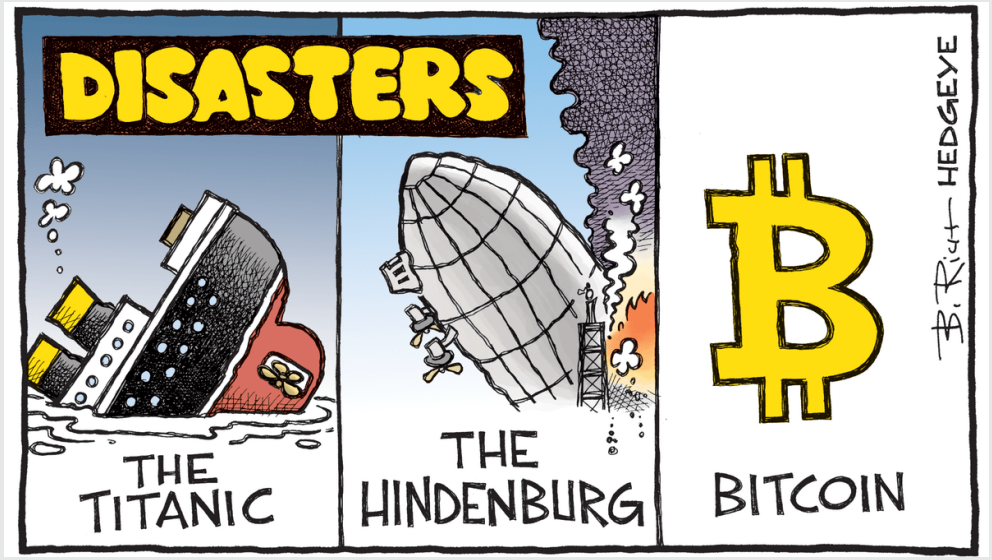
Blockchain Testing Community presenteert:

Smart Contract Disaster Stories



Blockchain Testing Community

Momenteel 62 leden actief, met diversiteit aan ervaring.

-ook een Testnet werkgroep.

Ruimte voor geïnteresseerden om aan te haken!

Diverse aandachtsgebieden:

- Full nodes & periodieke updates van Bitcoin Core,
- Smart contracts / Ethereum,
- Blockchain Testing Framework.

Ca. elke 6 weken een meeting

https://www.meetup.com/nl-NL/BlockchainTestingCommunity/

Disaster Stories

Focus op Smart Contracts

Twee bekende blockchains:

- Ethereum
- Bitcoin

Doel: Wat zijn (veel voorkomende) fouten in smart contracts en welke lessen kunnen we hieruit trekken?

zodat we de volgende keer presenteren over

"Smart Contract Disaster **Prevention** Stories"

Sanne Visser

Blockchain Tester

Contact Information

Twitter: @SimplySanne

Email: blockchainbugs@gmail.com

Capgemini

- Twitter: @CapgeminiNL
- Marktleider in consulting, technology services en digitale transformatie. Onderdeel van Capgemini Group, 200.000 medewerkers in ruim 40 landen.

Blockchain Testing

- Voorzitter Blockchain Testing Community
- Bug Taxonomy
- Blockchain Testing Framework

Nutshell Nuggets

- Consultant bij Capgemini
- Sinds 2008 in het testvak
- Favoriete eten: pizza
- Knitting nerd
- Wandelen en boeken lezen (meestal tegelijk)

Niels Thijssen

testconsultant

Contact Information

Twitter: @thijssen_niels

Email: Niels.thijssen@improveqs.nl

Improve QS

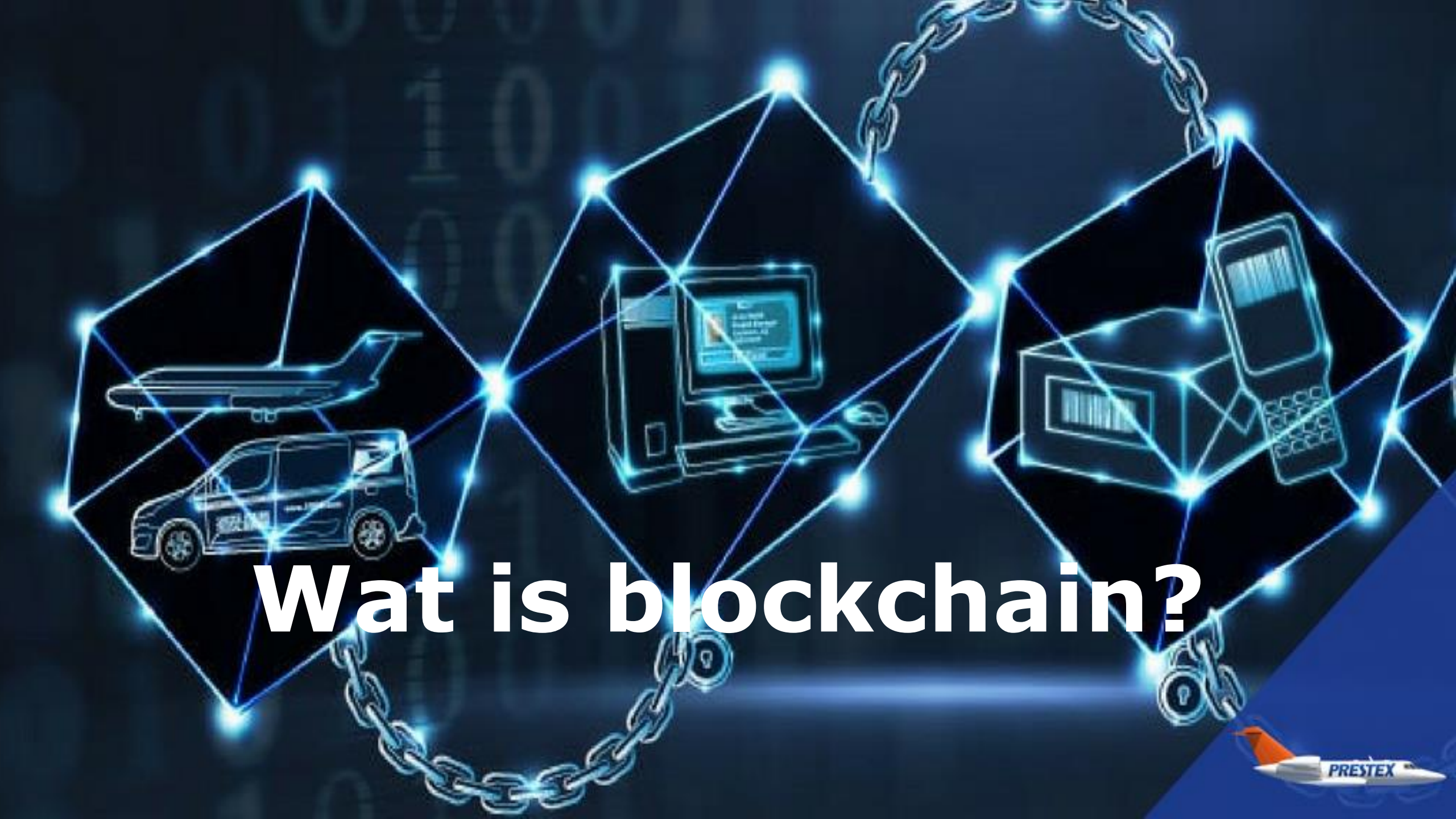
- Twitter: @improveqs
- Improve Quality Services is specialist in innovatieve en hoogwaardige dienstverlening op het gebied van testen, requirements engineering en agile werken.

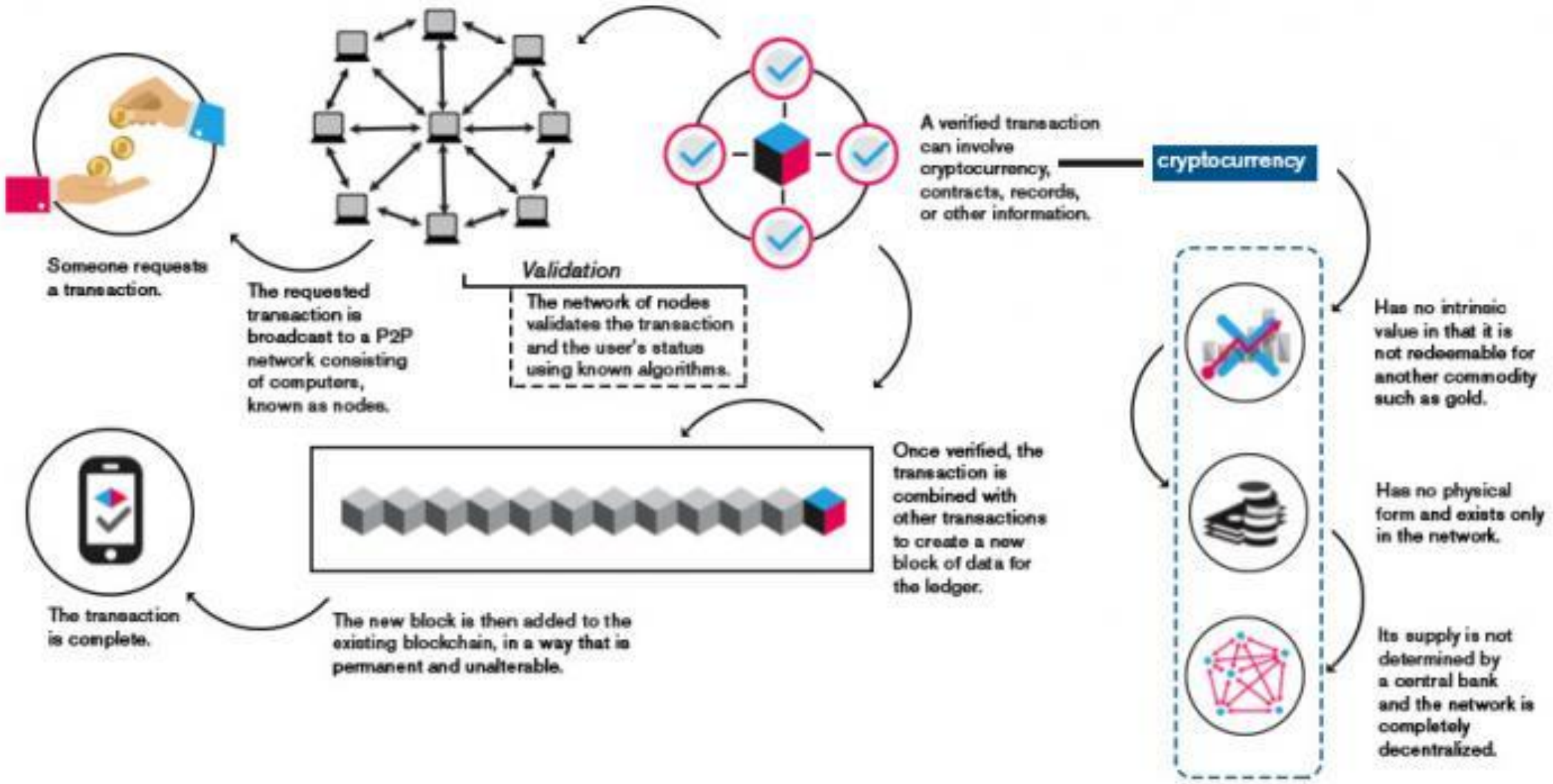
Blockchain Testing

- Persoonlijk betrokken bij opzetten van ‘full nodes’ voor bitcoin netwerk.
- Interesse voor cryptovaluta in het algemeen
- Ervaringsniveau gemiddeld

Nutshell nuggets

- Consultant bij Improve Quality Services,
- Sinds 2006 in het testvak
- Mountainbiking, wielrennen, bioscoop bezoek, oosters eten;


Wat is blockchain?
PRESTEX



Smartcontract (op Ethereum)

Voorbeeld:

- Veerle en Ed zijn voetballiefhebbers.
- Veerle is voor haar club AJAX

Ed is voor FC Utrecht.

- Ze wedden op de volgende wedstrijd met een inleg van €10
- Als Ajax wint, betaalt Ed €10 aan Veerle
- Als FC Utrecht wint, betaalt Veerle €10 aan Ed

Match over, Veerle’s AJAX wint. En wat als Ed niet betaalt?

Smart Contract op Ethereum

- De KNVB maakt een smart contract voor de komende wedstrijd AJAX – FC Utrecht.
- Veerle en Ed betalen elk €10 aan het contract en stellen het contract in :
  - bij gelijkspel krijgt ieder €10 uitgekeerd
  - wint Ajax, dan ontvangt Veerle €20
  - wint FC Utrecht, dan ontvangt Ed €20

- Contract op de blockchain: decentraal, open te controleren, onmogelijk aan te passen
- Zodra KNVB de officiële uitslag uitbrengt, treedt het contract in werking

Code zien? https://medium.com/coinmonks/create-a-sports-betting-dapp-on-the-ethereum-blockchain-part-1-1f69f908b939

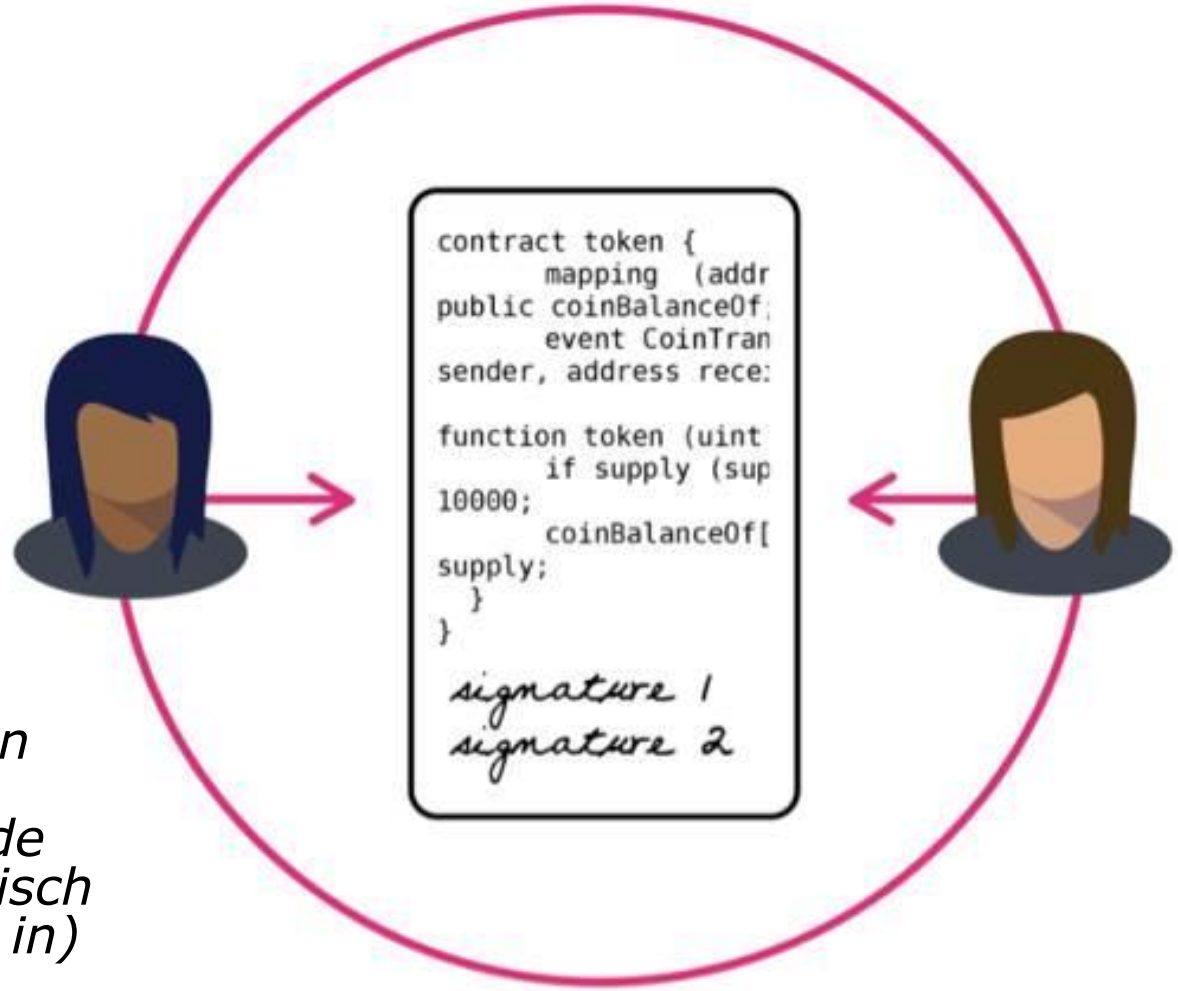
Wat is een dApp?

dApp is een smart contract?

- Zelf-uitvoerende scripts
- Uniek eigen adres
- Bevoegdheid over assets

Definitie:

Een smart contract (slim contract) is een geprogrammeerd contract waarvan de afspraken in code staan vastgelegd op de blockchain. Het contract wordt automatisch uitgevoerd zonder dat hier (vertrouwen in) een tussenpartij voor nodig is. Deze afspraken zijn altijd in te zien, maar kunnen ***onmogelijk*** *nog worden aangepast*



Vulnerabilities

De bugs in deze presentatie:

Cryptokitties
Ethereum

PARITY Multisignature
Ethereum

CVE – 2010 -5139
Bitcoin

DOS Attack
Electrum

CVE – 2013 -3219
Bitcoin

Constantinople Upgrade
Ethereum

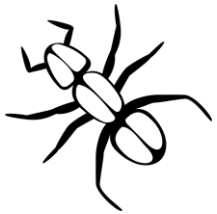
Vulnerabilities (1/2)

Reentrancy

- Onveilige call naar een subroutine.
- Extern smart contract mag nieuwe call aanmaken voordat eerste call compleet is.
- Constantinopel Ethereum Upgrade

Access control

- Correct ownership bij betreffende contract;
- Beschermen contract tegen onbevoegde aanpassingen;
- Bug: Ethereum Parity Multi-sig wallet



Arithmetic

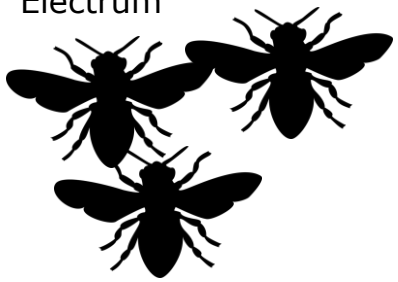
- Beveilig contract tegen over/underflow
- Misbruik van de *withdraw()* function in een smart contract.
- Voorbeeld: CVE-2010-5139

Unchecked low level calls

- Low level calls moeten voorkomen worden, i.v.m. ongewenst gedrag
- External Smart contract stuurt betaling die intern smart contract moet afwijzen. External smart contract draait alsof de afwijzing niet is gebeurd.
- Real world example: King of the Ether Throne

Denial of Service

- Smart contract offline, geen recovery mogelijkheden.
- Vele manieren waaronder triggeren ‘Kill Switch’
- Vele voorbeelden: Ethereum Parity Multi-sig wallet, Cryptokitties, Electrum



Vulnerabilities (2/2)

Bad randomness

- Randomness is lasting in programeertaal Solidity.
- loterij met een contract waarbij randomness bepaald wordt door block timestamp.
- Voorbeeld:

SmartBillions Lottery

Front running

- Exploitatie van belonging miners voor verwerken transacties
- Transacties in die in de wacht staan kunnen gelezen worden en dan ingehaald worden door een transactie met een kopie van het antwoord en hogere transactie kosten waardoor dan sneller verwerkt dan de eerlijke vinder.
- Voorbeelden TheRun

Time manipulation

- De verkoop van token stopt op een specifiek tijdstip.
- Block mining tijd manipuleren dat er toch tokens gekocht/gemined kunne worden.
- Voorbeeld:

GovernMental

Short addresses

- EVM accepteert foutief padded arguments.
- De EVM corrigeert een data string door de ‘missende’ byte toe te voegen. Maakt het mogelijk 256 keer meer over te maken dan gepland.
- Nog geen voorbeelden.

Unknown Unknowns

- Er gaan grote hoeveelheden geld om in een systeem dat complex is en niet ge-audit wordt. En soms is de tooling om een blockchain te controleren nog niet beschikbaar.
- Voorbeeld: CVE-2013-3219

Constantinopel Ethereum Upgrade

bron: Decentralized Application Security Project

Smart Contract Disaster Story

PARITY multi-sig *ethereum*

Parity multi-sig wallet (Ethereum)

Multi-signature wallet van Parity Technologies

- Gebruikers van deze wallet krijgen de mogelijkheid meerdere signatures te benutten. Voorbeeld: bedrijf autoriseert administratiemedewerker tot verrichten van betalingen namens hen aan derden, gebruikmakend van het bedrijfsaccount/wallet;

- Combinatie van commando's 'initWallet' en 'kill' ownership werd verkregen van het contract (per ongeluk)

  - Resultaat:
    - 500k ETH bevroren (ca. 300 miljoen USD (@ USD300/ETH)
    - Stortvloed aan Twitter response
    - Imago van bedrijf beschadigd, geloofwaardigheid verloren

Comment on GitHub #6995: "I accidentaly killed it..."

Smart Contract Disaster Story

CVE-2010-5139

bitcoin

Bitcoin – CVE-2010-5139

Gedrag:

- Mogelijkheid tot hacken van 92 miljard Bitcoins,
- Overtreding bitcoin ‘business rules’: er kunnen maximaal 21 miljoen bitcoins beschikbaar komen.

Analyse

- Nummer overflow

Impact: critical, tot op heden voor bitcoin de grootste fout

Oplossing:

- Soft fork op de consensus rules (‘business rules van bitcoin’),
- Harde limiet op max. 21 miljoen Bitcoins verder doorgevoerd.

Smart Contract Disaster Story

CVE-2013-3219 *bitcoin*

Bitcoin – CVE-2013-3219

btc

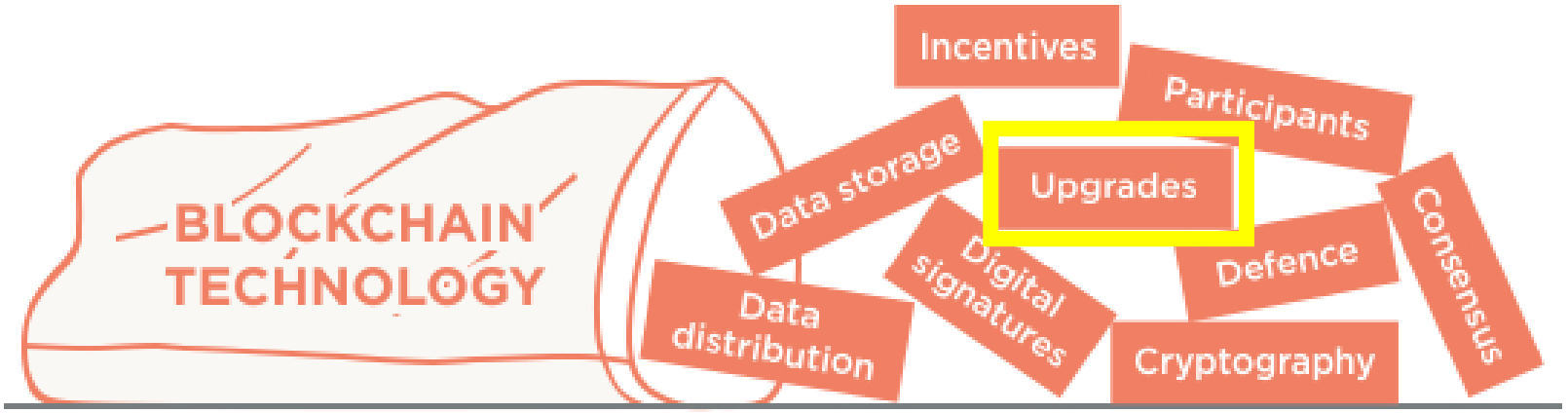
Gedrag:

- Met node software v0.8 trad incompatibiliteit op met voorgaande releases,
- Faciliteerde grotere block sizes t.o.v. voorgaande versies.

Oplossing:

- ‘Hard fork’ terug naar eerdere branch,
- Fix op node software.

Impact: critical



Smart Contract Disaster Story

Constantinopel Upgrade *Ethereum*

Constantinopel Ethereum Update

btc

Gedrag:

- De Constantinople upgrade voor het ethereumnetwerk met als doel goedkoper maken om smartcontracts te draaien,
- Faciliteerde nieuwe smart contract store (SSTORE) operaties t.o.v. voorgaande versies,

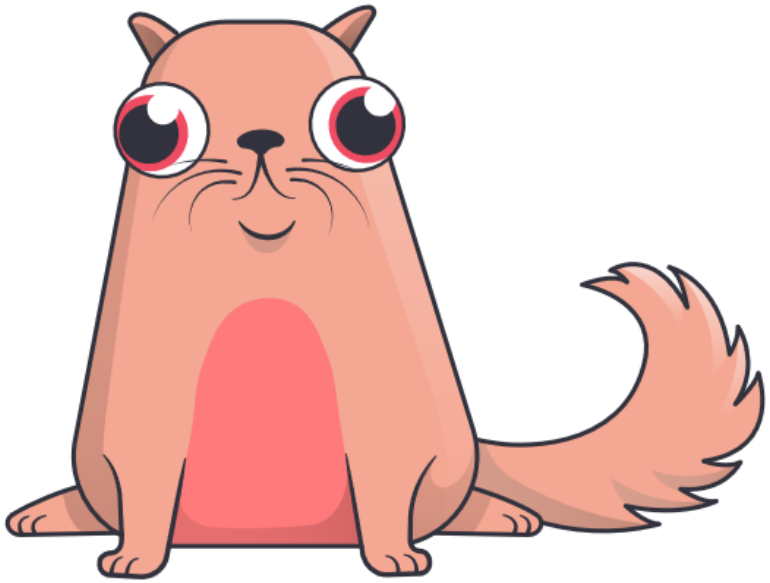
Side effect: Enabled reentrancy attacks die eerder veilig waren bevonden.

Oplossing:

- Geplande release datum uitgesteld,
- Fix op node software.

Unintended side effect: BlockCypher’s Ethereum API was knocked out for almost a month due to the Constantinople Hard Fork

Hard Forks en Soft Forks



Smart Contract Disaster Story

Cryptokitties
Ethereum

dApp Game Cryptokitties legt ethereum stil

Gedrag:

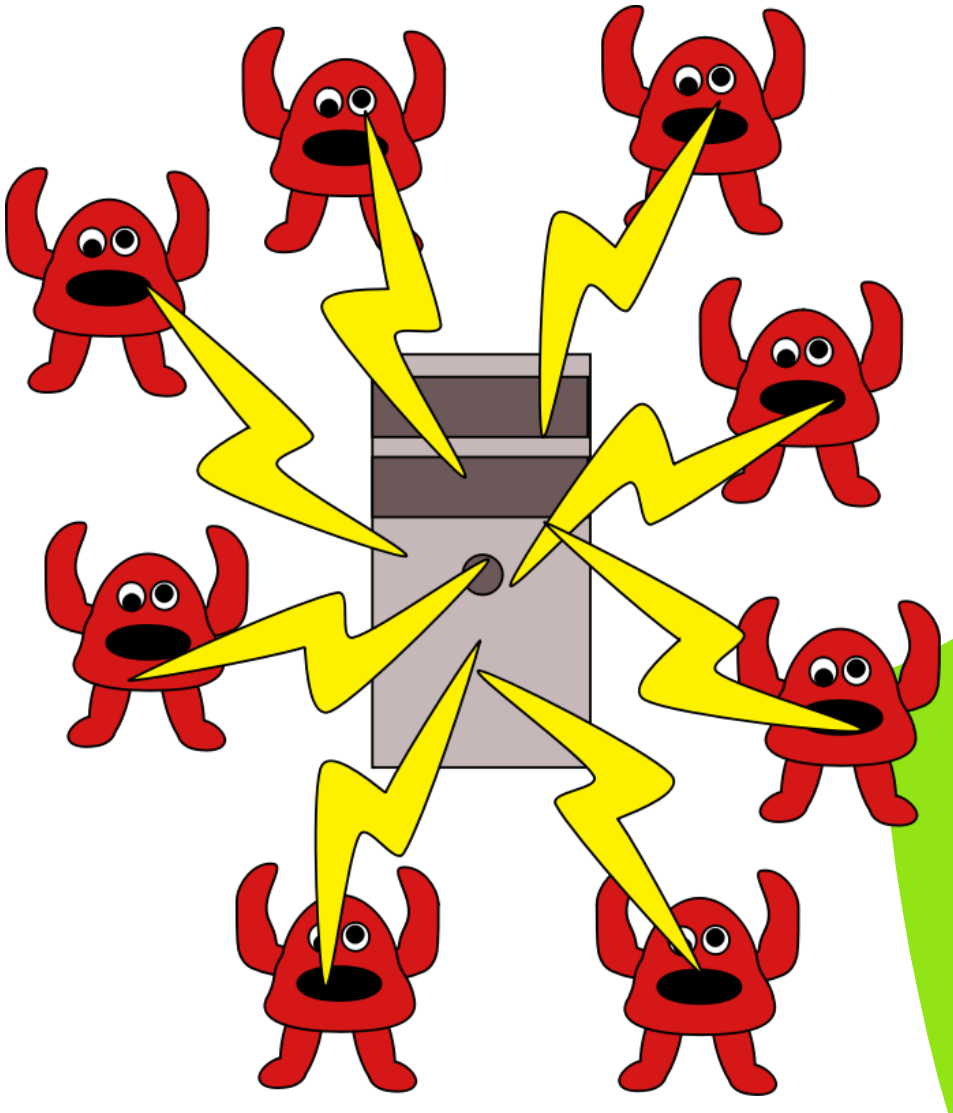
- Performance: Populair spel vertraagt gehele blockchain +24H

Side effect: Alle netwerk transacties vertraagd of geannuleerd gedurende 24 uur na release spel, nog maanden daarna eist het spel 20% van alle

Oplossing:

- Prijs van een Cryptokitty wordt verdubbeld

Unintended side effect: ICO’s uitgesteld, discussie gestart over de beperking van het Ethereum network op 17transactie/sec



Smart Contract Disaster Story

DoS

Electrum

/ PRIVACY & SECURITY

Landon Manning

Guest Contributor

Landon Manning is an editorial intern at BTC Media and writes articles for its publications, including Distributed.com and Bitcoin Magazine.

10 April **2019**!

SUBSCRIBE

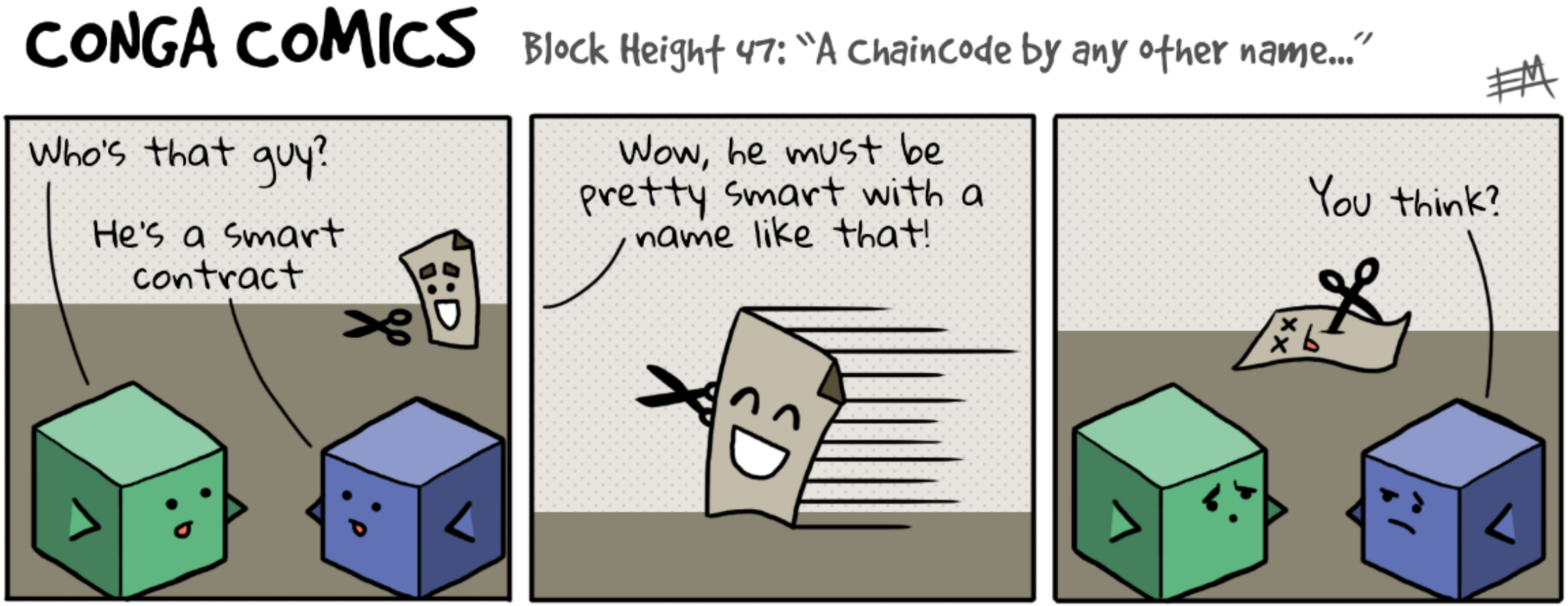
Electrum Servers Remain Under Sustained DoS Attack

Electrum servers are still under a sustained Denial-of-Service (DoS) attack. The wallet developers announced the issue o

April 7 2018

In correspondence with *Bitcoin Magazine*, Electru per Thomas Voegtlin speculated that the attack may be a form of retaliation from a

One more thing...



https://www.meetup.com/nl-NL/LiskCenterUtrecht/events/258641216/

Referenties

http://www.youtube.com/.....BTC

https://en.bitcoin.it/wiki/Common_Vulnerabilities_and_Exposures

https://www.youtube.com/user/aantonop

https://github.com/bitcoinbook/bitcoinbook (Mastering Bitcoin)

https://bitcoin.org/nl/

https://bitnodes.earn.com/

https://www.oreilly.com/library/view/mastering-bitcoin/9781491902639/ch06.html

https://www.oreilly.com/library/view/mastering-bitcoin/9781491902639/images/msbt_0602.png

https://dasp.co/