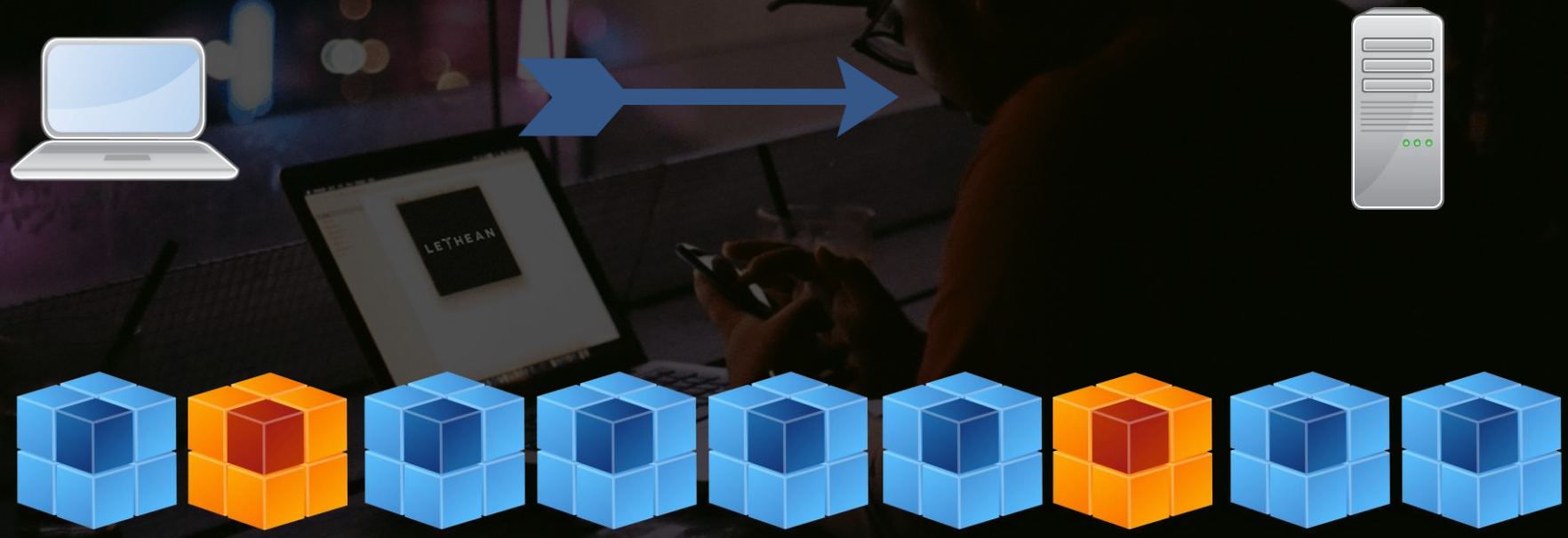
Securing and Monitoring Blockchain Systems with Zabbix

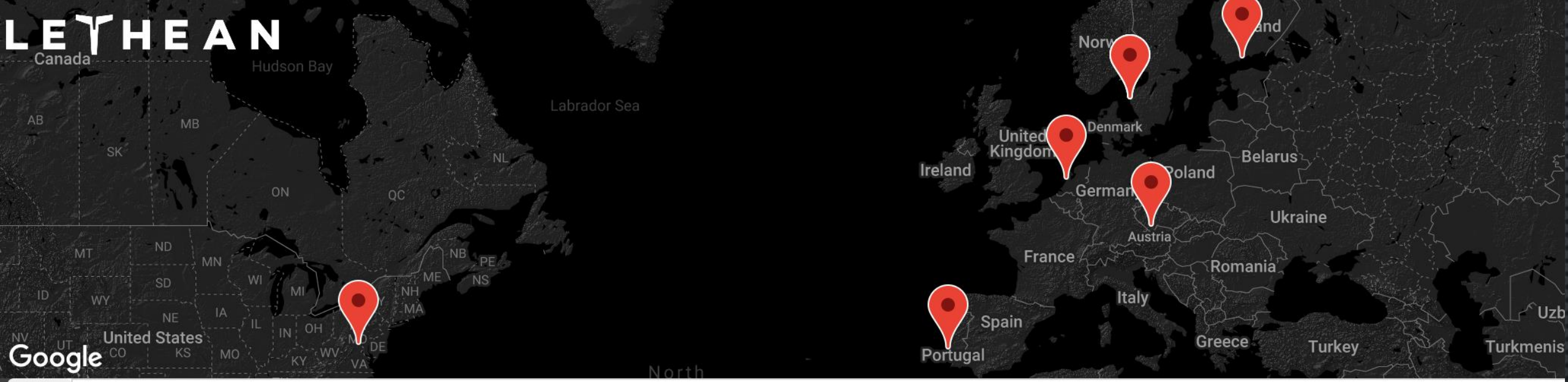
Lukas Macura

CTO @ Foresight Cyber & developer @Lethean project

LETHEAN – THE SAFEST WAY TO BE ONLINE
A VPN PLATFORM WITH BLOCKCHAIN



HTTPS://LETHEAN.IO/



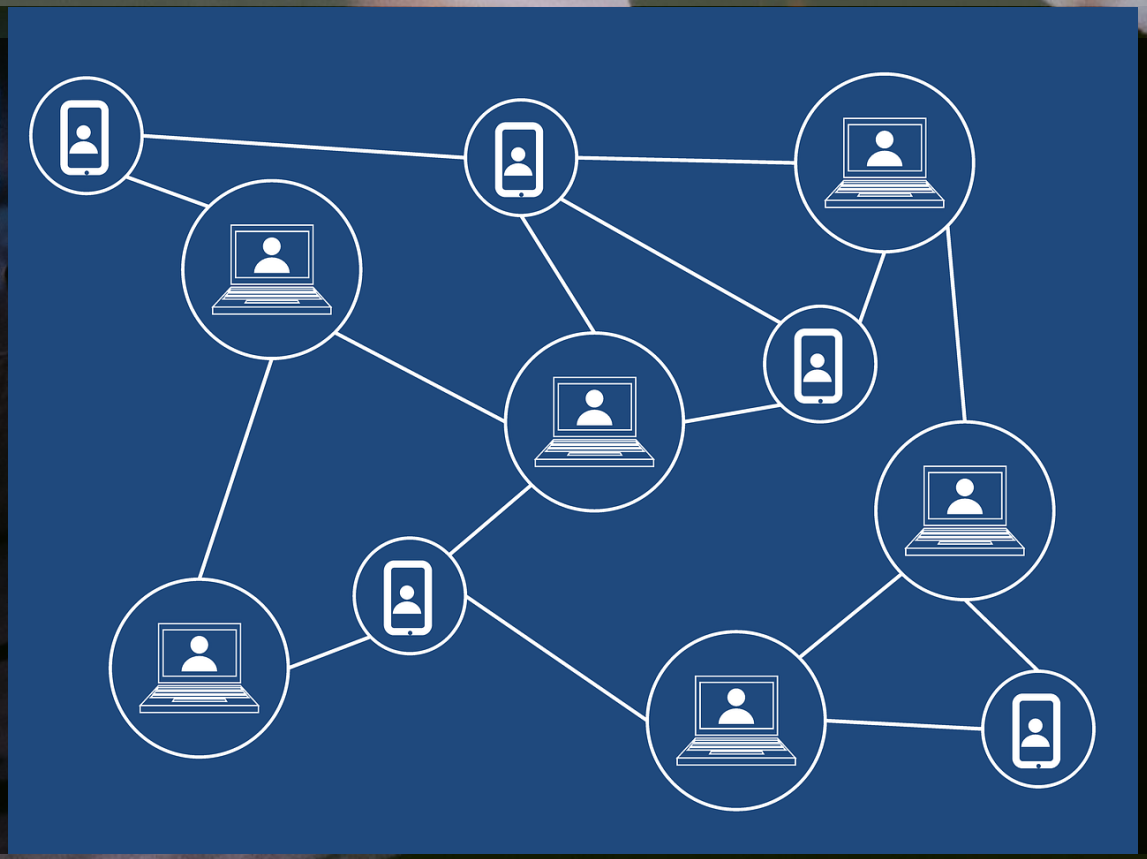
Type to search...

Rating	Provider	Location	Speed (Down/Up)MB/s
5 of 5	**Lethernet.com** Lethernet.com NL01	Haarlem, Netherlands (EU) nl01.lethernet.com:8080/TCP (proxy)	2.00 Mbps / 2.00 Mbps
0 of 5	**Test** Test	Helsinki, Finland (EU) 95.216.160.70:8888/TCP (proxy)	1 bps / 1 bps
4.8 of 5	**ITNSTest** ProxyDev	?eské Bud?jovice, Czechia (EU) monitor.intensecoin.com:20006/TCP (proxy)	5 bps / 5 bps

MESSAGE FROM THE PROJECT FOUNDER

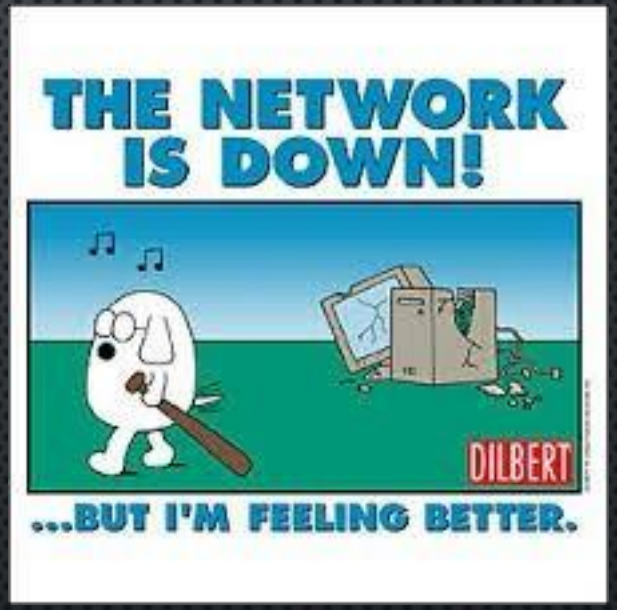

Vailiant
founder, Lethean project

BLOCKCHAIN – WHAT IS IT?



WHAT TO MONITOR

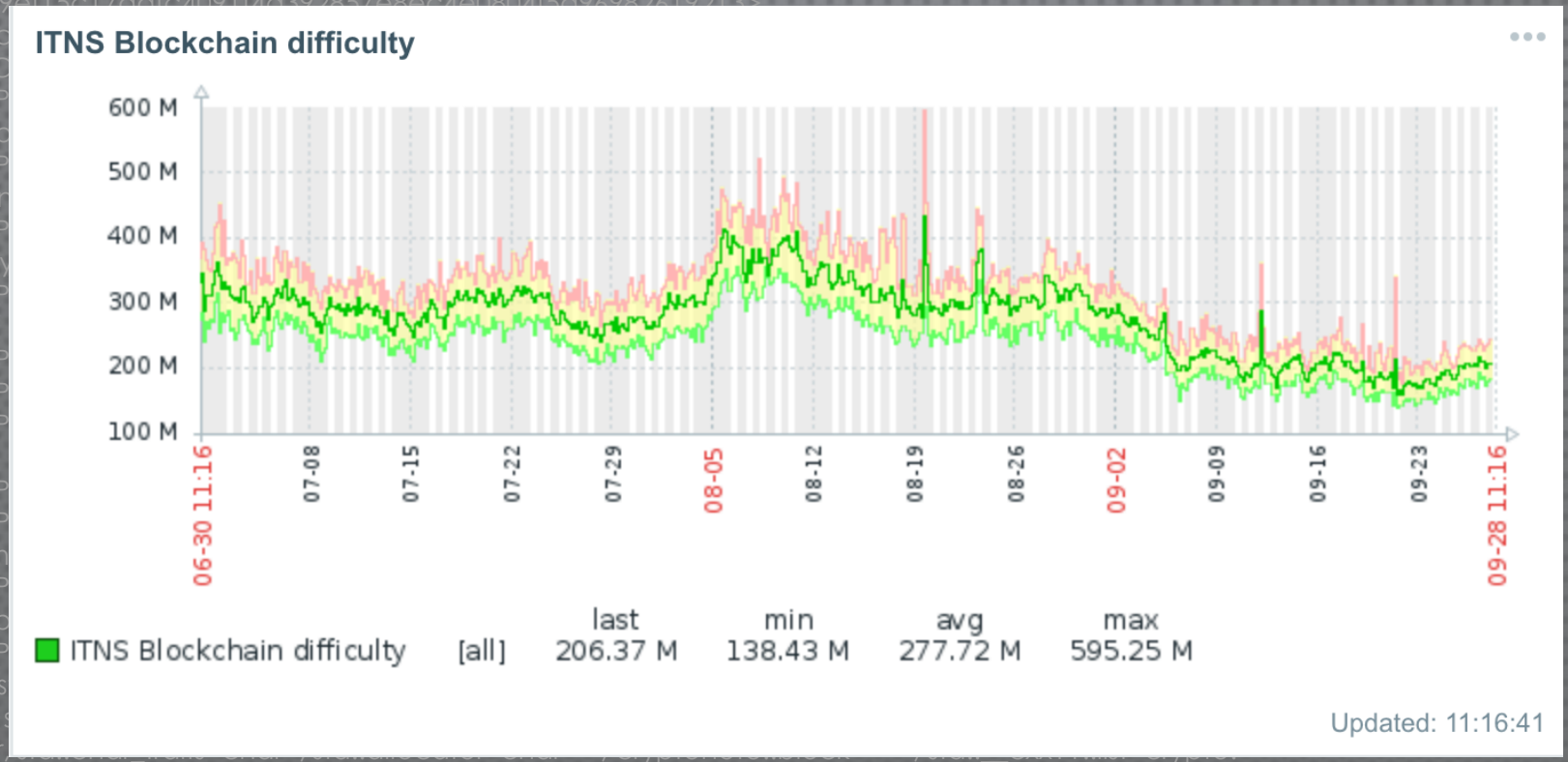
- Timestamp – variation against system time
- Block height – too fat, too fast, stuck, reversed
- Difficulty – too fast a change
- Transaction pool – filled to the brim
- Sync of data on seed nodes – possible blockchain fork



Blockchain attacks – 51% attack

- Difficulty: 4 of 5
- Impact: 4 of 5
- We need to monitor unusual blockchain height changes and difficulty changes
- Triggers: No change in height, reversed height, Too fast, Blocks too fat

2018-09-27 15:18:51.243 [P2P6] INFO global src/cryptonote_core/blockchain.cpp:1461 ESC[1;32m###### REORGANIZE on height: 280084 of 280084 with cum_difficulty 103117521301376
alternative blockchain size: 2 with cum_difficulty 103117730551521ESC[0m
2018-09-27 15:18:51.289 [P2P6] INFO global src/cryptonote_core/blockchain.cpp:1472 ESC[1;34m----- BLOCK ADDED AS ALTERNATIVE ON HEIGHT 280084
id: <7095d05e3ec815d9ef15c17dafc4091f4a392857e8ec4e0804f5a9488219213>
PoW: <0b4e4e90a6486c
difficulty: 221350345ESC
2018-09-27 15:18:51.311 [P
ction mode already enab
2018-09-27 15:18:51.333 [P
t: 280084, new blockchain
2018-09-27 15:18:51.536 [P
254.244.232:49576 INC] Sy
2018-09-27 15:18:51.536 [P
HRONIZED OKESC[0m
2018-09-27 19:04:37.294 [P
2018-09-27 19:04:37.316 [P
2018-09-27 19:04:37.320 [P
ow+0x102 [0x896a62]
2018-09-27 19:04:37.320 [P
2018-09-27 19:04:37.320 [P
kchainLMDB::get_block_h
2018-09-27 19:04:37.320 [P
kchainLMDB::get_block_b
2018-09-27 19:04:37.320 [P
:Blockchain::get_blocks<s
cxx11::basic_string<char, s
_cxx11::basic_string<char,
:hash, std::allocator<crypto::hash> > >(std::__cxx11::list<crypto::hash, std::allocator<crypto::hash> > const&, std::__cxx11:
:list<std::pair<std::__cxx11::basic_string<char, std::char_traits<char>, std::allocator<char> >, cryptonote::block>, std::all
ocator<std::pair<std::__cxx11::basic_string<char, std::char_traits<char>, std::allocator<char> >, cryptonote::block> > >&, st
d::__cxx11::list<crypto::hash, std::allocator<crypto::hash> >&) const+0x206 [0x830e06]
2018-09-27 19:04:37.320 [P2P1] INFO stacktrace src/common/stack_trace.cpp:159 [6] intensecoind:cryptonote::Bloc
kchain::handle_get_objects(cryptonote::NOTIFY_REQUEST_GET_OBJECTS::request&, cryptonote::NOTIFY_RESPONSE_GET_OBJECTS::request
&)+0x1b2 [0x8159d2]

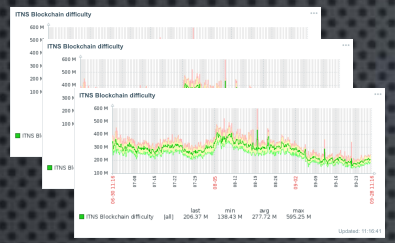


Blockchain attacks – time-based

- Difficulty: 5 of 5
- Impact: 4 of 5
- We need to monitor timestamp being tricked in last blocks
- Triggers: Timestamp being tricked

NOW TO THE ZABBIX PART

Calculate:
Sync of data



Zabbix monitors and alerts Lethean operational team

GET Timestamp, Block height ,
Difficulty, Transaction pool, …

Blockchain distributed over daemon

Improvement request

GUEST PERMISSIONS

- LOCATION ~ (^/$) | ^/INDEX.PHP | ^/SCREENS.PHP | ^/SRV_STATUS.PHP | ^/ZABBIX.PHP\?ACTION\=(MAP | PROBLEM) | ^/SCREENS.PHP | ^/CHARTS.PHP | ^/SYSMAPS.PHP | ^/LATEST.PHP | ^/OVERVIEW.PHP { RETURN 301 "/ZABBIX.PHP?ACTION=DASHBOARD.VIEW&DASHBOARDID=2&FULLSCREEN=1&PERIOD=25920000";

Improvement request

KIOSK MODE AND NICE URLS

SMALL GIFT FOR YOU

```
def json_daemon_call(burl, method):
    if (method != ""):
        d = {
            "id": "0",
            "method": method,
            "jsonrpc": "2.0"
        }
        url = burl + "/json_rpc"
        logging.warning("Calling RPC " + url)
        r = requests.post(url, data=json.dumps(d), headers={"Content-Type": "application/json"})
    else:
        logging.warning("Calling RPC " + burl)
        r = requests.post(burl, data="", headers={"Content-Type": "application/json"})
    if (r.status_code == 200):
        return(r.text)
    else:
        logging.error("RPC error %s!" % (r.status_code))
        return(None)

def zsend(key, value, timestamp):
    global cfg
    line = '"%s" "%s" "%s" "%s"' % (cfg.zhost, key, round(timestamp), value)
    logging.debug("Sending data to zabbix: " + line)
    print(line)
sys.stdout.flush()
```

CRYPTONOTE-ZABBIX

OPEN SOURCE BLOCKCHAIN MONITORING

HTTPS://GITHUB.COM/LIMOSEK/CRYPTONOTE-ZABBIX

Credits

- Pallas – Blockchain expert
- Jordan – Lethean project founder

FORESIGHT™
CYBER

BLOCKCHAIN ATTACKS - LINKS

- 51%: Group of miners owns more than 50% of hash power
- Sybil attack: A node acquires multiple identities
- DDoS attack: Large number of similar requests sent to a daemon
  - https://resources.infosecinstitute.com/blockchain-networks-possible-attacks-ways-protection/#gref
- Timestamp attacks: Deceive daemon into accepting alternate blockchain and enable double spending
  - http://culubas.blogspot.com/2011/05/timejacking-bitcoin_802.html?m=1