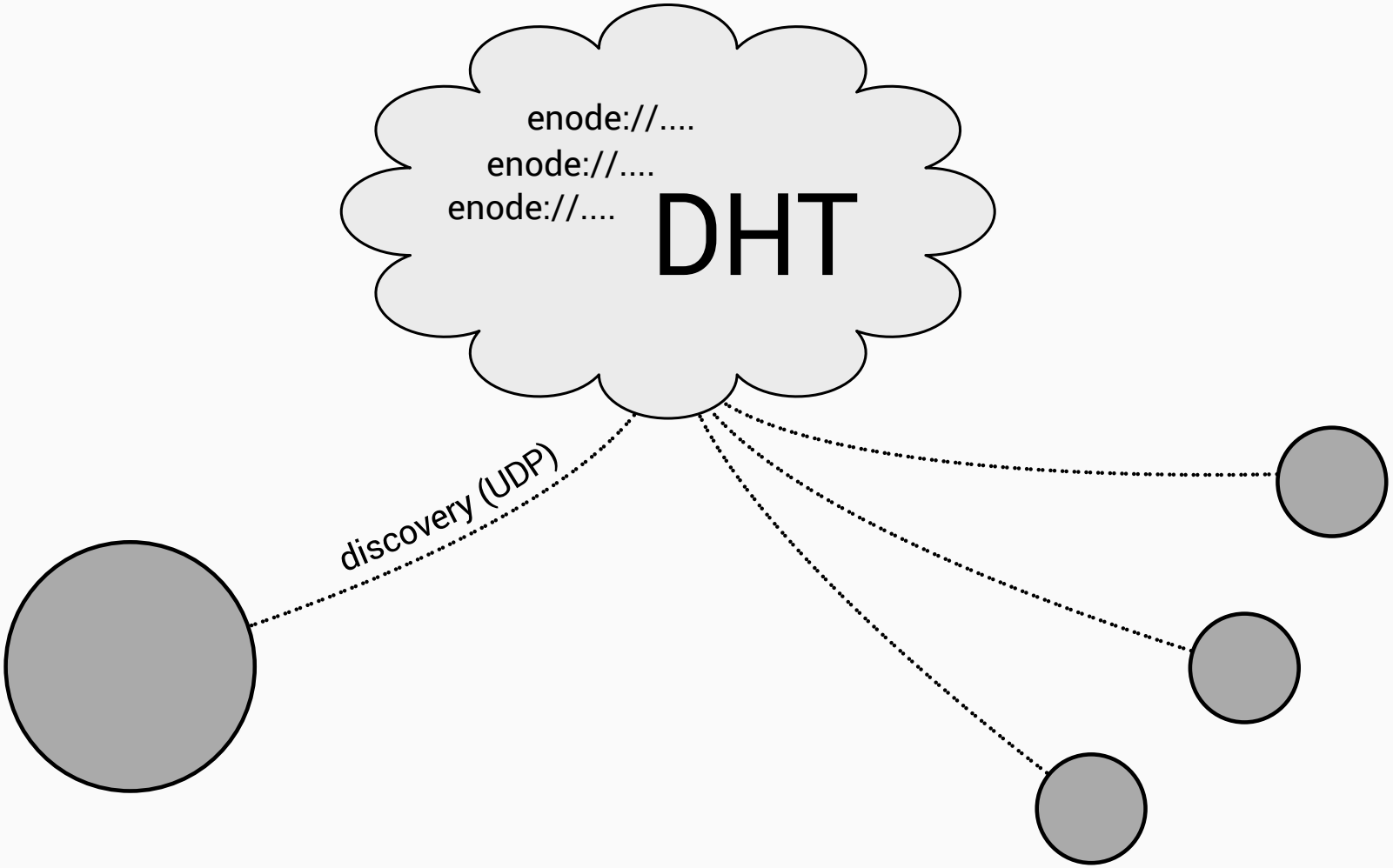
v4: A lonely node



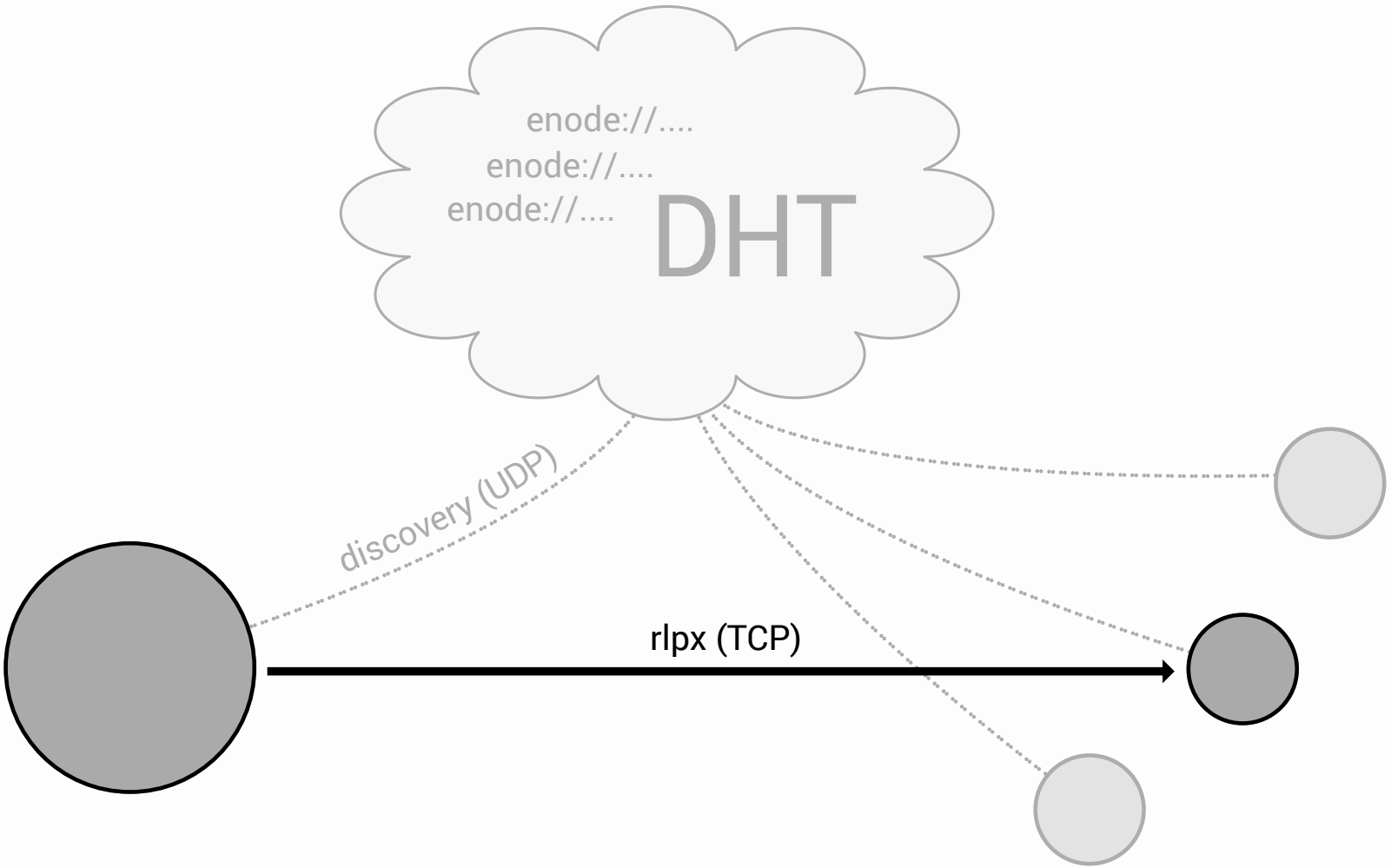
v4: Connecting to the DHT



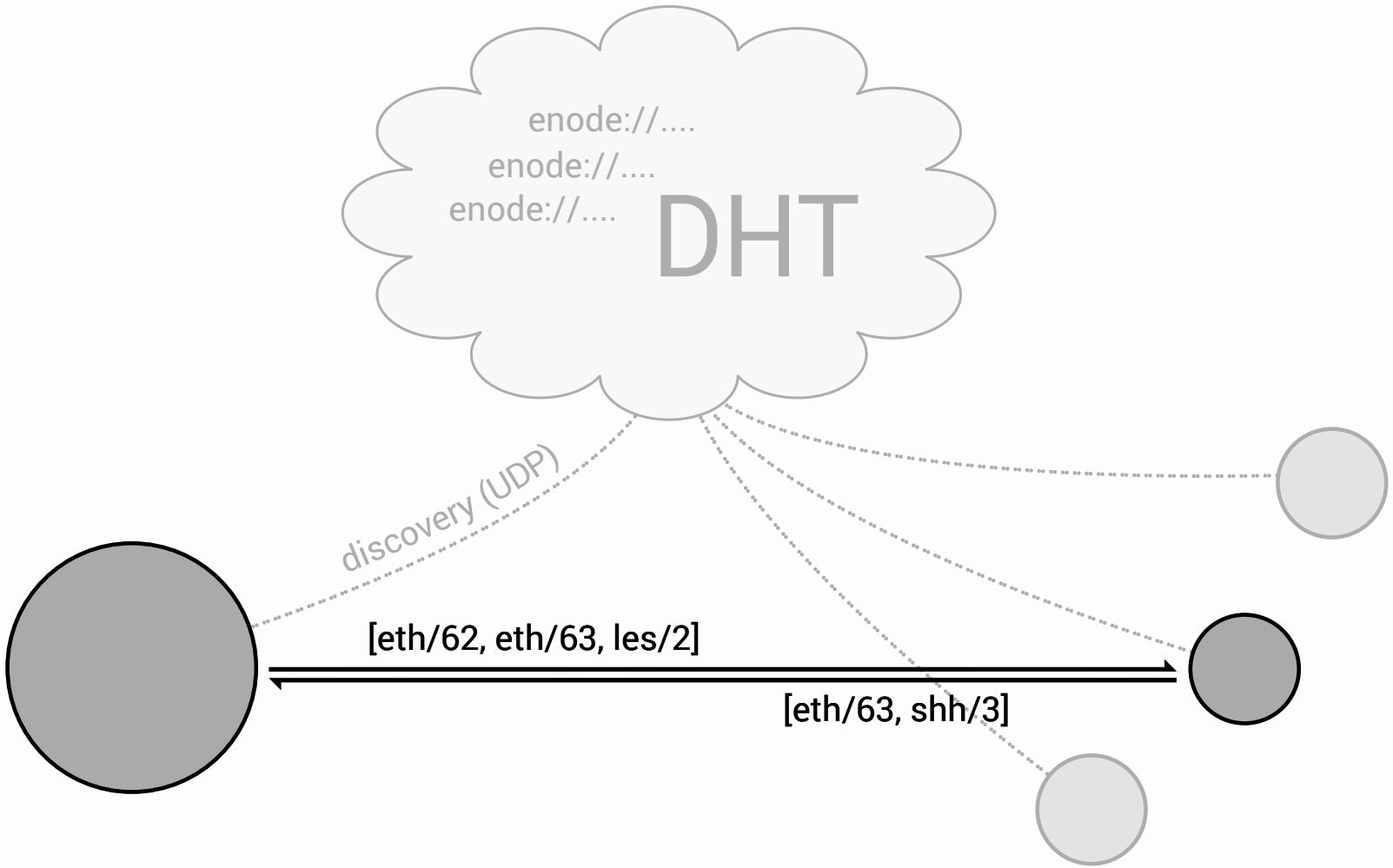
v4: Finding other nodes



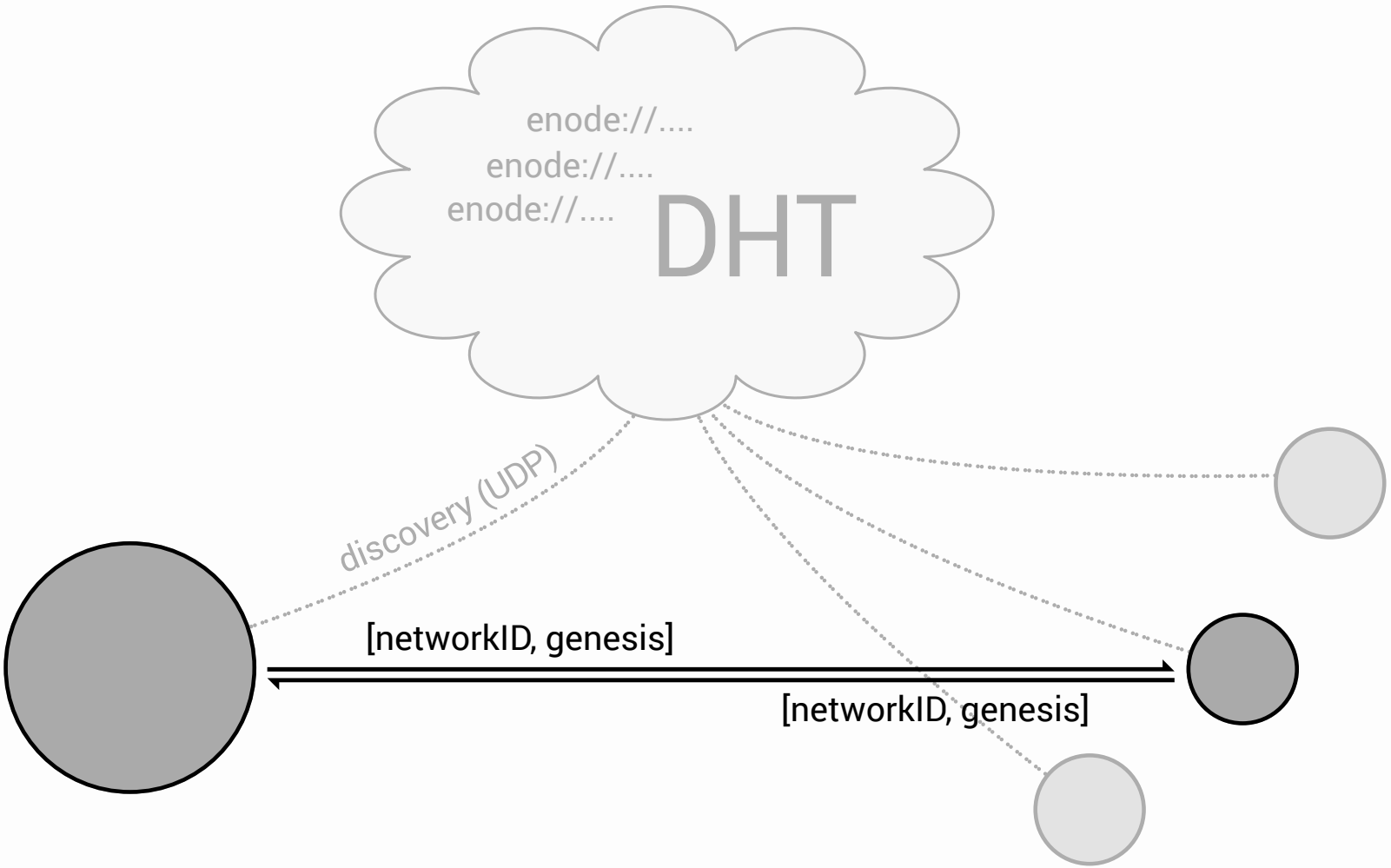
v4: Connecting via TCP



v4: Negotiating devp2p capabilities



v4: Exchanging eth information



Issues with v4

- So many roundtrips!
- Upgrades need tight coordination
  - Everything needs to be backwards-compatible
  - Past upgrades tied to Ethereum mainnet hard forks
- Stuck with RLPx, secp256k1, keccak256

Node Discovery v5

Node Discovery v5

- Finding nodes more efficiently
- Knowing more about those nodes before we connect

ENR

- Ethereum Node Record
- Replaces `enode://...`
- RLP `[sig, seq, key, value, key, value, ...]`
- At most 300 bytes
- Signed (`sig`), Ordered (`seq`)

Transport Agility Through ENR

- `key`, `value` arbitrary
- Node identity, transports encoded in `key`, `value`
- RLPx remains common transport for now
- Sunset RLPx when there is a viable alternative
- We can try ipfs/libp2p transports

Discovery v5 Kademlia Protocol

Similar to v4, but:

- ENR
- Remove dependency on absolute time
- Require endpoint proofs to reduce dead/spam nodes

Topic Advertisement Protocol

- v4 DHT: public key $\rightarrow$ address
- Topic index: topic $\rightarrow$ nodes

Design Constraints

- One DHT for everyone
- Scale to arbitrary number of topic members
- Should deal with spam

Advertisement Inertia

- When advertising a topic, there is an artificial delay
- Combats many attacks, reduces misue
- Use topics for announcing big decisions

Node Discovery v5

- Prototype (without ENR) used by `geth --light`
- EIPs forthcoming
  - ENR
  - Topic Ad Protocol
  - Discovery v5 Wire Protocol
- Nothing set in stone yet, come talk to us!

Thank You