Why blockchain is the solution to IoT security

Dominic Letz / CTO Diode

COSCUP 2019 Taipei

(alternative title)

Doing Blockchain with elixir 

The Good - The Bad - The Ugly

About Me

- Dominic Letz / 陳多米
- Co-Inventor of BlockQuick algorithm
- Working since Nov 2018 on BlockQuick implementation
- CTO Exosite https://diode.io
- Founding Member of Ethereum  Magicians Ring: Constrained Resource Clients

PHP => C++ => Erlang => Elixir

Blockchain + IoT ??

Typical IoT Devices

smart lock

connected smoke detector

Today's Security Problems

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

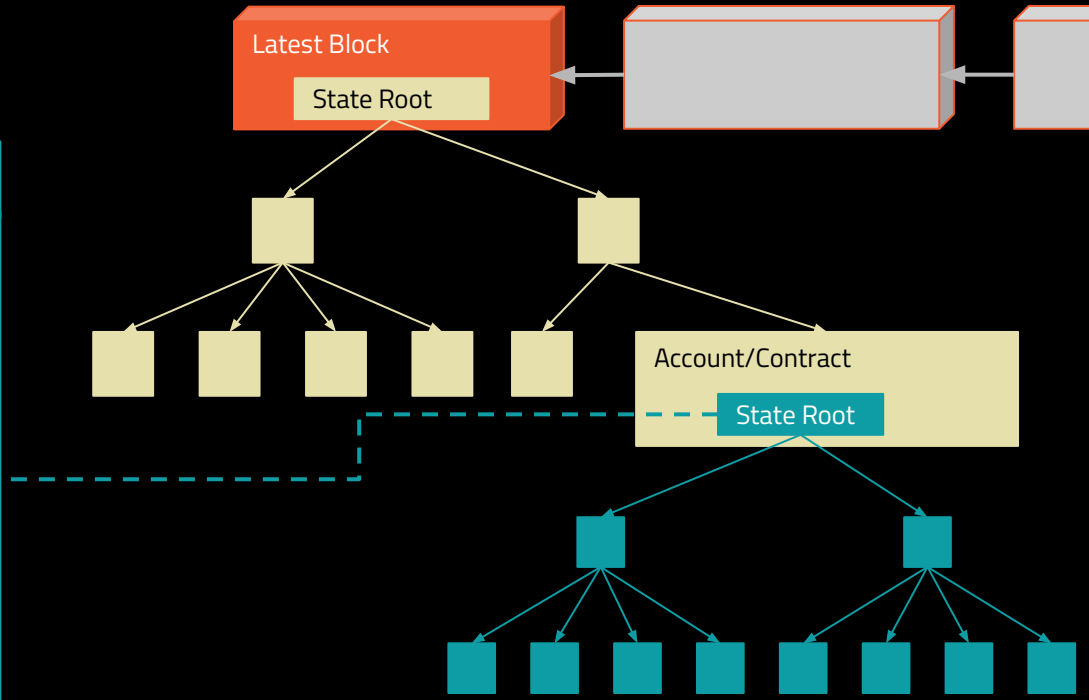
getting secure timestamp

fetching contract state & merkle proofing

Today's Security Problems

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

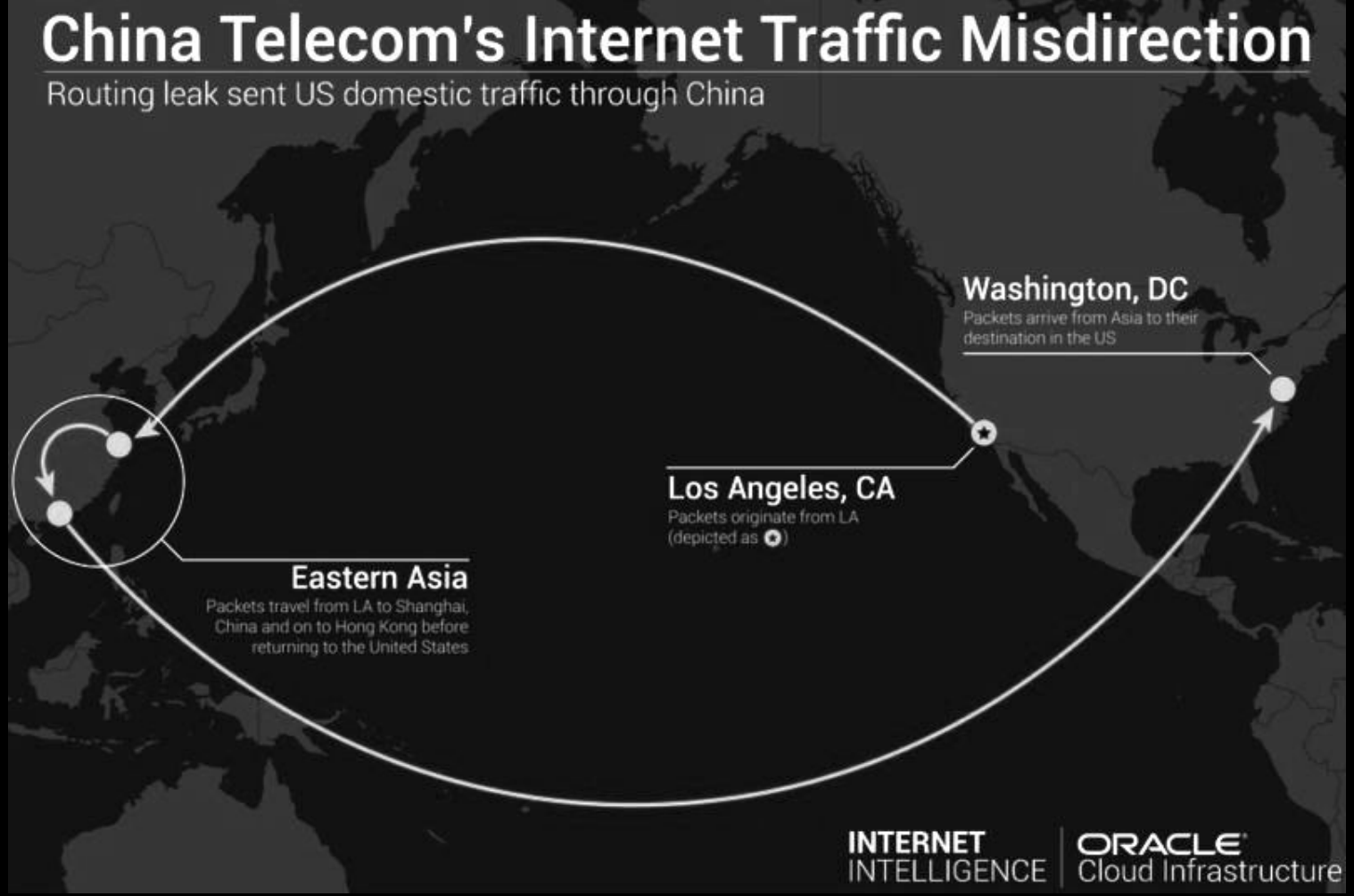
```
pragma solidity ^0.4.0;

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

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



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.

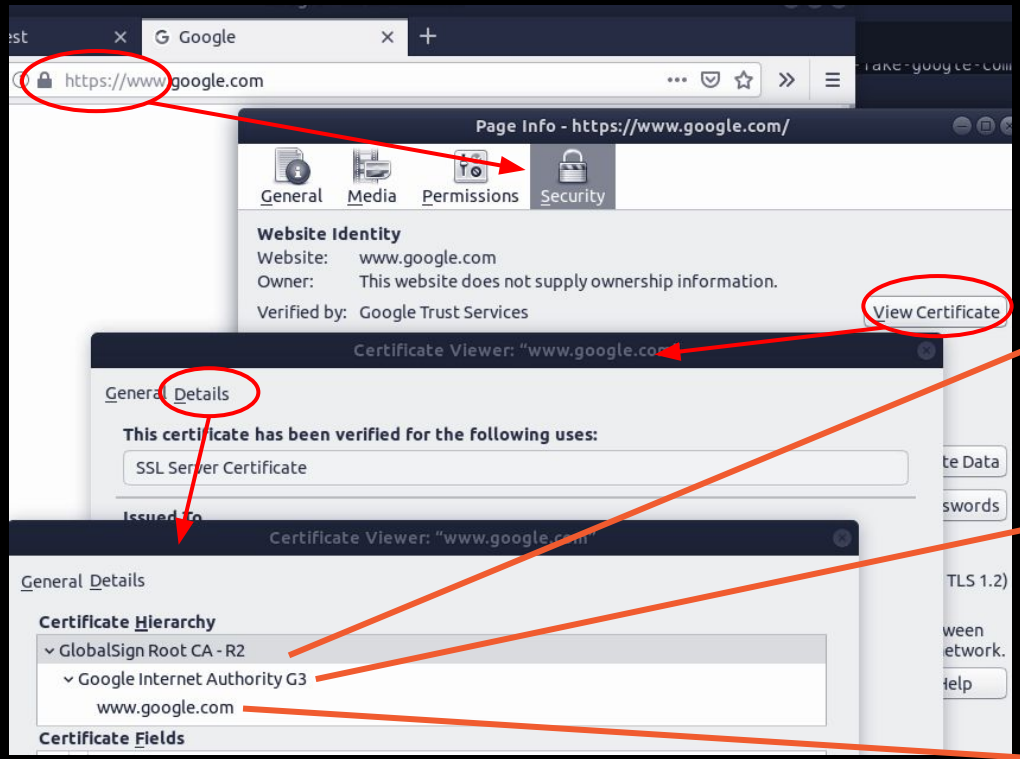
And since 2018 by private unidentified groups.



China Telecom's Internet Traffic Misdirection in 2017

Public Key Infrastructure (PKI) enables Spying

Hierarchy of Certificates, Higher Can Sign



Pre-Installed in your Browser / OS

Intermediate

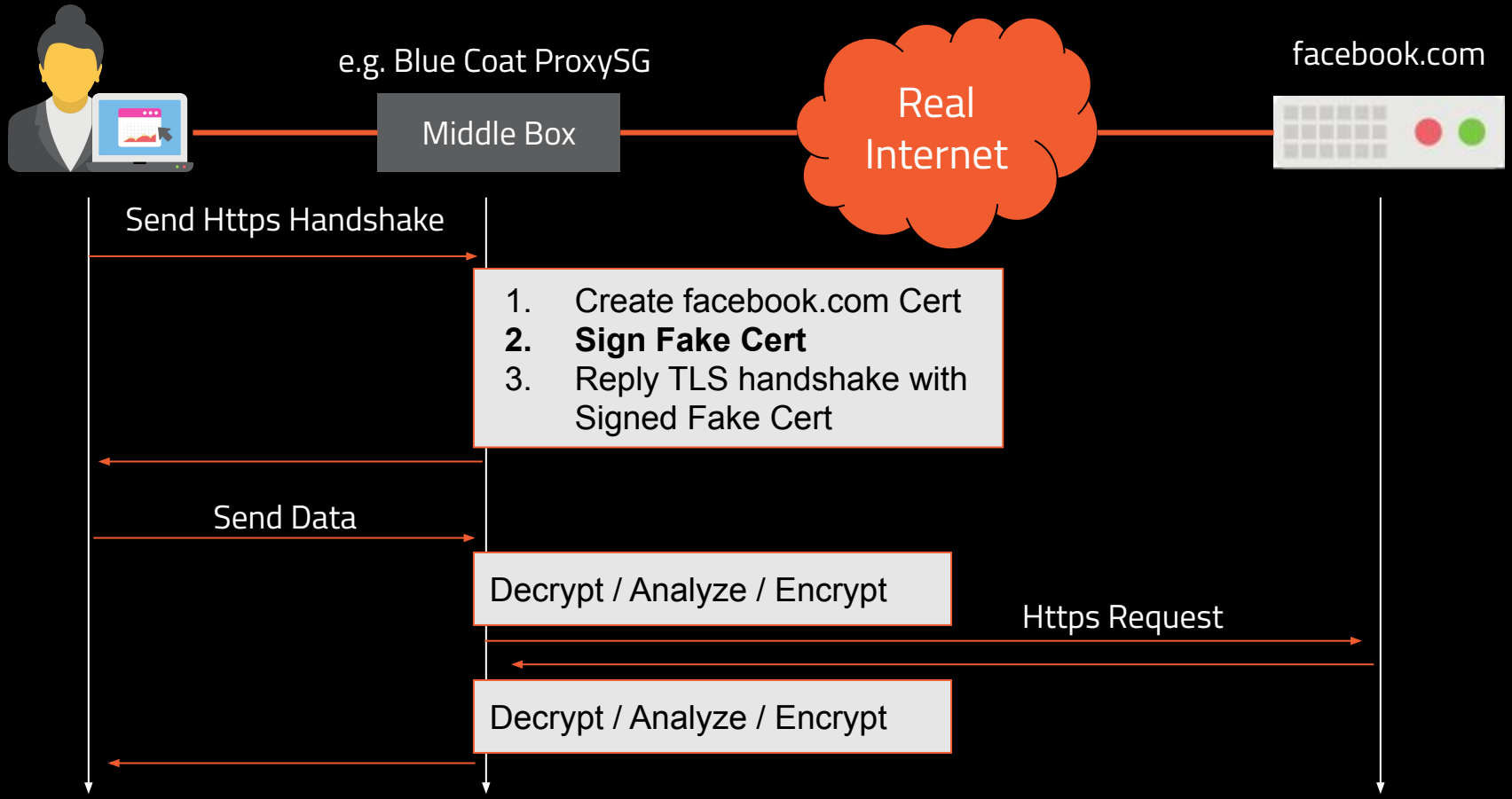
Entity

Root Store ~50 certs

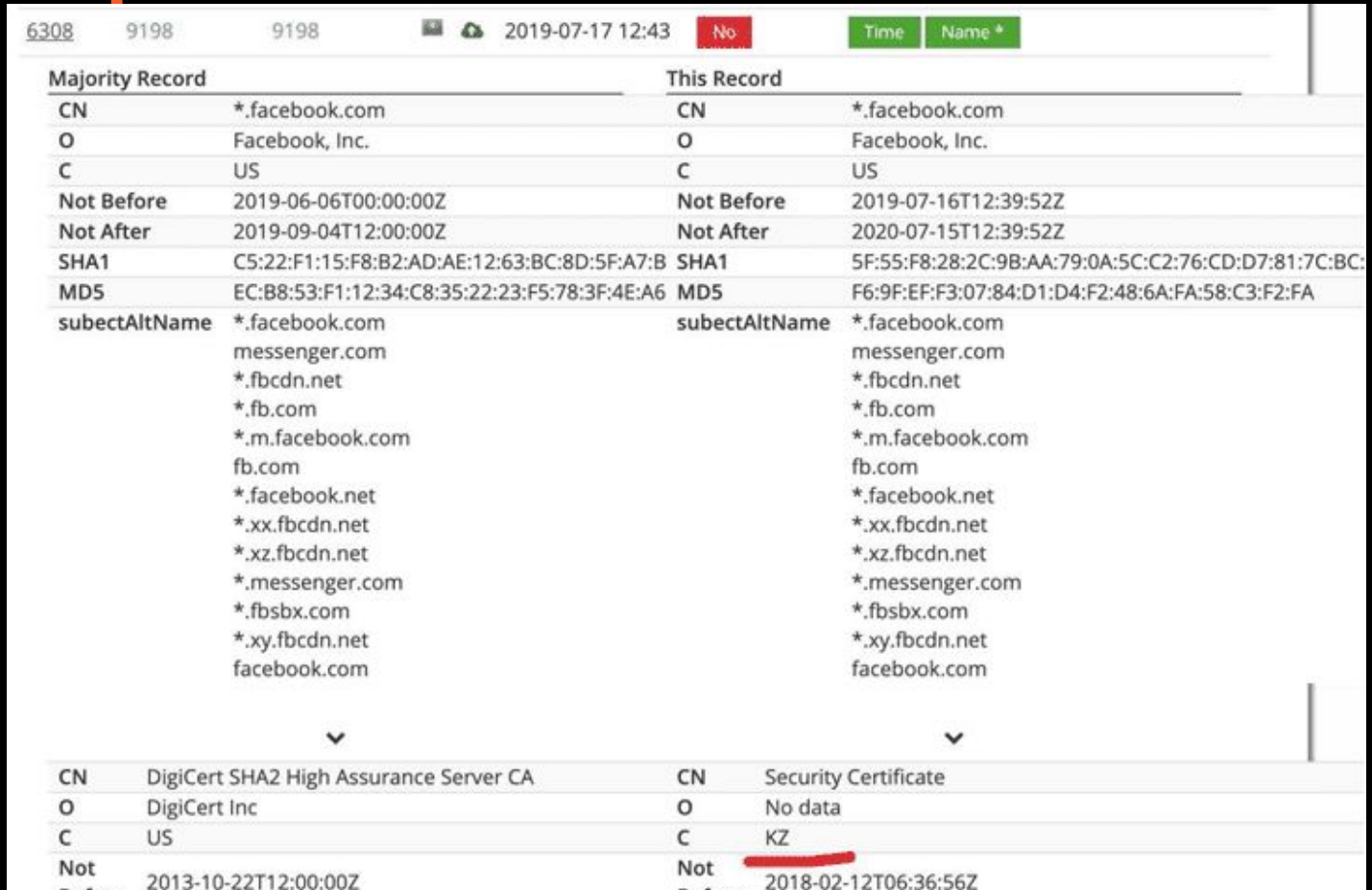
>3000 certs

millions of domain certs

PKI enabled Man-In-The-Middle (MITM)



Example: Facebook in Kazakhstan



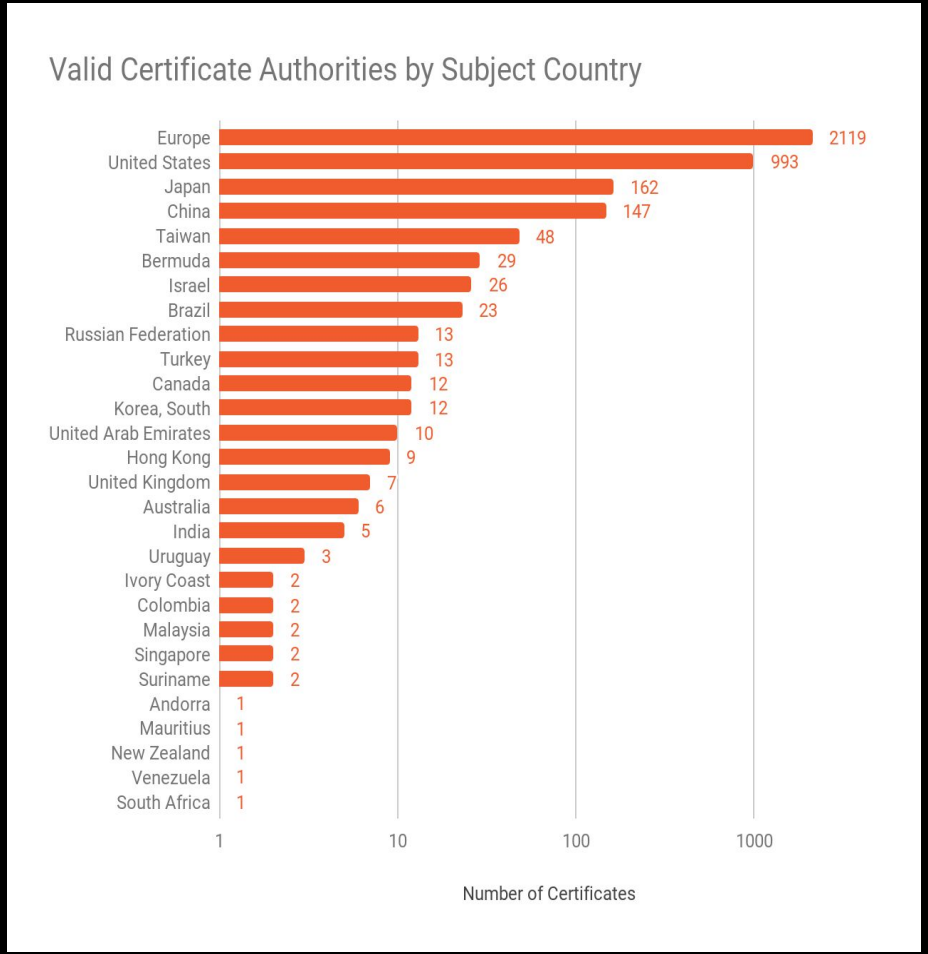
6308 9198 9198 2019-07-17 12:43 No Time Name *

Majority Record		This Record	
CN	*.facebook.com	CN	*.facebook.com
O	Facebook, Inc.	O	Facebook, Inc.
C	US	C	US
Not Before	2019-06-06T00:00:00Z	Not Before	2019-07-16T12:39:52Z
Not After	2019-09-04T12:00:00Z	Not After	2020-07-15T12:39:52Z
SHA1	C5:22:F1:15:F8:B2:AD:AE:12:63:BC:8D:5F:A7:B	SHA1	5F:55:F8:28:2C:9B:AA:79:0A:5C:C2:76:CD:D7:81:7C:BC:
MD5	EC:B8:53:F1:12:34:C8:35:22:23:F5:78:3F:4E:A6	MD5	F6:9F:EF:F3:07:84:D1:D4:F2:48:6A:FA:58:C3:F2:FA
subectAltName	*.facebook.com messenger.com *.fbcdn.net *.fb.com *.m.facebook.com fb.com *.facebook.net *.xx.fbcdn.net *.xz.fbcdn.net *.messenger.com *.fbsbx.com *.xy.fbcdn.net facebook.com	subectAltName	*.facebook.com messenger.com *.fbcdn.net *.fb.com *.m.facebook.com fb.com *.facebook.net *.xx.fbcdn.net *.xz.fbcdn.net *.messenger.com *.fbsbx.com *.xy.fbcdn.net facebook.com

CN	DigiCert SHA2 High Assurance Server CA	CN	Security Certificate
O	DigiCert Inc	O	No data
C	US	C	KZ
Not	2013-10-22T12:00:00Z	Not	2018-02-12T06:36:56Z

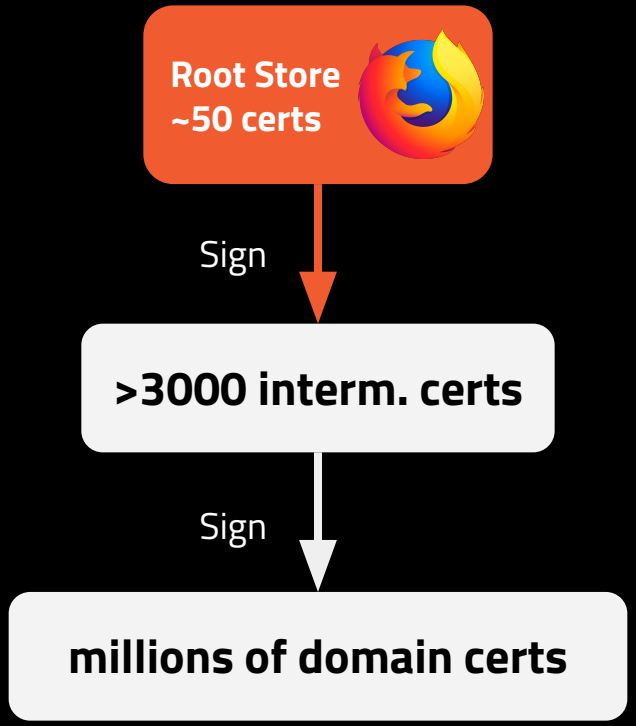
3,675 Intermediates

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

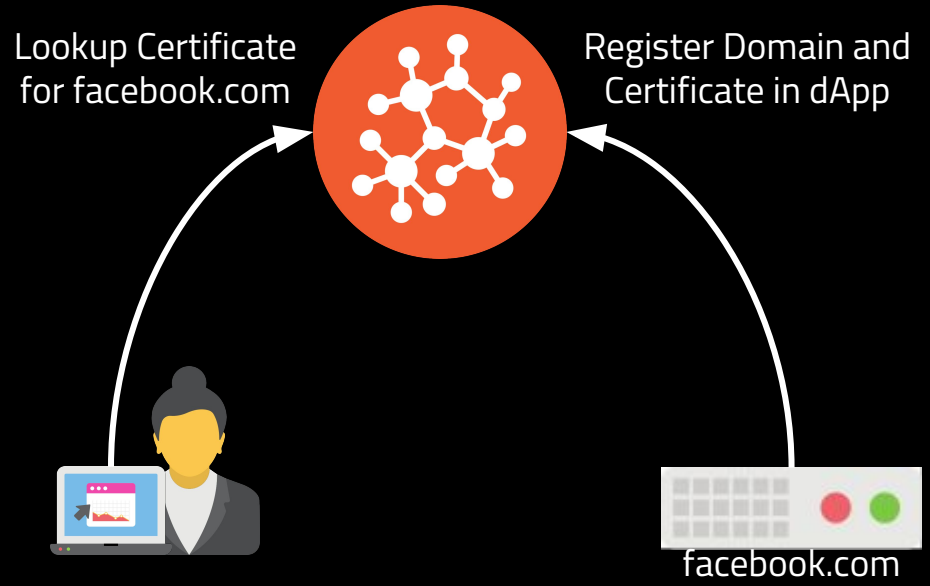


Solution

Today
Trust By Trusted Roots



Blockchain
Trust By Consensus



MITM becomes impossible, Time problem solved

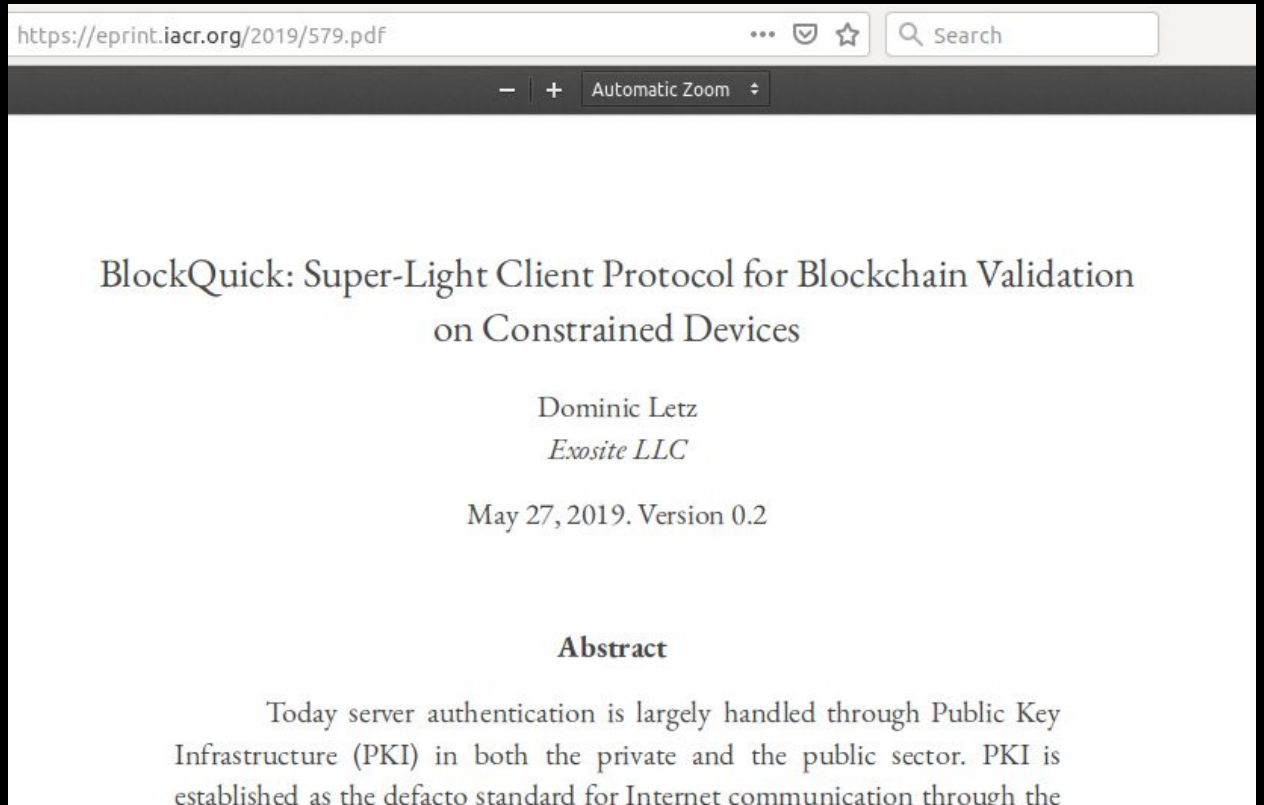
So Why Has Nobody Else Done That Yet?

The Challenge - Read Blockchain on a MCU

Client	Storage	RAM	Sync Bandwidth
geth --syncmode=fastsync	200 GB	1,000 MB	~100 MB per day
geth --syncmode=light	1.2 GB	150 MB	~3.5 MB per day
IOTA Node	8 GB	4,000 MB	1 GB per day

Hardware	Storage	RAM	Bandwidth
ESP32	4-16 MB	520 KB	WIFI
Linkit 7697	4 MB	352 KB	WIFI

Challenge Accepted!



A New Hope

Client	Storage	RAM	Sync Bandwidth
geth --syncmode=fastsync	200 GB	1,000 MB	~100 MB per day
geth --syncmode=light	1.2 GB	150 MB	~3.5 MB per day
IOTA Node	8 GB	4,000 MB	1 GB per day
BlockQuick	20 KB	50 KB	20 KB per sync

Hardware	Storage	RAM	Bandwidth
ESP32	4-16 MB	520 KB	WIFI
Linkit 7697	4 MB	352 KB	WIFI

+ BlockQuick

+ P2P Transmission

=

How much code do I need to read to understand Ethereum?

```
dominicletz@toshi:~/projects/parity-ethereum$ cloc --quiet --git master

github.com/AlDanial/cloc v 1.74  T=6.07 s (159.9 files/s, 48551.0 lines/s)
-------------------------------------------------------------------------------
Language                     files          blank        comment           code
-------------------------------------------------------------------------------
Rust                           750          28628          27228         145636
JSON                            69             10              0          78479
Markdown                        31           1037              0           9782
```

145k Rust

```
dominicletz@toshi:~/projects/aleth$ cloc --quiet --git master

github.com/AlDanial/cloc v 1.74  T=3.02 s (176.2 files/s, 39420.4 lines/s)
-------------------------------------------------------------------------------
Language                     files          blank        comment           code
-------------------------------------------------------------------------------
C++                            216           7675           4961          72080
C/C++ Header                   183           4448           4991          17047
CMake                           42            317            342           1527
```

89k C++

```
dominicletz@toshi:~/projects/go-ethereum$ cloc --quiet --git master

github.com/AlDanial/cloc v 1.74  T=17.11 s (126.7 files/s, 55026.1 lines/s)
-------------------------------------------------------------------------------
Language                     files          blank        comment           code
-------------------------------------------------------------------------------
Go                            1763          56608          73801         612630
C                               55          17257          29082          86546
C/C++ Header                    97           2560           5957          15342
JavaScript                      13           1845           4495           7986
```

612k Go

Elixir Prototype

Good: Many Places to Lend Pieces From

Erlang EVM: Aeternity
https://github.com/aeternity/aeternity

Elixir Network Explorer:
https://github.com/poanetwork/blockscout

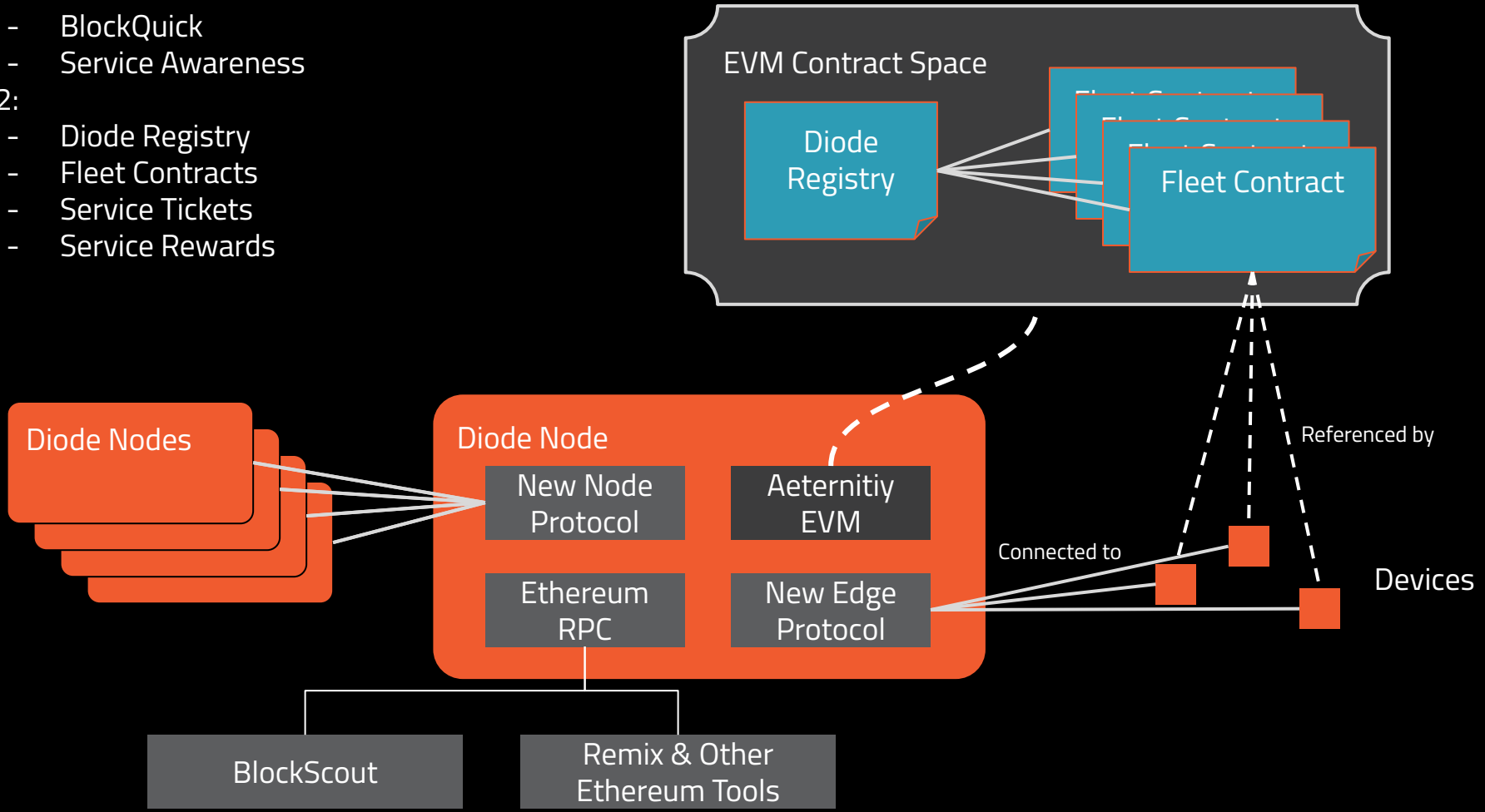
Erlang secp256k1

https://hex.pm/packages/libsecp256k1

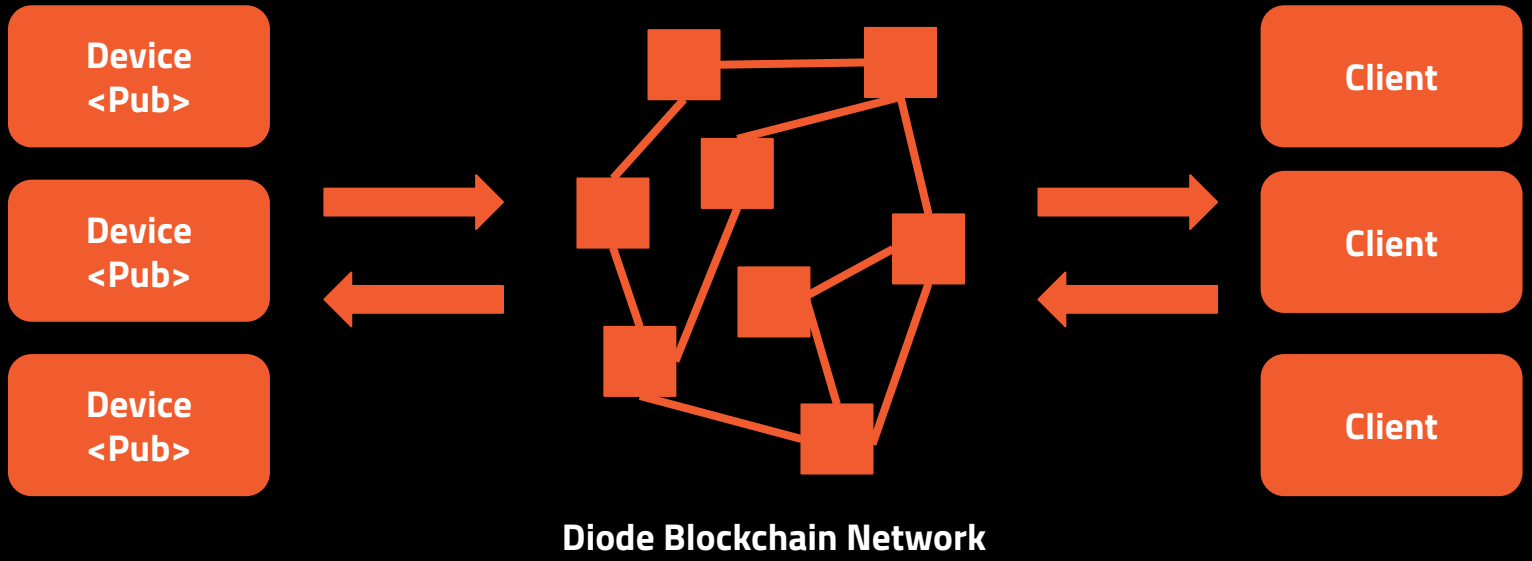
Elixir Full Node: Mana-Ethereum (not used)
https://github.com/mana-ethereum/mana

L1:
- BlockQuick
- Service Awareness

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

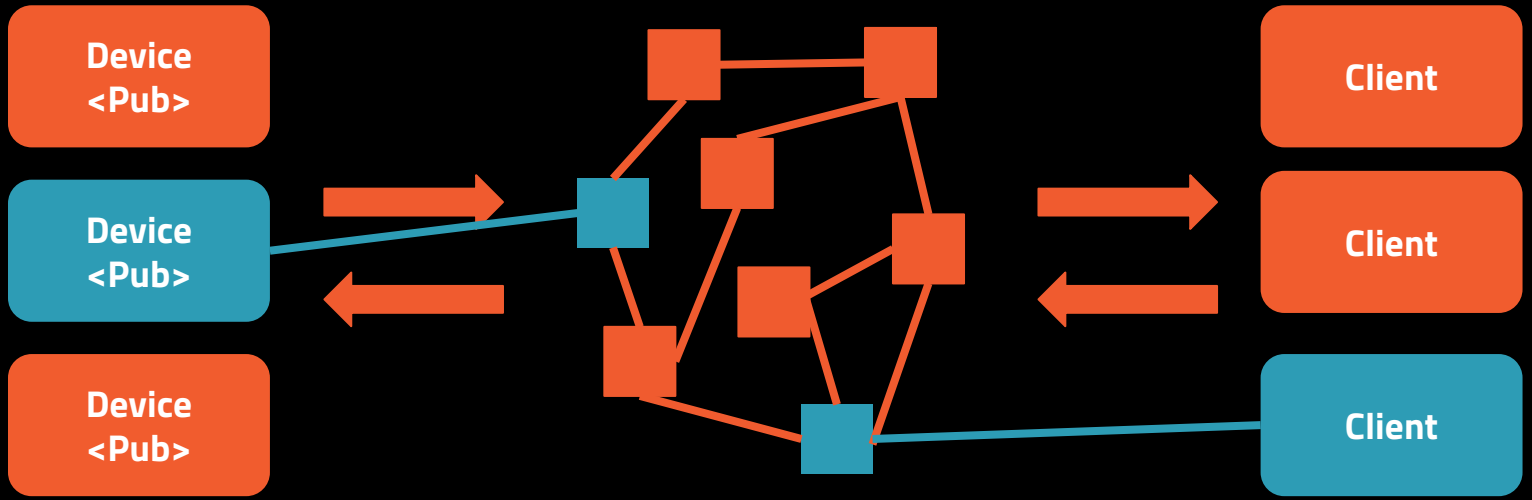


Decentralized IoT



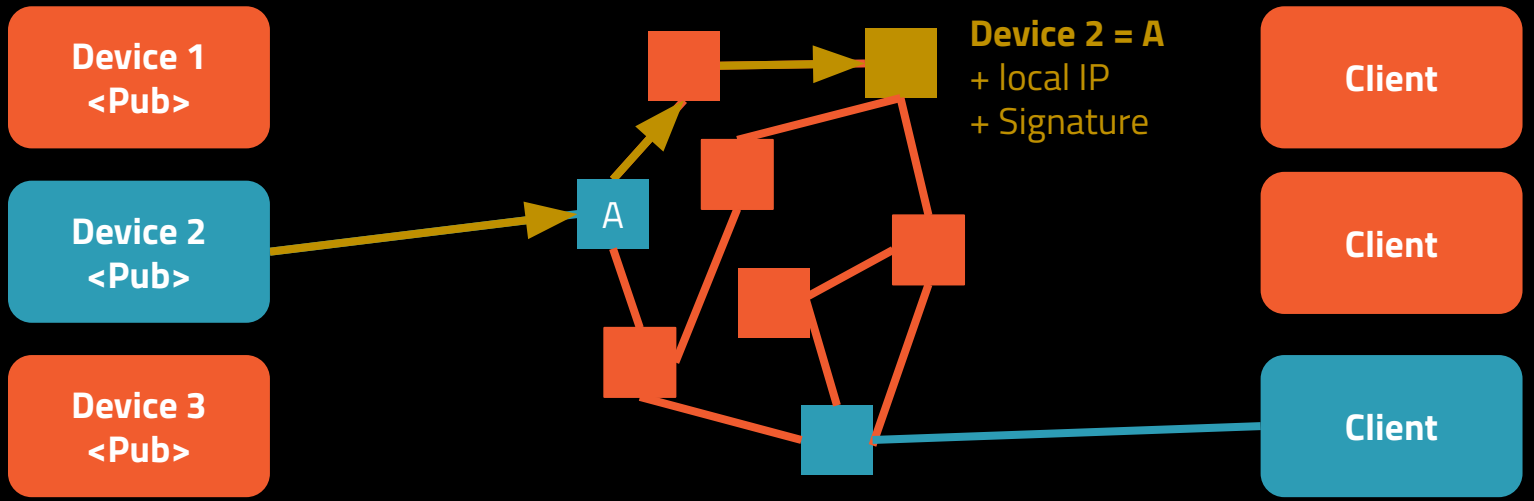
Decentralized IoT

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



Decentralized IoT

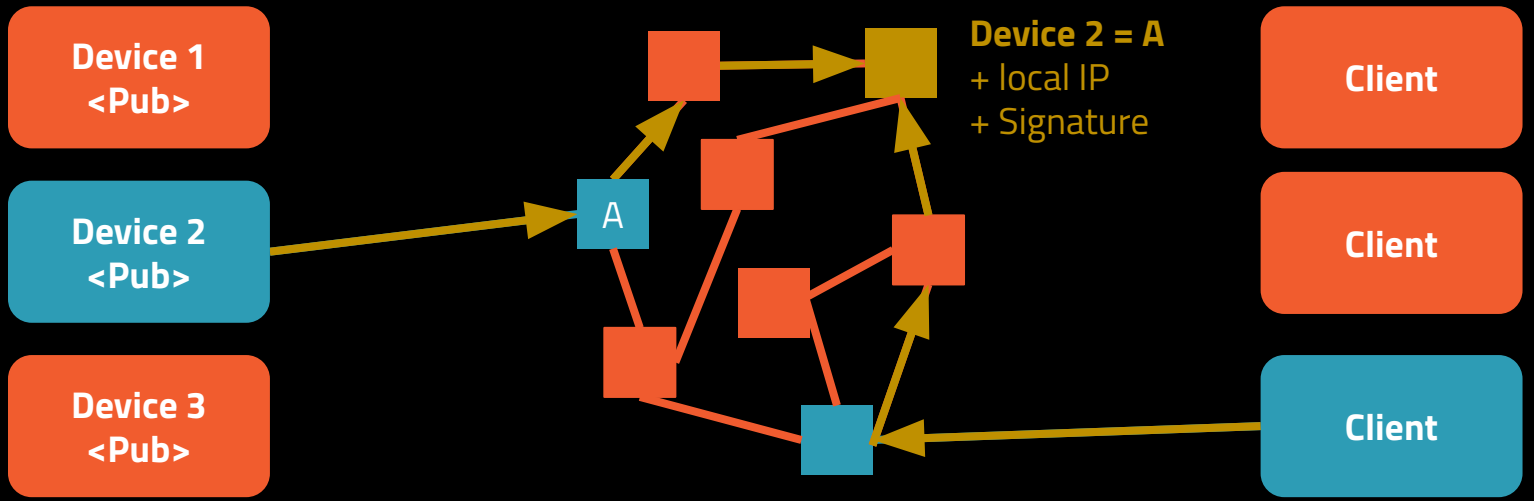
1. Store device location



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

Decentralized IoT

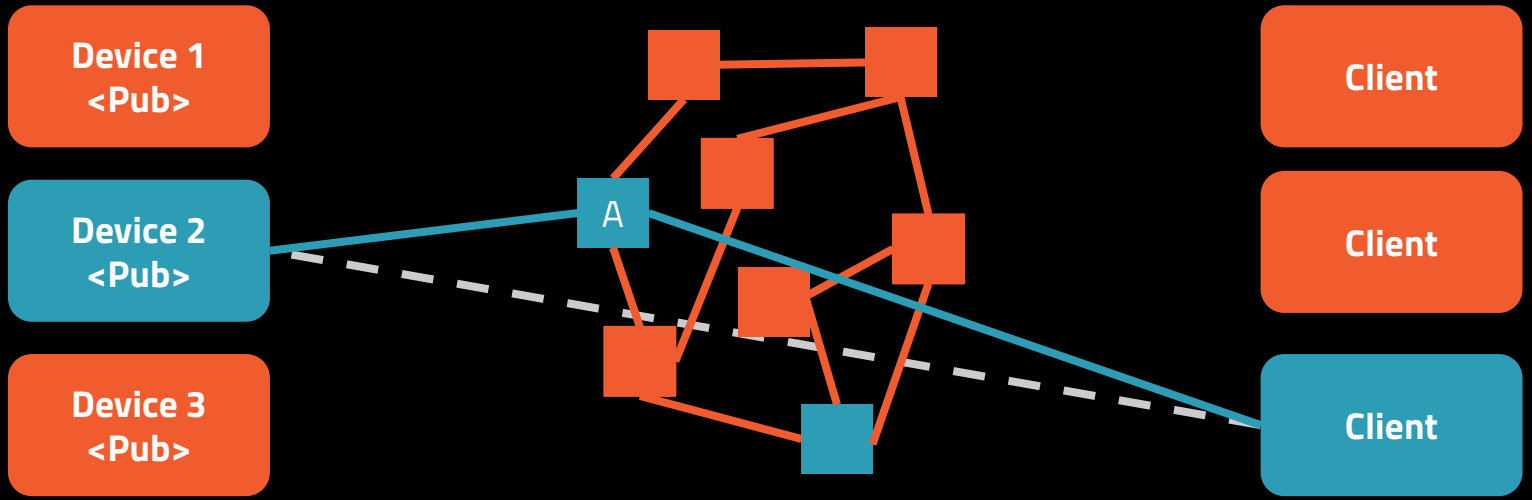
2. Find the device location



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

Decentralized IoT

3. Connect to device



Direct Connection is Possible

otherwise proxy connection

Writing your own Ethereum Node in Elixir

- Elixir is perfect for short network & tree code
- It's fun
- You'll learn a lot
- Afterwards you should give us a call

```
dominicletz@toshi:~/projects/diode$ cloc --quiet --git master

github.com/AlDanial/cloc v 1.74  T=0.56 s (153.7 files/s, 23832.9 lines/s)
-------------------------------------------------------------------------------
Language                     files          blank        comment           code
-------------------------------------------------------------------------------
Elixir                          57           1398            545           6489
Erlang                          20            403            993           3444
```

The Bad

You can't be 100% Elixir. Crypto routines will stay in C.

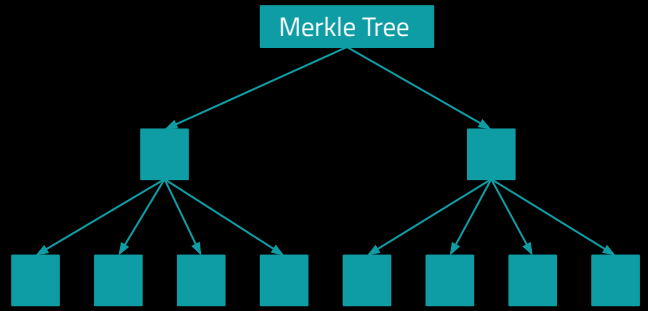
Don't Rewrite in Elixir!

If you do. Don't expect it to be nice or fast

https://github.com/dominicletz/exsha3/

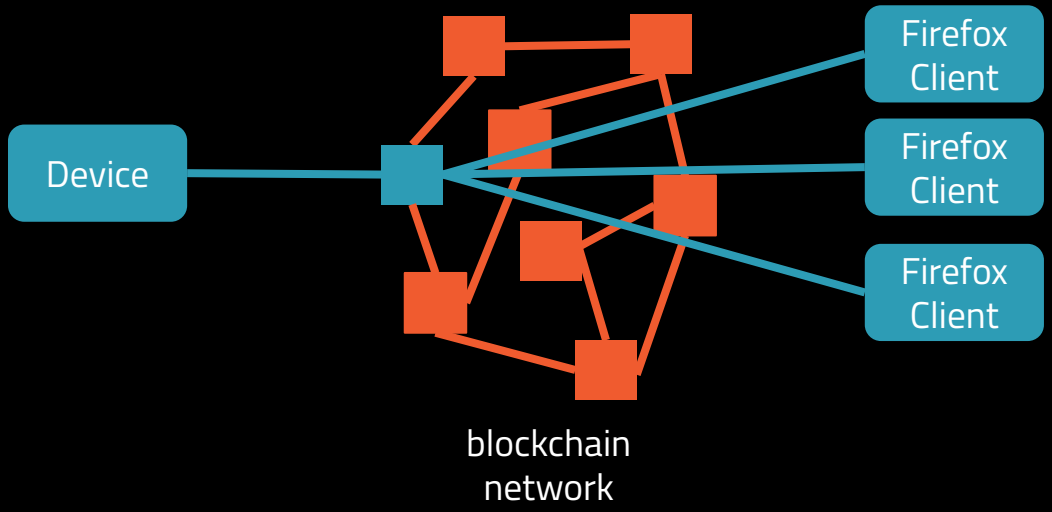
The Ugly

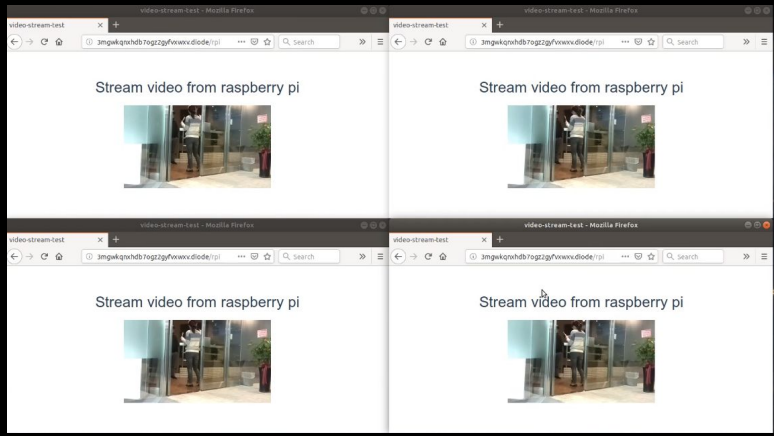
Elixir is great to write SHORT CODE for (merkle) trees



But shared nothing means you have many copies, or only one process to work in the tree.

DEMO DATA BROADCAST





How To Deploy Your Devices

1. Setup dApp (Fleet Contract)
    a. `git clone` Fleet Contract Template
    b. Set permissions, rules, behaviour
    c. Deploy Contract to Diode ProtoNet!
2. Setup Raspberry PI
    a. `git clone` go client
    b. Set contract id
    c. `go run`
3. Get Diode for Firefox
    a. `git clone` diode client for Firefox
    b. Run

https://github.com/diodechain

Decentralized

Secure

Serverless

No-Ops

Always On

(well, not the testnet)

Q&A

Our Vision is a secure Internet through trustless key infrastructure.

We only succeed when all Internet-capable systems can participate - help us by bringing things online!

Q&A Topics

- Distributed Internet, no central servers anymore
- Federated DNS/PK
- No Centralization / No Fragmentation

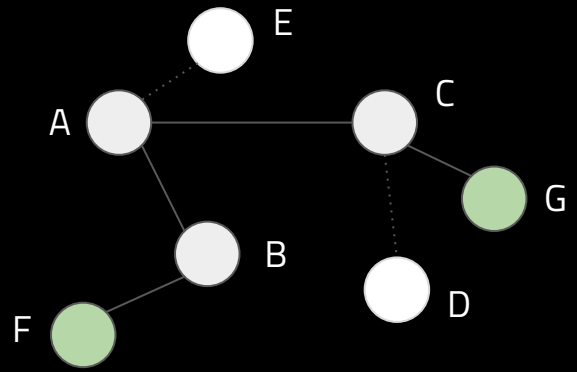
WELCOME TO THE FUTURE OF IOT

https://diode.io
Get Involved

BACKUP

BlockQuick

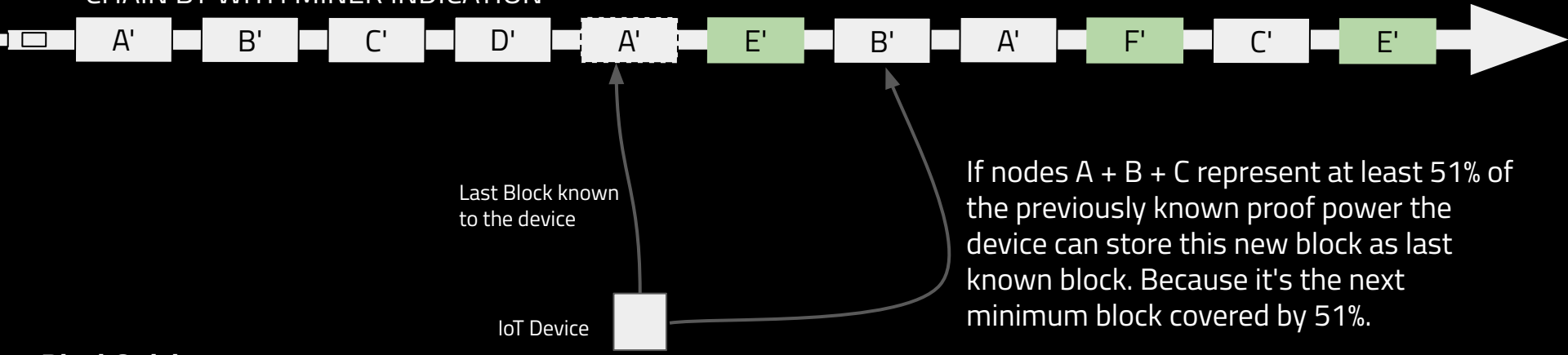
BLOCKCHAIN NODES



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

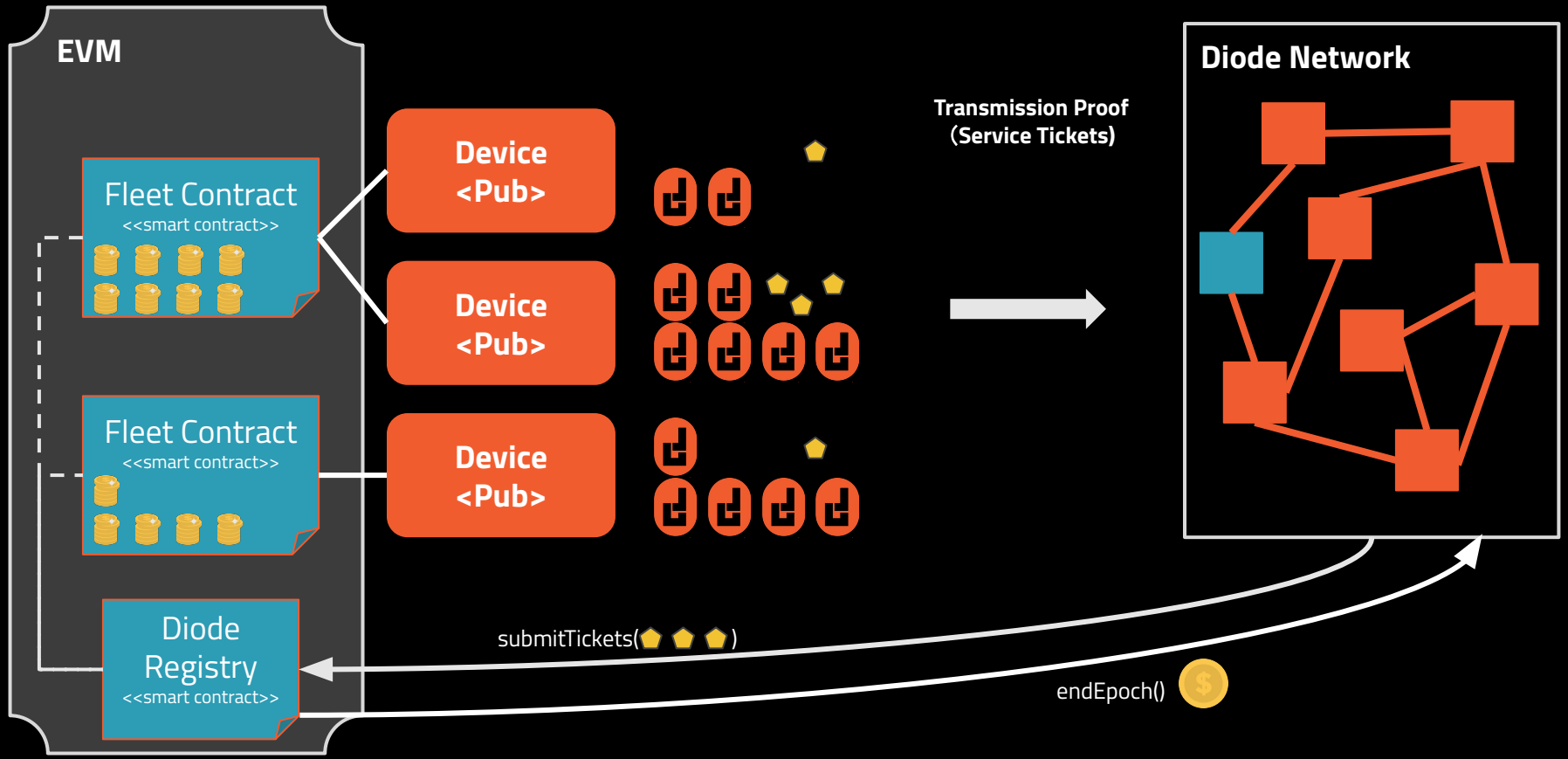


If nodes A + B + C represent at least 51% of the previously known proof power the device can store this new block as last known block. Because it's the next minimum block covered by 51%.

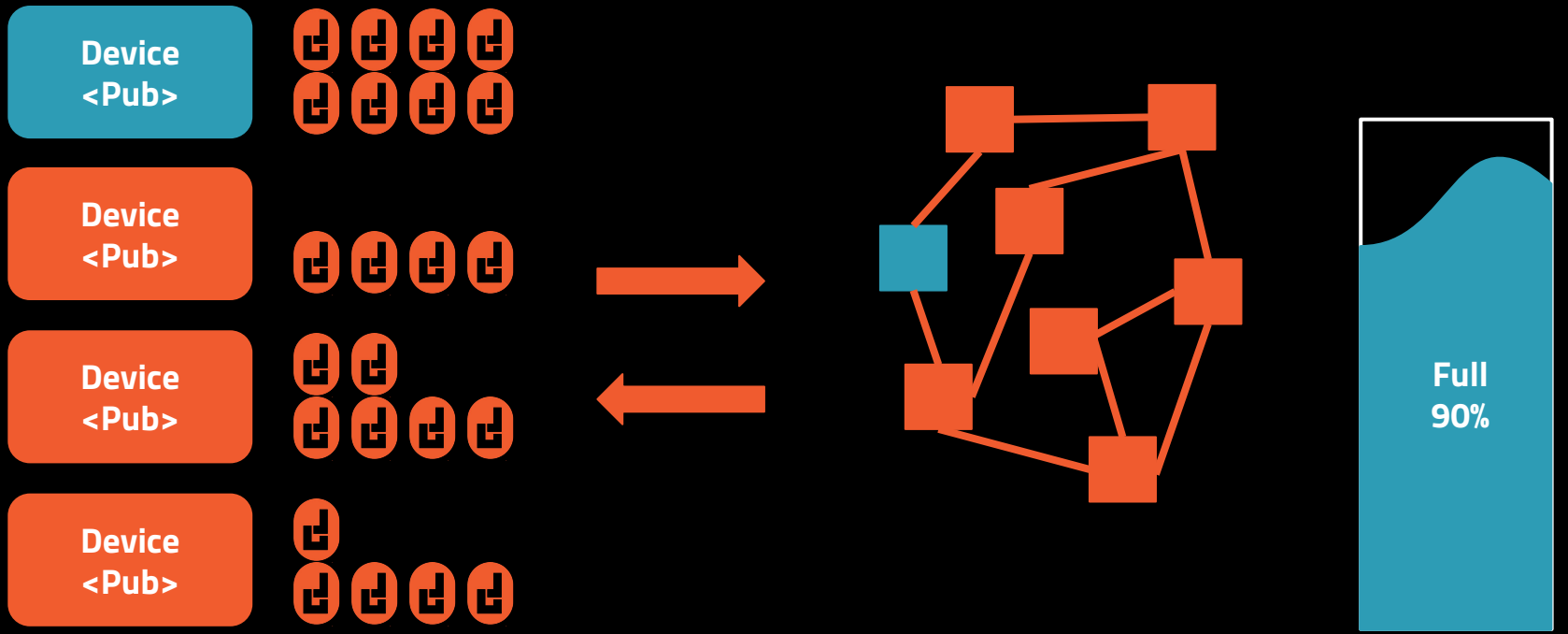
BlockQuick

Miner Incentives
and
Tickets ≠ Transactions

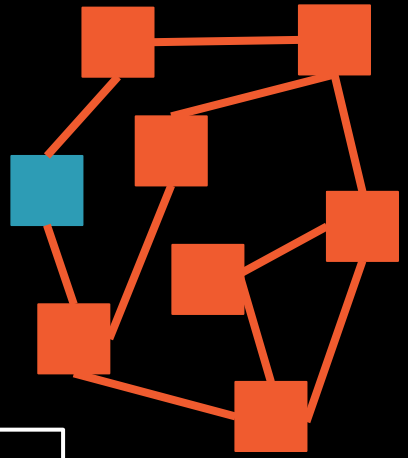
How does a miner work?



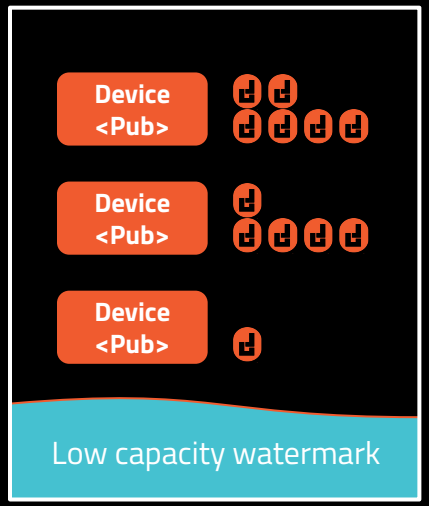
How does a miner work?



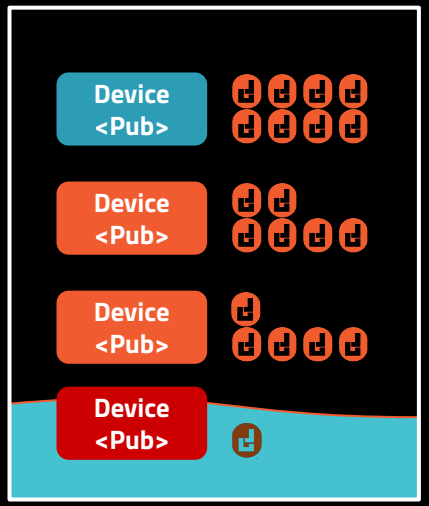
Miners select devices



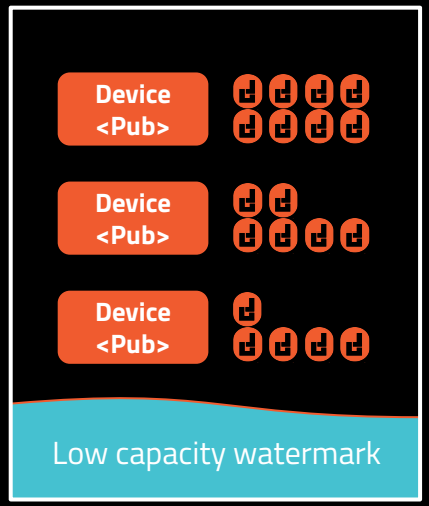
1. New device connects



2. Server at capacity, cheap device removed



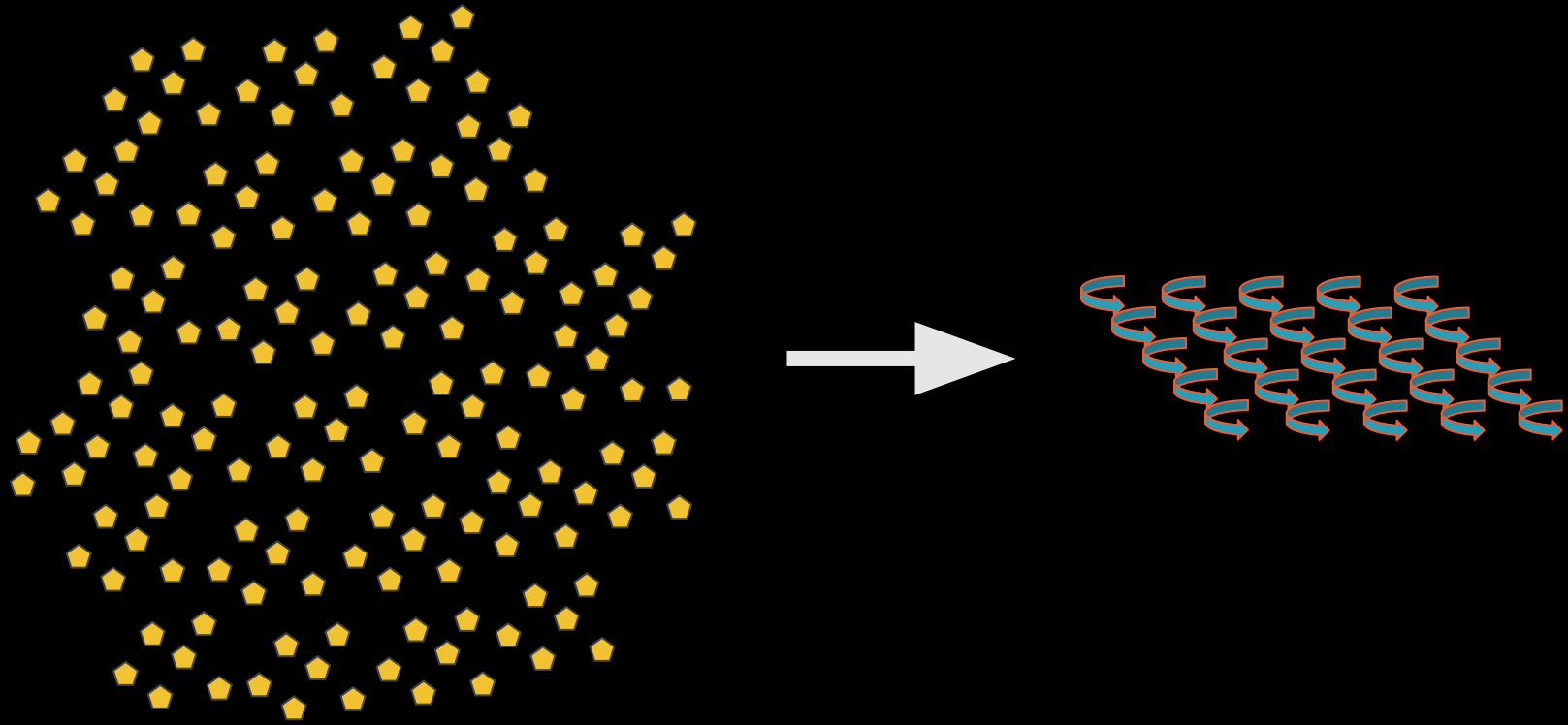
3. Miner optimizes revenue



Layer 2 Scaling Solution

Millions of Tickets

25 Transactions/s



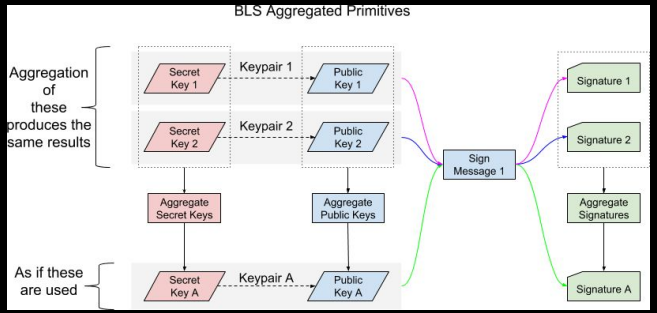
Ticket Aggregation #1

- 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

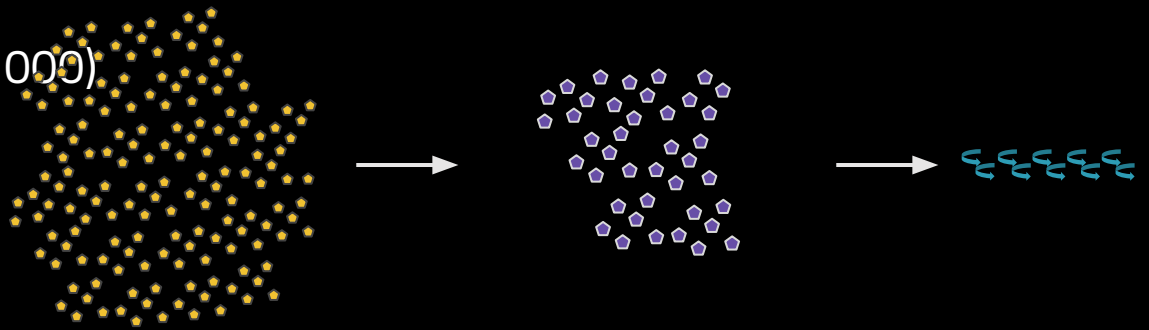
- 1,836 gas (68 * 27) => ~4,000 Tickets per Block
- 172,800 Blocks per Epoch * 4,000 Tickets per Block

- ~691,200,000 Monthly Active Devices

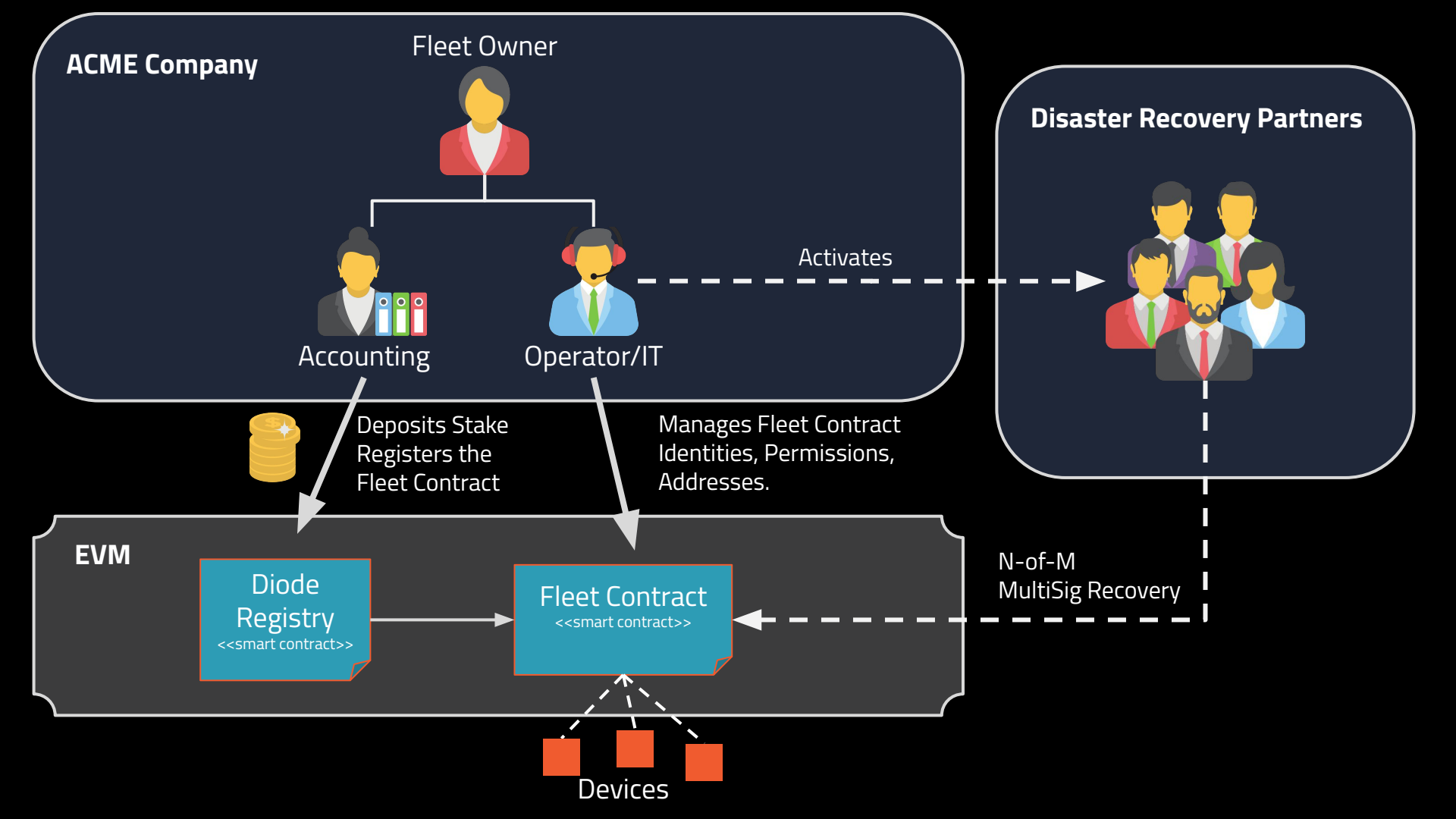


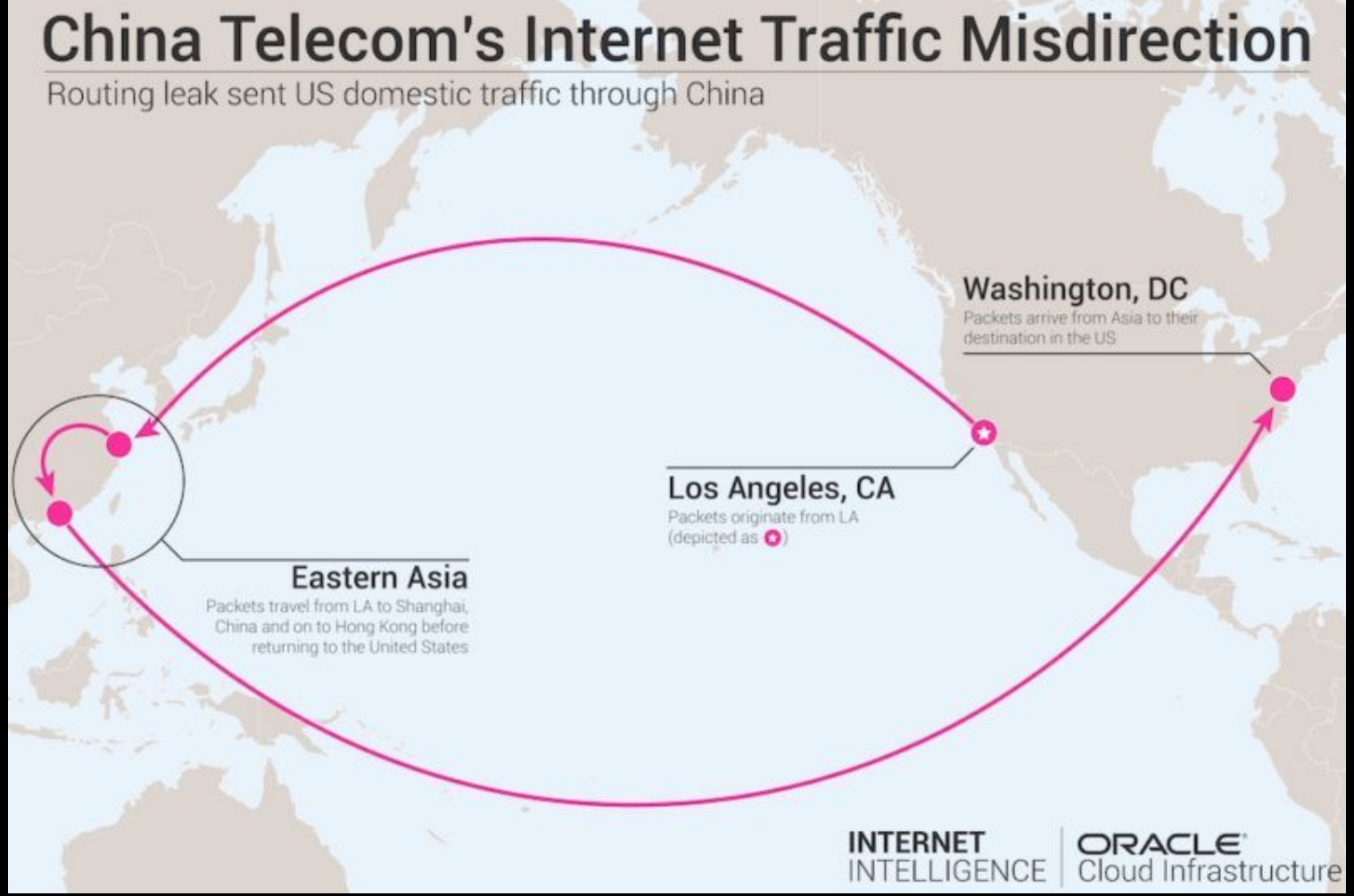
Ticket Aggregation #2

- 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



China Telecom's Internet Traffic Misdirection in 2017

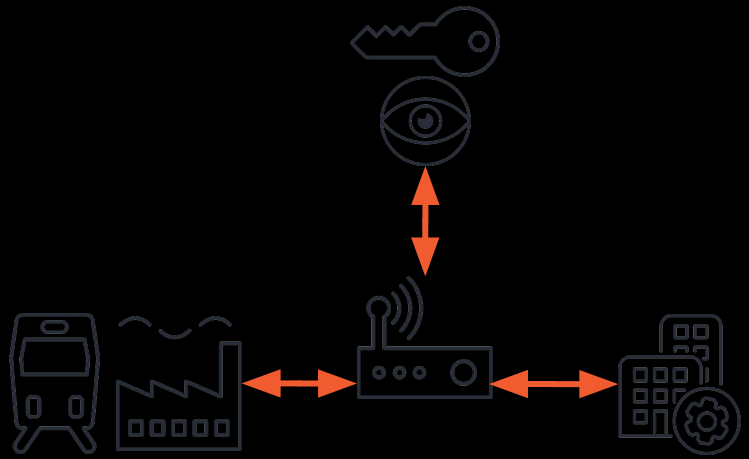
1

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.

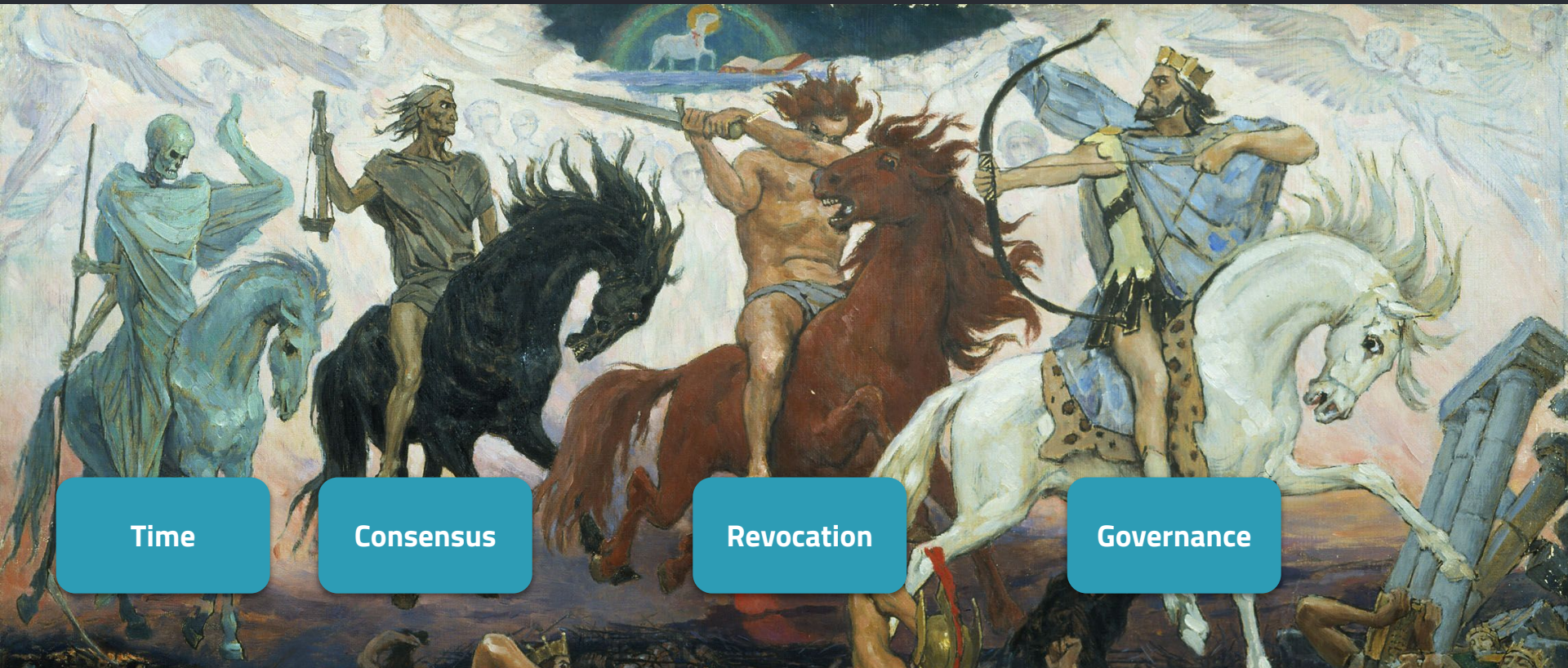
The Internet

Three centralized systems:

DNS	example.com	93.184.216.34
BGP	93.184.216.34	ME -> lwlcom -> cogentco -> DEST
PKI	https://	IANA **verified by** DigiCert

etc

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

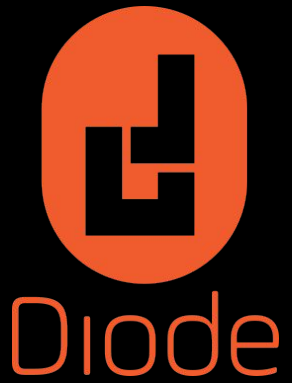
Step #1: Replace PKI

Step #2: Decentralize IoT

Step #3: World Peace

Step #1: Replace Internet PKI

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