

# Web3 PKI Security through Decentralization



**Dominic Letz**

Chief Technology Officer

<https://diode.io>

ETHKL Meetup / Ethereum Malaysia Group  
With Host Harith Kamarul  
Thursday, October 1, 2020  
**Blockchain and IOT**



# ABOUT US



## Diode

Founder team from the IoT and Telecommunications..  
We started Diode to  
**solve IoT Security using Blockchain.**

- [BlockQuick paper](#) published on May 27, 2019
- PreNet Launched January 2020
- Diode Client v0.4.10
- Offices in Berlin and Taipei

Focusing on makers, Raspberry Pi. Driving Network versatility. Broadcasting, secure tunneling, fleet management, VPN security, and storage.

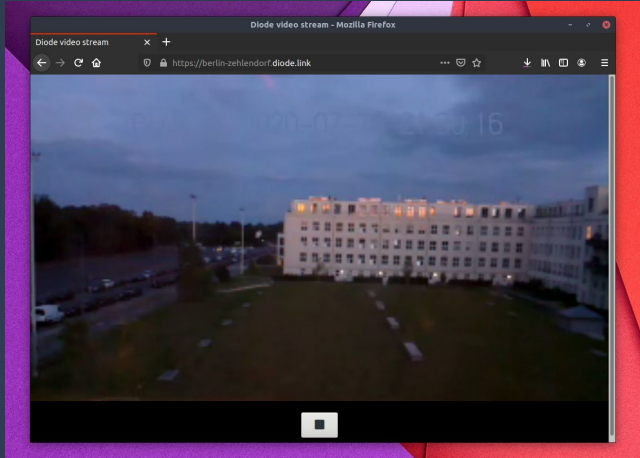
BlockQuick Validation for IoT



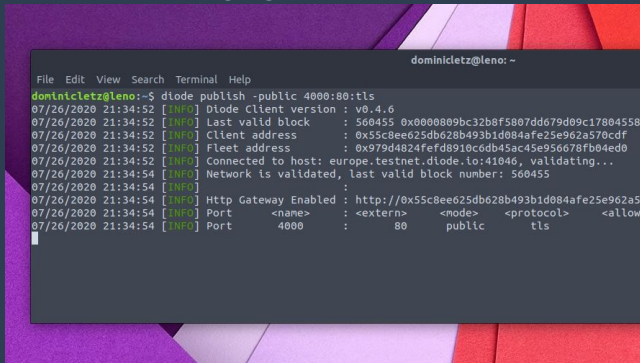
Client	Storage	Sync/Day
geth fast sync	200 GB	~100 MB
geth light	1.2 GB	~3.5 MB
IOTA	8 GB	~1 GB
BlockQuick	20 KB	20 KB

# APPS

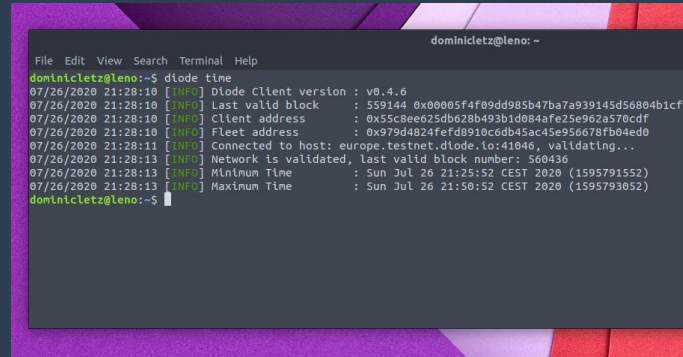
## Video Broadcasting



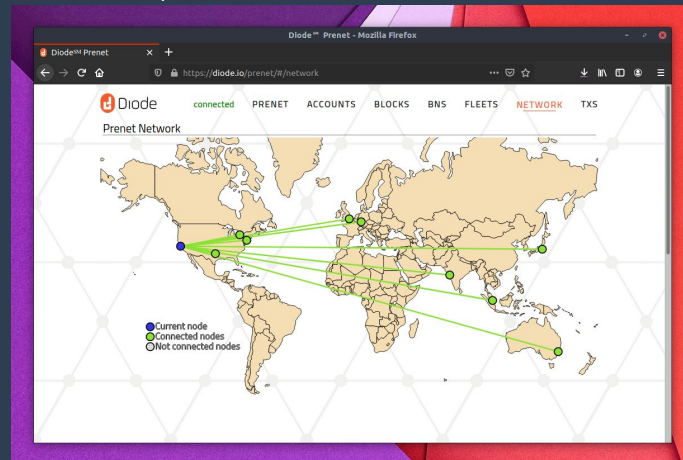
## Domain Publishing (ngrok on blockchain)



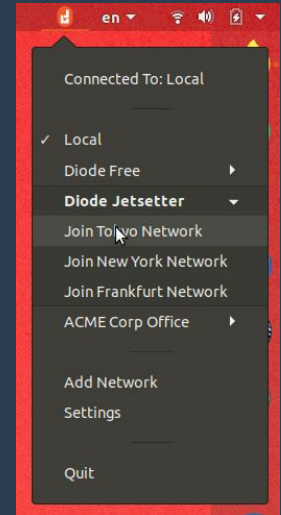
## Secure Time Consensus



## Network Explorer



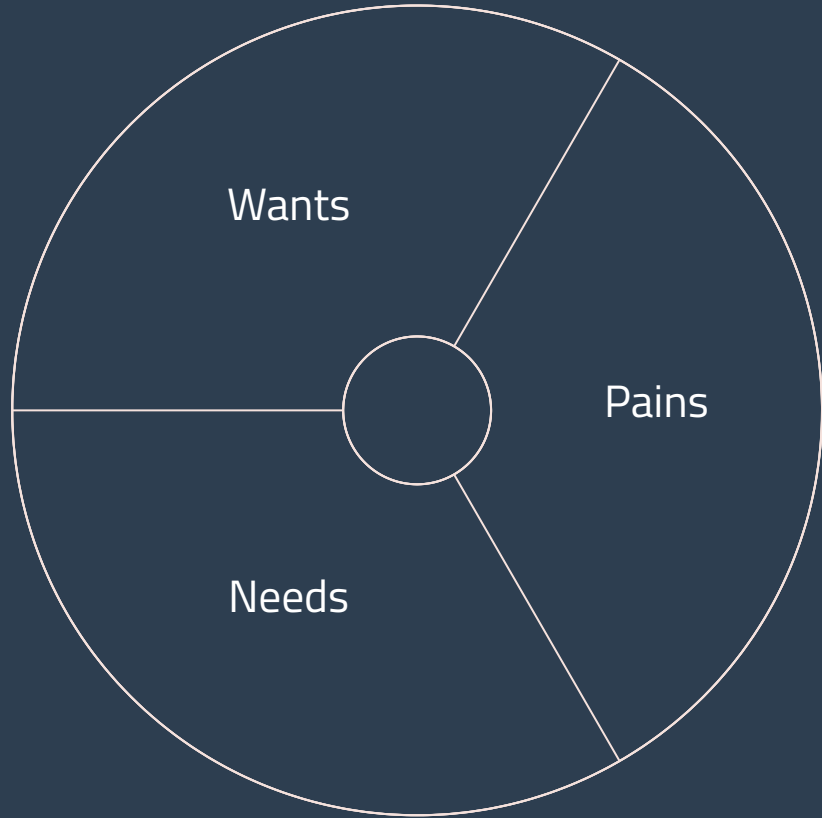
## Enterprise VPN



# Why should I care about Web3?

*"What is my return on investment?"*

# Business Blockchain Application



## ROI?

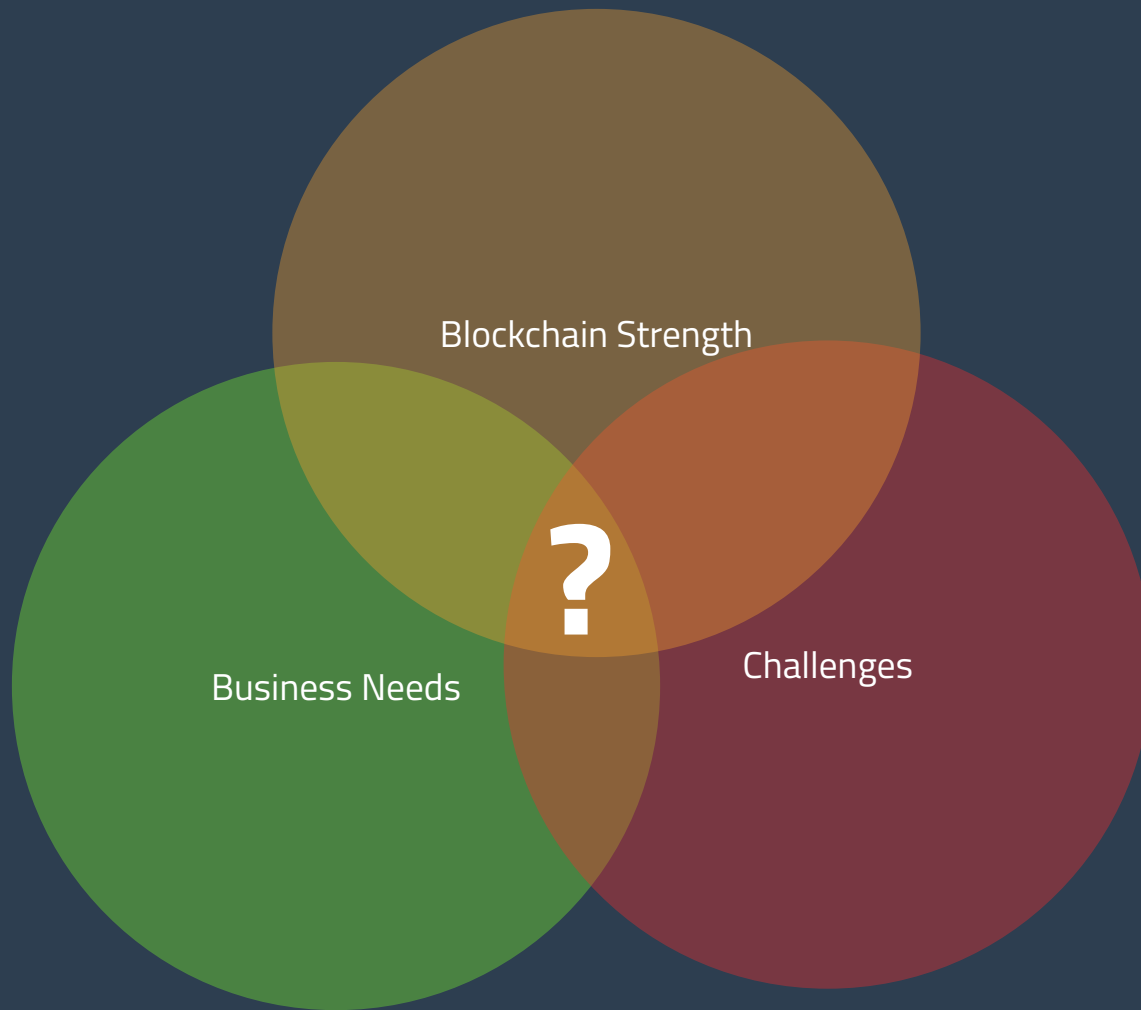
# Use Cases

## IoT

- Automotive
- AR/VR
- Smart Watches, Fitness Trackers
- M2M (Industrial IoT)
- Supply Chains
- Drones
- Smart Cities
- Healthcare

## Blockchain

- Digital Identity
- Supply Chain
- Voting
- Fundraising
- Notary
- Food Safety
- Intellectual Property
- DeFi
  - Flash Loans
  - Exchanges
  - ...



# WEB3 SECURITY



Uber

Uber  @Uber · 3m

Due to Covid-19, we are giving back over \$10,000,000 in Bitcoin!



Jeff Bezos   
@JeffBezos

I have decided to give back to my community.

All Bitcoin sent to m  
doubled. I am only c

bc1qxy2kgdygjrqtz

Enjoy!

5:07 PM · Jul 15, 2020 · Twitter

1.4K Retweets and comments



Joe Biden   
@JoeBiden

I am giving back to the community.

All Bitcoin sent to the address below will  
doubled! If you send \$1,000, I will send  
Only doing this for 30 minutes.

bc1qxy2kgdygjrqtzq2n0yrf2493p83kk



Bill Gates   
@BillGates

Everyone is  
time.

I am doub!  
the next 3  
\$2,000.



Apple  @Apple · 35s

We are giving back to our community. We support Bitcoin and we believe  
you should too!

All Bitcoin sent to our address below will be sent back to you doubled!



Barack Obama   
@BarackObama

I am giving back to

All Bitcoin sent to my address  
doubled. If you send \$1,000, I will send

Only doing this for the next 30 minutes

2:35 PM · Jul 15, 2020 · Twitter Web App



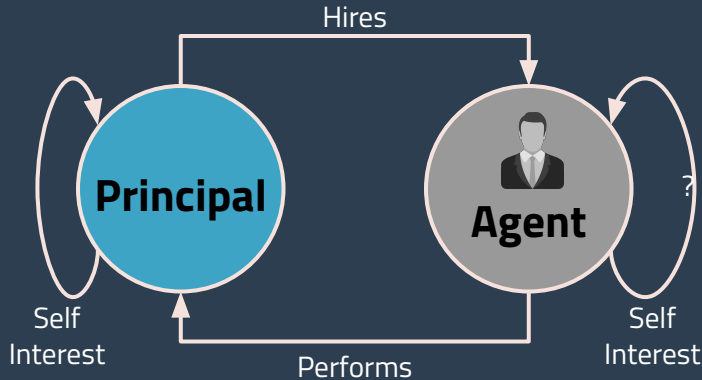
Elon Musk   
@elonmusk


I'm feeling generous because of Covid-19.

I'll double any BTC payment sent to my BTC address for  
the next hour. Good luck, and stay safe out there!

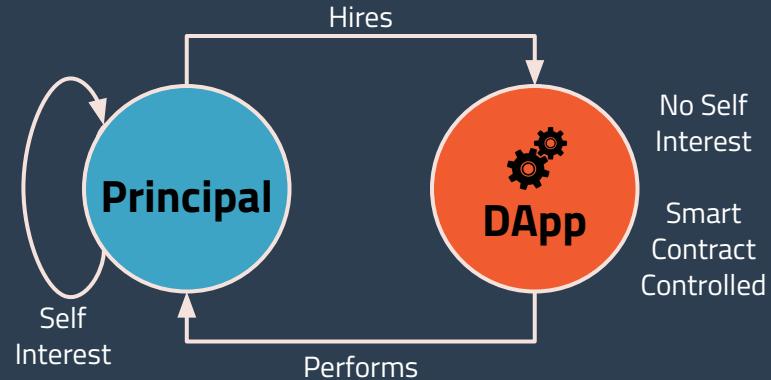
# The Principal-Agent Problem

Web2



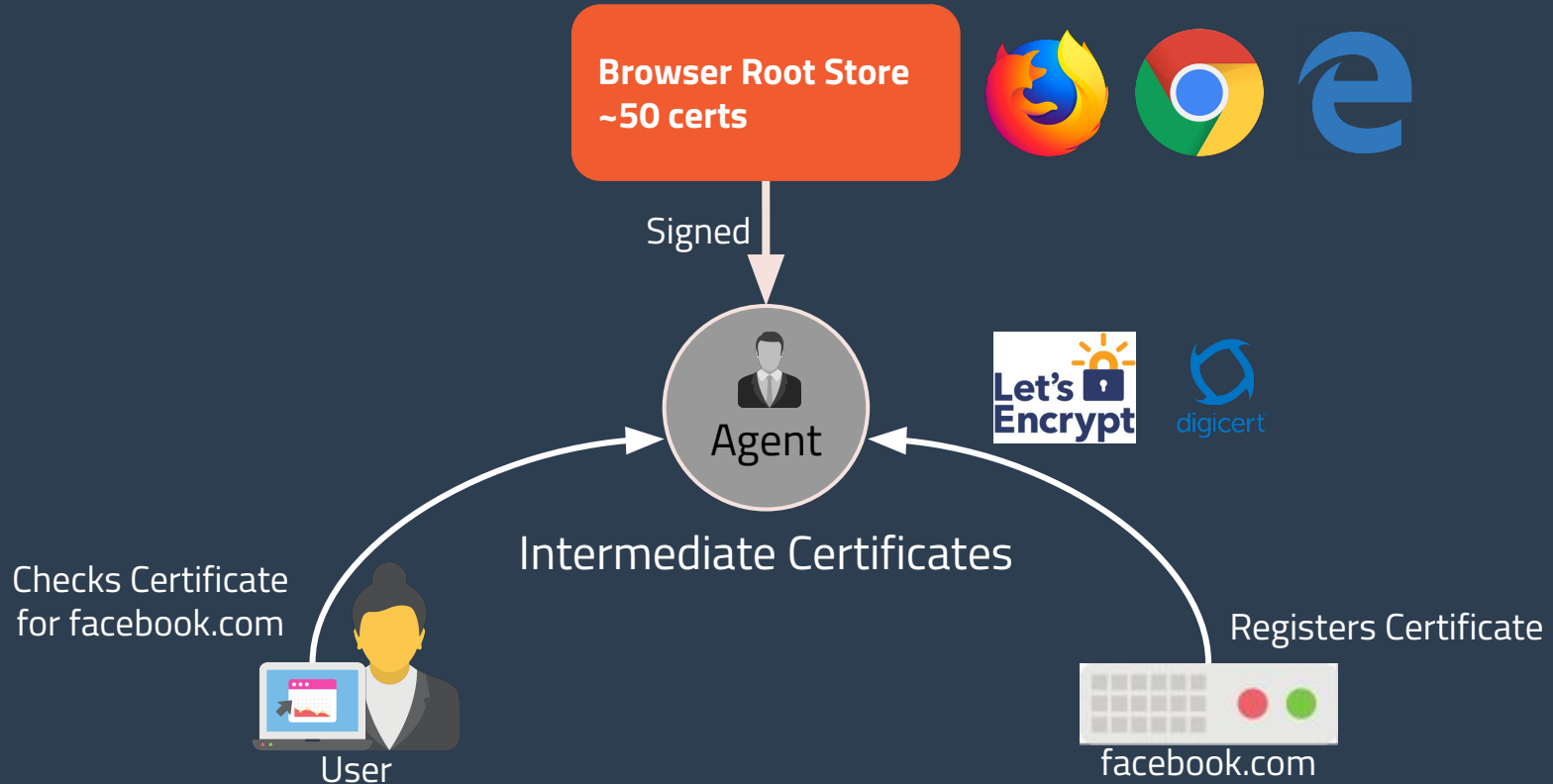
E.g.  **Dropbox** "Platform" is the **Dropbox, Inc.:** employees, **hidden** information, **hidden** data, it's own compliance rules and budget.

 **Diode**  
Web3



Diode is a **public blockchain** owned by nobody, driven by **auditable smart contracts**. Guaranteed to behave as agreed.

# Principal-Agent In PKI

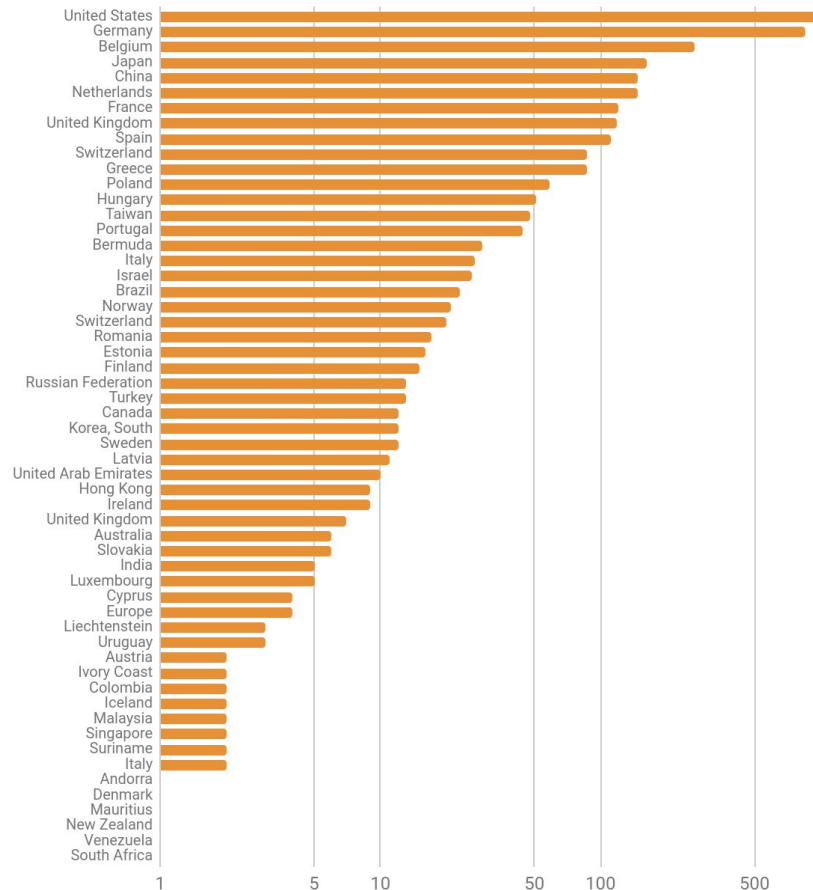


# Interm. Certificate Authorities



Координационный центр  
национального домена сети Интернет

>3000 entries



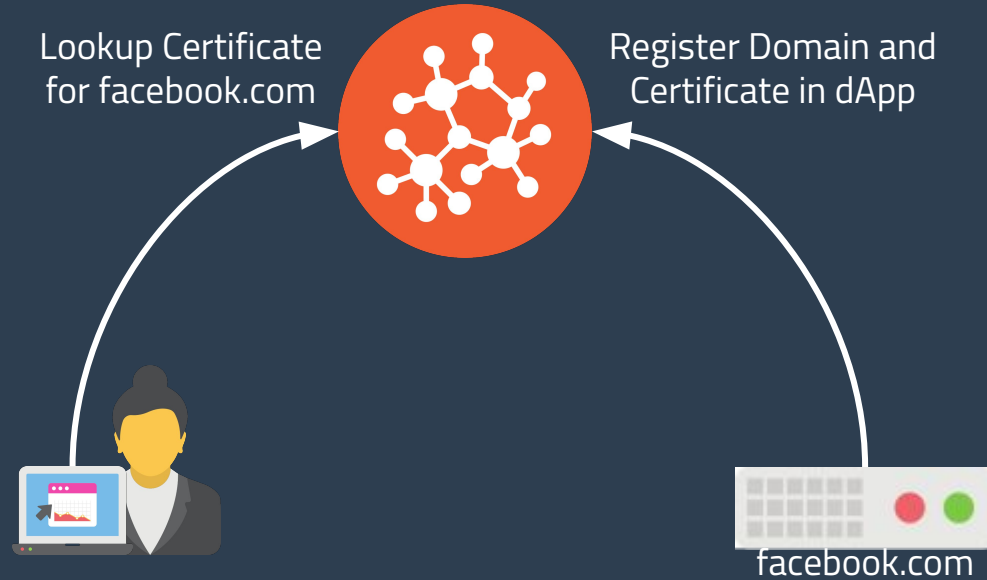
# When Indirect Trust Fails

6308	9198	9198	2019-07-17 12:43
Majority Record			
CN	*.facebook.com		
O	Facebook, Inc.		
C	US		
Not Before	2019-06-06T00:00:00Z		
Not After	2019-09-04T12:00:00Z		
SHA1	C5:22:F1:15:F8:B2:AD:AE:12:63:BC:8D:5F:A7:B		
MD5	EC:B8:53:F1:12:34:C8:35:22:23:F5:78:3F:4E:A6		
subjectAltName	*.facebook.com messenger.com *.fbcdn.net *.fb.com *.m.facebook.com fb.com *.facebook.net *.xx.fbcdn.net *.xz.fbcdn.net *.messenger.com *.fbstatic.com *.xy.fbcdn.net facebook.com		
▼			
CN	DigiCert SHA2 High Assurance Server CA		
O	DigiCert Inc		
C	US		
Not	2013-10-22T12:00:00Z		

No	Time	Name *
This Record		
CN	*.facebook.com	
O	Facebook, Inc.	
C	US	
Not Before	2019-07-16T12:39:52Z	
Not After	2020-07-15T12:39:52Z	
SHA1	5F:55:F8:28:2C:9B:AA:79:0A:5C:C2:76:CD:D7:81:7C:BC:	
MD5	F6:9F:EF:F3:07:84:D1:D4:F2:48:6A:FA:58:C3:F2:FA	
subjectAltName	*.facebook.com messenger.com *.fbcdn.net *.fb.com *.m.facebook.com fb.com *.facebook.net *.xx.fbcdn.net *.xz.fbcdn.net *.messenger.com *.fbstatic.com *.xy.fbcdn.net facebook.com	
▼		
CN	Security Certificate	
O	No data	
C	KZ	
Not	2018-02-12T06:36:56Z	

# DPKI

## Trust By Consensus



Man-In-The-Middle attacks become impossible

# Decentralization: Business Case

- More Secure, Easier to be Compliant. Trust into Agents can often be replaced with Smart Contracts
- Reduced cost, because the Agent is disintermediated

# IoT Device Boot



## 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

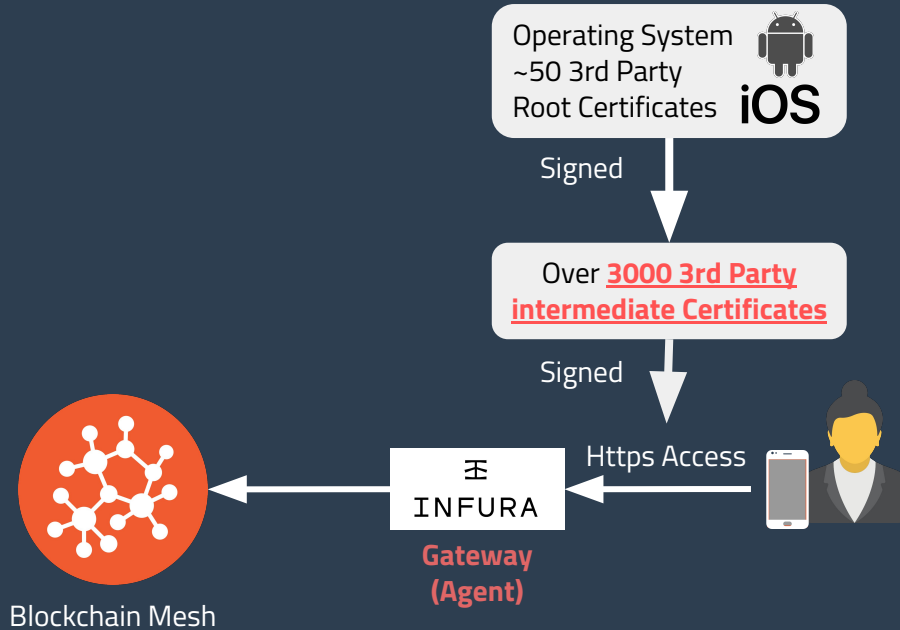
getting secure timestamp

fetching contract state &  
merkle proofing



# Traditional Web3 Gateway

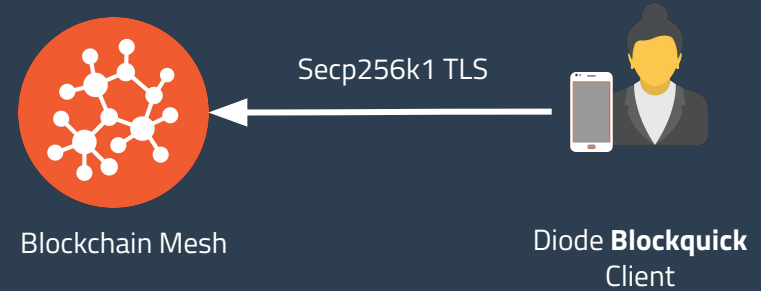
Because of complex validation  
Is still insecure



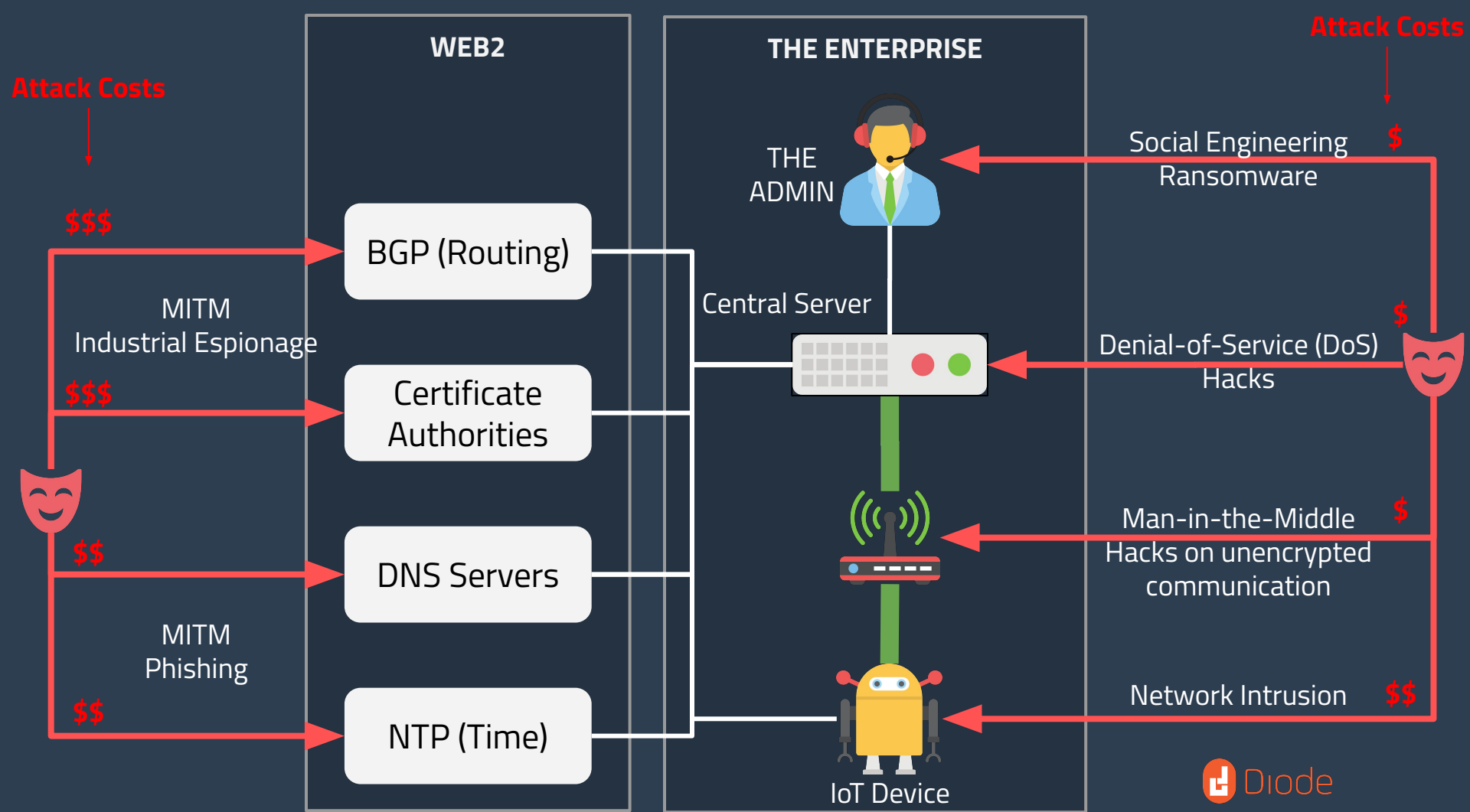
1. Https Certificate Management required
2. 3,000 3rd party orgs can intercept traffic
3. Single failure of **Gateway** is catastrophic

# Diode BlockQuick

100% Decentralized



1. No-Ops
2. Interception (MITM) impossible.
3. 51% Failure resistance.



372

2.157

6.828



**Twitter Support** ✓ @TwitterSupport · 16. Juli

Our investigation is still ongoing but here's what we know so far:

484

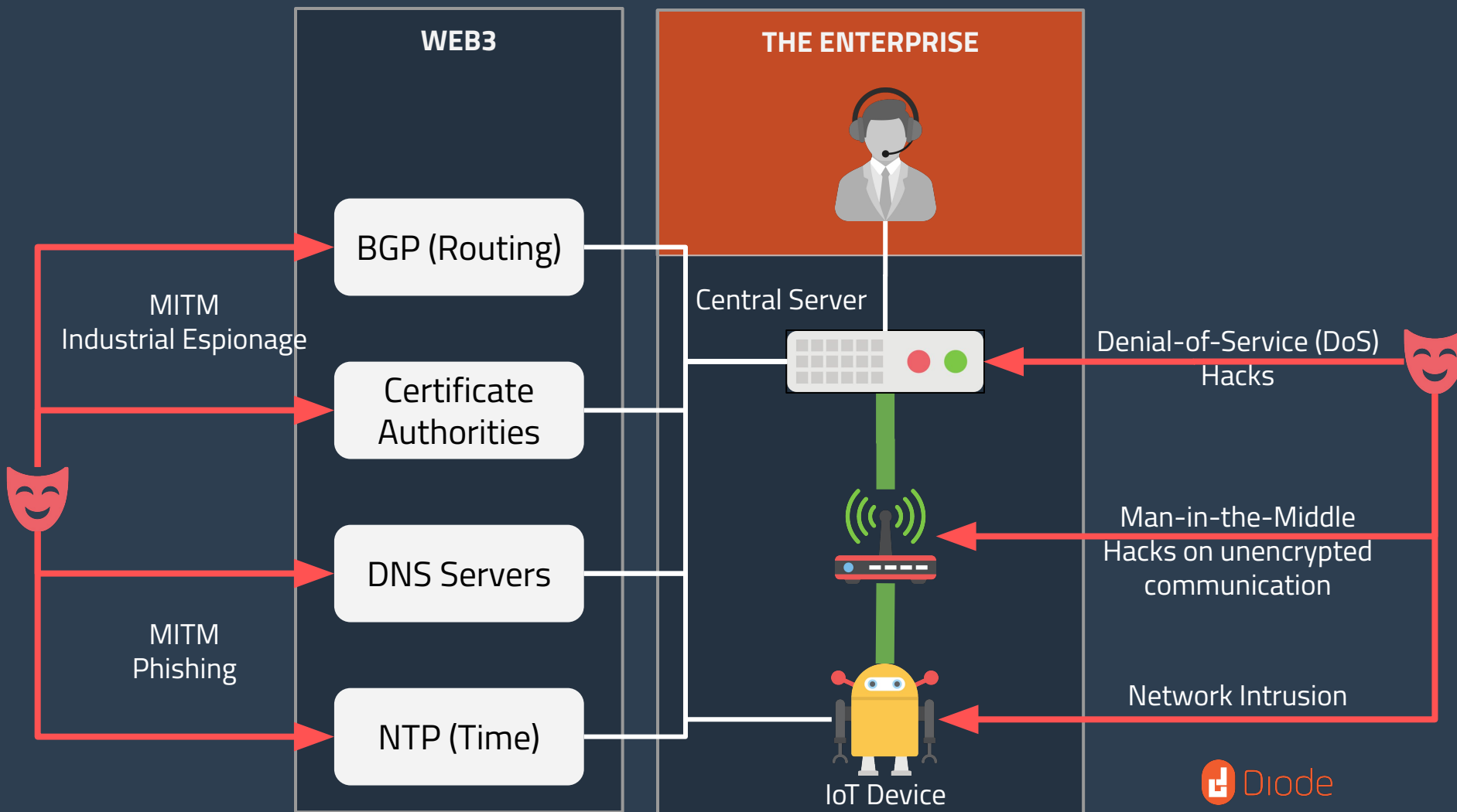
4.214

8.790



**Twitter Support** ✓ @TwitterSupport · 16. Juli

We detected what we believe to be a coordinated **social engineering** attack by people who successfully targeted some of our employees with access to internal systems and tools.



# Garmin

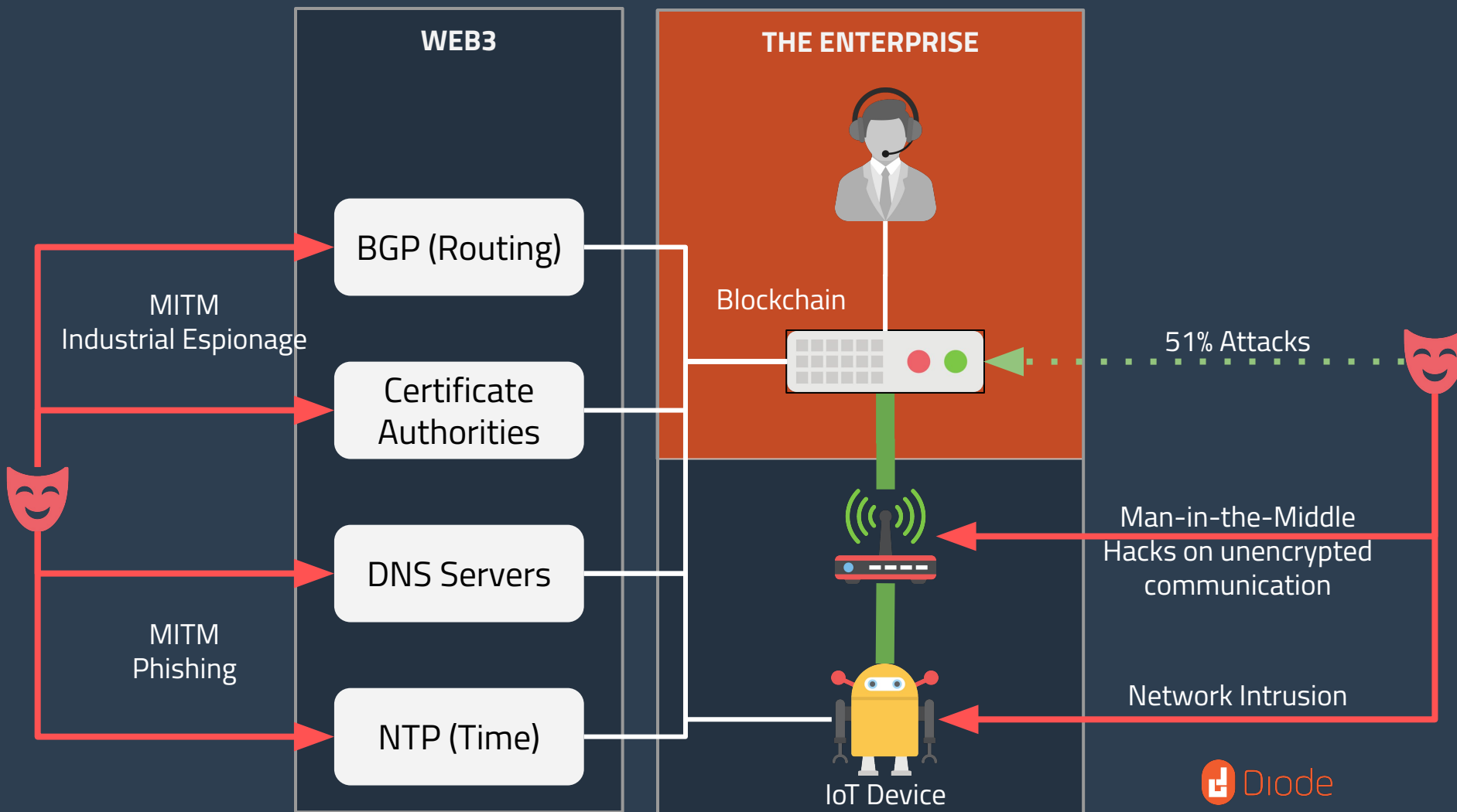
The screenshot shows the 'connect.garmin.com/status/' page. At the top, the 'connect' logo is on the left and 'Get' is on the right. The main content area has a title 'Current Status at 5:16:54 PM GMT+2' and a message: 'We are currently experiencing an outage that affects Garmin.com and Garmin Connect. We are currently unable to receive any calls, emails or online chats. We are working to resolve this as quickly as possible to minimize inconvenience.' Below this is a list of services, each with a red 'DOWN' button and the service name: ActivityDetails, ActivityUploads, Challenges, Connections, Courses, DailySummary, DeviceRegistration, GearTracking, Leaderboards, ModernDashboard, MyFitnessPal, PushAPI(ThirdParties), Reports, SegmentMatching, SleepSync, StepSync, and Status.

connect Get

Current Status at 5:16:54 PM GMT+2

We are currently experiencing an outage that affects Garmin.com and Garmin Connect. We are currently unable to receive any calls, emails or online chats. We are working to resolve this as quickly as possible to minimize inconvenience.

- DOWN** ActivityDetails
- DOWN** ActivityUploads
- DOWN** Challenges
- DOWN** Connections
- DOWN** Courses
- DOWN** DailySummary
- DOWN** DeviceRegistration
- DOWN** GearTracking
- DOWN** Leaderboards
- DOWN** ModernDashboard
- DOWN** MyFitnessPal
- DOWN** PushAPI(ThirdParties)
- DOWN** Reports
- DOWN** SegmentMatching
- DOWN** SleepSync
- DOWN** StepSync
- DOWN** Status



# 2019

https://www.bbc.com/news/technology-48770128



iod

## Second US town pays up to ransomware hackers

26 June 2019



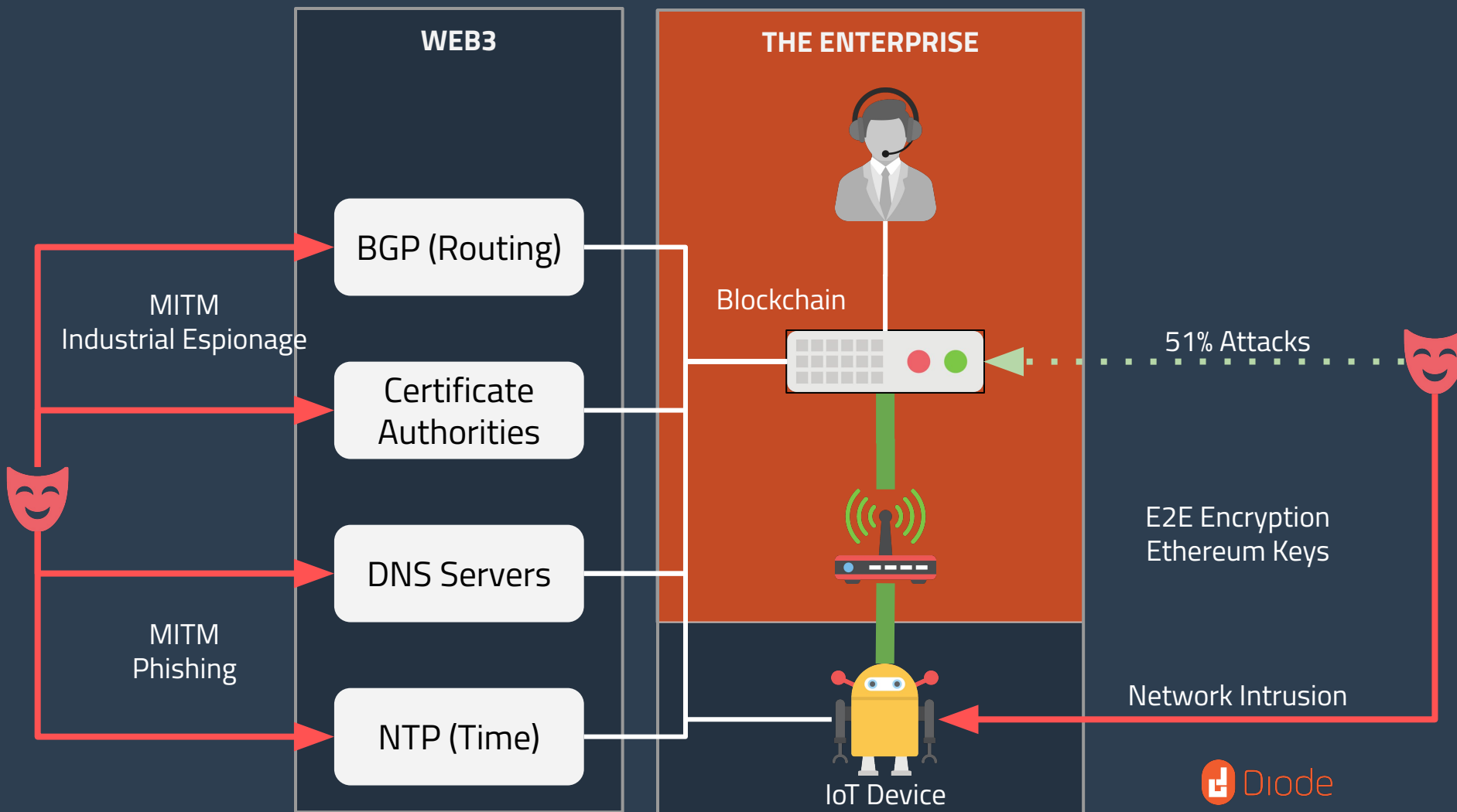
## 22 Texas towns hit by coordinated ransomware attack

POLICY TECH CYBERSECURITY

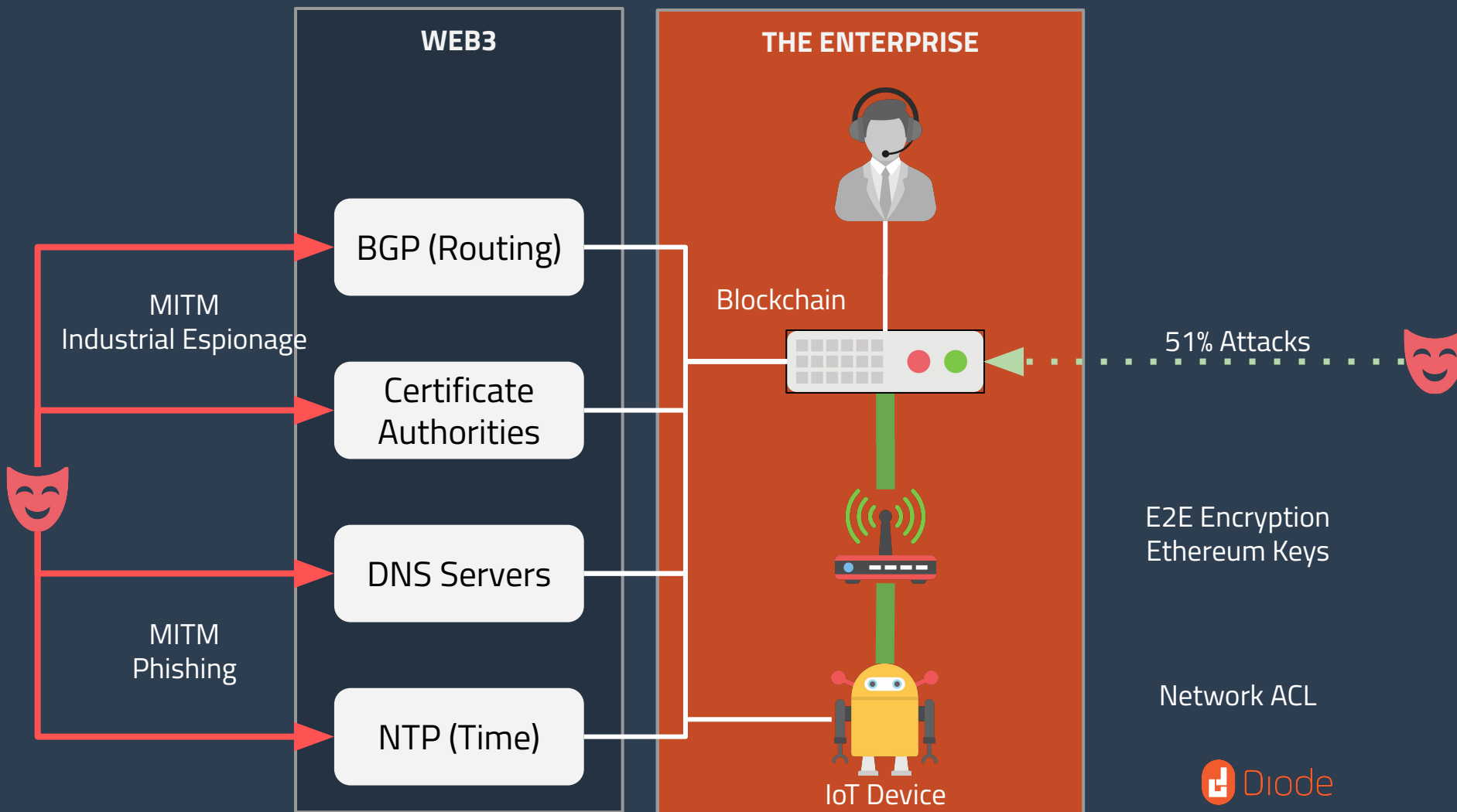
*The latest of several recent ransomware attacks on US municipalities*

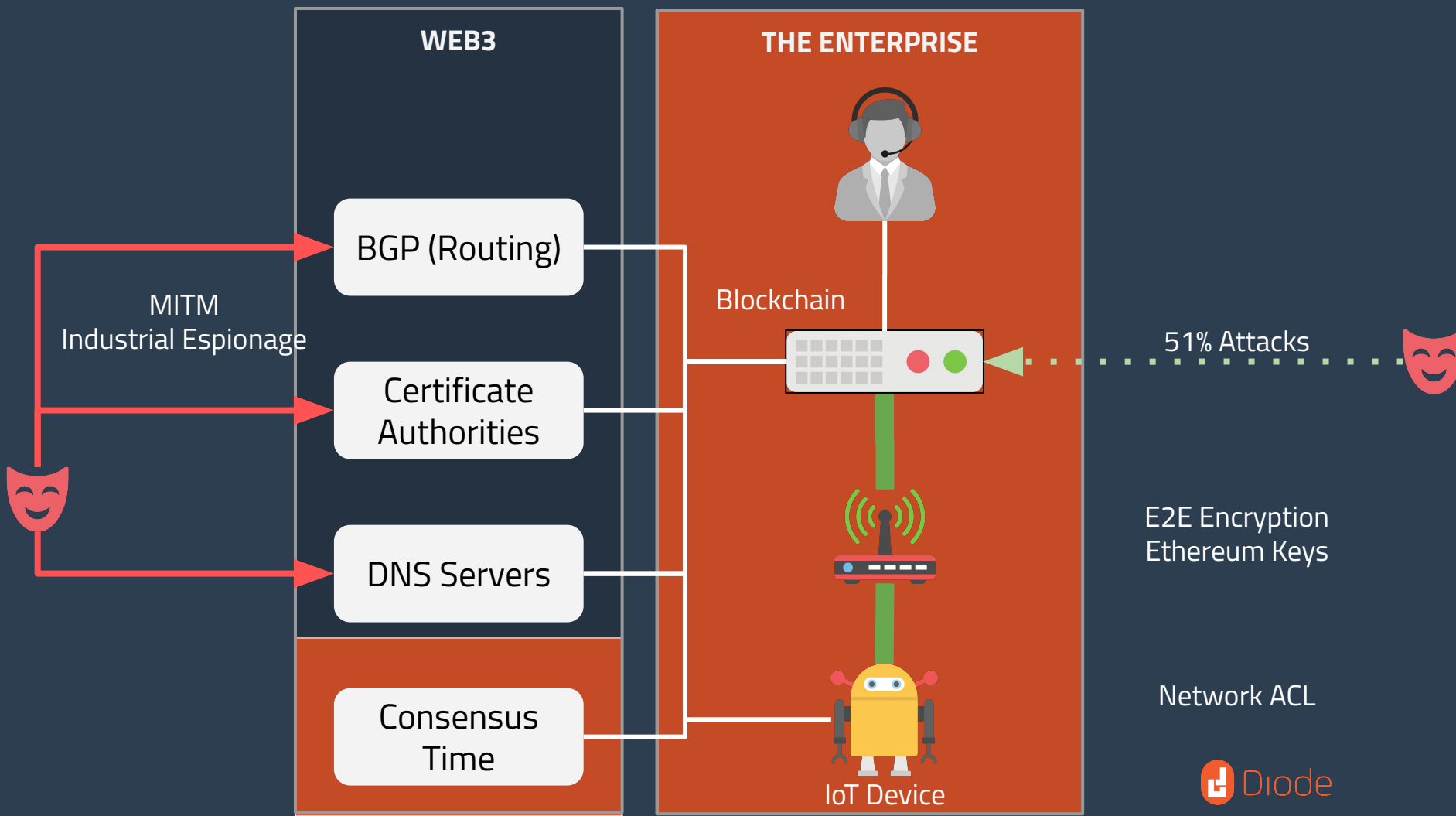
By Jay Peters | Aug 20, 2019, 3:55pm EDT

- July 25, 2019: City Power, the electric utility for Johannesburg, South Africa, discloses ransomware attack.
- June 26, 2019: Lake City, Florida agrees to pay ransomware.
- June 20, 2019: Riviera Beach, Florida, discloses ransomware attack and payment.
- May 7, 2019: City of Baltimore hit with ransomware attack.
- April 2019: Cleveland Hopkins International Airport suffered a ransomware attack.
- April 2019: Augusta, Maine, suffered a highly targeted malware attack that froze the city's entire network and forced the city center to close.
- April 2019: Hackers stole roughly \$498,000 from the city of Tallahassee.
- March 2019: Albany, New York, suffered a ransomware attack.
- March 2019: Jackson County, Georgia officials paid cybercriminals \$400,000 after a cyberattack shut down the county's computer systems.
- March 2018: Atlanta, Georgia suffered a major ransomware attack.
- February 2018: Colorado Department of Transportation (CDOT) employee computers temporarily were shut down due to a SamSam ransomware virus cyberattack.



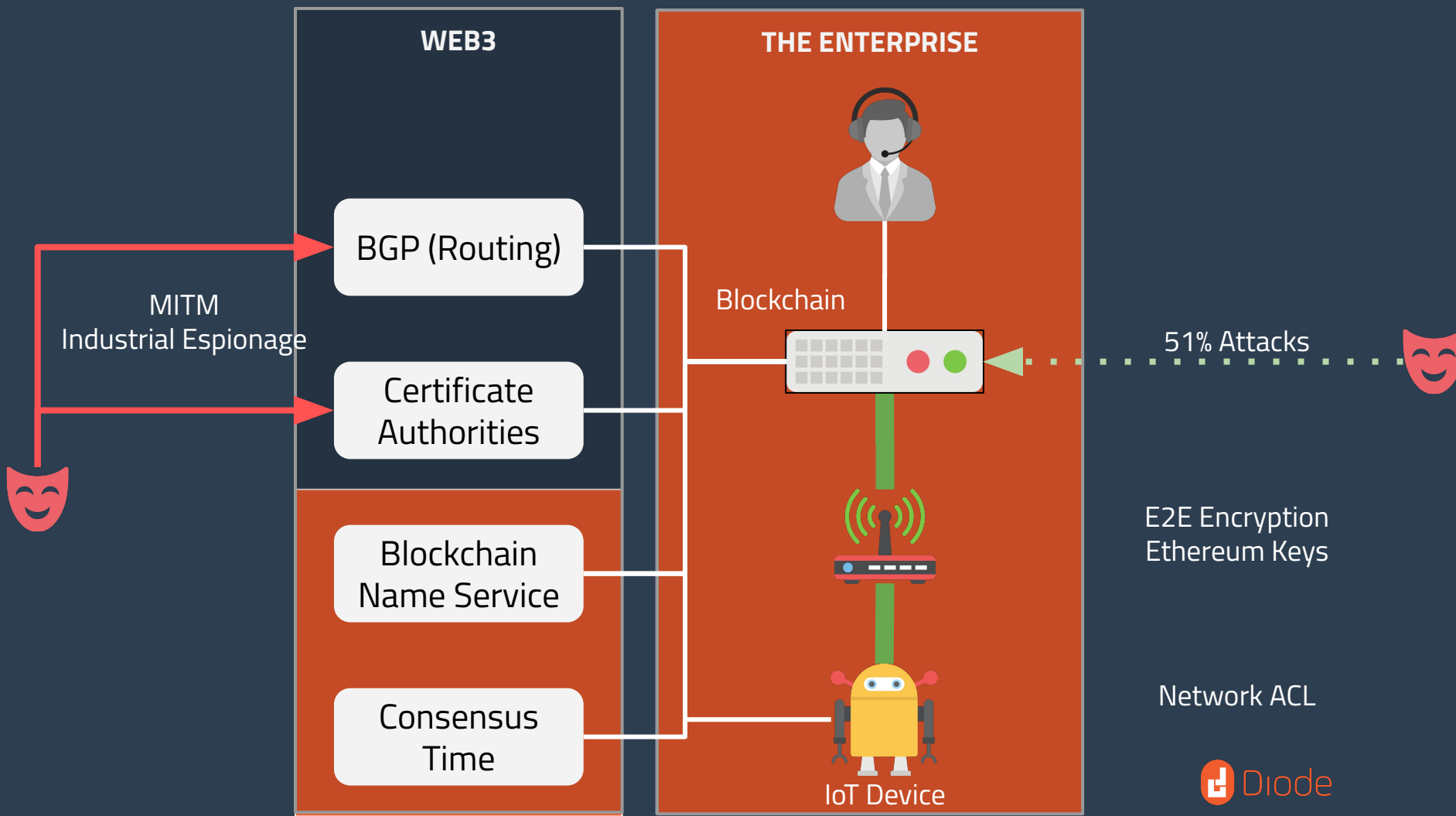






# Time is required for Certificates

*.zoom.us	DigiCert SHA2 Secure Server CA	DigiCert Global Root CA
<b>Subject Name</b> _____		
<b>Country</b> US		
<b>State/Province</b> California		
<b>Locality</b> San Jose		
<b>Organization</b> Zoom Video Communications, Inc.		
<b>Common Name</b> *.zoom.us		
<b>Issuer Name</b> _____		
<b>Country</b> US		
<b>Organization</b> DigiCert Inc		
<b>Common Name</b> DigiCert SHA2 Secure Server CA		
<b>Validity</b> _____		
<b>Not Before</b> 5/24/2020, 2:00:00 AM (Central European Summer Time)		
<b>Not After</b> 6/1/2022, 2:00:00 PM (Central European Summer Time)		
<b>Subject Alt Names</b> _____		
<b>DNS Name</b> *.zoom.us		
<b>DNS Name</b> zoom.us		
<b>Public Key Info</b> _____		
<b>Algorithm</b> RSA		
<b>Key Size</b> 2048		
<b>Exponent</b> 65537		
<b>Modulus</b> F8:90:32:FF:BC:A0:C8:E1:A5:E0:C6:B5:5F:B5:B0:9D:58:89:83:7A:5E:30:88:6E:CE:C3:88:24:3E:74:EA:4F:8F:54:88:...		
<b>Miscellaneous</b> _____		
<b>Serial Number</b> 08:83:EA:80:A4:04:9E:C3:73:4A:74:D7:D1:E6:8F:D5		
<b>Signature Algorithm</b> SHA-256 with RSA Encryption		
<b>Version</b> 3		
<b>Download</b> PEM (cert) PEM (chain)		



# Brazilian banking customers targeted by IoT DNS hijacking attacks

Aug 15, 2018

NEWS by [Robert Abel](#)

A DNS hijacking campaign has been discovered targeting Banco de Brasil and Itau Unibanco customer credentials through the end-user IoT devices.

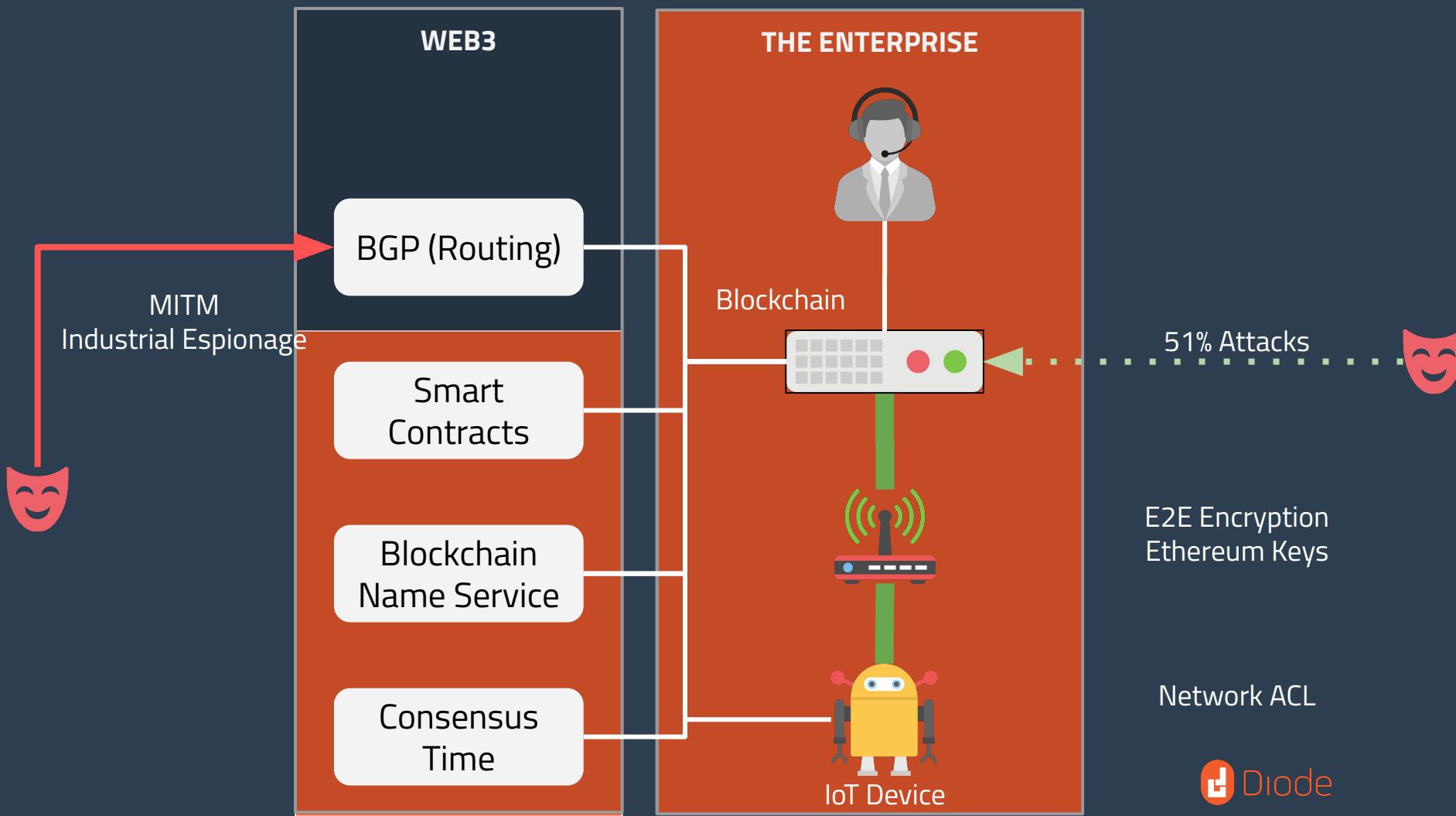


A DNS hijacking campaign has been discovered targeting Banco de Brasil and Itau Unibanco customer credentials through the end-user IoT devices.

Radware researchers said this is the first time modems and routers have been remotely exploited for performing DNS hijacking and as a result of the compromise any device with internet access in the home of an affected user is prone to be redirected to the fake websites, according to an 10 August [advisory](#) from the firm.

All the while, the user is completely unaware of the change since the hijacking works without crafting or changing URLs in the user's browser.

The attack redirects users seeking popular financial site, such as those used to pay a bill or check a bank statement, to a phishing site instead. Researchers said the malicious DNS server controlling the attacks effectively becomes the middleman that provides the malicious actor with the flexibility to bring up fake portals and web fronts to collect sensitive information from users whose routers were infected.



## WEB3

## THE ENTERPRISE

BGP not yet solved but  
data is secured through  
E2E Encryption with  
Ethereum Keys

\$\$\$\$

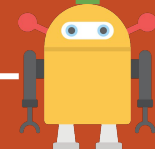
BGP (Routing)

Fleet  
Contracts

Blockchain  
Name Service

Consensus  
Time

Blockchain



IoT Device

51% Attacks \$\$\$\$



E2E Encryption  
Ethereum Keys

Network ACL

# China Telecom's Internet Traffic Misdirection

Routing leak sent US domestic traffic through China



## Traffic misdirection by AS4134

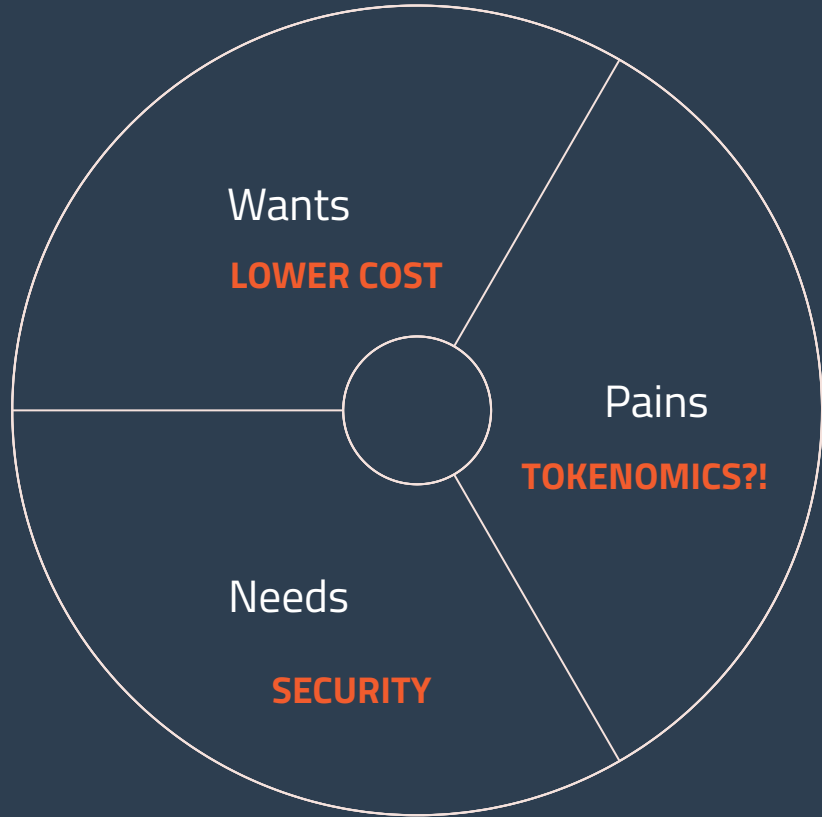
On 9 December 2015, SK Broadband (formerly Hanaro) experienced a brief routing leak lasting little more than a minute. During the incident, SK's ASN, AS9318, announced over 300 Verizon routes that were picked up by OpenDNS's BGPstream service:



The background is an abstract composition of various-sized triangles in shades of orange and yellow, creating a dynamic, low-poly geometric pattern.

**SECURITY!**

# Enterprise Blockchain Application



# SECURITY

# Diode Next Steps



Diode Client



Work In Progress



On Roadmap

DNS 3.0

VPN

Blockchain  
SD-WAN

Data  
Storage

Managed  
Certificate  
Chains

Network  
Tunnel

Data  
Broadcast

Desktop  
Client

Websocket  
Translation

Secure  
Time

E2E  
Encryption

Remote  
Access

Fleet  
Access  
Control

Managed  
DNS

Global  
Endpoint  
Publishing

## BlockQuick Security



Diode

# Takeaways

1. Diode are the guys who did BlockQuick
2. We have to decentralize "THE ADMIN"

# Thank You!



<https://diode.io>



[https://t.me/diode\\_chain](https://t.me/diode_chain)



[https://twitter.com/diode\\_chain](https://twitter.com/diode_chain)



<https://www.linkedin.com/company/diode-chain>



[partner@diode.io](mailto:partner@diode.io)

# BACKUP

# Team

Our team consists of IoT and Blockchain experts both with from technology and business backgrounds. We're dedicated to deliver a new level of security to IoT



**DOMINIC  
LETZ**

Chief  
Technology  
Officer



**GREG  
BELCHER**

VP Business  
Development



**HANS  
REMPEL**

CEO



**PETER LAI**

Blockchain  
Security  
Software  
Engineer



**YAH SIN  
HUANG**

Social Media  
Manager