TestOnNeed

Blockchain Security Audit with TestOnNeed

Solution Specification Sheet

Blockchain, the talk of the industry, is foreseen as the future for transaction what the internet did for information. The information is the data as processed, stored or transmitted, whereas transaction is the exchange of virtually anything of value. The action of conducting business exchange is by buying and selling anything of value; that is a business deal, demands strong security guarantees than ever before. The blockchain is fit for purpose.

For companies and individuals, the blockchain enables peer-to-peer shared, immutable, distributed ledger infrastructure that facilitates the process of recording transactions and tracking assets. The best of all, it is distributed helps to reduce cost by disintermediation of a centralized institution. Although the blockchain address natively protecting the integrity of data, it does not mean the solution is immune from attacks.

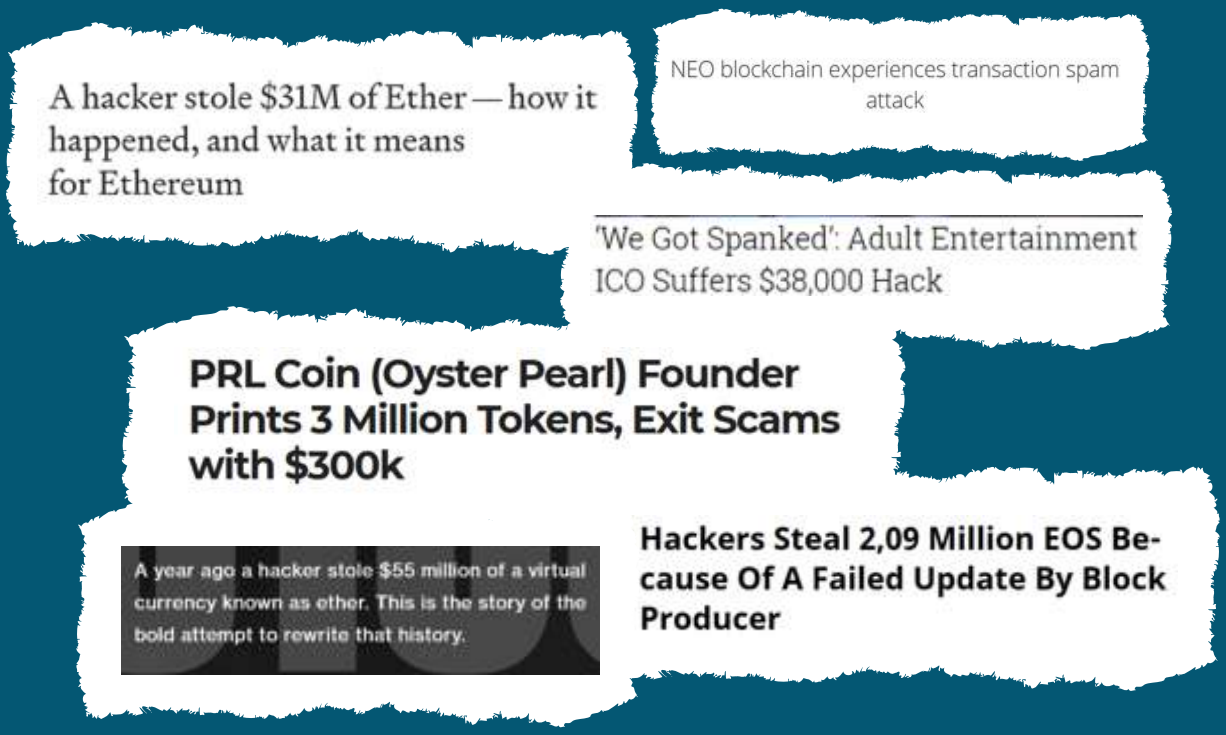

Figure 1 Example Victims of Security Vulnerabilities

Still, even the staunchest advocates admit that securing blockchain from the attack is challenging, but it is business critical and must be addressed. If not guaranteed, your company may have to face challenges as other victims. Every day new attacks are launched exploiting vulnerabilities of blockchain such as re-entrancy attack, oyster pearl attack, parity attack, and others. As a result, more and more company becoming the victim, lose money, customer, and even business.

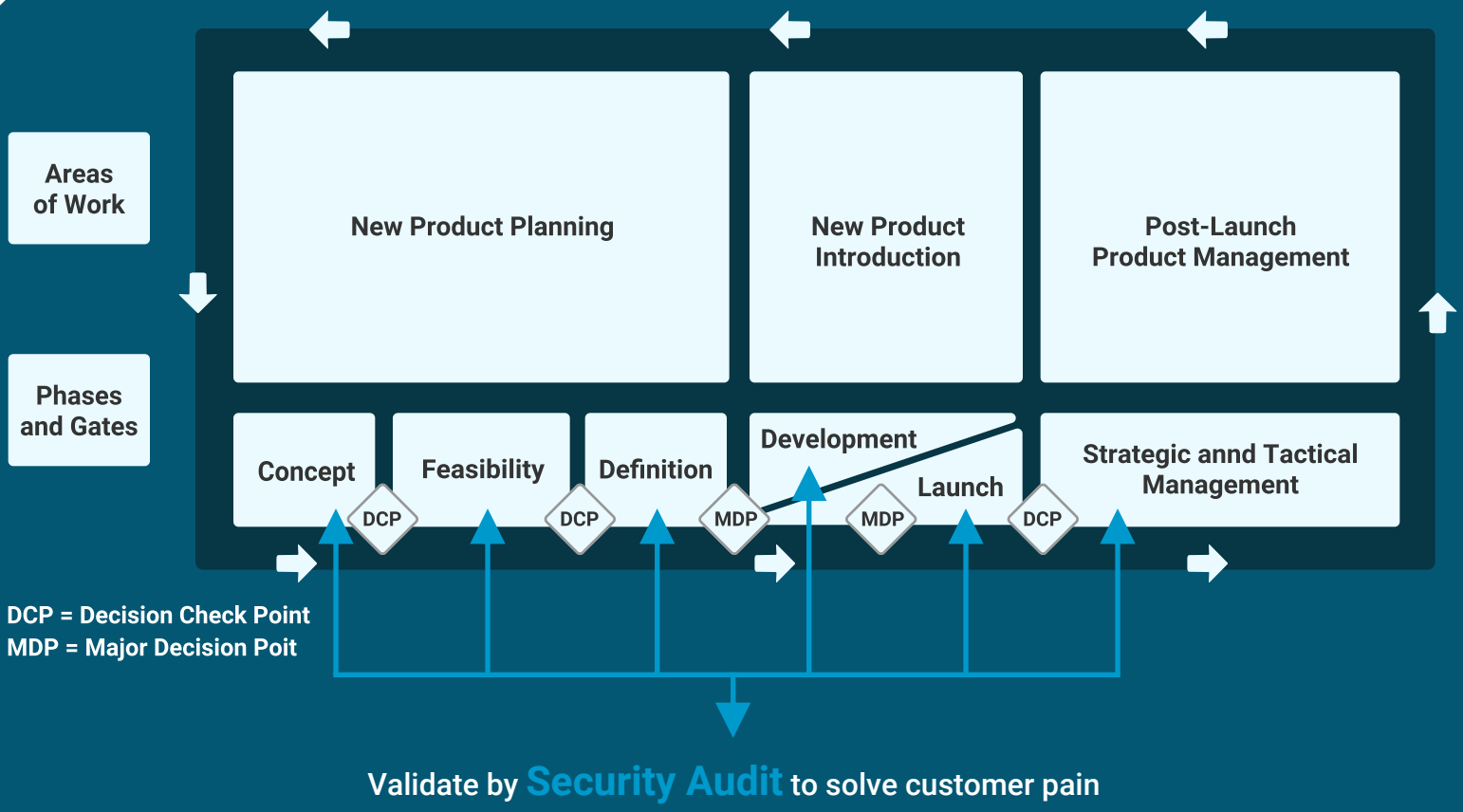

Figure 2 Product Development Life Cycle (PDLC)

The security audit is a process intended to reveal flaws in the security mechanisms of a product to ensure customer pain is addressed and protected throughout the product development life cycle (PDLC). Actual security requirements audited depend on the product implementation that is responsible for collecting, processing, storing, transmitting, and exchanging valuable information as intended. It may span across users, devices, decentralized application (DApps), connectivity, protocols, cloud, centralized applications, and others. The companies implementing blockchain must prevent security risks and should plan to prepare, protect, and test their end-to-end solutions before and after deployment.

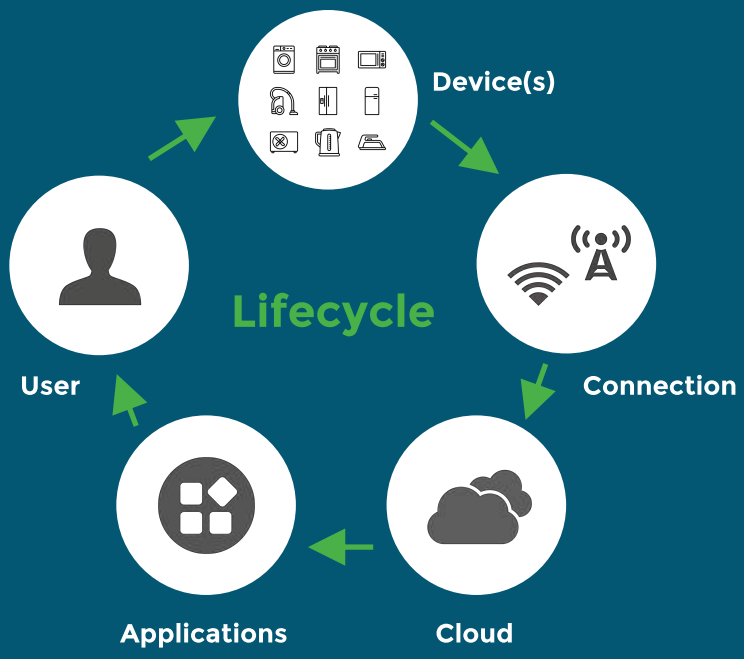

Figure 3 End to end Security Audit

The end-to-end blockchain testing requires a unique skill set to characterize the performance from installation to infrastructure, business or public network and applications. And, the security audit requires mindset as that of hackers using the best features from multiple tools, techniques, and practices to secure from identity and access to public key infrastructure, and smart contract. Among others, the smart contract security audit is of critical importance as it defines the set of rules that govern all of the transaction in the blockchain network. The audit should cover a broad range of areas from utility tokens to security tokens, DApps, protocols, APIs, and others.

Not all smart contracts are “Smart.” The recent hacks and loss of dollars are proof. In many cases, not detecting defects early enough in the product life cycle and deploying in the production network is the root cause for the failure. To avoid such costly mistakes and becoming another victim of crypto hacks, a security audit from a trustful third-party partner before and after deployment is the most ingenious way. The trusted partner must validate the reliability of the smart contract by complete assessment of your system architecture and your smart contract codebase using industry best practices and processes. The validations checklist of the smart contract must include and not limited to:

- Definition of the visibility specifier functions
- Data in storage and memory
- Overflow and underflow of variables
- Secure external calls from re-enterancy attack and untrusted code
- Optimize Gas to avoid or minimize consumption

- Analyzing the security of the on-chain data
- Deploying the code on testnet using multiple clients to run live tests
- Bug bounty, Race conditions, transaction ordering dependence, DDOS attacks
- Timestamp dependencies, compiler related, oracle calls and others

Besides, the audit process should cover various validation aspects such as manual, automation and penetration testing. It should be performed by audit experts using the combination of best features available in multiple open sources and internal automation tools that covers the following and more:

- Visualization (e.g.) Sūrya, Solgraph, EVM Labs, ethereum-graph-debugger
- Static and Dynamic Analysis (e.g.) Mythril, Oyente, Securify, SmartCheck
- Weakness OSS Classification & Test Cases (e.g.) SWC-registry, SWC Pages
- Test Coverage (e.g.) solidity-coverage
- Linters (e.g.) Solcheck, Solint, Solium, Solhint

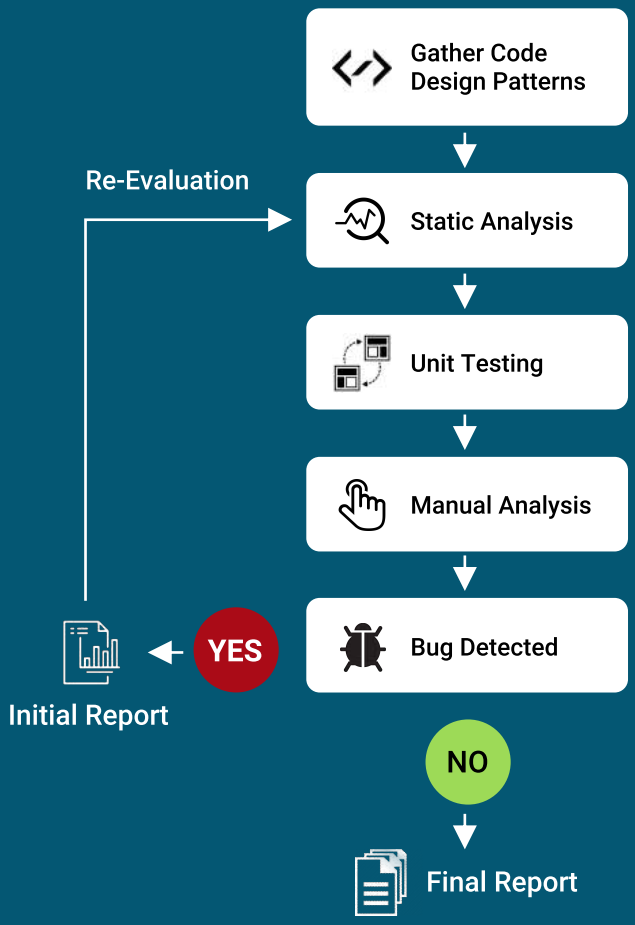

Figure 4 Audit Practices and Processes

Finally, the trusted third-party provider should deliver a detailed security audit report including an executive summary that outlines the overall state of the smart contract and the technical findings, coupled with recommendations. It should include documentation of defect severity (low, medium, high) involving multiple exploits compiled to outline how an attacker could chain vulnerabilities together to compromise your smart contract. Also, a root-cause analysis to provide both tactical and strategic implementation recommendations.

About TestOnNeed

Being efficient and fast is all about transformation and success is all about welcoming it. We at TestOnNeed, the trusted third-party partner, live only to create flawless software application products on-demand. We better the speed, scale, coverage, and quality of Blockchain, and assisting technologies such as Artificial Intelligence (AI), Internet of Thing (IoT), and Multi-Edge (Mobile) Edge Computing (MEC) software application products. We provide ready-to-go **Hyperledger BTaaS (https://bit.ly/2W5ie4t)** end-to-end private blockchain solution with test plan that consists of 350+ automated testcases covering Installation, Infrastructure, business network and applications, and performance benchmarking.

Figure 5 Hyperledger ready-to-go BTaaS Solution

QuillAudits

To redefine blockchain security standards and to provide end-to-end blockchain solution that includes both private and public blockchains, TestOnNeed teamed up with Quillhash, the blockchain consultancy, and development experts, to launch **QuillAudits – The Security Audit Platform.**

Figure 6 Partnership to Accelerate Blockchain Adoption

The QuillAudits is a fully automated platform to verify smart contracts, DApps, protocol, and decentralized exchange to prevent security vulnerabilities that may harm our customer's blockchain platform integrity.

Figure 7 QuillAudits – The Security Audit Platform

As a trusted partner, we are engaged with some of the customers who benefit from our QuillAudits solutions as depicted in Figure 8. And, you may refer the example published security audit reports at **https://bit.ly/2JkaFFQ** and **https://bit.ly/2Tatpas**

Figure 8 QuillAudits Customers

https://testonneed.com/

Contact Information

At TestOnNeed, we don't just test, automate and DevOps; we make products better. Our 'Testopers,' do this by testing, automation, and DevOps with open sources using an open source testing ecosystem. We may be the best opportunity for your future business.

If you need additional information or have questions about our solutions or demo, pricing, and purchase, please reach out to us at sales@testonneed.com, and visit us to start your project at **https://testonneed.com**

QuillAudits Solution Ordering Information	
TON-BTaaS-QA-SC	The Security Audit for the blockchain smart contract