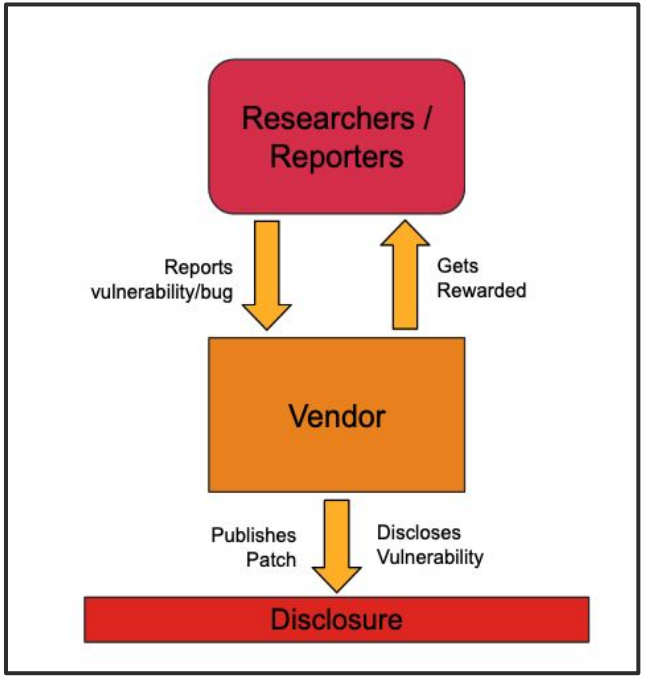
CRYPTOVULNERABILITY

Responsible Vulnerability Reporting and Disclosure on Blockchain

Kanak Dahake - kdahake3

Problem Statement:

- Vulnerability reporting is the practice of reporting security vulnerabilities in computer software or hardware.
- These vulnerabilities must be addressed by the vendors of this software or hardware before any malicious adversary could take advantage of them. Furthermore, the addressed vulnerabilities should be disclosed to the public or the customers promptly.
- Current Reporting platforms have shortcomings. Such as:
    - Managed by private centralized entities.
    - No assurance of fair rewards.
    - Minimum incentives driving the vendors for timely public disclosure.
    - Customers are often unaware of the potential vulnerabilities and risks to their assets.
- The complete lifecycle of vulnerability from discovery, reporting, resolving, patching, and disclosure involves multiple parties. Each party has different motivations and barriers that needs to be addressed.
- Silos of market solutions to address specific functions in the vulnerability lifecycle fail to work together and needs third party involvement.



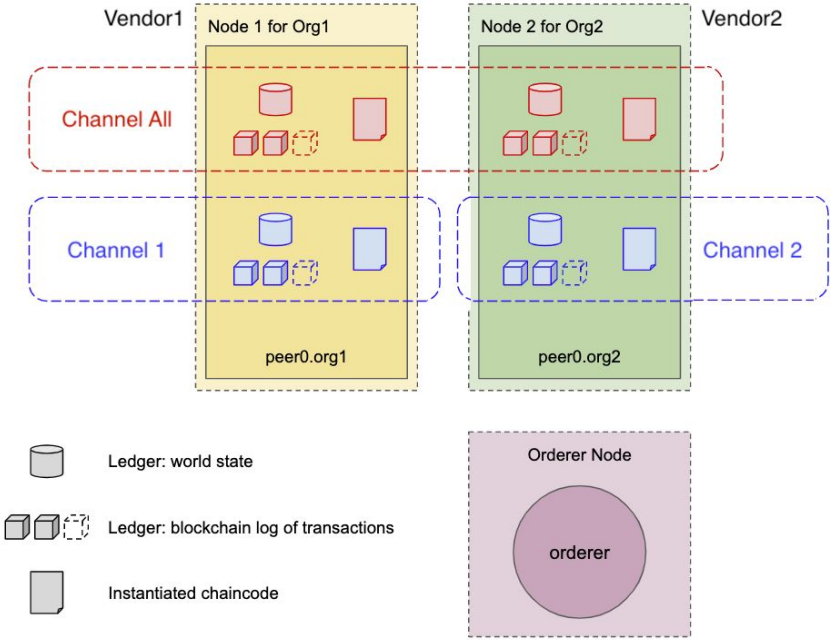
Solution Statement:

- Using blockchain to implement a Transparent, Privacy-focused, and Incentive-driven system to the traditional vulnerability reporting and disclosure processes.
- Provide immutability to the vulnerability report and track any modifications throughout the vulnerability lifecycle.
- Reporters and vendors can work on the same report adding/appending their detailed findings.
- Provides transparency to the process by making the number of solved and unsolved vulnerabilities of each product available to the customers. Thus provides clear incentives and enforced deadlines for the vendors to patch their products in time.
- Ensure a responsible disclosure using the deterministic smart contracts.
- Maintain the privacy of the reporters and ensures rewards for a valid report.

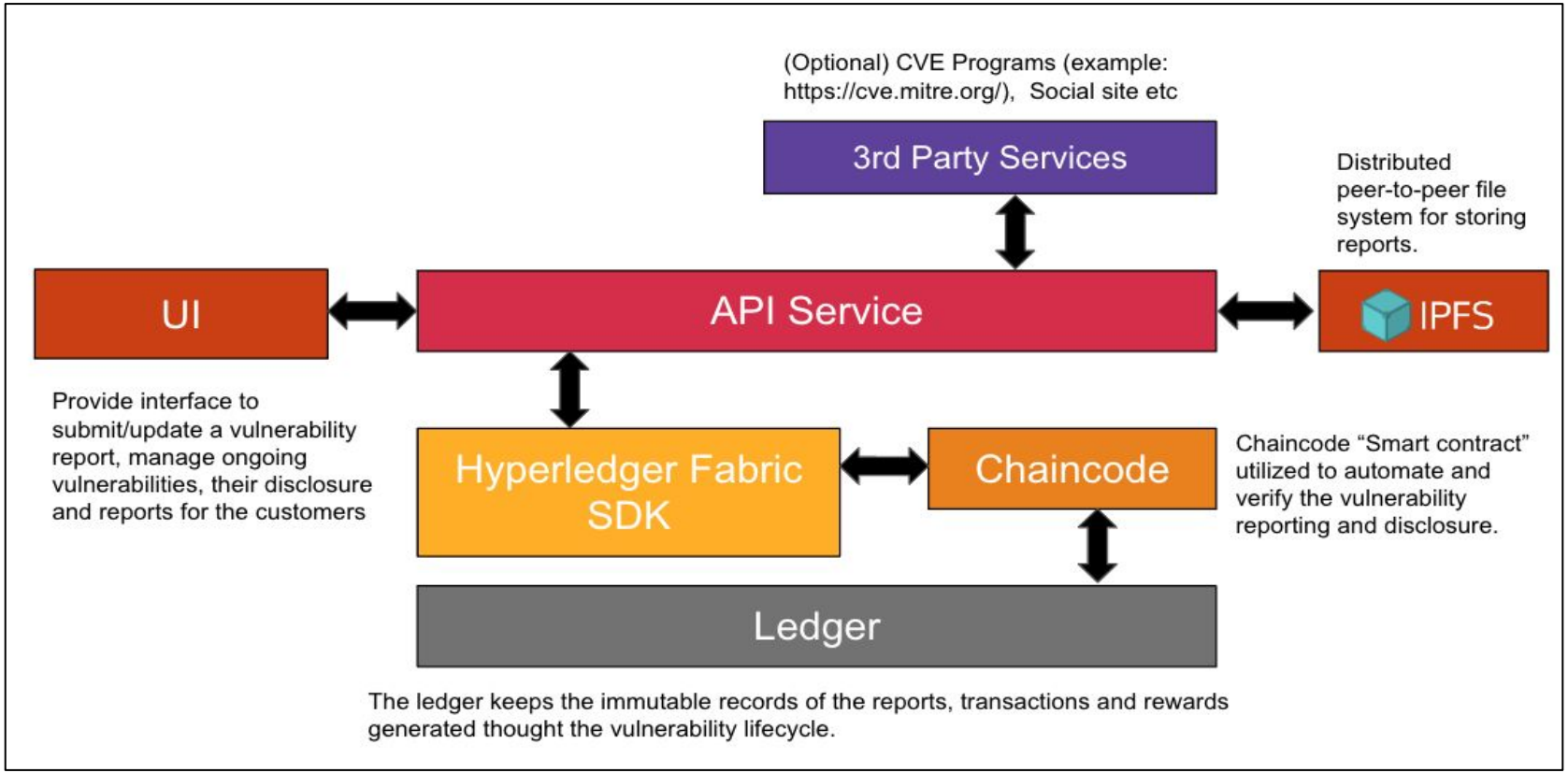
Solution Design:

- A Blockchain-based framework that can bring the best of both worlds i.e. bug bounty and in-house Vulnerabilities reporting programs.
- The solution will allow vendors to participate in a permissioned network. Multiple vendors will form a network which will then execute smart contracts and validate the transactions flowing through the network.
- Each vendor will have its secure and private channels/ledger where most of the vulnerability-related transactions would be handled.
- However, the chaincode used by each vendor would be distributed and managed by a common orderer, thus maintaining the integrity of transactions.
- A central ledger will keep track of metadata and metrics across the network. This ledger is associated with the common channel accessible by all participating parties.

Hyperledger Fabric Network:



Architecture of the System:

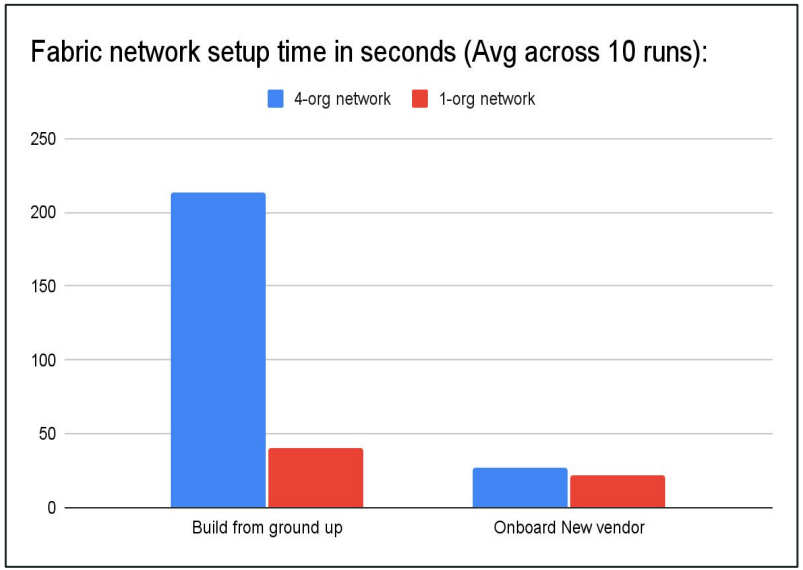


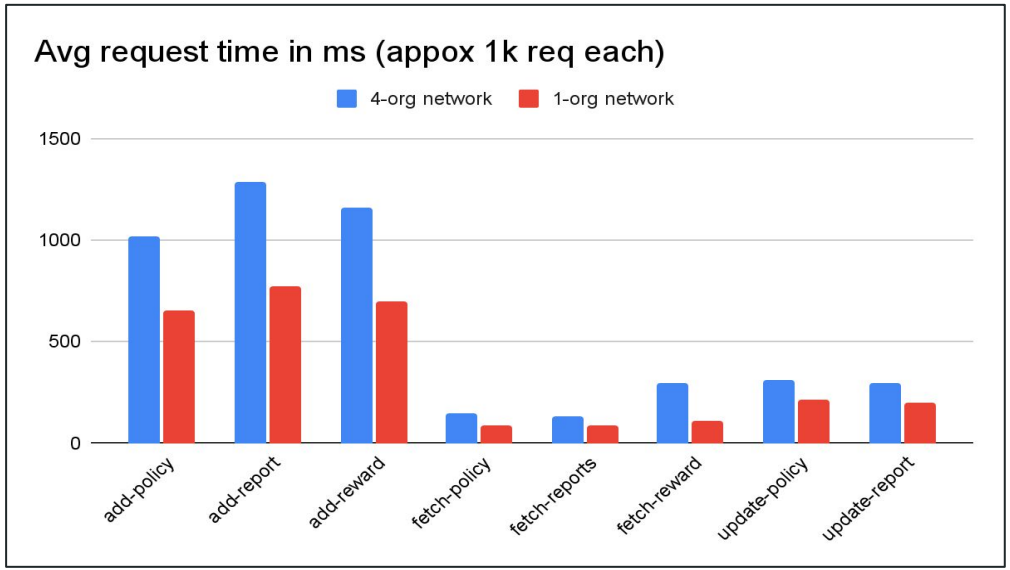
CRYPTOVULNERABILITY

#Crypto-Vulnerability

Evaluation:

- Since we cannot work with real vulnerabilities, evaluation metrics were collected using simulation cases based on the different states in the vulnerability lifecycle.
- Thinking of it as a decision tree, for example, starts with a vendor creating a policy, then reporter creating a report against the policy. This report can be valid, invalid, duplicate, rejected, etc.
- Further reporters could dispute or negotiate and so on till it's rewarded or just dropped.





Limitation

- Current implementation which is based on permissioned blockchain requires some level of configuration and efforts for onboarding a new vendor.
- Majority of vendors can form consensus and manipulate new vendor onboarding or transactions coming into the network (51% attack or majority attack). Although they can’t alter the data on the ledger.
- In current architecture the “API Server” is a single point of failure. However by adding redundancy and scaling this can be solved.

Future Work

- A CVE specific unique **NFT** rewarded to the reporter, which they can showcase or trade.
- Integrate native payments in cryptocurrency (**Bitcoin**, **Etherium**, etc) to User wallets.
- The common ledger can be piped on to a Public blockchain for maintaining public trust.
- Integration with third party services like CVE Programs (example: https://cve.mitre.org/), Social feeds (twitter, slack) etc.

CVE
@CVEnew · 8h

CVE-2022-45188 Netatalk through 3.1.13 has an afp_getappl heap-based buffer overflow resulting in code execution via a crafted .appl file. This provides remote root access on some platforms such as FreeBSD (used for TrueNAS). cve.mitre.org/cgi-bin/cvenam...

CVE
@CVEnew · 9h

CVE-2022-40773 Zoho ManageEngine ServiceDesk Plus MSP before 10609 and SupportCenter Plus before 11025 are vulnerable to privilege escalation. This allows users to obtain sensitive data during an export of requests from the list view. cve.mitre.org/cgi-bin/cvenam...

CRYPTOVULNERABILITY

Thank You!