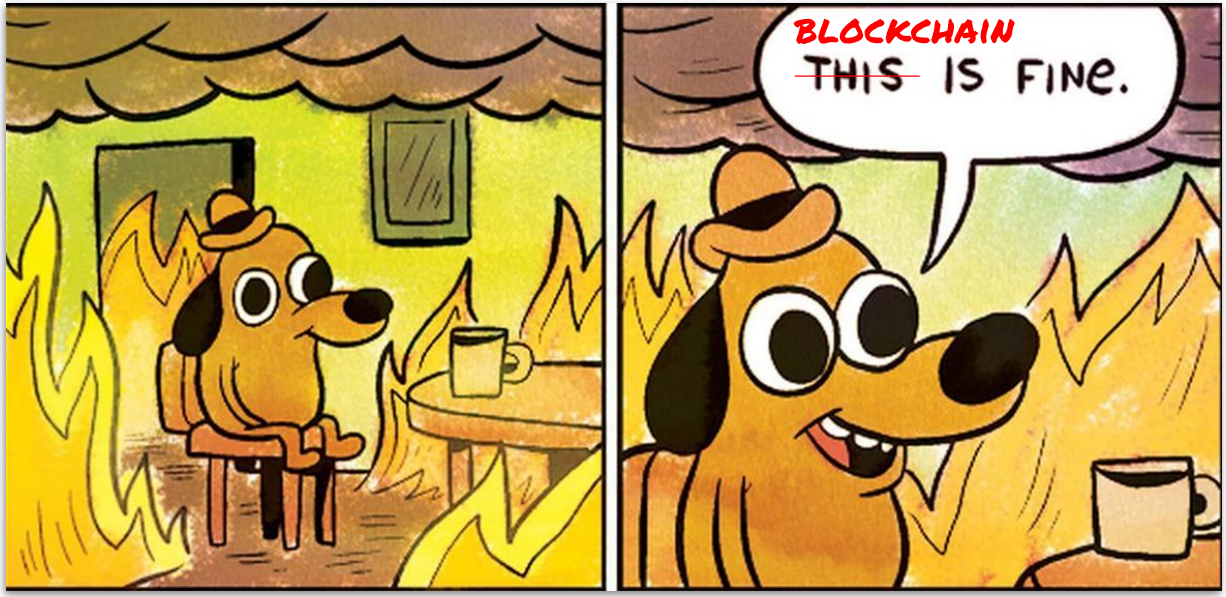
Blockchain & smart contract security



Doelstellingen

Introductie geven
Doorverwijzen naar open leermateriaal

Agenda

Blockchain (security)
Smart contract (security)

Mastering Bitcoin
Mastering Ethereum
Ethereum Yellow & Beige Paper
Ethereum EVM illustrated

Blockchain

Wat

Wat is distributed ledger technology?

Distributed ledger technology is een instrument voor het vastleggen van eigendom, bijvoorbeeld het eigendom van geld of activa (zoals onroerend goed). Tegenwoordig is het zo dat wanneer banken transacties verrichten (d.w.z. wanneer het eigendom van geld of financiële activa in andere handen overgaat), ze dat doen via gecentraliseerde systemen, die vaak worden beheerd door centrale banken. Banken volgen hun transacties in lokale databases, die worden geüpdatet nadat de transactie in het gecentraliseerde systeem heeft plaatsgevonden.

Een 'distributed ledger' (lettelijk: gedeeld grootboek) daarentegen is een database van transacties die over een netwerk van vele computers is verspreid, in plaats van opgeslagen op één gecentraliseerde locatie. Doorgaans hebben alle leden van het netwerk toegang tot de informatie. Tevens kunnen ze, mits ze schrijfrechten hebben, informatie daaraan toevoegen.

Het meest voorkomende type DLT heet 'blockchain'. De naam is afgeleid van het feit dat de transacties worden samengebundeld tot een blok, en die blokken worden in chronologische volgorde met elkaar verbonden om zo een keten te vormen. De hele keten wordt beschermd door complexe wiskundige algoritmen die tot doel hebben de integriteit en veiligheid van de gegevens te waarborgen. Deze keten vormt de totale registratie van alle transacties die in de database zijn opgenomen.

Bron: ECB

Distributed Ledger Technology

“Gedeeld grootboek”

Cryptografie

Gedistribueerd

Publiek of privaat (digitale €, $, ¥)

Native tokens vs cryptomunten vs NFT’s vs …

Bitcoin vs Ethereum vs …

Blockchain

Waarom

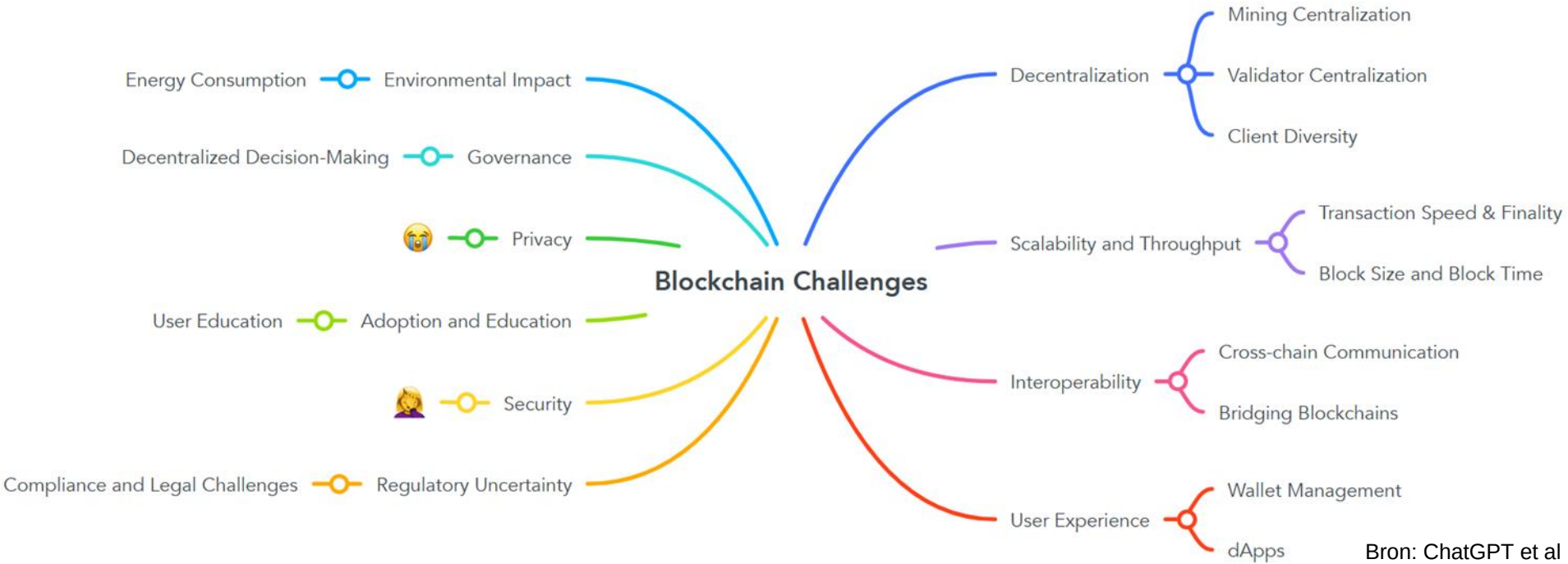
- **Efficiënt(er)**
  - Minder tussenpersonen *(of andere?)*
  - Minder complex *(zeker van?)*

- **Veilig(er)**
  - Cryptografie *(dus… het zal wel veilig zijn?)*
  - Auditeerbaar, minder fraude gevoelig *(zoals bij open source software?)*
  - Geautomatiseerd *(dus kans op fauten is kleiner?)*

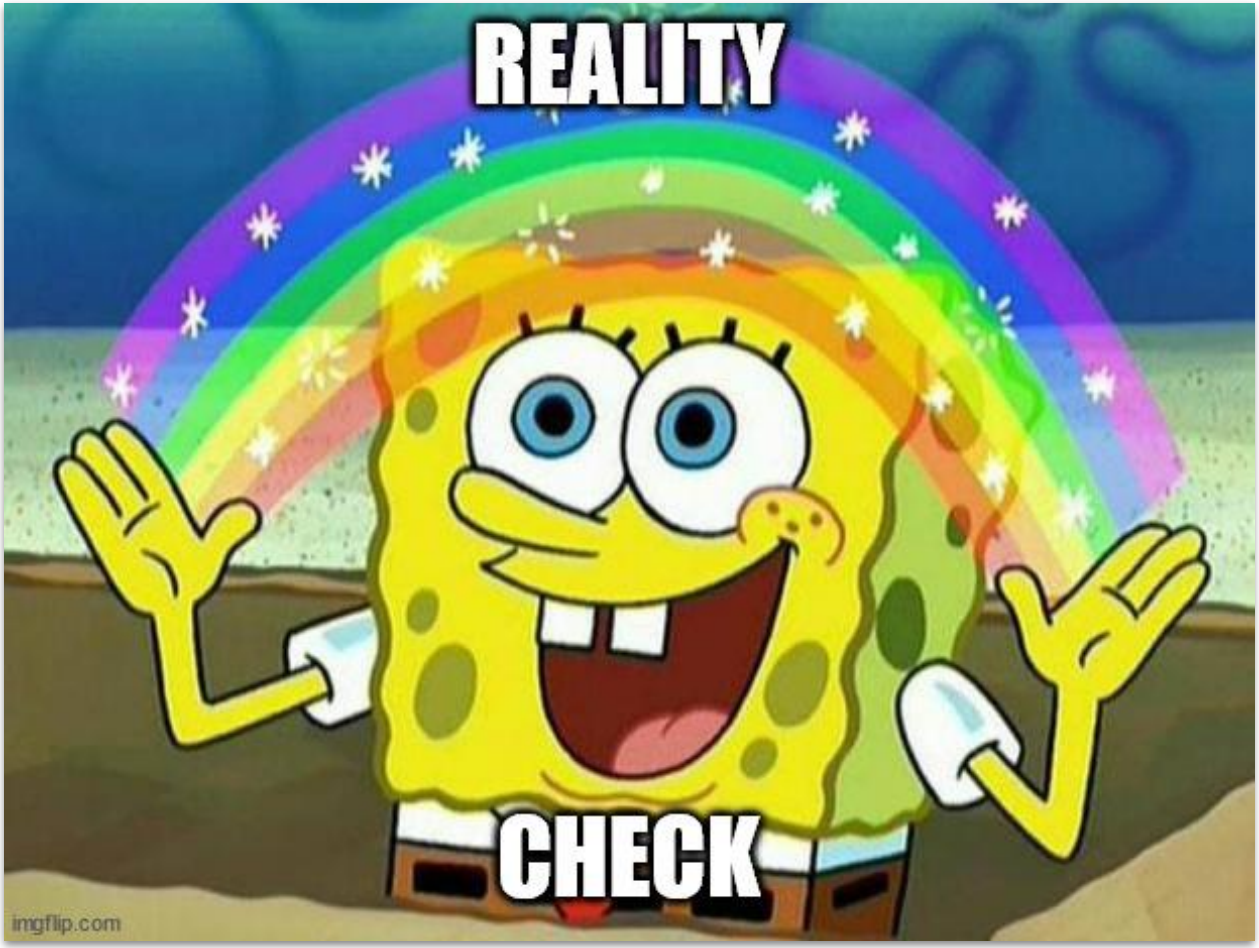
- **Robuust(er)**
  - Gedistribueerd / decentraal *(veel kritieke infra draait alsnog bij de grote cloudproviders…)*

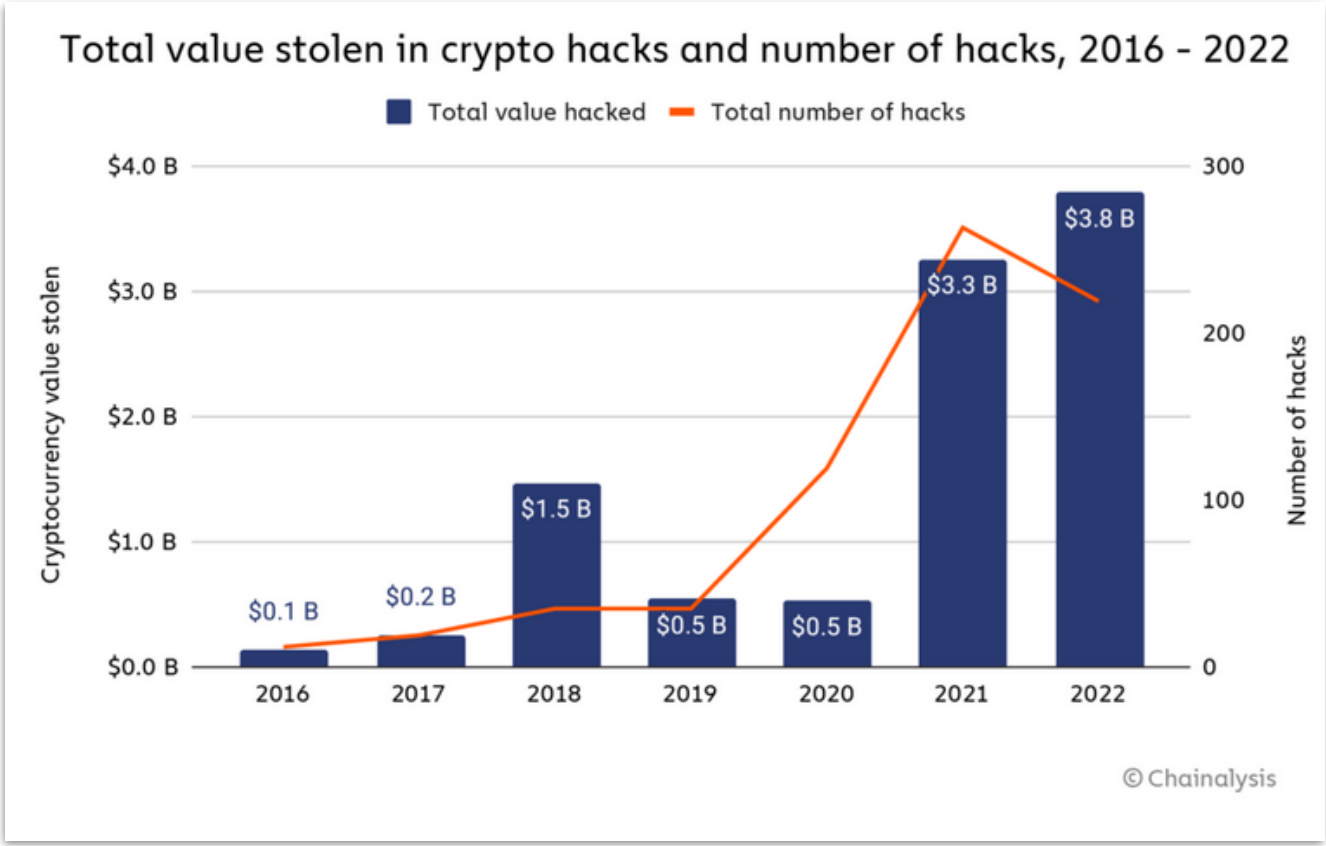
Blockchain

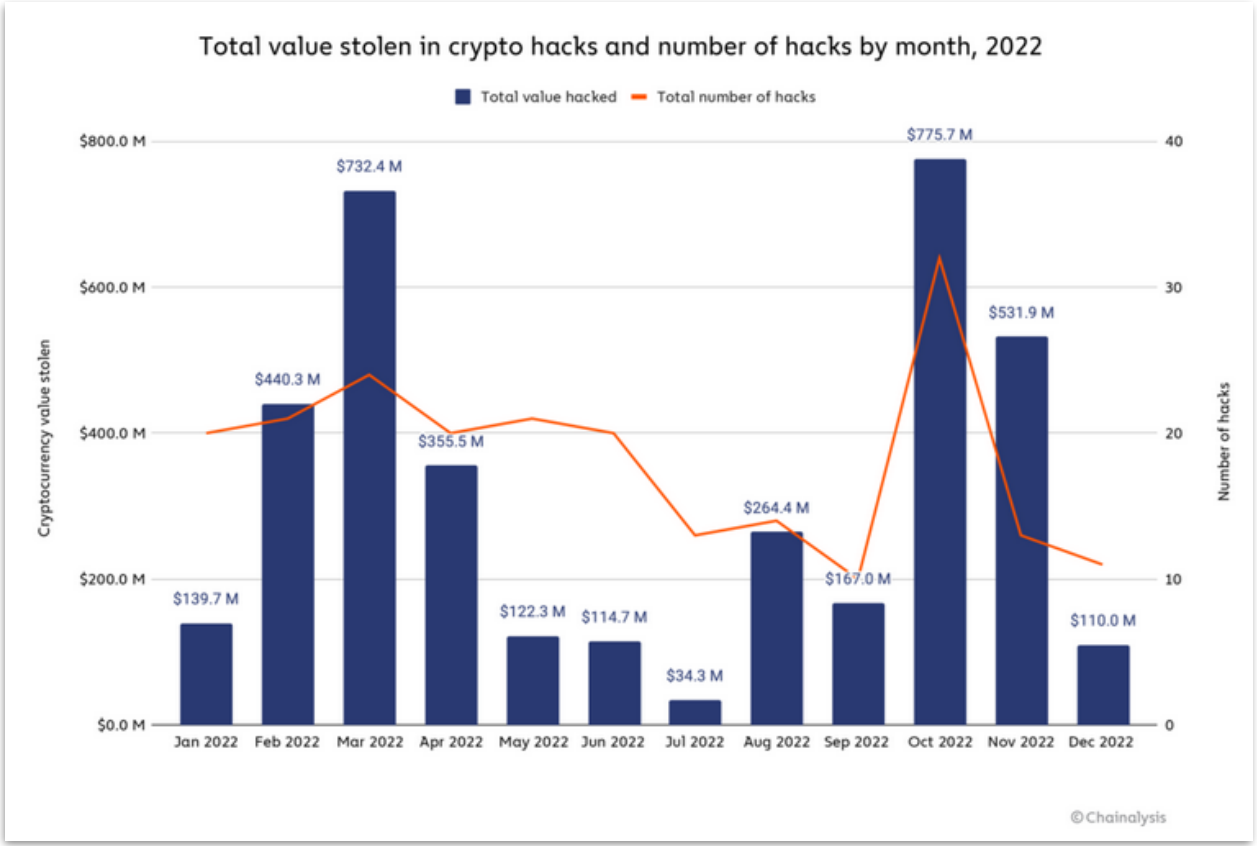
Uitdagingen



Bron: ChatGPT et al


REALITY
CHECK
imgflip.com


Total value stolen in crypto hacks and number of hacks, 2016 - 2022
Total value hacked
Total number of hacks
Cryptocurrency value stolen
Number of hacks
$4.0 B
$3.0 B
$2.0 B
$1.0 B
$0.0 B
300
200
100
0
$0.1 B
$0.2 B
$1.5 B
$0.5 B
$0.5 B
$3.3 B
$3.8 B
2016
2017
2018
2019
2020
2021
2022
© Chainalysis

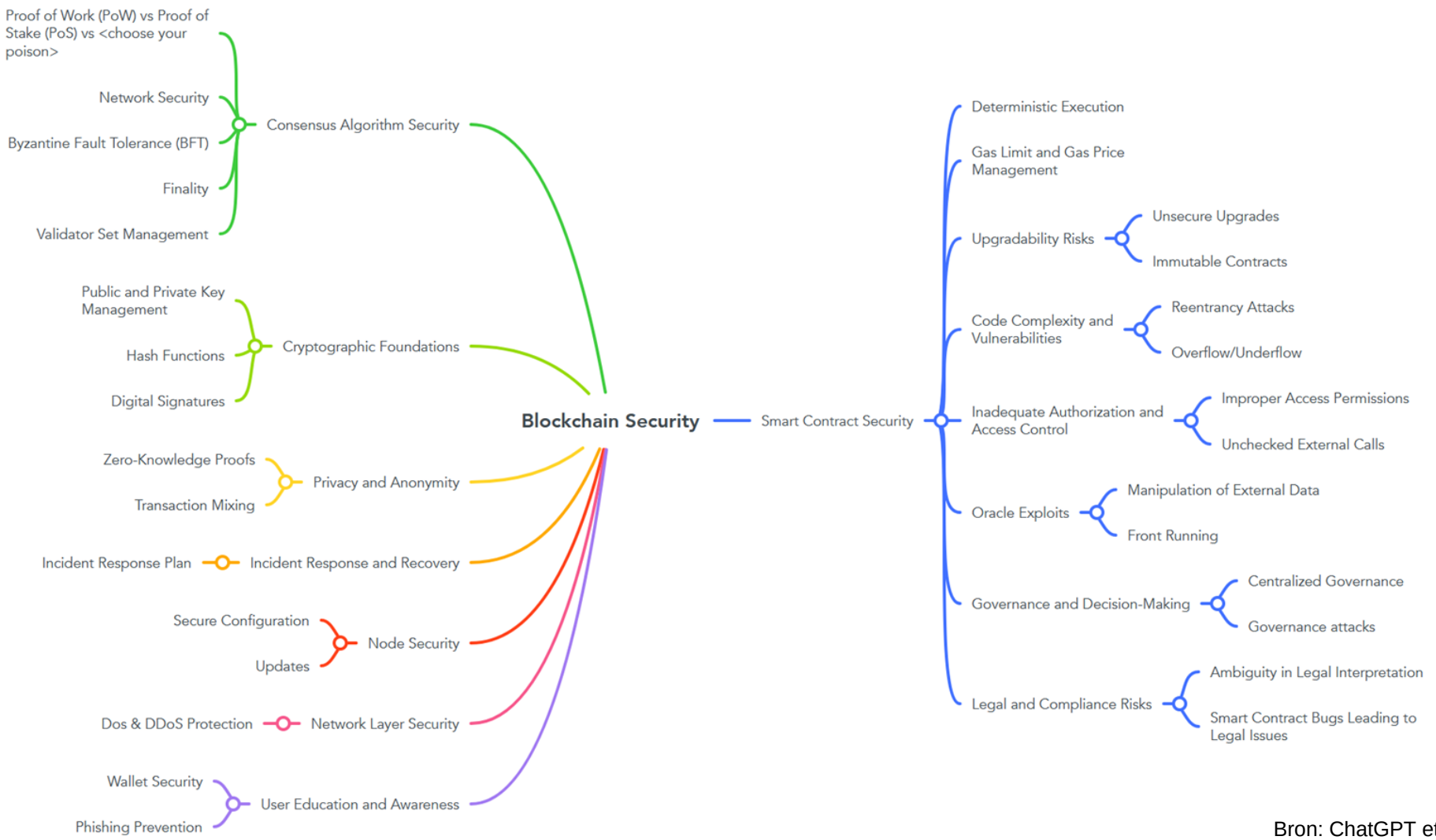


Bridges vormen geliefd doelwit (2022: Wormhole - $320 mio, Nomad - $190 mio, Harmony Horizon - $100 mio)

Aanvallen zijn vaak te linken aan Noord-Korea die de gestolen fondsen gebruiken om economische & financiële sancties te omzeilen

Prognose 2023 ook vlot richting > $1 mia

Blockchain security



Bron: ChatGPT et al

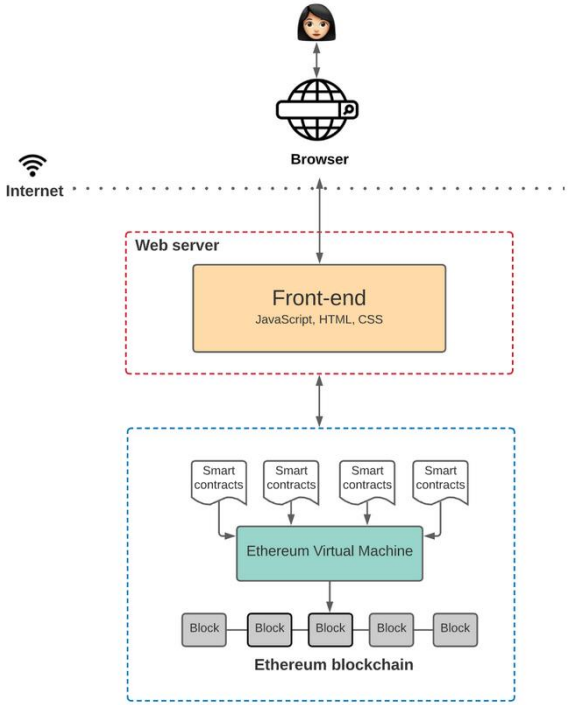
Smart contracts

Wat

"Een smart contract (slim contract) is een geprogrammeerd contract waarvan de afspraken in computercode 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." *(bron: allesovercrypto.nl)*

Waarom

- Betrouwbaar
- Autonoom
- Veilig
- Snel
- Robuust
- Goedkoop
- Nauwkeurig



(bron: The Architecture of a Web 3.0 application - Preethi Kasireddy)

Ethereum (smart contract) security: Secureum
Bug bounty: Immunefi, Code4rena, Hats.Finance
Capture The Flag: DamnVulnerableDefi, Ethernaut

Smart contract security

Open Standard Web3 Attack Reference (OSWAR)

Vragen?