

Kairos and libp2p

The immutable edge Kubernetes



Kairos



Summary

- Introduction
- Kairos and (lib)p2p
 - Design
 - Self-coordination
 - Network isolation
- Demo

Introduction

Kubernetes Immutable Edge Infrastructure

Introduction - Kubernetes to the Edge

- What's the challenge?
 - Boost large scale Kubernetes adoption at the Edge
 - Zero touch configuration, lifecycle completely managed
 - Zero network configuration
 - Self-coordination

Kairos

- Enabling Kubernetes workload at the Edge with an easy but resilient approach
- Immutable OS
- Meta Distribution (openSUSE, Ubuntu, Alpine, ...)
- Highly customizable
- Container based
- Self-coordinated, p2p

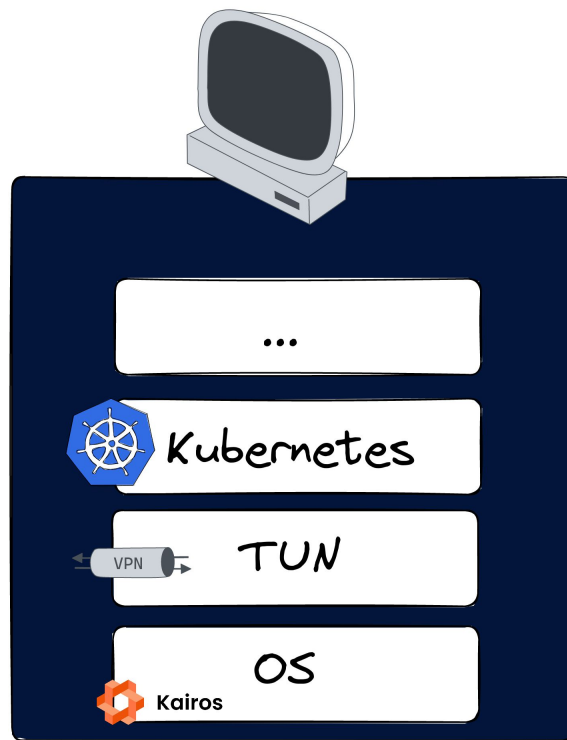


Kairos and P2P

Kubernetes Immutable Edge Infrastructure

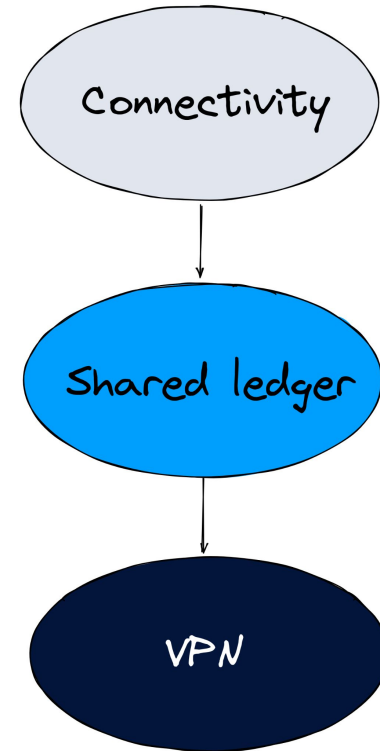
Design - Internal components

- Kairos as Base OS
- VPN tunnels created with EdgeVPN/libp2p
- Kubernetes (K3s)
- Any application that needs to access to nodes of the cluster is routed through VPN



Design - Decentralization

- Libp2p used as transport layer
- Shared ledger is accessible to all the nodes of the network
- Optionally a VPN is established between the nodes
- The shared ledger is used as coordination layer between the nodes
- A shared token between the nodes is used to encrypt symmetrically packets, and as seed for rendezvous points



Design - Network token

```
$ docker run -ti --rm quay.io/mudler/edgevpn -b -g | base64 -d
```

```
otp:
```

```
  dht:
```

```
    interval: 9000
```

```
    key: ObHRseYtDxZszBTJYZIE4Mxi0z10oC9hpkeXG8MJQ4W
```

```
    length: 43
```

```
  crypto:
```

```
    interval: 9000
```

```
    key: FIiphshxLcgBbcrW8NzY1is2YD17xNDkUWAzMM1mv4R
```

```
    length: 43
```

```
room: CI1ln2ok5BQai04ocSPS9ozdW18sF0023ep3rWyrjOk
```

```
rendezvous: HZ22jkZP61msORtHqXTBx9UCINdg0MKbfxJzd0Trq1F
```

```
mdns: NutZDGo1BD1D8TVGoL7mDap6xkprjwbsiFUPqEhga8Q
```

```
max_message_size: 20971520
```

OTP
Rendezvous
Seed



Coordination Mechanism

DHT and mDNS peer discovery

Peers discover autonomously via mDNS and DHT with dynamic rendezvous OTP keys from the token.

A bootstrap node list can be used for **airgap**.

Gossip network

A Gossip network is formed between nodes, where the - **AES GCM** symmetrically encrypted (**OTP** rotated) - blockchain state is being shared.

Nodes communicate over an e2e ECDSA asymmetrically encrypted channel.

At this point API to interact with the ledger is available in each node.

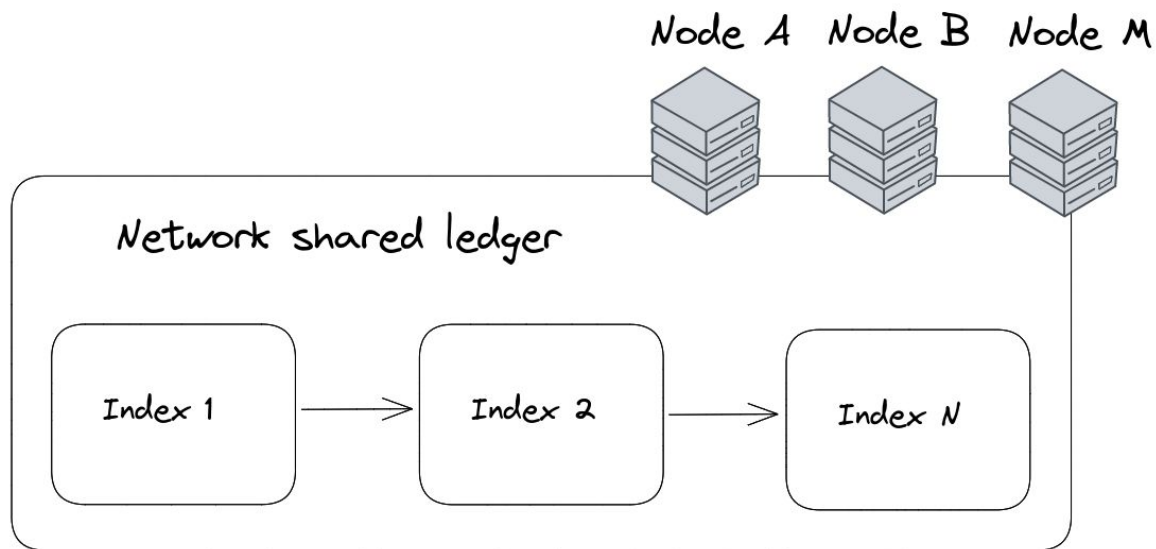
Full Connectivity (opt)

When the blockchain state is synchronized, hosts can talk each other via p2p, with hops if required (nodes behind NAT) over an e2e encrypted traffic (ECDSA).

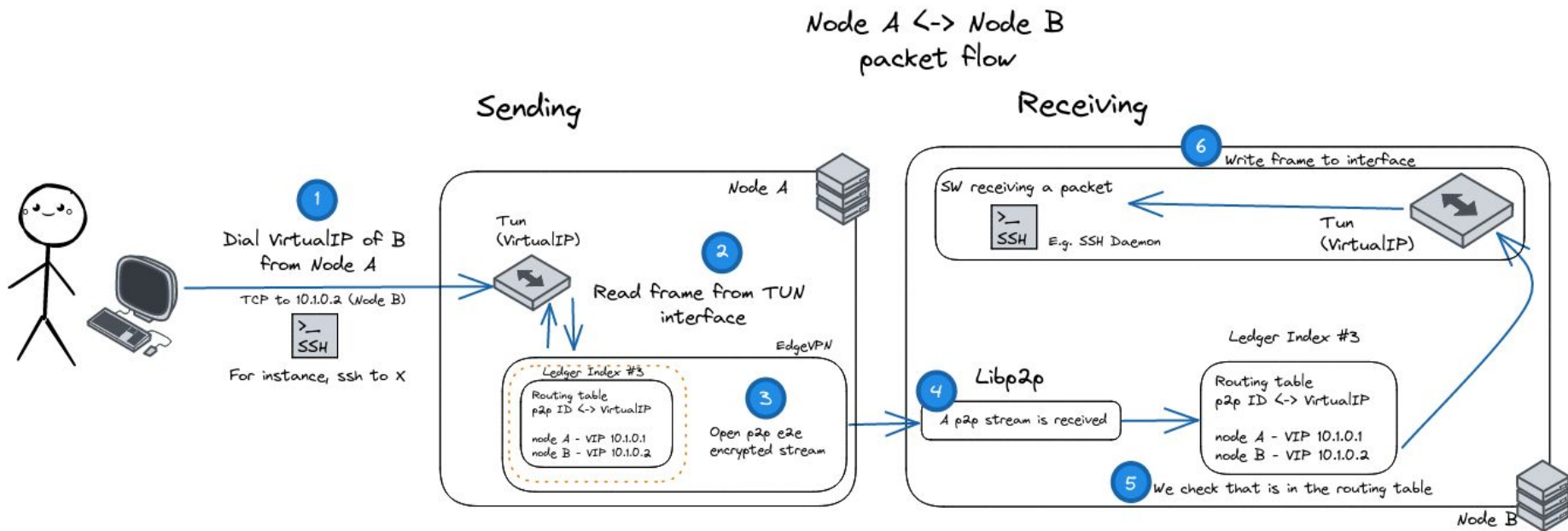
The traffic is routed to a tun/tap device.

Network Shared Ledger

- AES Encryption
- OTP rotated key



Packet flow



Compared to alternatives

	Wireguard	OpenVPN	EdgeVPN
Memory Space	Kernel-module	Userspace	Userspace
Protocol	UDP	UDP, TCP	TCP, UDP/quick, UDP, ws, everything supported by libp2p
P2P	Yes	Yes	Yes
Fully meshed	No	No	Yes
Management Server (SPOF)	Yes	Yes	No
Self-coordinated	No	No	Yes

Implications for Kubernetes

K8s Without VPN	K8s With VPN
<p>Nodes needs to have static IP assigned by DHCP or manually configured(can be automated)</p>	<p>Automatically coordinated Virtual IPs for nodes. Or manually assign them</p> <p>No additional network configuration required. Etcd knows about VirtualIPs, not real IPs.</p>
<p>Traffic is unencrypted between the nodes</p>	<p>There is an additional e2e encrypted network layer (additional latency, 0-1ms in LAN)</p>
<p>Cluster IPs, and networking is handled by CNIs natively (no layers)</p>	<p>Kubernetes Network services will have Cluster IPs sitting below the VPN. Every internal kubernetes communication goes through VPN.</p>

Usage in Kairos

```
#cloud-config

hostname: kairoslab-{{ trunc 4 .MachineID }}
users:
- ...

p2p:

  disable_dht: true # set to true if LAN

  network_token: ""
```

Demo

Bootstrapping a Multi-node, decentralized Kubernetes cluster with Kairos and [AuroraBoot](#)

1. Run [AuroraBoot](#)
2. Start VMs/Machines...
3. Enjoy!



Want to know more or try it out?

Learn more about Kairos at <https://kairos.io/>

Check out the code at
<https://github.com/kairos-io/kairos>

Download a release
<https://github.com/kairos-io/kairos/releases>

Matrix: [#kairos-io:matrix.org](https://matrix.org/#kairos-io:matrix.org)

GitHub Discussions: <https://github.com/kairos-io/kairos/discussions>

Office Hours (Wednesdays 17:30-18:00 CET): <https://meet.google.com/aus-mhta-azb>



Thanks!

