Blockchains for Decentralized PKI on IoT Devices

Diode CTO Dominic Letz
https://diode.io/
Taipei Ethereum Meetup, March 2019

Blockchain + IoT ??

Diode

PKI - The system that protects the Internet & IIoT is **fundamentally** broken

Is here to replace it

On April 8th, 2010 China Telecom hijacked 15% of the Internet traffic for 18 minutes, this was an early experiment of a reroute-and-open attack against BGP and PKI two fundamental Internet Protocols.

Since 2015 Internet Traffic is being hijacked regularly by groups from Russia, Iran, China.

And since 2018 by private unidentified groups.

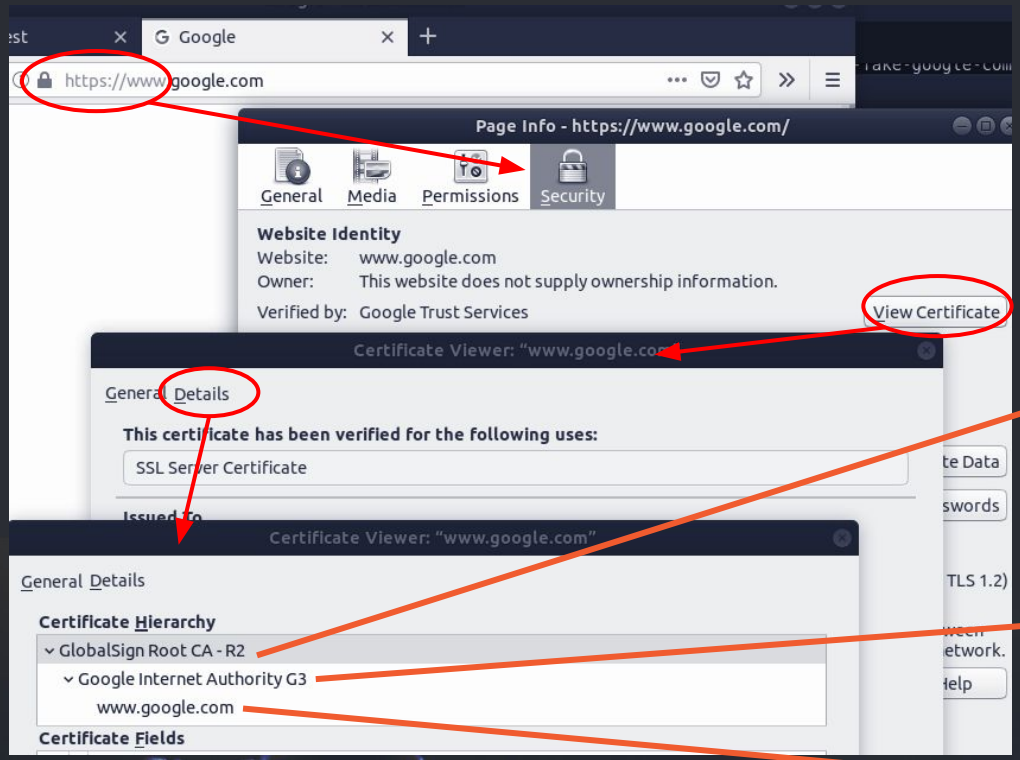
China Telecom's Internet Traffic Misdirection in 2017

My traffic is encrypted! So they can't read it.

My traffic is encrypted! So they can't read it.

RIGHT?

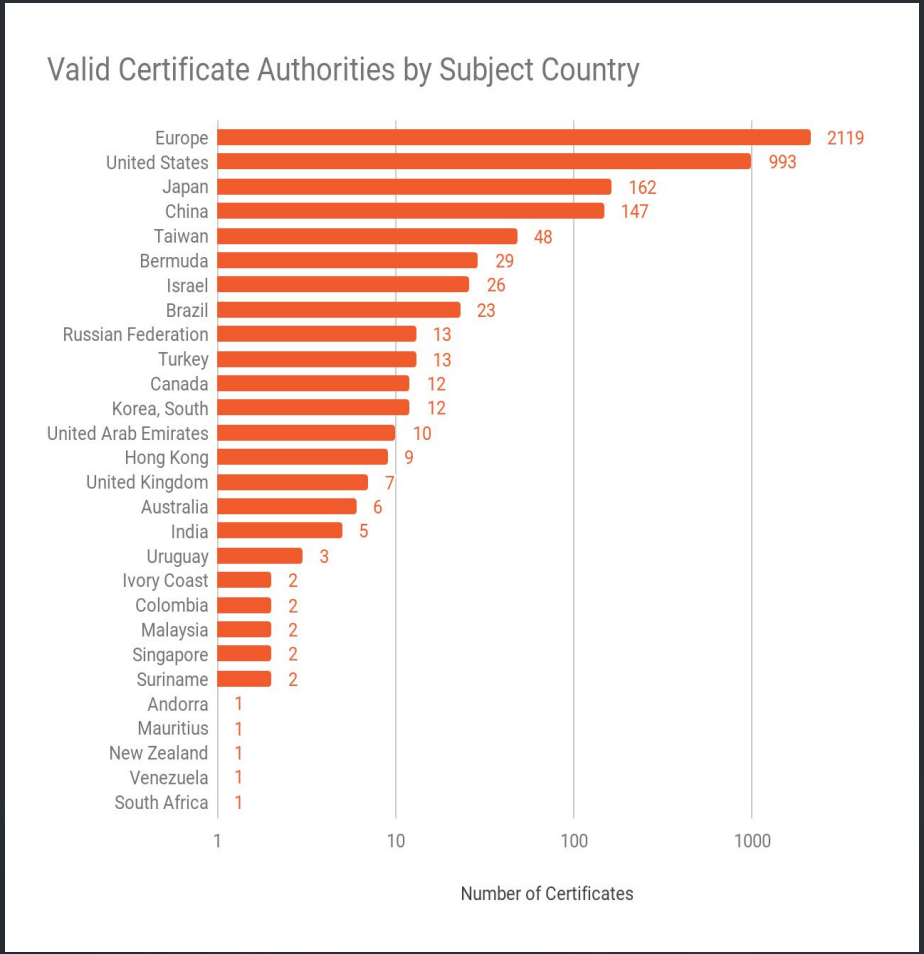
WRONG! - Let's talk about PKI



- Pre-Installed in your Browser / OS
- Intermediate
- Entity

3,675 Intermediates

- Each intermediate can create certificates for *__all__* domains.
- Everyone has a root key.
- Each country not on the list wants to get one.



Safe or not Safe?

GRC's | Security Cer

Secure | https://revoked.grc.com

Security Certificate

Revocation Awareness

If you can see this (and apparently you can
are using a **revocation UNaware** web bro

TLS security certificate for this special websi
tely revoked. Since you **are** seeing this page
web browser is allowing a site with a **known inv**
to display its pages. This is likely not the behavior yo

Here's what we know:

Problem loading page - Mozilla Firefox

Problem loading page

https://revoked.grc.com

Secure Connection Failed

An error occurred during a connection to revoked.grc.com. Peer's Certificate has be
SEC_ERROR_REVOKED_CERTIFICATE

- The page you are trying to view cannot be shown becau ity of th verified.
- Please contact the website owners to inform them of t

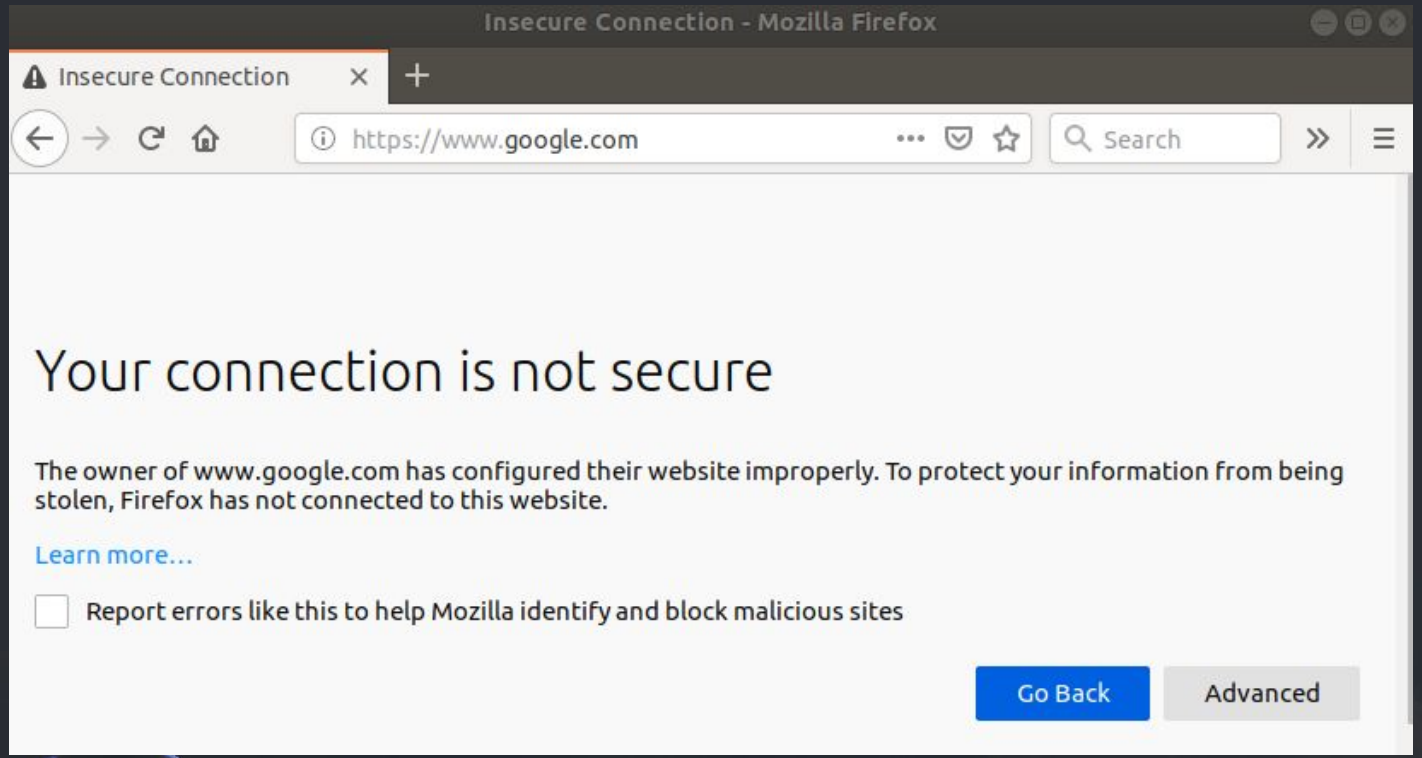
Learn more...

Report errors like this to help Mozilla identify and block malicious sites

功課: Try yourself https://revoked.grc.com

Diode

Time?



功課: Set your clock to 2020 and try browsing the web.

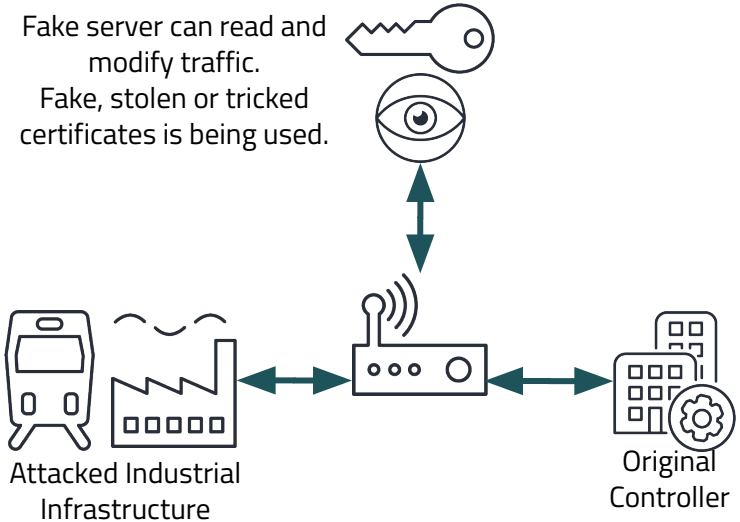
1

reroute

- February 2016 and **for about 6 months**, routes from Canada to Korean government sites were hijacked by **China**
- April 2017: **Russian** company Rostelecom. The hijacked prefixes belonged to financial institutions (most notably MasterCard and Visa), other telecom companies, and a variety of other organizations.
- April 2018: Roughly 1300 IP addresses within Amazon Web Services space, dedicated to Amazon Route 53, were hijacked by eNet (**or a customer thereof**), an ISP in **Columbus, Ohio**.
- July 2018: **Iran** Telecommunication Company originated 10 prefixes of Telegram Messenger.
- November 2018: US-based **China** Telecom site originated Google addresses.

2

open



- **Fake** March 2015 **Egypt-based** MCS Holdings, an intermediate certificate authority that operates under the **China Internet Network Information Center** (CNNIC) created fake certificates
- **Stolen** June 2015 Hackers of **unknown origin** infect Kaspersky Labs using a stolen Foxconn root certificate
- **Fake** September 2015 Symantec has fired an undisclosed number of employees after they were caught issuing unauthorized cryptographic certificates
- **Trick** October 22, 2017: Hackers of **unknown origin** take control of **Brazilian banks** DNS server and trick a CA into issuing a valid certificate to them.
- **Fake** 2017: **Chinese** WoSign & StarCom are banned from Firefox&Chrome after being found to have created invalid certificates.

Diode by ENOSITE

Diode

Solution

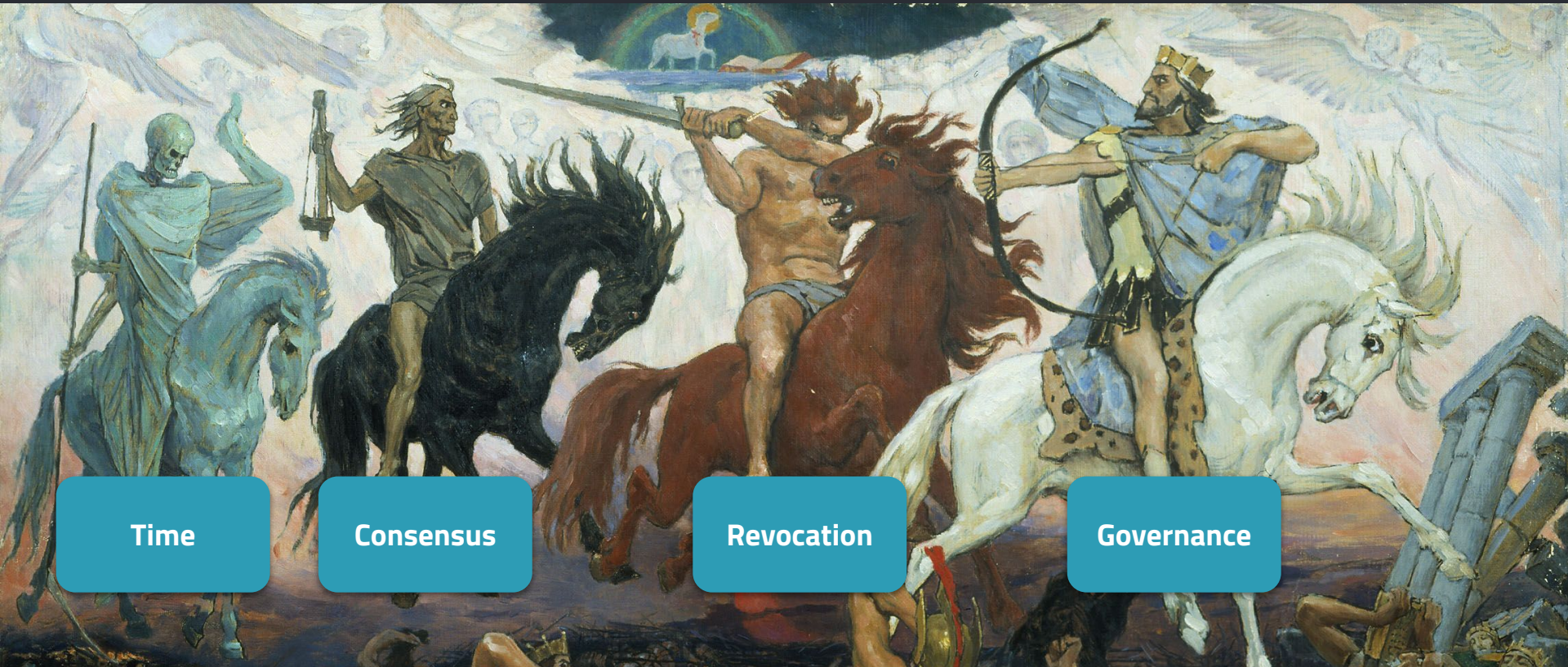
blockchain based key infrastructure

Industrial IoT

Everything will be connected,
let's ensure it is secure!

Diode

The Four Horsemen of the PKI Apocalypse



Time and PKI certificates are in **cyclic dependency** stolen, revoked, expired?

Time

N many certificates for the same identity?

Consensus

CRL & OCSP lists are outdated, and often not even implemented on IoT devices.

Revocation

Who gets the keys for all doors?
gov is hard: money, countries, politics

Governance

Time

Time and current state are be resolved trustless from the blockchain

Diode

Consensus

There is **one agreed owner** per identity

Revocation

Revocations happen **in-chain**, are part of the core protocol

Governance

No "global keys" anymore. Governance can be decided per fleet in smart contracts

Step #1: Replace PKI

Step #2: Decentralize IoT

Step #3: World Peace

Step #1: Replace Internet PKI

Traditional PKI

```
int main() {

    IP address = dns_lookup("time.google.com");

    Date timestamp = ntp_lookup(IP);

    address = dns_lookup("plant-control.com");

    Connection conn = ssl_connect_with_pki(
        address, "plant-control.com", timestamp
    );

    ...
}
```

unsafe lookup

insecure protocol

unsafe lookup #2

validating using manipulated date,
wrong ips,
no revocation checking,

how & when update roots?

Blockchain Based

```
int main() {

    Diode io = connect_blockchain();
    Date timestamp = io.latest_block;

    char* FLEET = "0xdb0d6541b738c3f71b3a360b5bdaf5";
    IP address = lookup_map(io, FLEET, 0, "server_ip");
    char* signature = lookup_map(io, FLEET, 0, "signature");

    Connection conn = ssl_connect_with_signature(
        address, signature
    );

    ...
}
```

securely connecting to the blockchain

getting secure timestamp

fetching contract state & merkle proofing

Diode

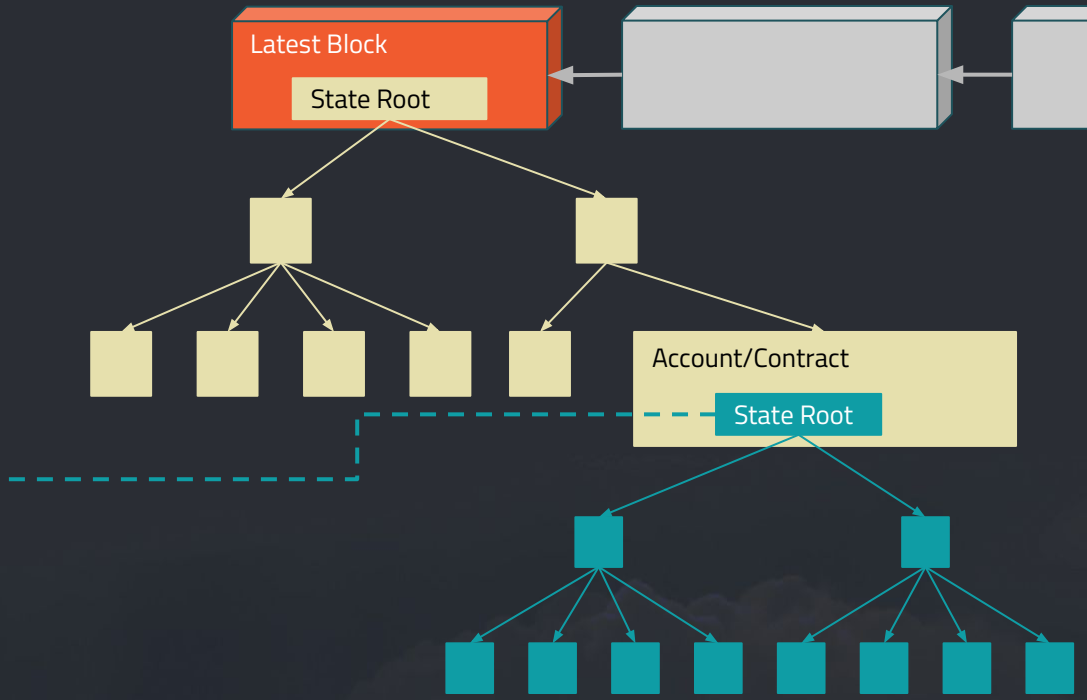
Step #1: Replace Internet PKI

```
char* FLEET = "0xdb0d6541b738c3f71b3a360b5bdaf5" ;
```

```
pragma solidity ^0.4.0;

contract Fleet {
   mapping (bytes32 => bytes32) public env;

   function setServer(bytes32 serverIP,
bytes32 fingerprint) public {
       env["server_ip"] = serverIP;
       env["signature"] = fingerprint;
   }
}
```

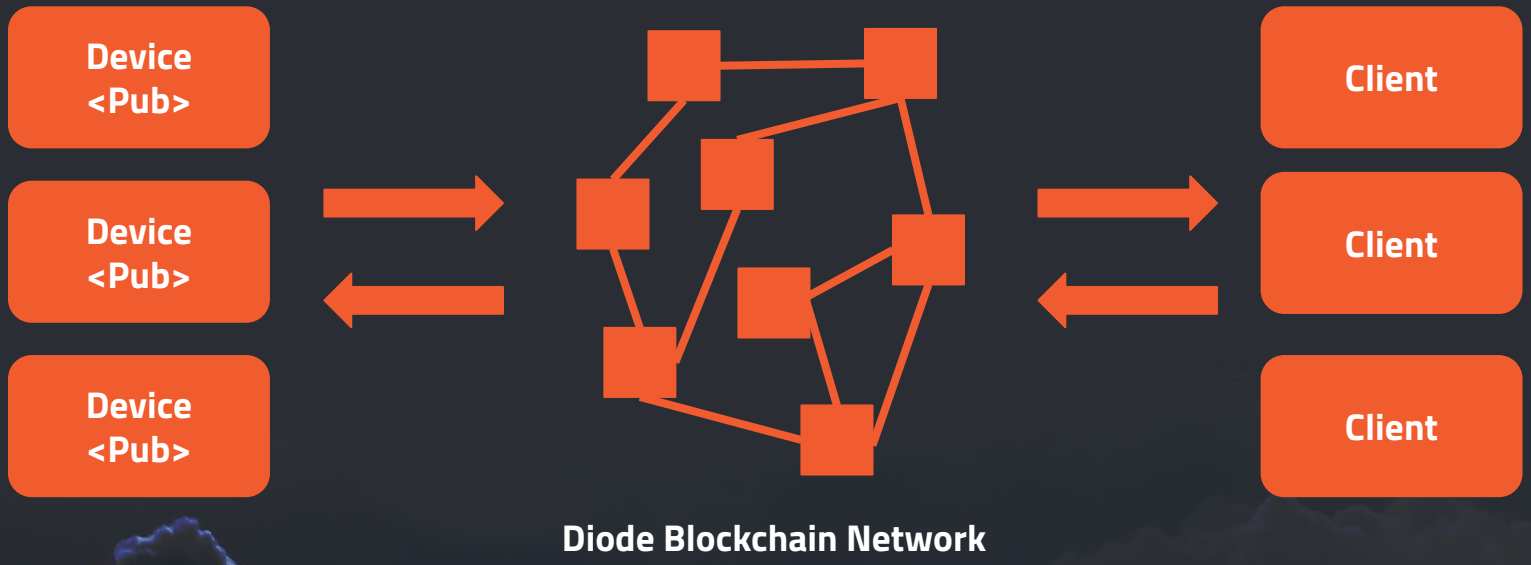


Step #1: Replace Internet PKI

In PKI there are currently 3,675 trusted certificate authorities. A **single point of failure** can be used to open any encrypted communication

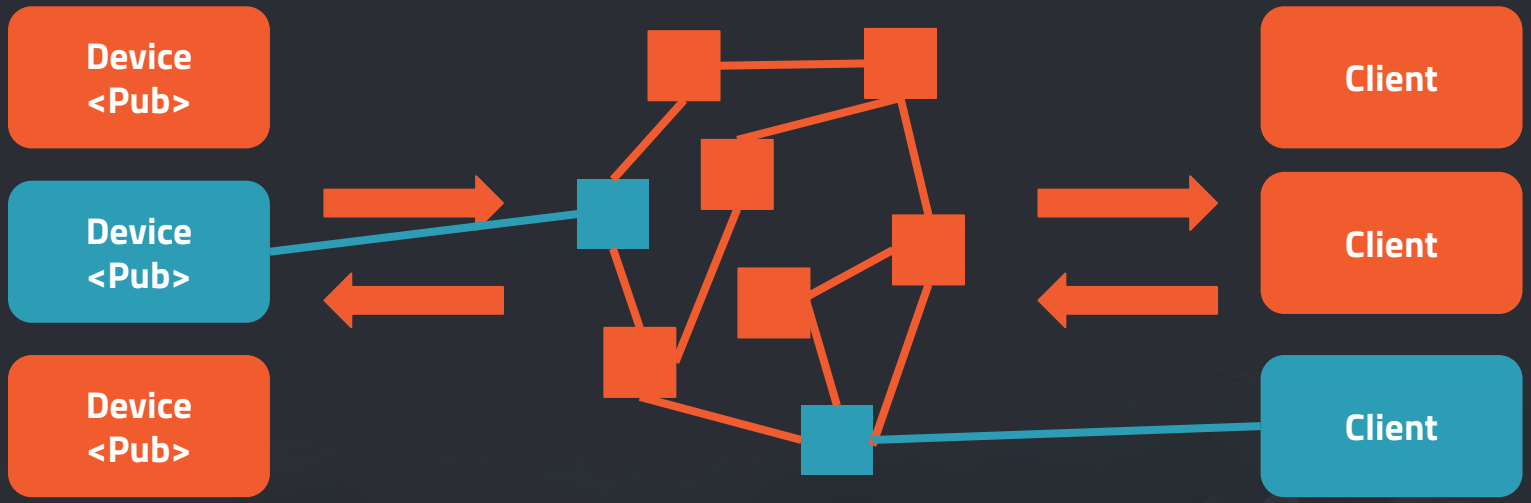
In contrast, because Diode is a blockchain based network it requires an attacker to compromise **51% percent of all peers** to break

Step #2: Decentralized IoT



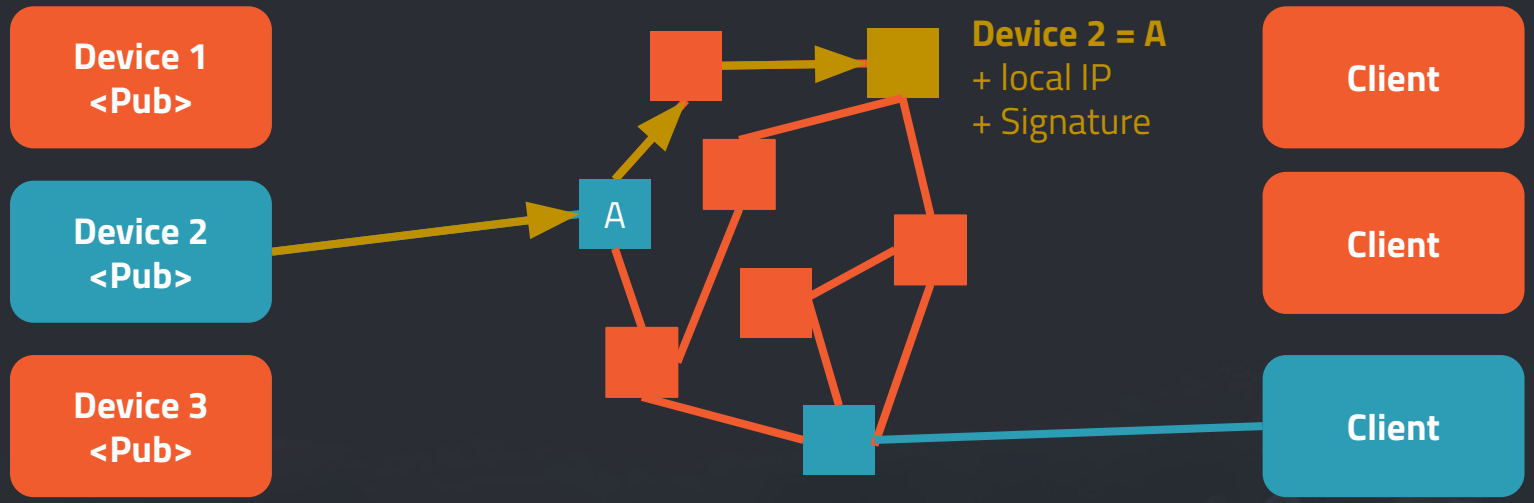
Step #2: Decentralized IoT

Device & Client Connect to the **NEAREST** node



Step #2: Decentralized IoT

1. Store device location

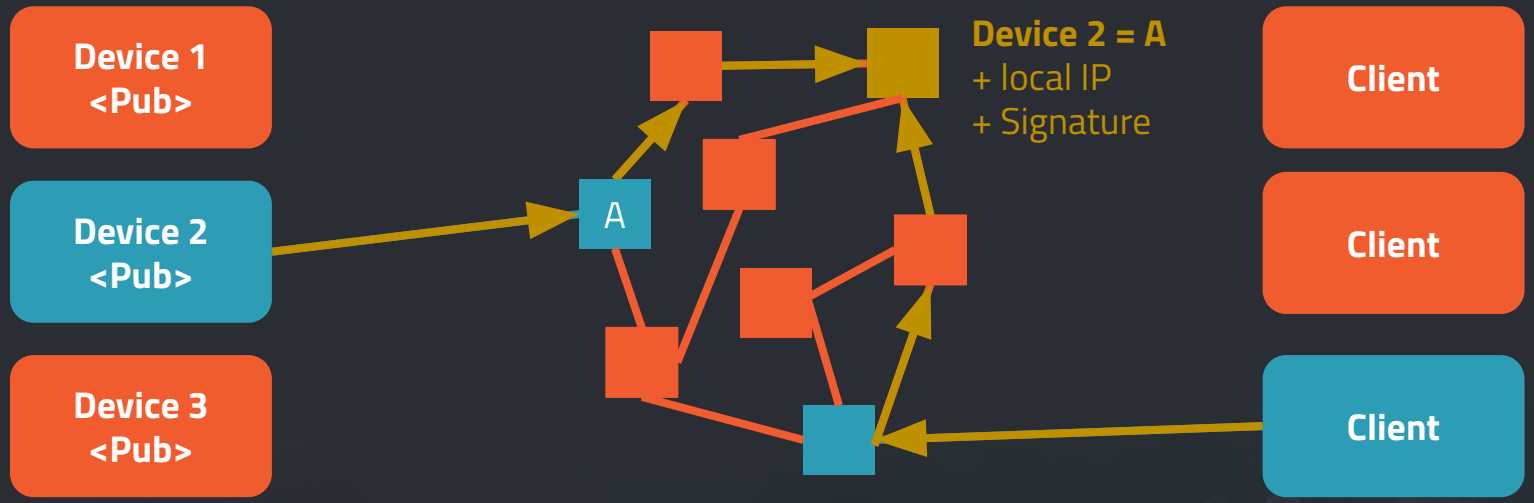


Kademlia p2p Key-Value Network
(like Ethereum / BitTorrent)

Diode

Step #2: Decentralized IoT

2. Find the device location

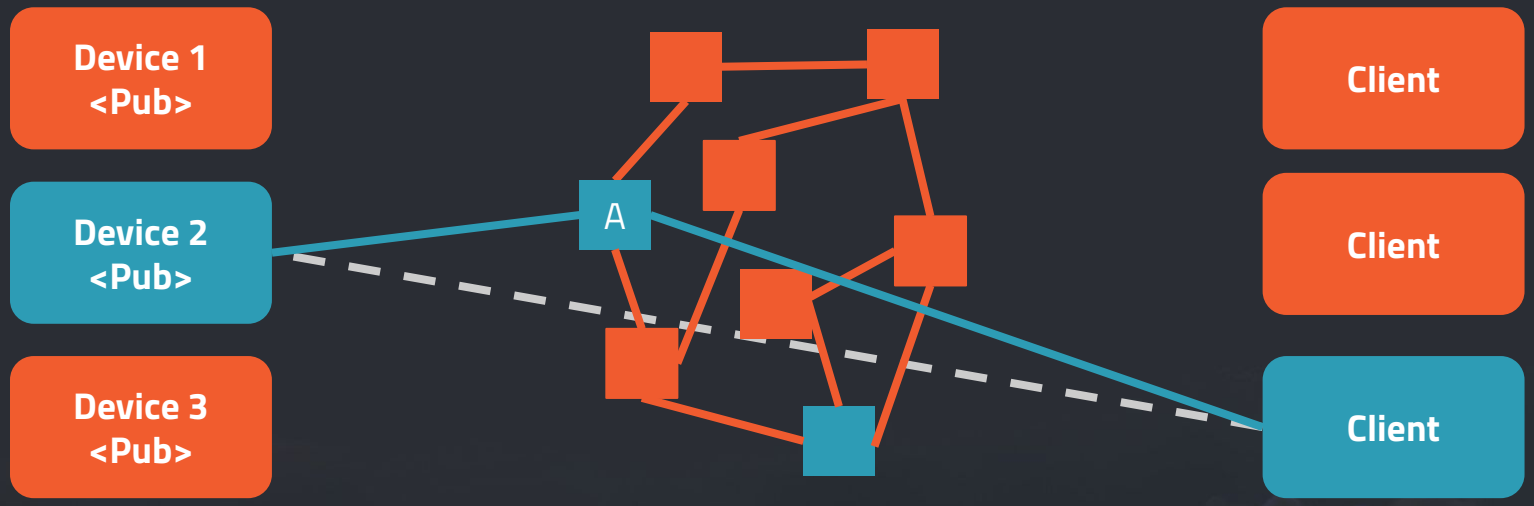


Kademlia p2p Key-Value Network
(like Ethereum / BitTorrent)

Diode

Step #2: Decentralized IoT

3. Connect to device



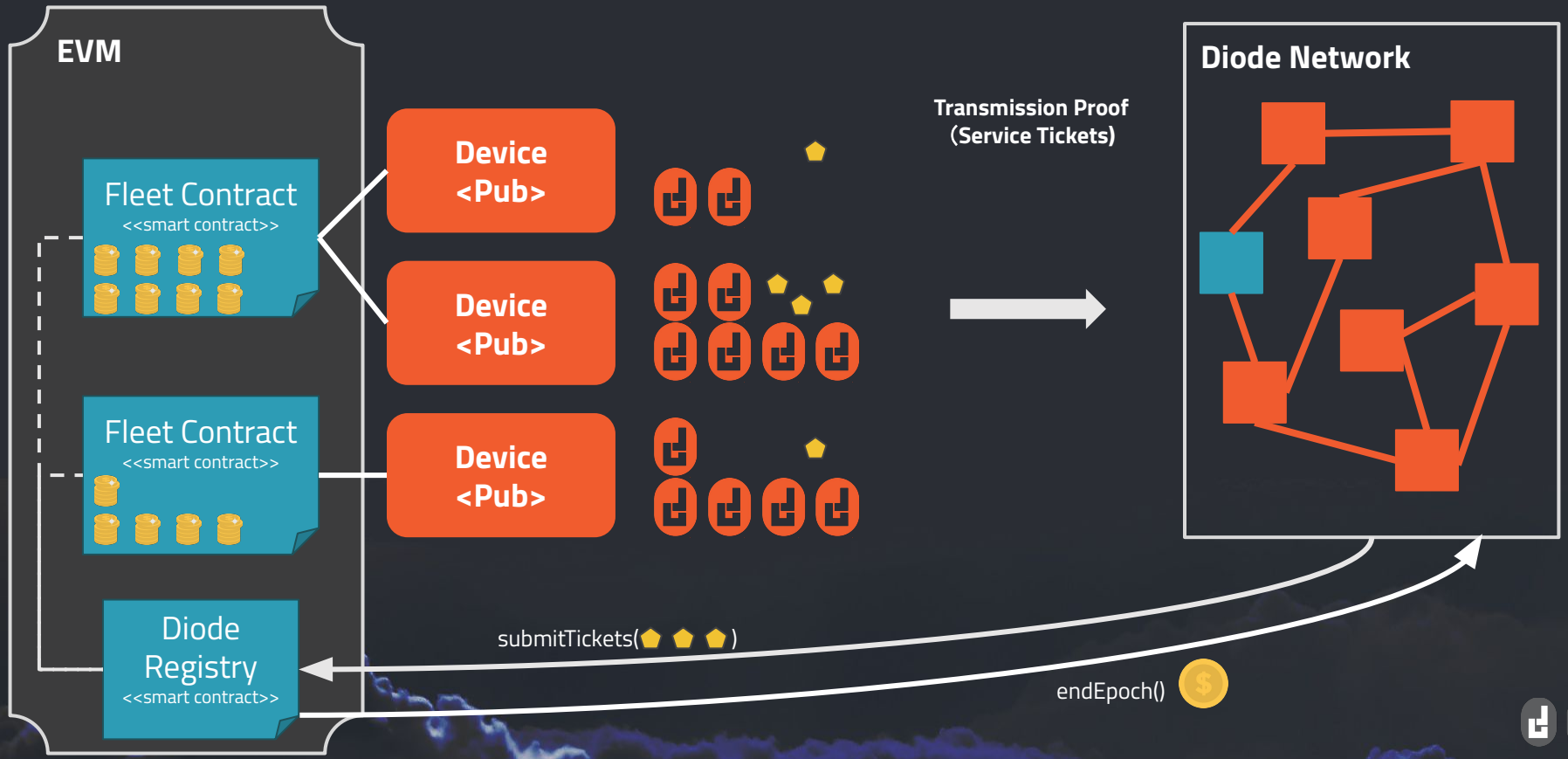
Direct Connection is Possible

otherwise proxy connection

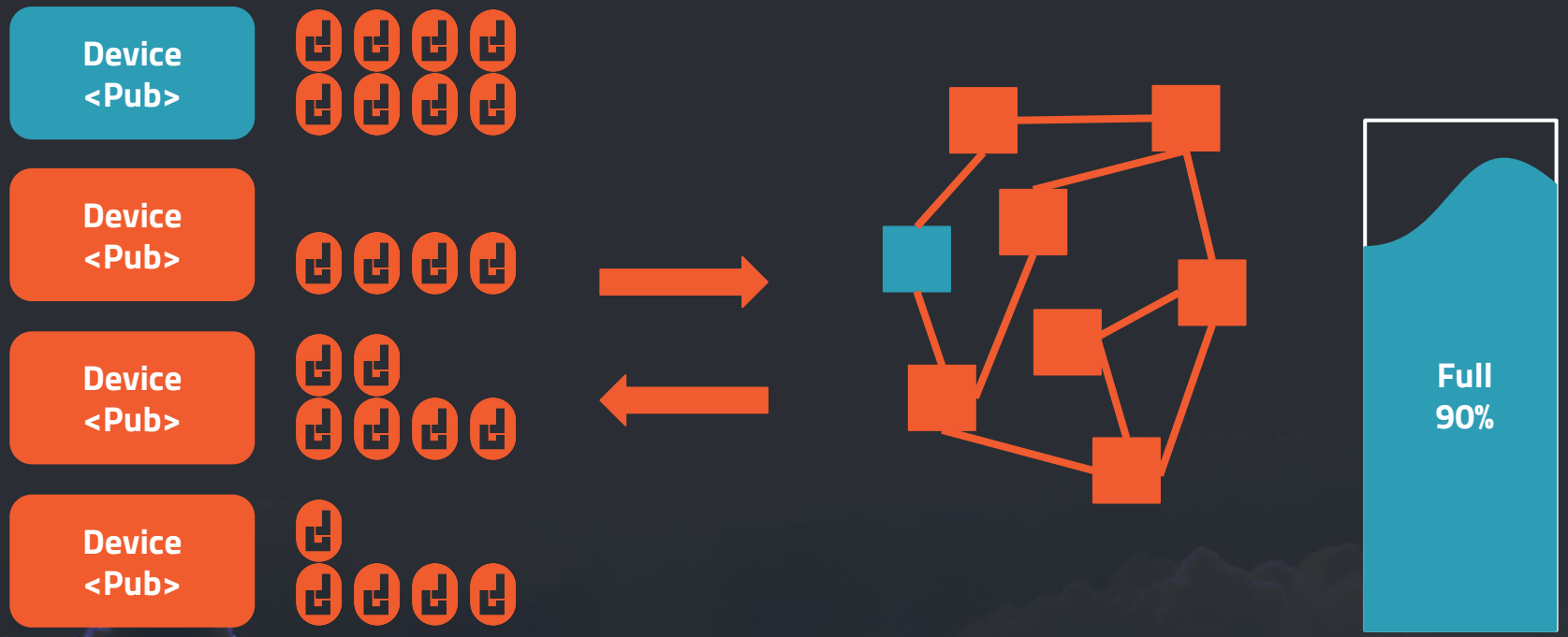
Diode

Miner Incentives
and
Tickets ≠ Transactions

How does a miner work?

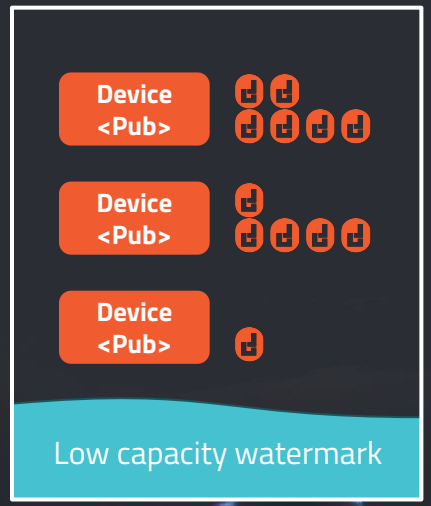


How does a miner work?

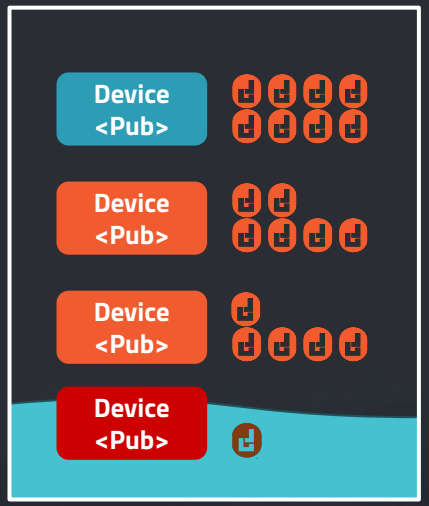


Miners select devices

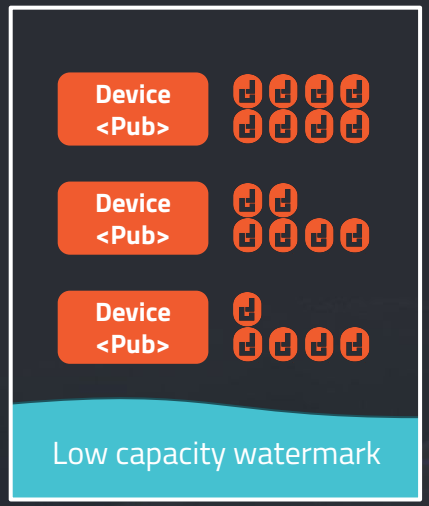
1. New device connects

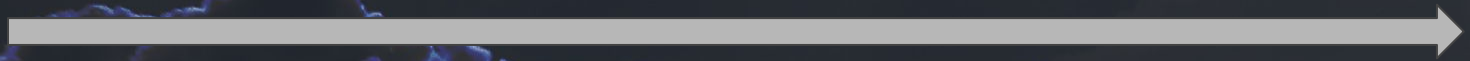


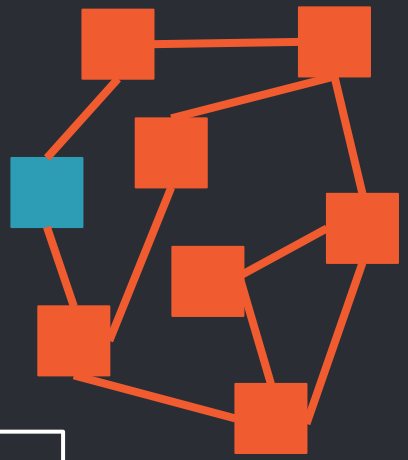
2. Server at capacity, cheap device removed



3. Miner optimizes revenue







Diode

Layer 2 Scaling Solution

Millions of Tickets

25 Transactions/s

Diode

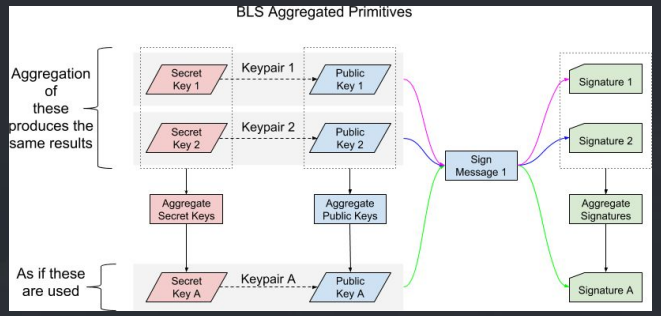
Ticket Aggregation #1

- For each Device/Server combination only the most recent ticket need to be kept. With the highest counter.
  => ~1 Ticket per Epoch and Device
- BLS Ticket signatures can be aggregated.

Epoch	Device	Node	Types	Counters	Signature (BLS)
2 byte	8 byte	4 byte	1 byte	12 byte	96 byte

- 1,836 gas (68 * 27) => ~4,000 Tickets per Block
- 172,800 Blocks per Epoch * 4,000 Tickets per Block

- ~691,200,000 Monthly Active Devices



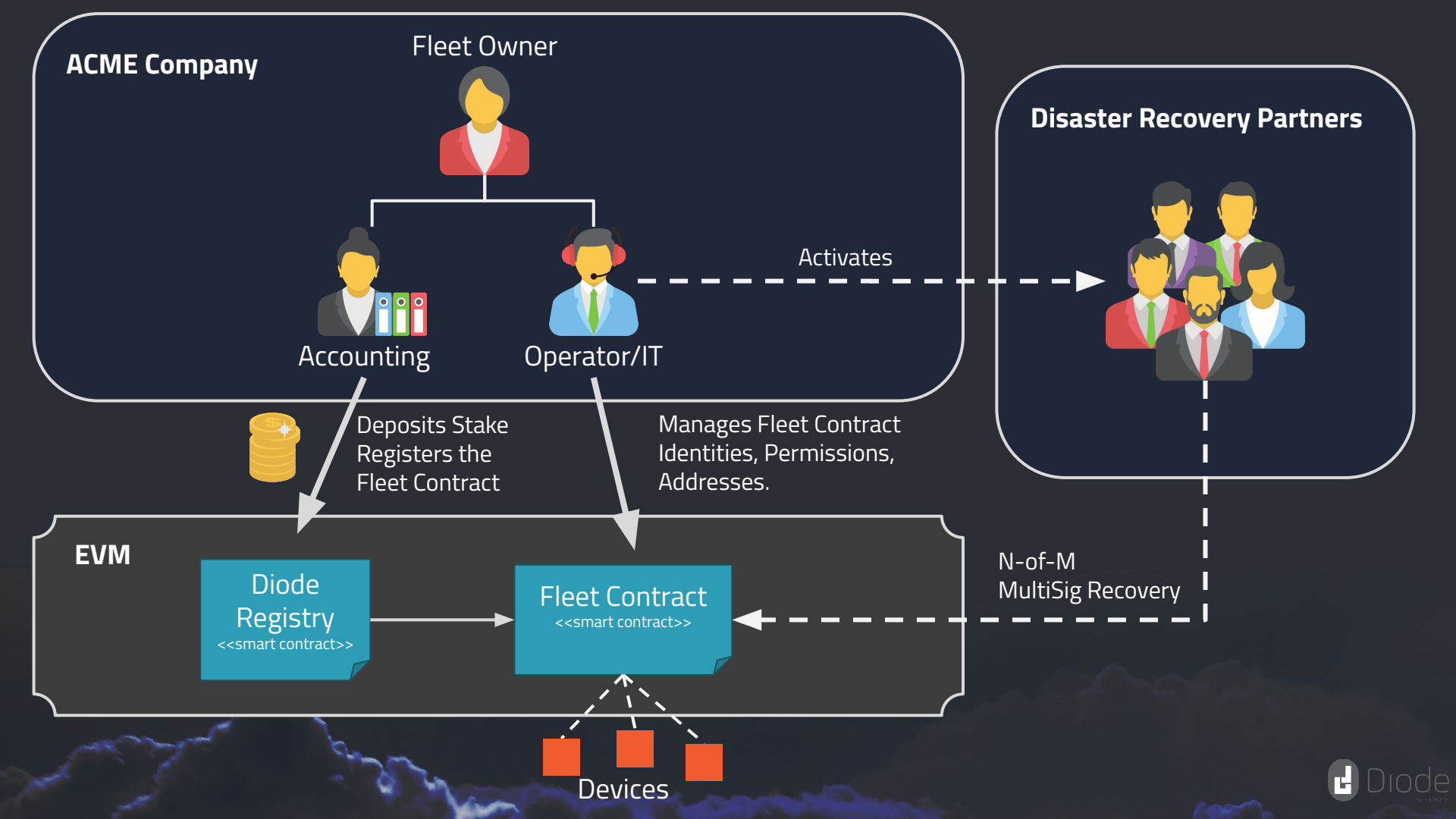
Ticket Aggregation #2

- Diode Registry reduces gas cost on valid ticket submission. 2x increase.

- Fleet Relayers take Tickets from same fleet contract and merge them. 100x - 1000x reduction in tickets.

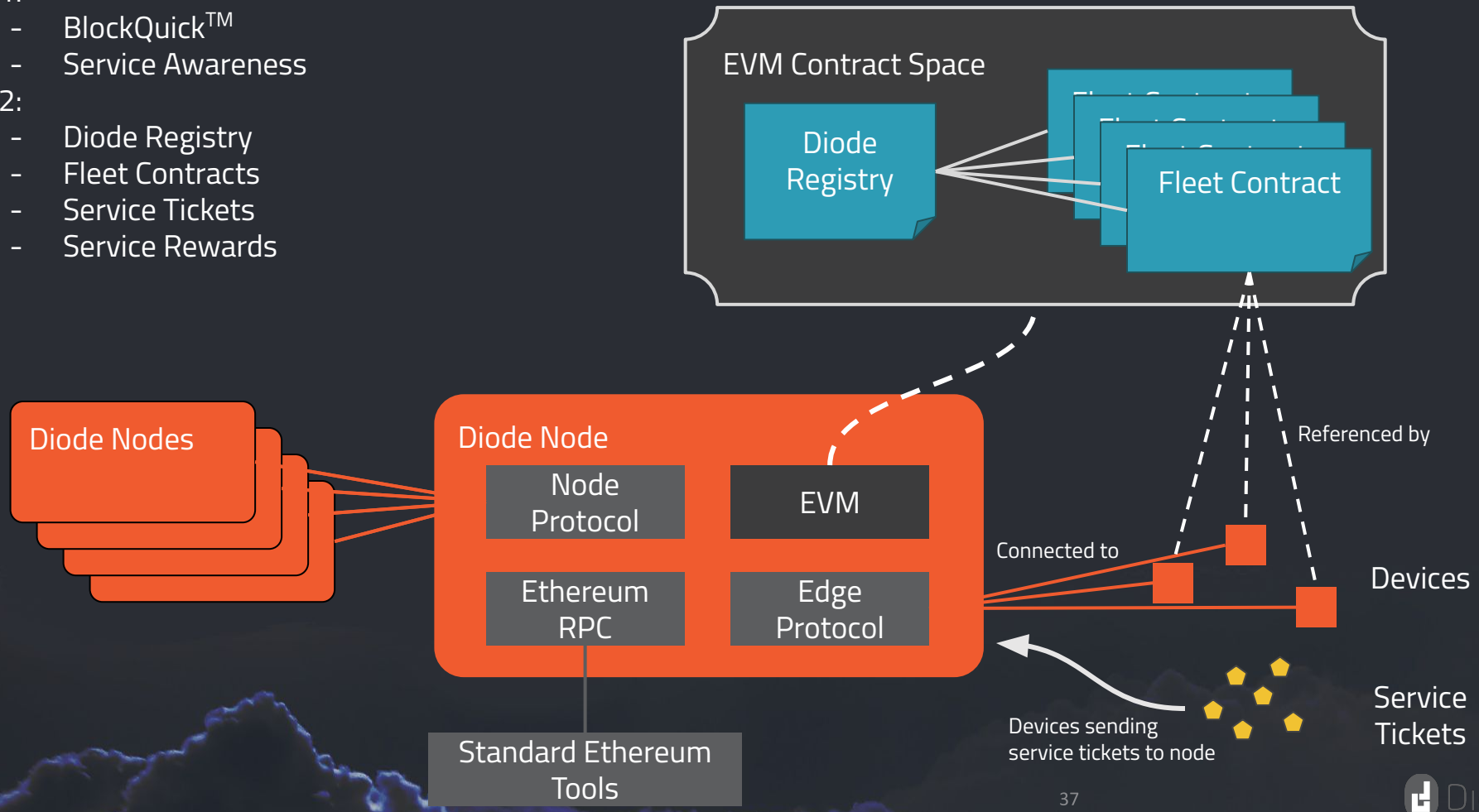
- 138,240,000,000 - 1,382,400,000,000 (1,3兆)
  Monthly Active Devices
  (691,200,000 * 2 * 100...1000)

Fleet Contracts


ACME Company
Fleet Owner
Accounting
Operator/IT
Activates
Disaster Recovery Partners
Deposits Stake
Registers the
Fleet Contract
Manages Fleet Contract
Identities, Permissions,
Addresses.
EVM
Diode
Registry
<<smart contract>>
Fleet Contract
<<smart contract>>
N-of-M
MultiSig Recovery
Devices
Diode

L1:
- BlockQuick™
- Service Awareness

L2:
- Diode Registry
- Fleet Contracts
- Service Tickets
- Service Rewards

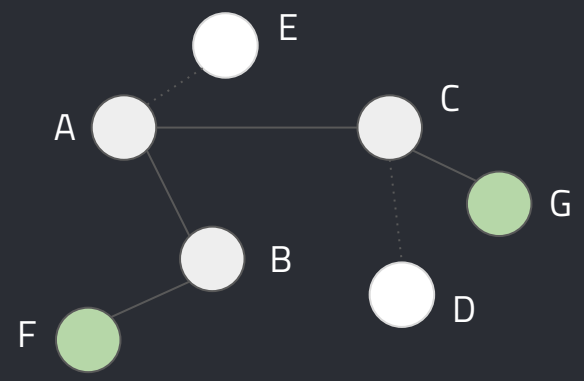


We're looking for reviewers for Light
https://diodechain.io

WELCOME TO THE FUTURE OF IOT

Q&A

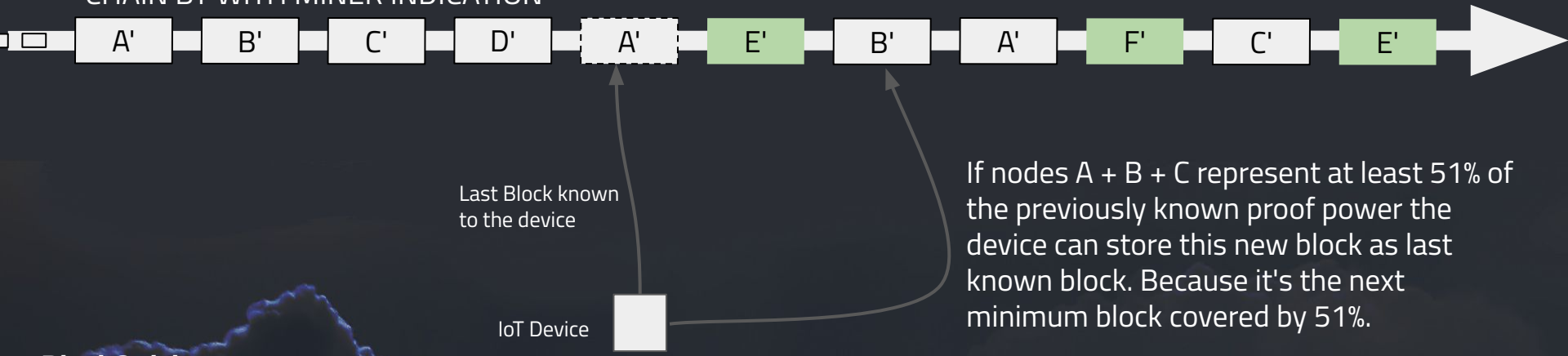
BLOCKCHAIN NODES



Device is following and validating new blocks only as far as they

1) Are hash-correct (standard blockchain rules)
2) Have follow up-blocks that represent at least 51% of the previous known proof power (PoW or PoS)

CHAIN BY WITH MINER INDICATION



If nodes A + B + C represent at least 51% of the previously known proof power the device can store this new block as last known block. Because it's the next minimum block covered by 51%.

BlockQuick

Diode