Web3 security: same fundamentals, higher stakes

Dr. Gulnara Hein

20.03.2025

OWASP Frankfurt

About myself: Gulnara Hein

- 20 years in security
- PhD in Discrete Mathematics "Complexity of Private Information Retrieval Protocols"
- Vulnerability mgmt, infra- and application security, risk management @ Cargill, PwC
- 1st & 2nd LoD, cyber risk quantification projects @ Deutsche Börse
- CISO @ Chintai, regulated blockchain tokenization platform

Agenda

1. Blockchain and web evolution
2. Security mission
3. What do we learn from Web2 threat reports
4. What do we learn from Web3 threat reports
5. Security fundamentals Web2 and Web3

1. Blockchain and web evolution

Web Evolution

Web1 : Read

Early 1990s

Static content

Permissionless

Web2 : Write

Early 2000s

User-generated, dynamic content (social media, blogs)

Permissioned (Google, Facebook, Amazon)

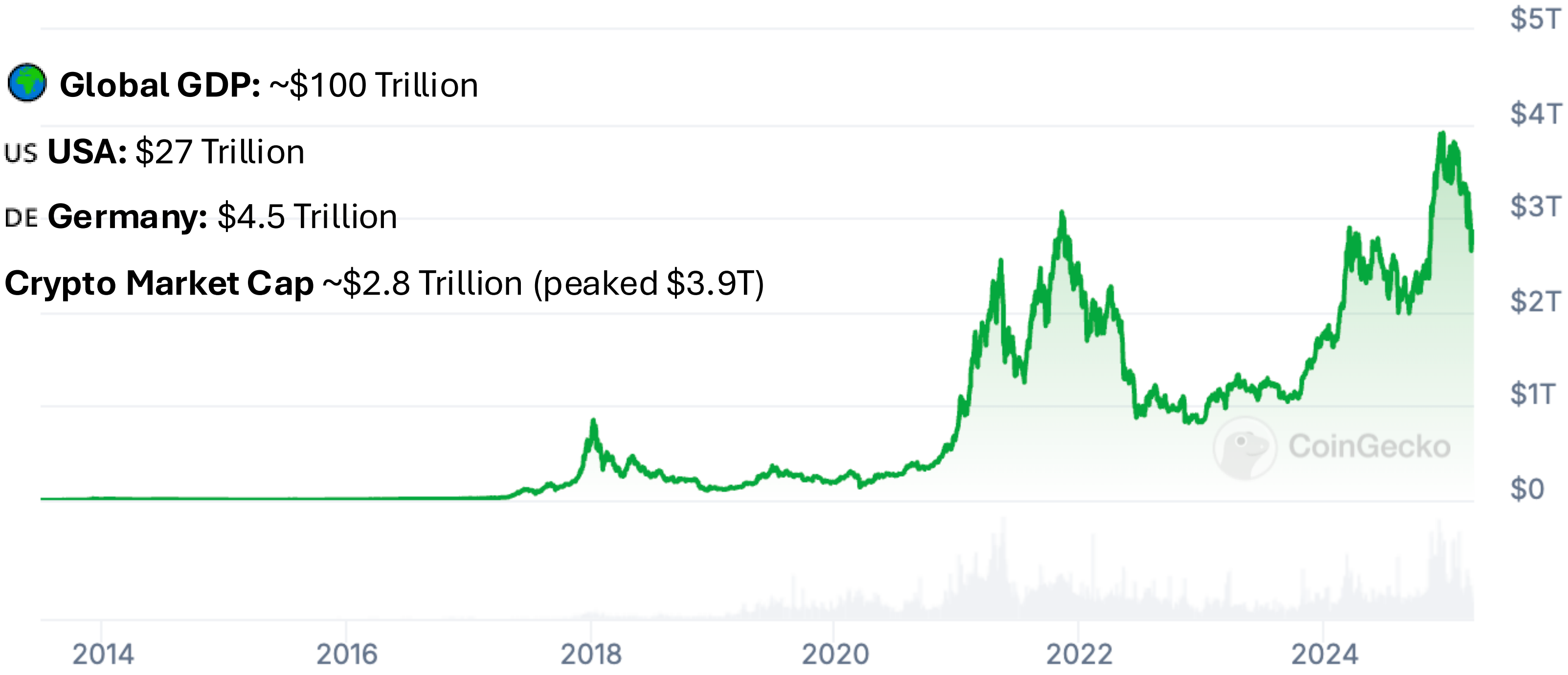
Web3 : Own

Bitcoin 2009, Ethereum 2015

Dynamic content

Permissionless, users own data and identity

Total Crypto Market Cap Chart



🌍 **Global GDP:** ~$100 Trillion

US **USA:** $27 Trillion

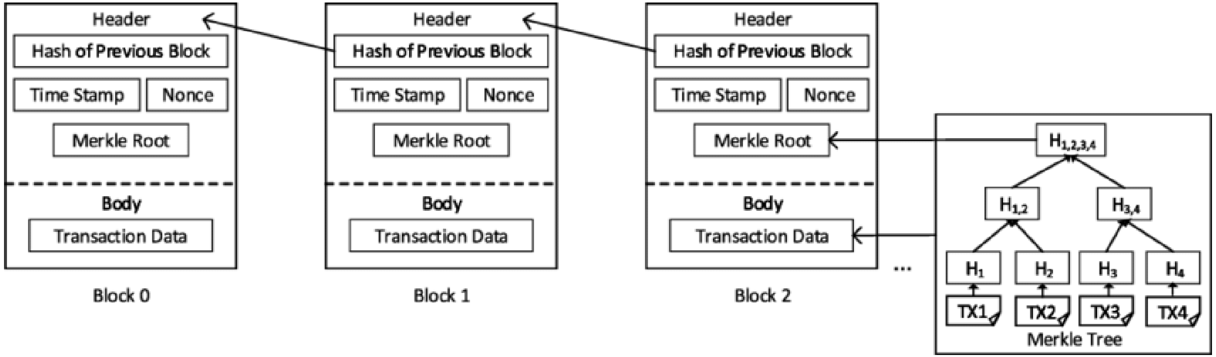
DE **Germany:** $4.5 Trillion

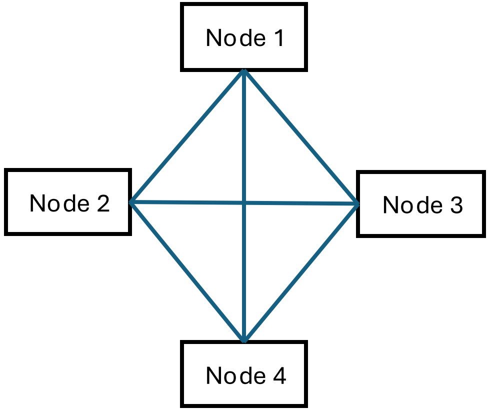
Crypto Market Cap ~$2.8 Trillion (peaked $3.9T)

*https://www.coingecko.com/en/global-charts

Blockchain: The Power of a Distributed Ledger

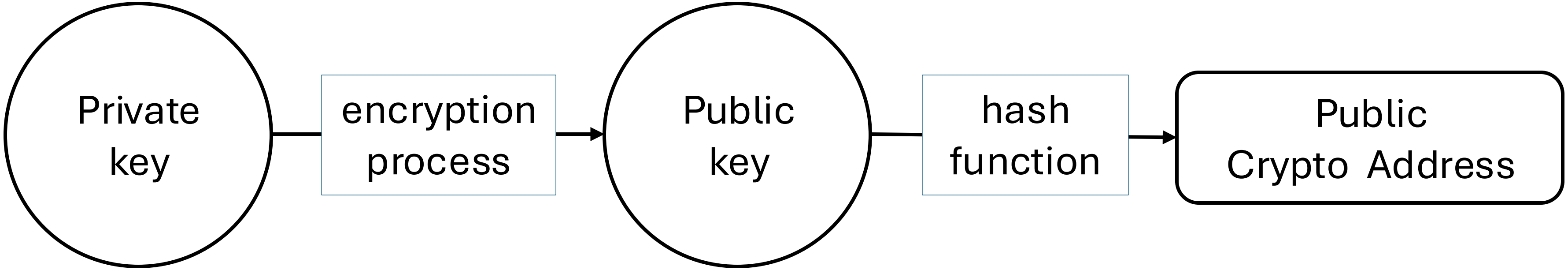
A Blockchain is a **method of storing data** in **blocks** which are **linked together in the form of a chain**.



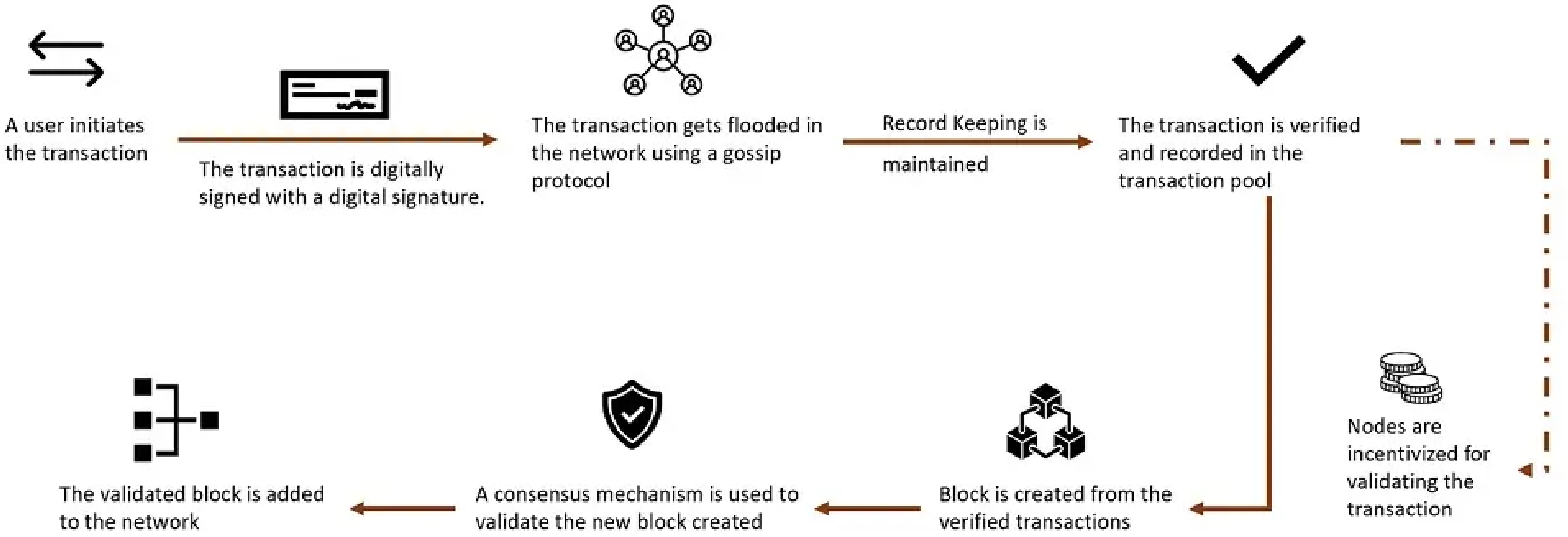


*Blockchain for Dynamic Spectrum Management, 2020, Ying-Chang Liang, University of Electronic Science and Technology of China

User wallet: private / public key



Transactions on blockchain



A user initiates the transaction

The transaction is digitally signed with a digital signature.

The transaction gets flooded in the network using a gossip protocol

Record Keeping is maintained

The transaction is verified and recorded in the transaction pool

Nodes are incentivized for validating the transaction

Block is created from the verified transactions

A consensus mechanism is used to validate the new block created

The validated block is added to the network

Smart contract

Smart contracts are a set of instructions executed in a decentralized autonomous way without the need for a third party or centralized intermediary.

Web3 umbrella

A blockchain-powered internet focused on decentralization, ownership, and transparency.

- Decentralized finance (DeFi)
- Non-fungible tokens (NFTs)
- Decentralized autonomous organizations (DAOs)
- Blockchain gaming / Metaverse

2. What is our security mission?

Our goal

WHAT: we want to ensure that the technology works as it supposed to, meaning ensuring the confidentiality, integrity and availability.

HOW: we want to do this as efficiently as possible (least resources for most results)

WHY: If we don’t do so, we might miss something important.

Core principles of “good” security

- Compliance: easy to use.
- Automation: minimize reliance on human action (no, user awareness doesn't work).
- Control and reinforce.
- Consistency is more important than complexity

Web2 security threats

As we assume that technology should work as expected, we also need to understand why it might fail. In other words, we need to identify our **THREATS**

- Accidental (unintentional) ← also security
- Malicious

3. What do we learn from Web2 threat reports?

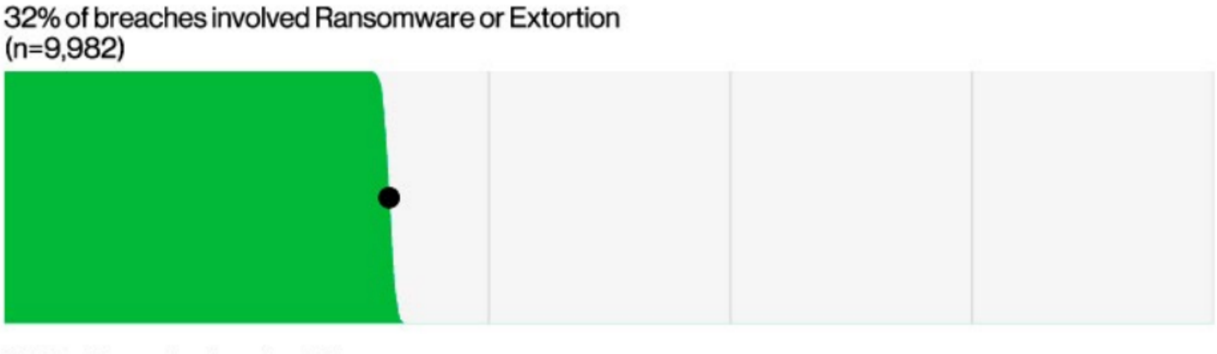
Data Breach Report Bingo

After human-related factors, the next most prevalent component of data breach is:

a) Ransomware

b) Errors (accidental, no attack involved)

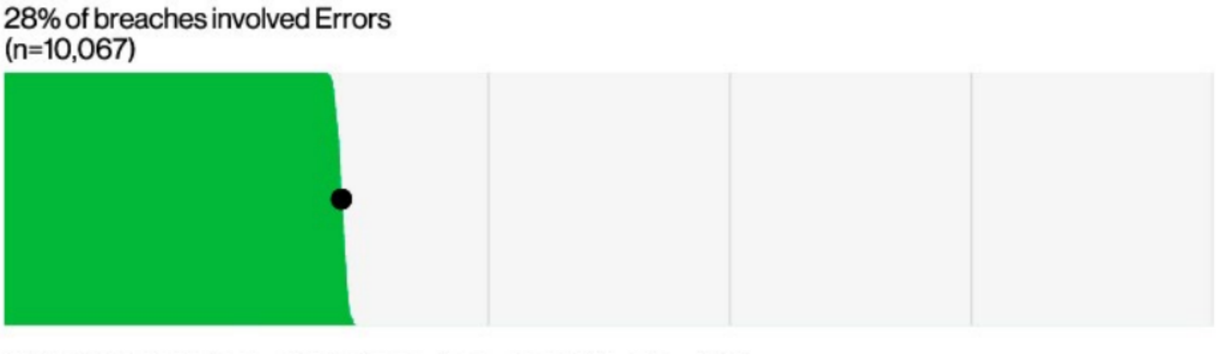
Verizon: total number of incidents analyzed : 30,458*



32% of breaches involved Ransomware or Extortion
(n=9,982)

32%

33%



28% of breaches involved Errors
(n=10,067)

*2024 Data Breach Investigations Report

Web2 leading attack patterns

- System Intrusion (Ransomware, Backdoors, Vulnerabilities) ~ 36%
- Social Engineering (Phishing, Impersonation Attacks) ~ 30%
- Human Errors (Misconfigurations, Data Exposure) ~ 27%
- Web Application Attacks ~ 9%
- Privilege Misuse ~ 8%

What does this mean for us if we want to be efficient (apply the 80/20 principle)?

* 2024-dbir-data-breach-investigations-report

4. What do we learn from Web3 threat reports?

Web3 tech stack

- Blockchain
- Smart contracts
- Development environments
- Testing frameworks
- File storage
- User identity management
- UI/UX components

Web3 vs 2.0

- **Blockchain:** 51% attacks, consensus manipulation, MEV (sandwich) attack
- **Smart Contracts:** reentrancy attacks, logic bugs, oracle manipulation
- **Development Environments:** compromised packages, malicious pull requests
- **Testing Frameworks** : Incomplete test coverage
- **File Storage :** cloud storage compromise
- **User Identity Management** : private keys theft, phishing seed phrases
- **UI/UX Components** : malicious frontends injecting rogue contracts

web2

What do we learn from Web3 threat reports?

Type of attack (number)*

- On-chain (smart contract exploitation, price manipulation, rug pulls, etc) – 42,5%
- Off-chain (Web2 attacks, private keys compromise) 57,5%

*Halborn “A COMPREHENSIVE REPORT BREAKING DOWN THE TOP 100 DEFI HACKS 2016-2023

Web3 hacks per type over the years 2016 – 2023*

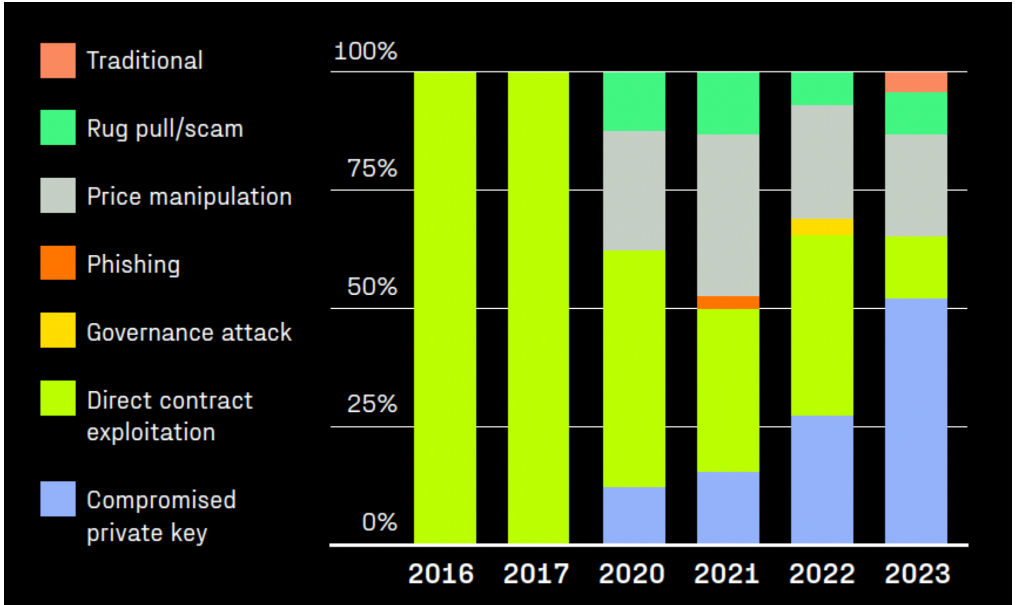
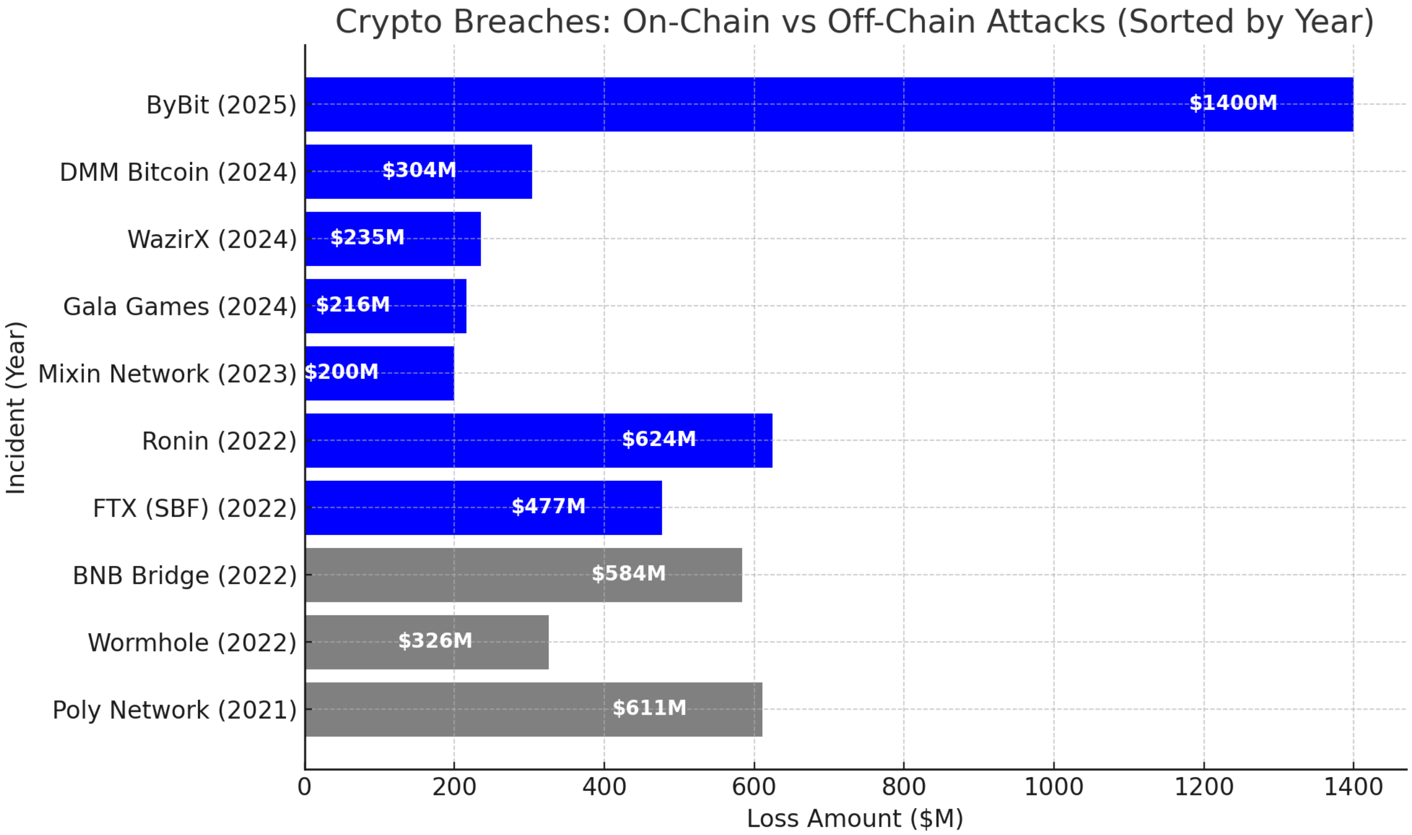


Figure 29: *Number of attack sub-categories per year [percentage]*

*Halborn-Top-100-DeFi-Hack-Report December 2024

Threat landscape Web3 : Top 10 attacks all time



Cost of breach: Web2 vs Web3

- Rising Breach Costs: The average cost of a data breach rose 10% in 2024, reaching $4.88M (IBM's Cost of a Data Breach Report 2024).
- Crypto Hacks Are Costly: In 2024, $2.2B was stolen across 303 crypto hacks, averaging $7.26M per breach (Chainalysis).

What's Different?

- Web3 Breaches = Direct Financial Theft. Stolen funds can be instantly moved and relatively easy laundered. Not the case for Web2 breaches,
- Transparency, not Privacy. Web3 transactions are public and traceable, unless actively obfuscated (e.g., mixers, privacy protocols). Web2 breaches, however, often go undetected for months.

5. Security fundamentals: Web2 and Web3

Workstations

Web2: Workstation is the entry point for all social attacks, they must be protected at all costs:

- MacOS vs Windows (check number of zero-days)
- Hardening: MDM ensuring secure configuration and pushed patches, NO ADMIN
- 100% coverage with EDR (check the best MITRE coverage)

Web3: Rules for workstation that used to perform on-chain operations

- Hardened device (you can rollout new OS with MDM, Qubes OS, ephemeral VM)
- Used only for transaction, no email, no dev. tools, etc.
- Turned on only for performing transactions.

Asset Inventory

Build your asset inventory – a surprisingly difficult but very rewarding process*

Web2:

- Interview teams – Identify systems in use
- Check payments – follow financial records to uncover hidden services.
- Track data flows – map how data is created, stored, processed, and archived.
- Audit secrets – identify exposed credentials and access points.
- SaaS integrations / interfaces

Web3

- All smart contracts / including external, oracles and bridges.

*If you don’t know what you have, you can’t secure it.

Identity and access management - basics

Web2. IAM is the essence of data breaches which is the core issue in majority of hacks.

- **Phishing resistant 2FA** : get your FIDO2 hardware keys and enforce it everywhere.
- Minimum privileges: workstations, code repositories, prod env, critical SaaS

Web3

- Protect your private keys

Hardware wallet

A **hot wallet** is a piece of software you install on your smartphone or laptop to store private keys.

Cold wallet generates and stores your private keys in an offline environment, it never interacts with smart contracts, it signs transactions offline and never signs any smart contract approvals.

Hardware wallets generate and store your private keys offline in a secure physical device isolated from internet connection.

Identity and access management – next step

Web2

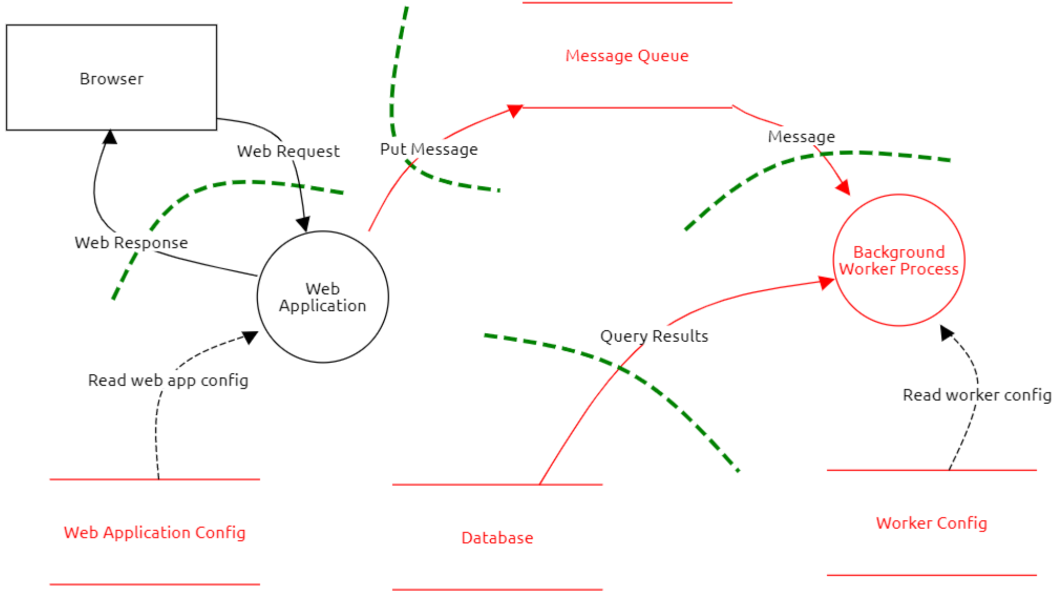
- Just-in-time instead of just-in-case
- Separation of duties : no single account can deploy critical change

Web3

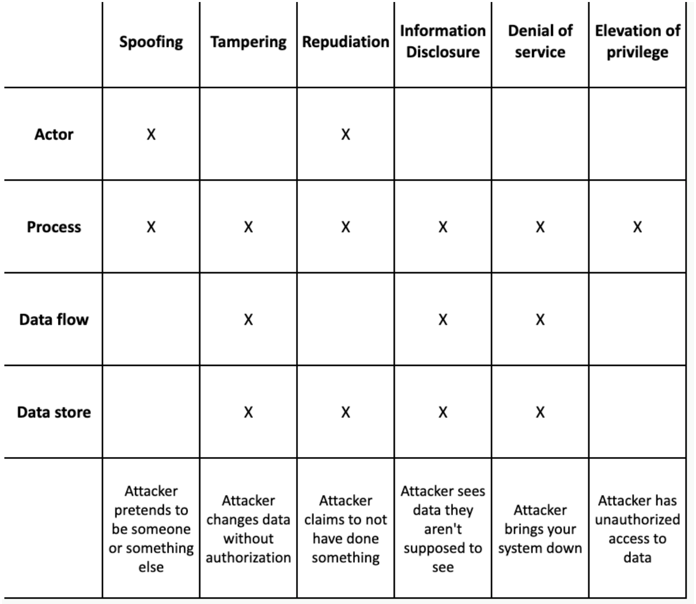
- Multi-signature wallet with keys in hardware wallet or HSM

Threat modelling

Data flow



Model



	Spoofing	Tampering	Repudiation	Information Disclosure	Denial of service	Elevation of privilege
Actor	X		X			
Process	X	X	X	X	X	X
Data flow		X		X	X	
Data store		X	X	X	X	
	Attacker pretends to be someone or something else	Attacker changes data without authorization	Attacker claims to not have done something	Attacker sees data they aren't supposed to see	Attacker brings your system down	Attacker has unauthorized access to data

Sources: https://github.com/OWASP/threat-model-cookbook/blob/master/INDEX.md

Vulnerabilities and misconfigurations

Web2. It may look like a big task, but reports are showing that if you do very basic things you are already doing better than 80% of companies that were breached:

- Patch your servers: be better than your peers.
- Cloud: track configuration baseline.
- Repos: scan for dependencies, misconfigurations and secrets.
- In-house apps: do pentests.

Web3

- Trusted open sources smart-contracts (like OpenZepppelin).
- Do third party smart-contracts audits.

Web3: Defeating on-chain threats

- Preview the transaction before execution to detect anomalies (Tenderly, etc)
- Verify raw transaction on trusted explorer, generate signature on the different device and compare it with one displayed on Ledger.
- Define slippage for transactions to prevent frontrunning and sandwich attacks.
- Use high liquidity in AMMs to reduce price manipulation.

Questions?