A Smart Contract Blockchain Penetration Testing Framework

Shyam Meshram

Received: 1 January 1970 Accepted: 1 January 1970 Published: 1 January 1970

Abstract
Likened to old-style contracts, smart agreements motorized by blockchain ensure that deal processes are real, safe, then well-organized. Without the need aimed at third-party mediators like lawyers, smart contracts enable transparent processes, cost-effectiveness, time efficiency, and trustlessness. While old-style cybersecurity attacks on keen agreement requests can be thwarted by blockchain, new threats and attack vectors are constantly emerging, which affect blockchain in a manner alike toward additional web and application-based systems. Organizations can develop and use the technology securely with connected infrastructure by using effective blockchain testing. However, the authors discovered throughout the sequence of their investigate that Blockchain technology has security issues like permanent dealings, insufficient access, and ineffective plans. Web portals and other applications do not contain attack vectors like these. This study introduces a brand new penetration testing framework for decentralized apps and clever contracts. Results from the suggested penetration-testing methodology were com-pared by those from automatic diffusion examination scanners by the authors. The findings revealed gaps in vulnerabilities that were not disclosed during routine pen testing.

Index terms—smart contracts, attack vectors, cyber-security, blockchain, cyber threats.

1 A Smart Contract Blockchain Penetration Testing Framework

Testing Framework
Abstract—Likened to old-style contracts, smart agreements motorized by blockchain ensure that deal processes are real, safe, then well-organized. Without the need aimed at third-party mediators like lawyers, smart contracts enable transparent processes, cost-effectiveness, time efficiency, and trustlessness. While old-style cybersecurity attacks on keen agreement requests can be thwarted by blockchain, new threats and attack vectors are constantly emerging, which affect blockchain in a manner alike toward additional web and application-based systems. Organizations can develop and use the technology securely with connected infrastructure by using effective blockchain testing. However, the authors discovered throughout the sequence of their investigate that Blockchain technology has security issues like permanent dealings, insufficient access, and ineffective plans. Web portals and other applications do not contain attack vectors like these. This study introduces a brand new penetration testing framework for decentralized apps and clever contracts. Results from the suggested penetration-testing methodology were com-pared by those from automatic diffusion examination scanners by the authors. The findings revealed gaps in vulnerabilities that were not disclosed during routine pen testing.

2 I. Introduction

Research into and adoption of blockchain technology has exploded across a wide range of businesses. Blockchain relies happening peer-to-peer dealings and is dispersed decentralized without any centralized authority or third-party involvement. Digital programmed scripts of codes known as Smart Contracts [1] are kept inside a Blockchain. Once sure sections [3] by particular predefined circumstances remain met, these programmed become anger resistant, being self-verifying, self-executing, and selfenforcing [2] numerical contracts. Smart Contracts are
3 II. LITERATURE SURVEY

The use of Blockchain technologies and Keen Agreements for numerous manufacturing areas was surveyed by
Ch et al. (2020) [33] suggested evaluating such attacks in order to offer security measures due to the daily rise in
cybercrimes. Controlling cyberattacks with manual methods and technical methods frequently fails [34,35]. The
writers suggested a computational application using mechanism knowledge that can analyses then categories the
prevalence of cybercrimes according to republic before national sites. To analyses and categories structured and
unstructured data, the writers applied security measures and data analytics. According to the testing analysis,
the accuracy was 99. specifically for script Keen Contracts, the writers used these earlier languages. The authors
concentrated on 14 main risks and noticed that some risks would not be covered by existing tools, so they also
created a static analysis detecting tool. The use of Blockchain technologies and Keen Agreements for numerous manufacturing areas was surveyed by

Concentrated on 14 main risks and noticed that some risks would not be covered by existing tools, so they also
Blockchain technology adoption and smart contracts for commercial sectors, particularly the manufacturing industry, was covered by Mohammed et al. (2019) [22]. The authors noted that there were difficulties to be overcome for effective integration with numerous systems and components. The authors suggested using a middleware approach to fully utilise Blockchain and its capabilities, which would result in smart manufacturing.

Draper et al. (2019) [23] examined blockchain difficulties as well as security programmes like PGP and Proxy chain. The authors looked at the main issues and discussed solutions for issues like latency, integration, throughput, and regulatory issues. They also gave suggestions for future research.

By means of smart agreements, large data, and ICT, Mah-mood et al. (2019) [24] concentrated happening refining the safety and output of logistics process. Customers were pro-vided with an email and SMS alerting system along with the application of cable for trailing ampules in actual period. The systems were used by customers to follow the delivery of their shipments both domestically and internationally.

By using a human-written and understandable Contract doc-ument, Tatesthielal. (2019) [25] obtainable a novel perfect to automatically make feasible Keen Agreements in Blockchain-founded Overexcited ledger. Utilising real-world case studies from Smart Contacts in various industries, the authors developed this by means of a pattern with skillful usual linguistic and assessed the outcomes.

Complete impression of Keen Associates founded on Blockchain was proposed by Wang et al. (2019) [26]. The six-layer architecture framework and the stages then workings of Keen Agreements were introduced by the authors. The authors also discussed the application security issues, reviewed the legal and technical challenges, and provided references for further study [27].

Blockchain-based Internet of Things were created by Ozyilmaz et al. (2019) [28] using cutting- After looking over investigate IDs happening blockchain and security tests, the authors found holes that essential toward remain filled.

The organization of the investigate papers themselves re-mains a major issue because novel organizations related toward blockchain and penetration testing need to be defined in contrast to OWASP or web and application security testing.

Numerous organizations and researchers also study other issues similar dormancy then the heftiness of the request then schemes.

Review then research happening the problems with lawful then controlling obedience transported on by the laws and regulations of various nations.

The most important features, and some of the hardest to deploy, are cybersecurity risks and privacy. Due to the permissionless nature of blockchain, nodes, which are public systems, can be manipulated and used for nefarious ends. The fact that all worldwide slightly oversight before participation from a centralized expert further complicates the process.

Scalability of the nodes then storing connected toward cryptocurrencies remains the ability to manage the fluctuating deal degree cutting-edge a centralized scheme while maintaining the skill’s fundamental integrity.

4 IV. System Perfect

5 III. Gaps Identified

In order to set up a blockchain environment, a few pre-requisites must be installed as part of the basic tools needed by blockchain nodes. The authors configured Ubuntu OS 18.04 over-all-drive cutting-edge postures consecutively manifold bulges on Amazon Web Service. A piece bulge built happening the AWS platform uses the T3 instance perfect and hardware intended for a solitary occupant. A piece node has been built by 8 vCPU (Alpha CC), 32 GB RAM, and a 300 GB SSD vigor toward run the Smart Contract application.

6 V. Proposed Framework

The core challenging methods and facilities comprised cutting-edge the penetration testing outline include mist challenging, useful challenging, API challenging, addition challenging, safety challenging, then presentation challenging. Additionally, the situation includes testing techniques exact to the blockchain, such by way of peer/node stimulating, intense agreement challenging, then block challenging. The writers suggest using still request safety examination early on, beforehand the blockchain cypher is executed. This in-corporates the Blockchain Request Server, Framework, and Cypher Libraries along with custom application code for the runtime stage. Dynamic application security testing typically only makes use of equipment that tests the live blockchain applications. This is accomplished using replicated targeted attacks or specially crafted HTTP inputs [38]. The HTTP reaction is examined to identify the vulnerabilities. But DAST only offers limited inclusion because it has no idea what goes on inside the application. Similar to SAST, DAST [39] tools remain reasonable; a typical examination movement can take hours or even days to complete. This analyses all of the incoming then outbound HTTP circulation generated during characteristic challenging of the request, in addition to execution a complete runtime info and change watercourse inspection, combined with static analysis of altogether the cypher, by way of shown overhead. Fig. ?? shows how this makes it possible to conduct dynamic investigations that are comparable to but more effective than DAST without the need for specific safety examinations, abuse of the
impartial request, before participation of safety experts in the testing process. 
Since evaluation takes Toward
track involuntary practice cases then cyberph, the outline smooth provides JS then
Hardness growth environments.
Pen testers can build a tube aimed at finish-toward-finish provision aimed at sole Blockchain procedures, track
automatic writings aimed at relocation then deployment, and rebuild assets during the development phase. 
The
Ethereum Tester tool is the second, and it performs a filled examination suite with customised API provision
toward increase the productivity, time, then efforts of Pen Testers and Developers. Particularly during the pre-
diffusion challenging investigation stage, these tools assisted in identifying and preventing vulnerabilities that
had never been discovered or reported before. Fig. ?? below depicts the architecture of the blockchain and
its execution environment. Blockchain has been exploited by cybercriminals who demand ransom in the form
digital currencies or ransomware attacks. However, at the moment the vulnerabilities in Blockchain Smart
Contracts are the main target of attacks, which are the main source of revenue. Fig. ?? shows the proposed
Penetration Testing architecture.

The entire relations aimed at a piec e danger in relation to the event are determined by the authors cutting-
edge instruction toward estimate the risk equal. The threat equal remains calculated through first estimating the
treat level using thresholds and then using biased practice. Danger opinion heights and the Danger score work

jointly. As shown cutting-edge Bench 4 underneath, the Entire Danger Opinions are intended using the threat

severity range of one to four. According to the risk point and ratings, this remains intended by way of the total
of the danger opinions by the danger harshness heaviness. As shown in Fig. ??

7 below, AWS Example

Capacity then Photos remained occupied on a regular basis following each significant application and configuration
change. The systems’ committed EBS transmission capacity is 3500 Mbps, with a maximum speed of 10 Gbps.
Utilizing latent sensors, this evaluates weaknesses [30,37]. (Table ??). The additional re-mains the central
management attendant, which monitors the organization’s resident combination by various tools similar IDEs then
CI/CDs and supports features aimed at announcement, notices, then API become-toward-process by Soothing
API for customised additions, as shown in Fig. [4] below. It also compiles and discloses vulnerabilities discovered
by the operators.

place within the application, it provides a more accurate examination than conventional Penetration (Pen)
Testing tools. Furthermore, they are non on overall similar SAST or DAST substances. The writers used Package
Arrangement Examination (SCA) toward compile a list of altogether external components, such as libraries,
structures, and open-source software (OSS), that the application uses. Using the right tools for penetration
testing is equally crucial. This aids in identifying the application’s and module’s known and unidentified
ambiguous vulnerabilities. The authors used two particular tools to conduct Blockchain Coop Tests and suggest
them to all future Blockchain Coop Samples. The primary remains Chocolate truffle Outline, which offers a
humble then convenient environment for management and pen testing of applications related to smart contracts.
This framework features linking libraries, customized deployment, and support for implementations based on
Blockchain that range from simple to complex.

The writers used IP v4 Public Addresses with RDP, Putty, and SSH toward attach the bulges using Amazon
Mesh Facilities Examples, as shown in Fig. ??, The challenging remained done cuttingedge a pre-manufacture
setting, through the dangerous flaws listed underneath, and the writers attained diffusion stimulating happening
a profitable blockchain request that remained ready for production. These flaws correspond to the serious flaws
that were identified then charted to the OWASP Top 10 aimed on Blockchain Keen Agreements. Susceptibility
Injection, kind High level of danger The database SQL query comes after the strings have been validated and
whitelisted.

8 VI. RESEARCH PERFORMED

The Smart Contract Parsing module on the system has detected a buffer-out-of-bound issue. Due to the
inadequate sensitization of contribution, verification could remain disregarded then unauthorized instructions
could remain run. Ampere opposite bomb was launched happening the network’s ill bulges by this Sandbox
vulnerability. Three functions that used string concatenation queries to perform database operations on
parameters supplied by packages were discovered by the authors in the code of the Data subdirectory. Broken
Authentication Vulnerability Type.

Without the users’ consent, Swap enables a third party to eavesdrop on their conversations and download
files from either of their devices. Flaws prevent an immediate binding of petite speeches toward community
solutions. Slightly explanation that is unclaimed is vulnerable to attack. Problem. The Nearby-Swap feature is
vulnerable to various attacks when it is not implemented correctly. The best choice is to restrict access to the
Web server. A certain level of authentication ought to be in place. The application’s Nearby feature In order to
highlight the advantages of using a manual penetration testing approach over an automated scanner, the authors
compared the physical repercussions against two cutting-edge dispersal challenging analyzers. The names cannot
be revealed due to privacy concerns. One of the tools is based on symbolic execution, while the other one is still
based on lively chance challenges. This made sure that any double-dealing-related smart contract vulnerabilities
were tested. Cutting-edge order to verify and correct slightly keen agreement inconsistencies, the authors carried
out functional and non-functional challenging. The presentation then safety diffusion challenging devices to
understand the effectiveness of the physical still diffusion challenging achieved. The results obtained are shown
in Tables ?? and ?? . The writers likened the outcomes with those of earlier form announcements in order to
verify the validity of the coop verified Blockchain’s official release. The four main safety topographies are Tamp
resistant, Verification, Devolution, and Approval, as shown in Table ?? . As a result, it is confirmed that there
are no significant problems with the four security features in the manufacture announcement following manifold
coop examination repetitions, as opposed toward the pre-pen examination before the manifold coop examination
repetitions.

9 VIII. Conclusion and Future Work

For the automatic mixture of Keen Agreements that ampule feat the weaknesses of prey bulges, the writers
likened physical diffusion challenging by deuce request safety challenging gears. The introduction of summary-
based symbolic evaluation helped to ensure that the synthesis was manageable. As a result, fewer data paths
needed to be travelled through and explored by tools though upholding the accuracy of susceptibility enquiries.
By expanding on the summary-based symbolic evaluation, the physical diffusion challenging offered additional
optimisations that permitted comparable examination and other kinds of cyberattacks. The authors examined
the whole information usual by more than 25,000 Keen Agreements and prearranged recognized Keen Interaction
susceptibilities in the hunt enquiry. According to the experimental findings, manual pen testing performed
noticeably better than automatic keen contract gears cutting-edge footings of execution speed, accuracy, and
soundness of issues found. Additionally, physical diffusion challenging exposed ended 12 examples of the Lot
Excess susceptibility that were previously undetected. Despite being relatively new, blockchain technology
for Smart Contract applications holds enormous potential aimed at the upcoming of agreements. Blockchain
bout methods that container compromise the networks’ cybersecurity by taking advantage of their flaws. The
adoption process may then take longer as a result. The majority of bout courses at the finish operator before
data integrity level can be effortlessly evaded finished raising user consciousness and implementing blockchain
technology effectively, but others, similar those at the residual and only expert knowledge can be used to
mitigate application levels. It also illustrates how greatest cybersecurity bouts container remain carried out
trendy composed cloud-hosted requests and Blockchain-based Keen Agreement re-quests by mapping the top 10
OWASP vulnerabilities toward intimidations and bouts happening Blockchain.

10 Global Journal of Computer Science and Technology

Volume XXIII Issue II Version I of the Smart Contract are given the utmost consideration during Non-Functional
Testing. Though the Presentation Pen Test certain peak deal amount aimed on agreement performances, the
Safety Coop Examination protected Communal Susceptibilities then Feats reentrancy, bumper below then excess,
noise aimed on representative be-fore discernibility. As shown in Figs. 9 and 10, during the functional testing,
border examination rubrics, lawful/inacceptable arguments, then quarrel mixtures were used to validate business
requirements and rules.

11 VII. Results

The displays an unproven contract that is susceptible to fraud. Nobody can guarantee that the operations are
carried out in the specified order in a parallel or decentralized world. Doubt the purchaser purposefully alters
the instruction of deal implementation, the buyer might defraud the seller of Product X. Keen Agreement is
used by way of contribution aimed at the comparison with the first tool and is examined for any consistency
with real suggestions cutting-edge the predefined safety possessions of the second tool [40][41][42][43]. This is
contrasted with the outcomes of the physical diffusion testing. The writers conducted deuce contrasts that
analyses after addressing the flaws found during the Smart Contract’s penetration tests. The viability of the
current reality’s vulnerabilities was addressed right away, and computerized penetration testing tools that are
used in the industry for testing smart contracts were also examined. With a maximum attack programmed size
of three and a postponement break of 15 minutes meant on apiece Keen Agreement, the makers comprised extra
than 30,000 Keen Agreements. Correlation was carried out using electronic lively
Table 2: Blockchain related literature review categorization

<table>
<thead>
<tr>
<th>Paper Classifications</th>
<th>Stage 1</th>
<th>Stage 2</th>
<th>Stage 3</th>
<th>Stage 4</th>
<th>Final Review</th>
<th>Breakup %</th>
</tr>
</thead>
<tbody>
<tr>
<td>Smart Contract</td>
<td>38</td>
<td>29</td>
<td>17</td>
<td>12</td>
<td>10</td>
<td>26.8%</td>
</tr>
<tr>
<td>Blockchain Threat</td>
<td>33</td>
<td>26</td>
<td>18</td>
<td>14</td>
<td>0</td>
<td>23.7%</td>
</tr>
<tr>
<td>Attack Vectors</td>
<td>38</td>
<td>30</td>
<td>21</td>
<td>16</td>
<td>10</td>
<td>26.3%</td>
</tr>
<tr>
<td>Blockchain Cybersecurity</td>
<td>35</td>
<td>28</td>
<td>20</td>
<td>15</td>
<td>9</td>
<td>23.2%</td>
</tr>
<tr>
<td></td>
<td>144</td>
<td>140</td>
<td>98</td>
<td>66</td>
<td>43</td>
<td></td>
</tr>
</tbody>
</table>

Figure 2: A

Figure 3:
**VII. RESULTS**

**Figure 4:**

```
<table>
<thead>
<tr>
<th>Name</th>
<th>Volume ID</th>
<th>Size</th>
<th>Volume Type</th>
<th>IOPS</th>
<th>Snapshot</th>
<th>Created</th>
<th>Availability Zone</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>vol4653c0f...</td>
<td>8 GB</td>
<td>gc2</td>
<td>100</td>
<td></td>
<td></td>
<td>April 10, 2020 at 10:20</td>
<td>us-east-1d</td>
<td>in-use</td>
</tr>
<tr>
<td>vol6657720a...</td>
<td>8 GB</td>
<td>gc2</td>
<td>100</td>
<td></td>
<td>snapshot-0079112...</td>
<td>April 10, 2020 at 10:20</td>
<td>us-east-1d</td>
<td>in-use</td>
</tr>
</tbody>
</table>
```

**Figure 2:** AWS Node Instance setup

**Figure 3:** AWS Node Volume and Snapshots for changes

**Table 3:** Blockchain environment setup prerequisite

<table>
<thead>
<tr>
<th>Tool Name</th>
<th>Installation Steps</th>
<th>Tool Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MIST Browser</td>
<td>$ sudo git clone <a href="https://github.com/ethereum/mist.git">https://github.com/ethereum/mist.git</a></td>
<td>$ cd mist; $ curl -o -L <a href="https://yarnpkg.com/install.sh">https://yarnpkg.com/install.sh</a></td>
</tr>
<tr>
<td>Nodejs &amp; NPM</td>
<td>$ sudo apt install nodejs; $ node --version; $ sudo apt install npm</td>
<td></td>
</tr>
<tr>
<td>Metamask</td>
<td>Open <a href="https://metamask.io/">https://metamask.io/</a> on Google Chrome</td>
<td>Use &quot;Get Chrome Extension&quot; to install Metamask; Select add to Chrome ➔ Add Extension ➔ click on Metamask logo and Agree terms to use;</td>
</tr>
<tr>
<td>Solidity Compiler</td>
<td>$ sudo npm install solc</td>
<td>Setup Solidity compiler;</td>
</tr>
</tbody>
</table>
Figure 5: Deep level application security test
VII. RESULTS

Figure 6:

<table>
<thead>
<tr>
<th>Layers</th>
<th>Blockchain</th>
<th>Environment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Layer</td>
<td>Node ID</td>
<td>Graphical User Interface</td>
</tr>
<tr>
<td>Data Level Layer</td>
<td>State Transaction</td>
<td>Database Store</td>
</tr>
<tr>
<td>Consensus Layer</td>
<td>Proof-of-Work</td>
<td>Data Integrity Validation</td>
</tr>
<tr>
<td>Network Layer</td>
<td>Auto Node Discovery</td>
<td>Shared Infrastructure</td>
</tr>
<tr>
<td></td>
<td>Smart Contract</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Propagation Delay</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Virtual Machine</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Transaction Event</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Incentive Values</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Transaction Hashing</td>
<td></td>
</tr>
</tbody>
</table>

Fig. 6 Blockchain environment setup

Fig. 7 Proposed architecture

Table 4 Threat Severity Levels

<table>
<thead>
<tr>
<th>Rating</th>
<th>Severity</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Insignificant</td>
<td>Result of low or irrelevant log entry, can be ignored,</td>
</tr>
<tr>
<td>2</td>
<td>Minor</td>
<td>Alert due to more than one node or transaction, can be false positive</td>
</tr>
<tr>
<td>3</td>
<td>Moderate</td>
<td>Verified security event leading to a true positive event</td>
</tr>
<tr>
<td>4</td>
<td>Major</td>
<td>Ongoing security breach, requires significant management intervention</td>
</tr>
</tbody>
</table>


[Alladi et al. ()] Blockchain applications for industry 4.0 and industrial IoT: a review. IEEE access, special section on distributed computing architecture for cyber-physical systems, T Alladi, V Chamola, R Parizi, R Choo. [10.1109/ACCESS. https://doi.org/10.1109/ACCESS 2019. 2019.2905674. 2019.


11 VII. RESULTS


