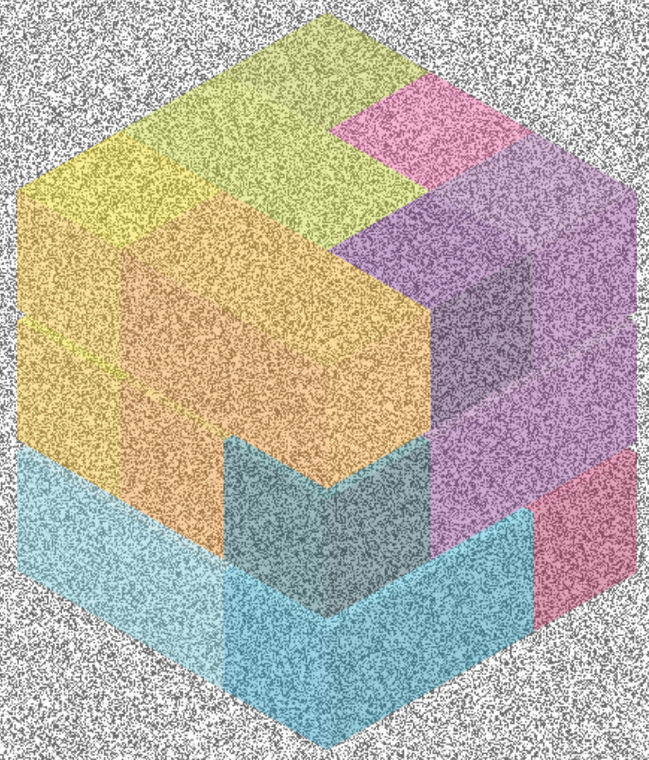


go-libp2p-noise

A new secure transport option for Eth2.0, Polkadot, Cosmos, and web3

ETHBerlin bzwei

Libp2p is a network layer framework that allows you to write decentralized peer-to-peer applications.

ETHBerlin bzwei

Eth2.0
uses libp2p for p2p messaging

IPFS
uses libp2p for p2p messaging

Cosmos
considering libp2p for p2p messaging

Polkadot
uses libp2p for p2p messaging

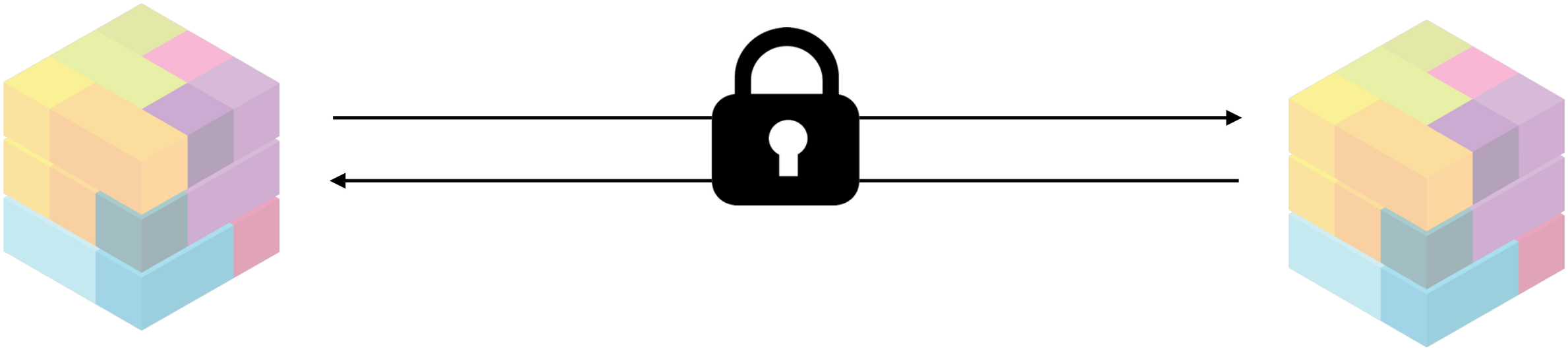
Why implement go-libp2p-noise?

“Ethereum 2.0 has tentatively picked the Noise Protocol Framework to conduct its cryptographic handshakes in mainnet. This decision is reflected in the Ethereum 2.0 networking spec.”

“Not implementing noise-libp2p would be a missed opportunity to improve libp2p's tech stack and grow the libp2p community, and may impact the roadmap for the Ethereum 2.0 mainnet launch.”

-libp2p devgrant brief

peerA



peerB

libp2p peers need a way to securely communicate.

ETHBerlin bzwei

what is noise protocol?

Framework for building security protocols by composing a small set of cryptographic primitives into patterns with verifiable security properties.

```
IK:
<- s
...
-> e, es, s, ss
<- e, ee, se
```

```
IN:
-> e, s
<- e, ee, se
```

```
IX:
-> e, s
<- e, ee, se, s, es
```

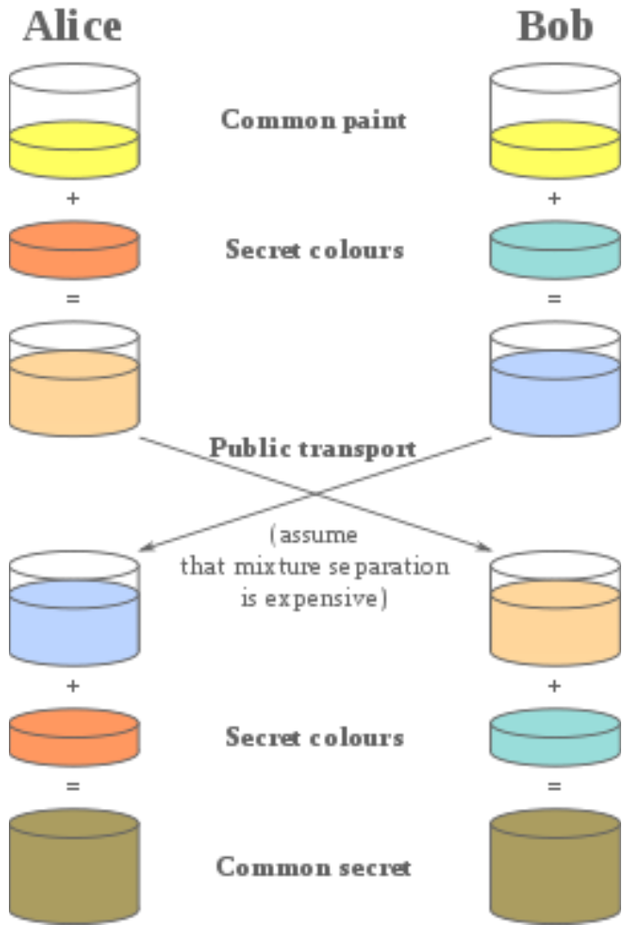
```
K:
-> s
<- s
...
-> e, es, ss
```

```
KK:
-> s
<- s
...
-> e, es, ss
<- e, ee, se
```

```
KN:
-> s
...
-> e
<- e, ee, se
```

ETHBerlin zwei

The noise protocol uses Diffie-Hellman operations to provide secure symmetric key encryption of messages.

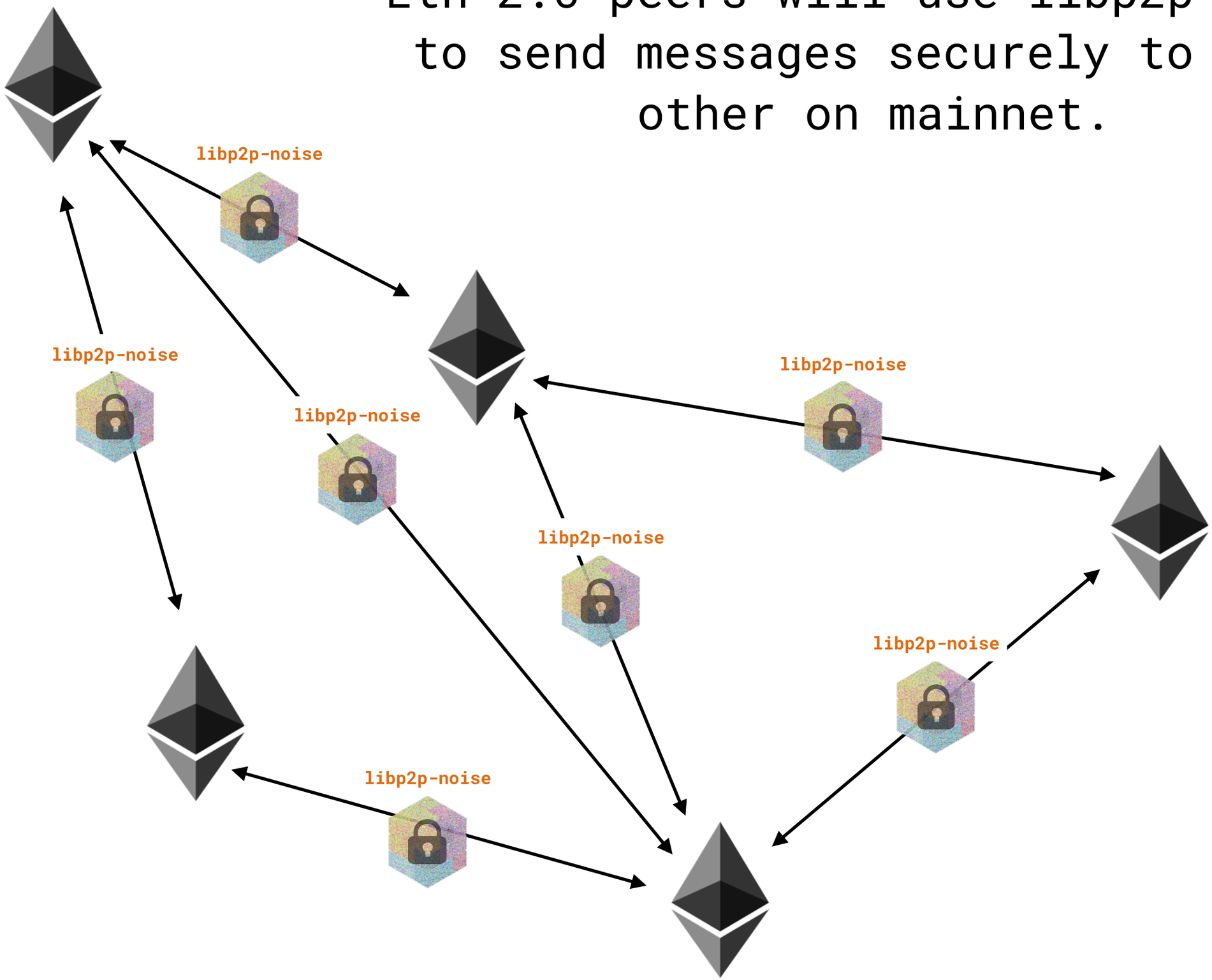


Paint color analogy for Diffie Hellman key exchange (wikipedia)

Why Noise Protocol?

- ✓ lightweight (lighter than TLS 1.3)
- ✓ well-vetted, soundly designed
- ✓ formally verified

Eth 2.0 peers will use libp2p-noise to send messages securely to each other on mainnet.



ETHBerlin bzwei