RadicalxChange Taipei

Chapter 2 - Radical Markets

Peter Lai, Blockchain Engineer Diode

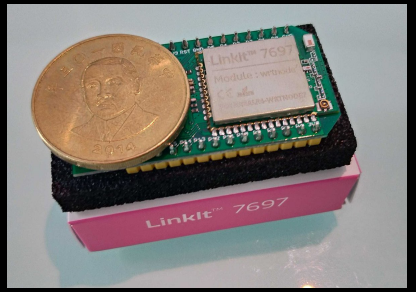
Maicoin HQ, Taipei City, Taiwan

August 6, 2019

About Me

- Blockchain Engineer at Diode.
- Editor of Taipei Ethereum Meetup.
- Open source contributor, eg. wallet, explorer, web3, etc.
- Love to learn new stuff, eg. web assembly.
- Programming languages: JS, GO, PHP, C, PYTHON.
- Twitter: @alk03073135, Github: @sc0vu

What is Diode

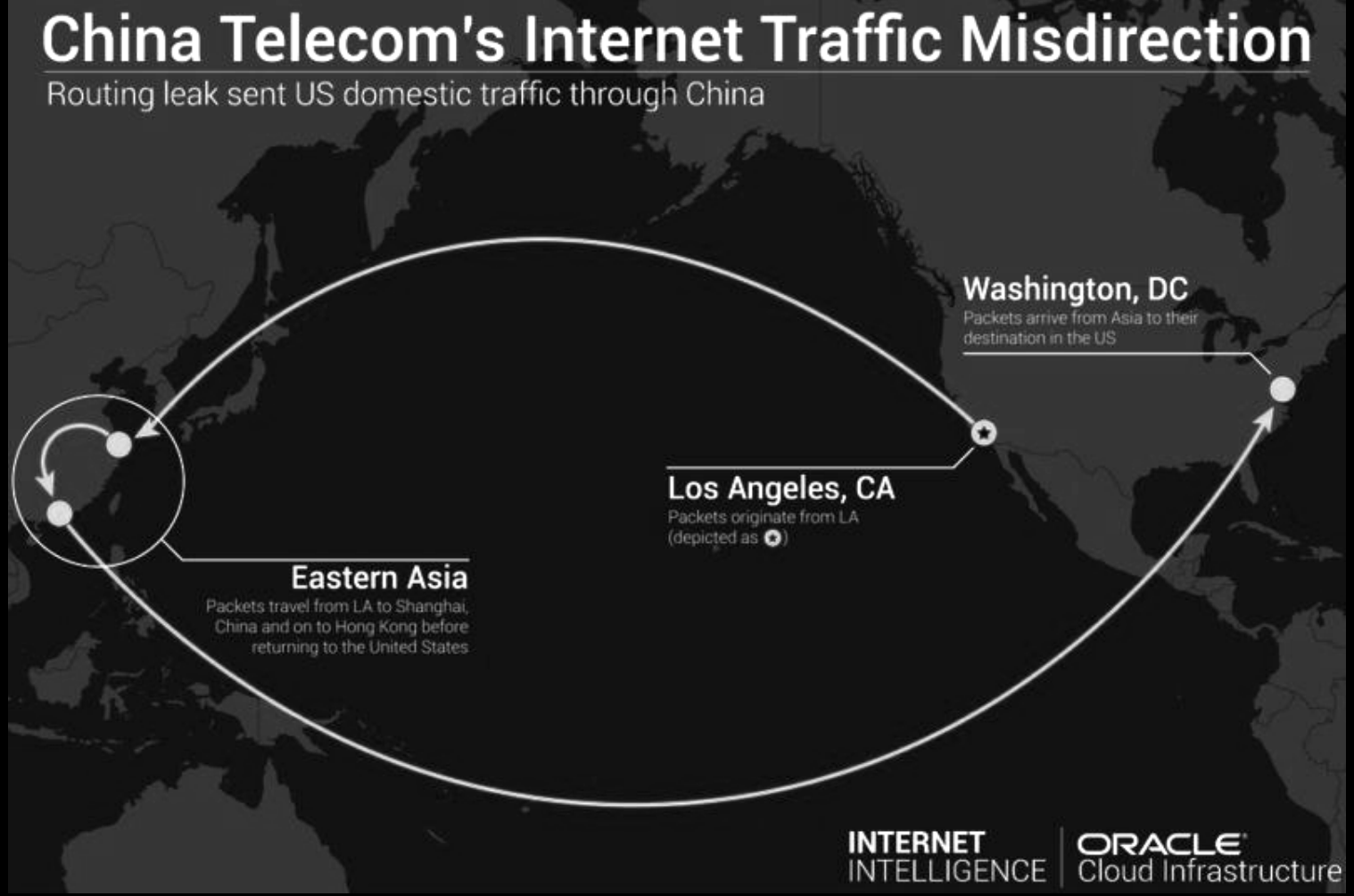


- Decentralized Public Key Infrastructure (PKI)
- Working on BlockQuick implementation
- Twitter: @diode_chain
- Website: https://diode.io

- Member of Ethereum Magicians Ring: Constrained Resource Clients

Today’s Security Problems (reroute)

- On April 8, 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.
- On Jun 6, 2019, Swiss data center colocation company AS21217 leaked over 70,000 routes to China Telecom (AS4134) in Frankfurt, Germany.



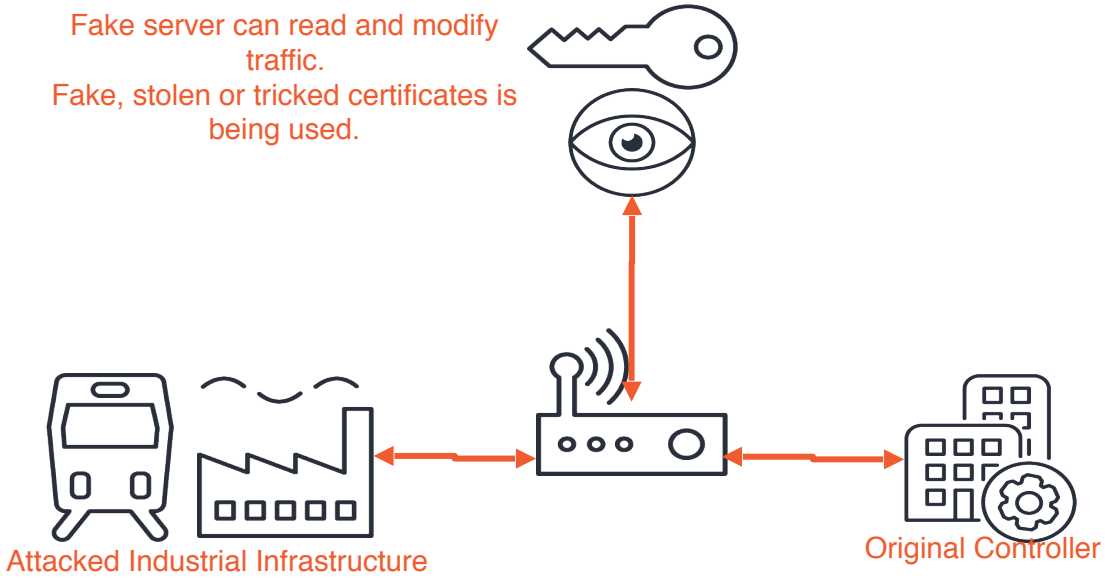
China Telecom's Internet Traffic Misdirection in 2017

Awesome Slide!

y Problems (PKI)

- 7: Hackers of unknown origin take anks 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.
- Spy July 18, 2019: Kazakhstan is forcing its users to install a custom government-issued root certificate on all devices in every browser.

Man in the Middle (MITM)



Solution

Today
Trust By Trusted Roots

Root Store
~50 certs

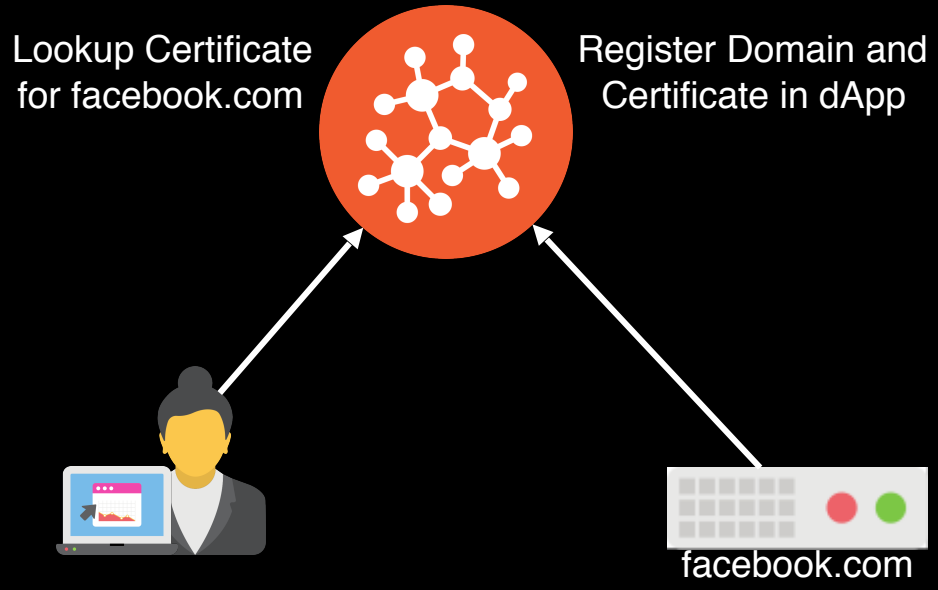
Sign

>3000 interm. certs

Sign

millions of domain certs

Blockchain
Trust By Consensus



MITM becomes impossible, Time problem solved

Origins of Democracy

- Athenian democracy, people had power to pass laws, issue decrees, grant special privileges.

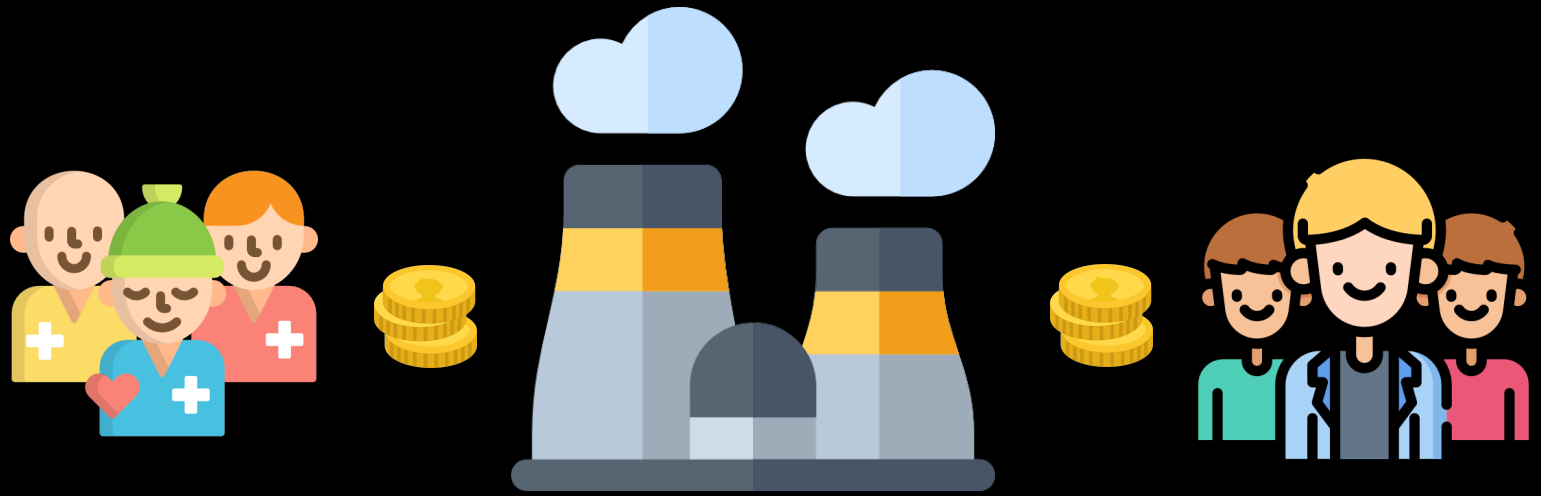
- Only adult male citizens could participate the Assembly.

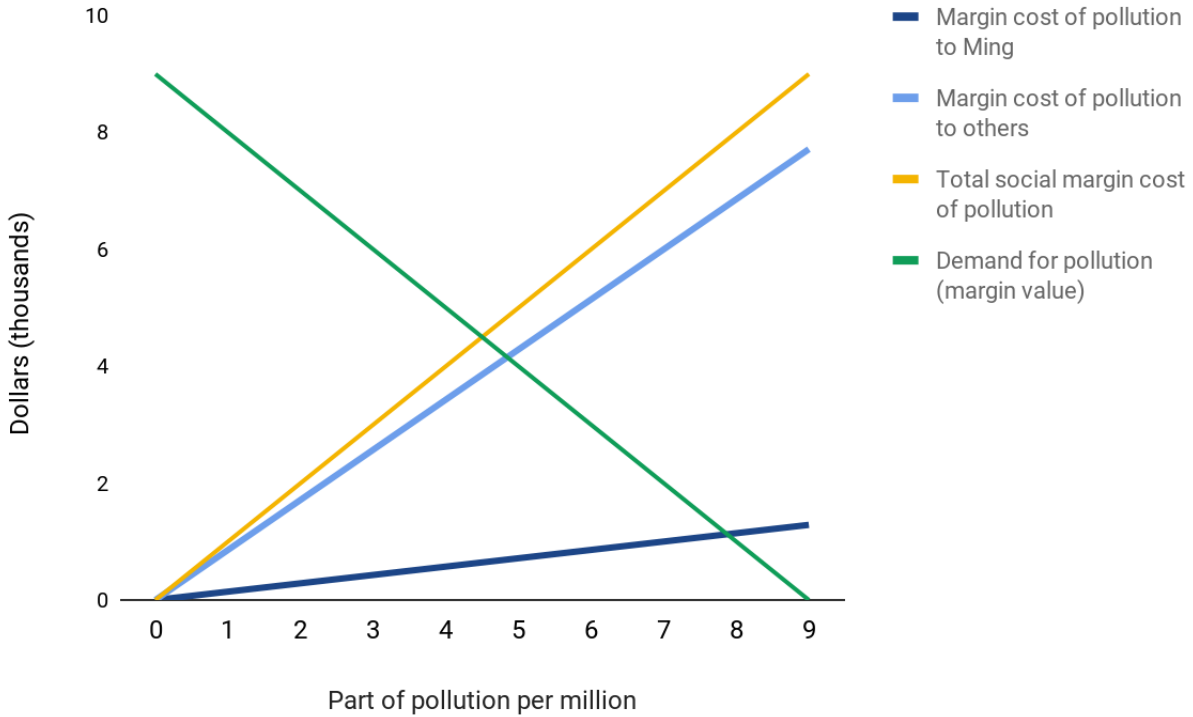
- One person one vote.

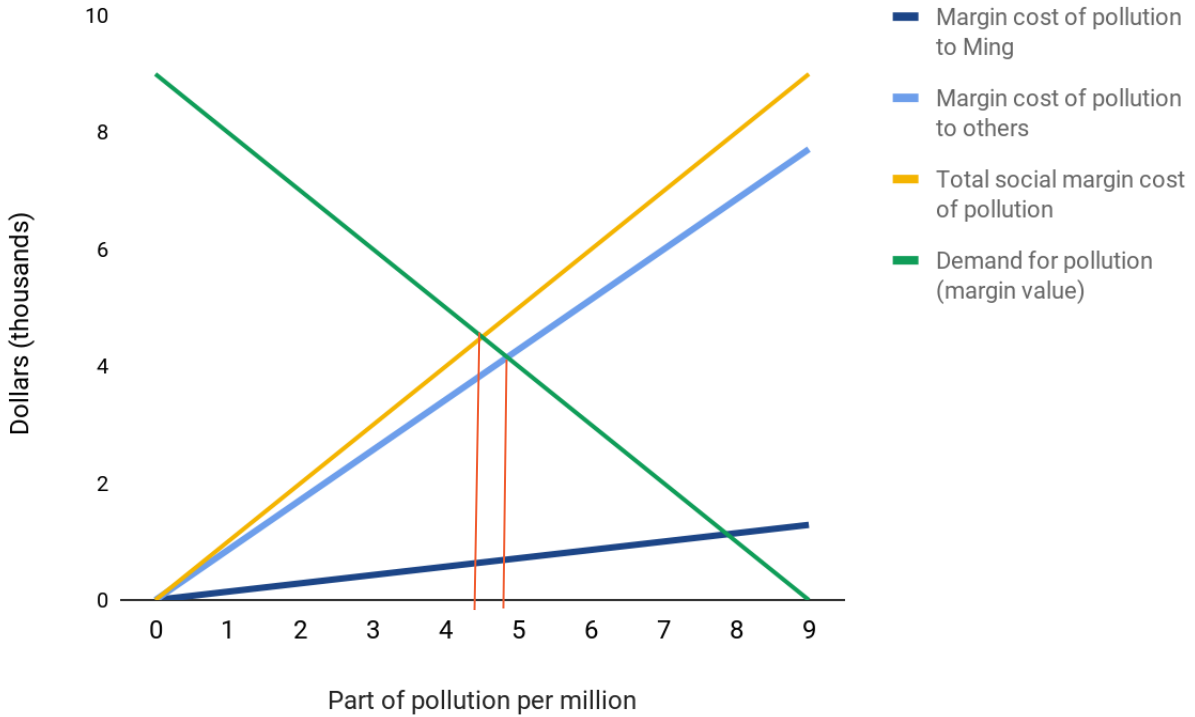
Problems in Athenian Democracy

- Mob rule or majority rule.
- Susceptibility to damagogic leadership.
- If someone is the expertise in the field, there is no difference in voting between than the others because of one person one vote.

Market for Collective Decisions




10
8
6
4
2
0
Dollars (thousands)
0
1
2
3
4
5
6
7
8
9
Part of pollution per million
Margin cost of pollution to Ming
Margin cost of pollution to others
Total social margin cost of pollution
Demand for pollution (margin value)

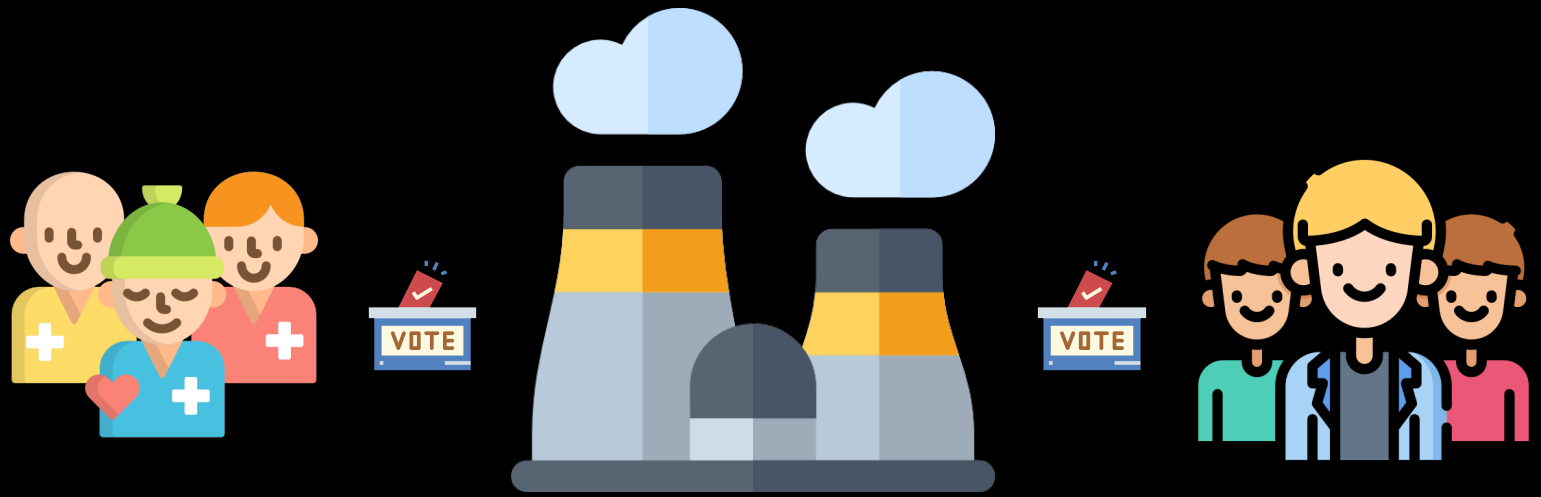

10
8
6
4
2
0
Dollars (thousands)
0
1
2
3
4
5
6
7
8
9
Part of pollution per million
Margin cost of pollution to Ming
Margin cost of pollution to others
Total social margin cost of pollution
Demand for pollution (margin value)

- Ming harms others by preventing them from consuming electricity.

- Ming is requesting the elimination of increasingly beneficial pollution-generating economic activity.

- Ming's cost should grow quadratically like the triangle ( ) instead of linearly in the chart.

Quadratic Voting


VOTE
VOTE

Votes & Cost under QV

Votes	Total cost	Marginal cost
1	1	1
2	4	3
3	9	5
4	16	7
5	25	9
6	36	11
7	49	13

Example - Presidential Hackathon

Select 20 teams out of 100 teams:

- They open up 30% of the entire scoring mechanism to people who have SMS and email authentication to allocate 99 points.

- To avoid people voting everything on the same project (10 votes 100 points).

Show me the code

Source: https://github.com/PDIS/quadratic-voting-frontend/blob/master/js/dvote.js#L91

```
function checkPoint(num) {
    var CostedPoint = 0;
    var Votes = document.getElementsByClassName('nvote');
    for (var index = 0; index < Votes.length; index++) {
        if (index == num) {
            CostedPoint += (parseInt(Votes[index].value)+1) * (parseInt(Votes[index].value)+1);
            continue;
        }

        CostedPoint += parseInt(Votes[index].value) * parseInt(Votes[index].value);
    }
    if (leftPoint - CostedPoint < 0) return false;
    else return true;
}
```

Thank you

Follow us on Twitter

- RadicalxChange Taipei: @rxctaipei
- Diode: @diode_chain
- Me: @alk03073135

Follow us on Github

- RadicalxChange Taipei: @radicalxchange-taipei
- Diode: @exosite
- Me: @sc0vu

Q&A