Global Journals LaTeX JournalKaleidoscope™

Artificial Intelligence formulated this projection for compatibility purposes from the original article published at Global Journals. However, this technology is currently in beta. *Therefore, kindly ignore odd layouts, missed formulae, text, tables, or figures.*

*CrossRef DOI of original article:*

# 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 trust lessness. 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

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 thirdparty mediators like lawyers, smart contracts enable transparent processes, cost-effectiveness, time efficiency, and trust lessness. 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

esearch into and adoption of blockchain technology has exploded across a wide range of businesses. Blockchain relies happening peer-topeer dealings and is dispersed decentralized without any centralized authority or third-party involvement. Digital programmed scripts of codes known as Smart Con-tracts [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 able to carry out transactions in real-time, for a small fee, and with a higher level of security [4]. Cryptocurrency nodes on the Blockchain network work toward inform the distributed, see-through ledger. All nodes view this inform, which remains checked [5] before it is accepted by the network.

Presumptuous the similar car's information, possession, IDs, then proposal are accessible, there is not at all involvement from a 3rd party, and advancedlevel security and information are obtainable, unaltered, and dispersed across the Blockchain network. Each network node verifies the information, but nobody has complete control. Use of the smart contract to carry out the purchase order. This system would be protected and instantaneously funded by cryptocurrency [6]. Instanta-neous ownership transfer takes place via digital identity on the blockchain ledger. The transaction is completed and the Blockchain network's ledger is updated by all nodes [7]. Banks or lending organizations use a similar procedure to process loans or receive automatic payments. Blockchain can be used by insurance companies to process claims. Instead of using a traditional transaction process, mail sections can procedure payment on distribution using Keen Agreement schemes [8].

This idea [6] is put into practise when a tenant and a prop-erty owner are involved in purchasing or renting apartments. Tokens or cryptocurrencies can be used to offset monthly rent or EMIs. Therefore, by means of Keen Agreement schemes that are motorized by Blockchain Technology, any transaction is handled effectively and securely [9]. These have been accepted by the worldwide securities connections in the United States government [10] and Australia [11]. Though, Blockchain networks are also subject to bouts similar Denial of Service (DoS) [12] and Autonomous Decentralised Organisation (DAO) [13], far similar cyber intimidations [10] and assaults on systems and applications held in the cloud. And cyberattacks that target blockchains, which are covered in the research's later sections. Blockchain environments, hosted applications, and conventional IT infrastructure all face com-parable cybersecurity risks. The attack vectors are mechanism bulges.

? Basis Code Issues: insecure basis code Reentrancy attacks container result in the control being transferred to un-trusted purposes of additional keen agreements, which may behave in an illogical manner or be used maliciously. In 2016, basis code flaws in an Ethereum [14] Smart agreement cost the company $80 million.

# 3 II. Literature Survey

Following a four-stage selection process that resulted in the shortlisting of 38 pertinent book the whole thing, as shown in Fig. **??** below, the authors identified 144 investigate papers on blockchain and security testing that had been published from 2016 to the present for this study. In this section, a few pertinent reviews are mentioned. We chose to focus on the last three years because they have seen the most significant development then alterations in the Blockchain Keen Agree-ment domain, as well as the most recent cyberattacks, threat vectors, and vulnerabilities that have been identified and used by cybercriminals. The general distribution of the investigate papers across the subgroups chosen for the works appraisal is shown in Table **??**. Micro-Service applications were used by Tonelli et al. (2019) [17] to implement a Blockchain-founded Keen Agreement. The authors used a collection of Smart Con-tracts to create a case study in which they examined and fake the Keen Agreement micro-service building. The outcomes demonstrated the feasibility of maintaining similar paradigms and functionality while implementing straightforward micro-services. Romoti A fault-tolerant application promoting con-sciousness then simplicity of programming in Blockchain was future by Amoordon et al. (2019) [18]. The authors' suggestion of one application per blockchain showed enhanced performance and decreased vulnerability to security attacks. The use of this platform for Smart Contract applications on Blockchain technologies like Ethereum and Bitcoin may be ideal.

A review on blockchain security risks, concentrating on the programming languages then Security risks related by keen agreements relate to a variety of areas, reaching after source code flaws, computer-generated mechanism vulnerabilities, unconfident runtime environments, to the Blockchain network itself, when developing with then applying blockchain-based keen agreement solutions. Among tedge are:

? Multifaceted Skill: Once attempting to project and con-struct Keen Agreements after cut or localised versions, the system is not at risk for security flaws but rather the execution. Blockchain cannot be implemented by standard programmers and developers. This calls for specialised knowledge. [14] concentrated on manufacturing IoT bulges [15] and created a novel dispersed model [16] founded on the Blockchain net. Compared to traditional architecture, this enhanced security and privacy [29] and optimized application delivery. The traditional architecture became ineffective as the network size and node count increased, though the future architecture arose as a workable answer. [32]. The authors talked about potential application areas, implementation difficulties, and problems preventing the acceptance of blockchain skill aimed at manufacturing 4.0.

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

Al-Jaroodi et al. ( ??019) [20]. The authors noted that while the cost of deployment and delivery was decreasing, the use of Blockchain augmented manufacturing transparency, security, efficiency, and traceability.

Blockchain technology adoption and smart contracts for commercial sectors, particularly the manufacturing industry, was covered by Mohammed et al. ( ??019) [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. ( ??019) [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 processs. 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, Tateshietal. (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-edgepostures consecutively manifold bulges on Amazon Web Service. Apiece bulge built happening the AWS platform uses the T3 instance perfect and hardware intended for a solitary occupant. Apiece 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 cyphers, 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 of 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 apiece 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 together. 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 [36,37]. (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 Near-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 summarybased 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

# 11 VII. RESULTS

12

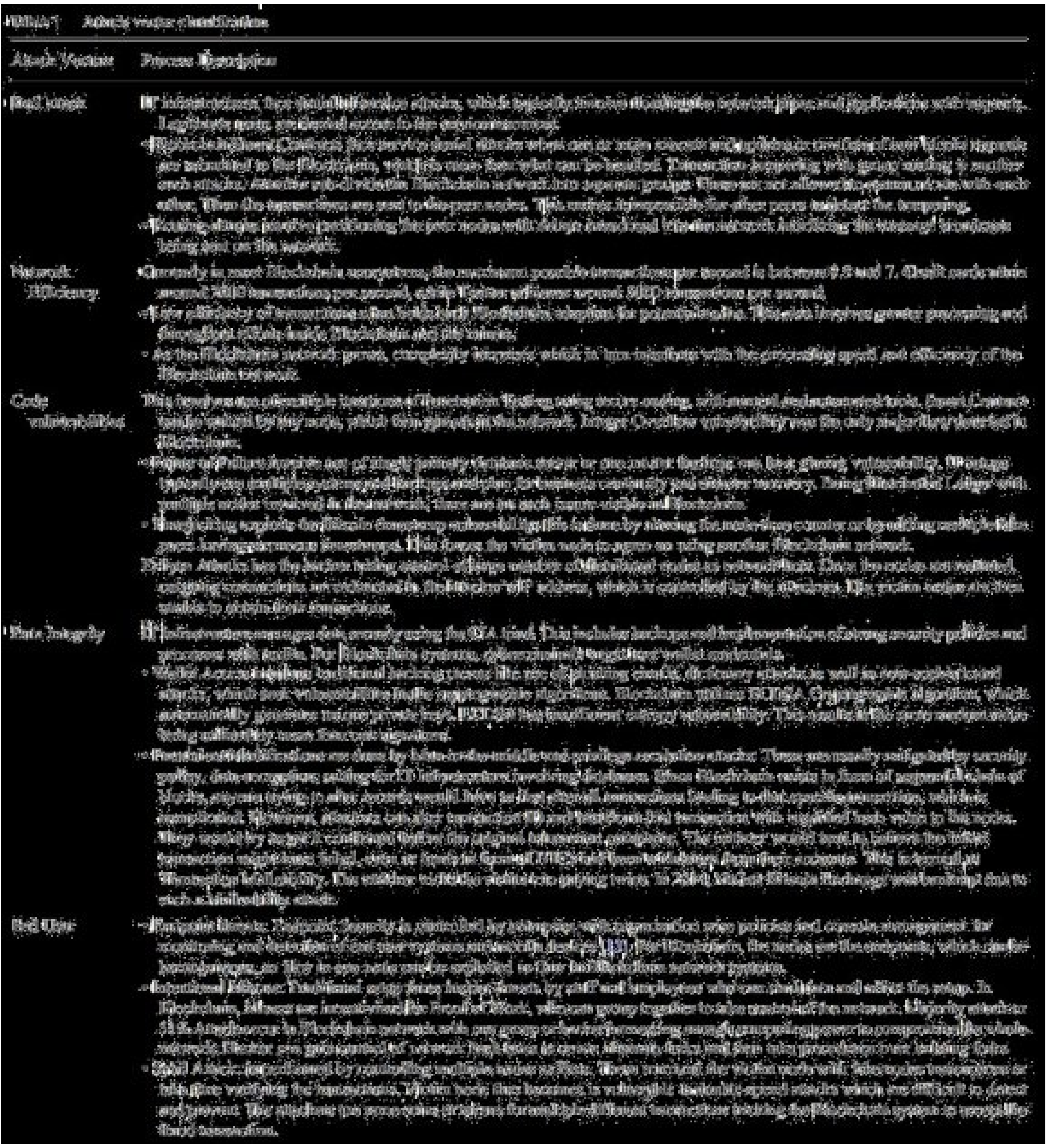
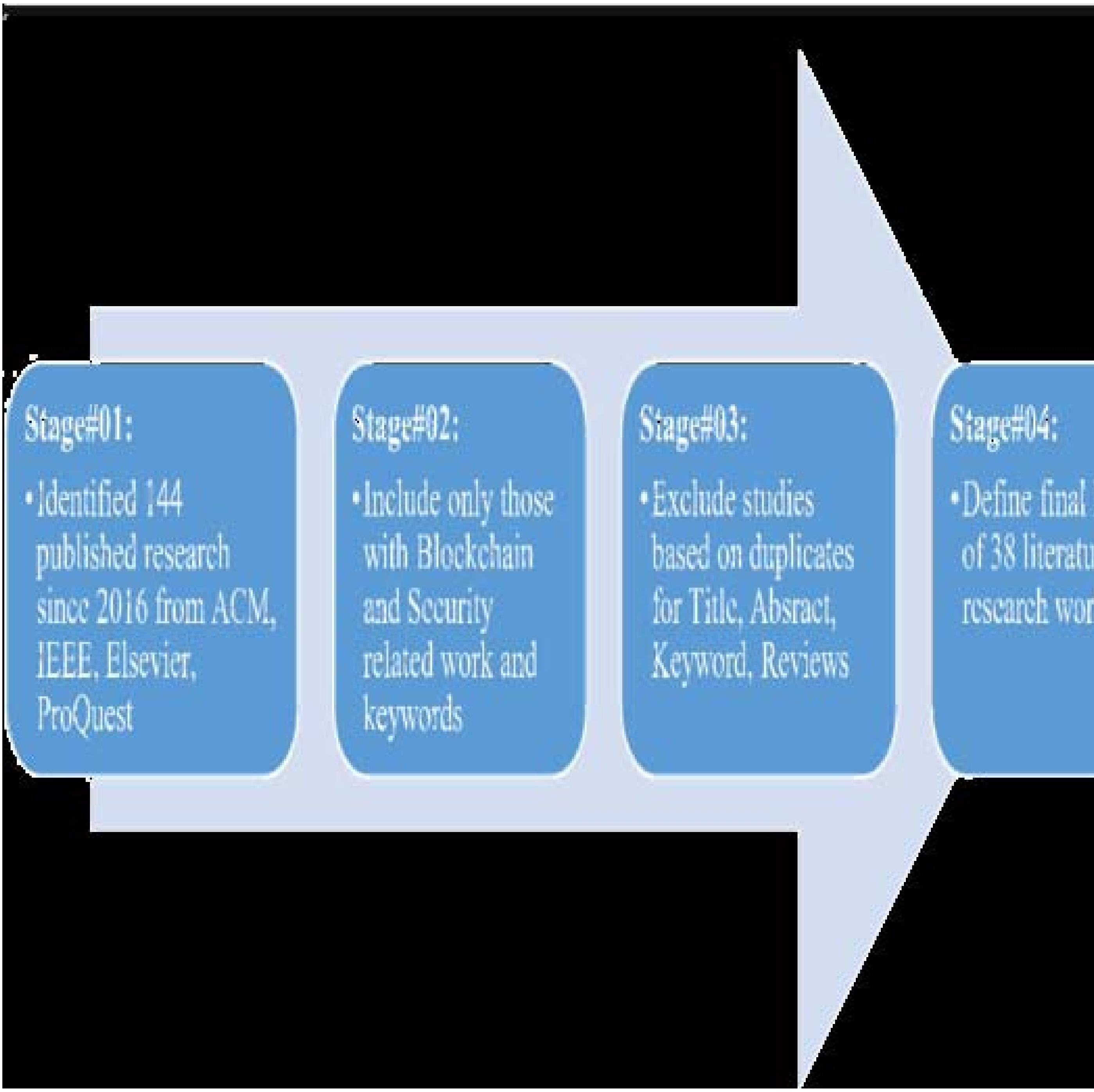


Table 1 Attack vector classification

| Attack Vectors | Process Description |
|---|---|
| [illegible] attack | IT infrastructure, [illegible] attacks, which typically involve [illegible] network pipes and applications with requests. Legitimate users are denied access to the environment.<br>• [illegible] denial [illegible] attacks [illegible] are submitted to the Blockchain, [illegible] than what can be handled. [illegible] each attacks [illegible] Blockchain network into separate groups. [illegible] other. Then the transactions are sent to the peer nodes. This makes it impossible for other peers to detect the tampering.<br>• Routing attacks [illegible] the peer nodes [illegible] network [illegible] being sent on the network. |
| Network Efficiency | • Currently in most Blockchain ecosystems, the maximum possible transactions per second is between 3.3 and 7. Credit cards [illegible] around [illegible] transactions per second, while Twitter [illegible] around [illegible] transactions per second.<br>• Low efficiency of transactions [illegible] Blockchain adoption for [illegible]. This also involves greater processing and [illegible] inside Blockchain and the miners.<br>• As the Blockchain network grows, complexity increases, which in turn interferes with the processing speed and efficiency of the Blockchain network. |
| Code vulnerabilities | This involves the [illegible] Testing using secure coding, with manual and automated tools. Smart Contracts can be [illegible] by any node, which then [illegible] the network. Integer Overflow vulnerability was the only [illegible] detected in Blockchain.<br>• [illegible] of Failure [illegible] single [illegible] vulnerability. [illegible] for business continuity and disaster recovery. Being Distributed Ledger with multiple nodes involved in the network, there are [illegible] Blockchain.<br>• [illegible] exploits [illegible] by [illegible] another Blockchain network.<br>Eclipse Attacks: [illegible] taking control of large number of [illegible] nodes [illegible]. Once the nodes are [illegible], outgoing connections are redirected to the attacker's IP address, which is controlled by the attackers. The victim nodes are then unable to obtain their transactions. |
| Data Integrity | IT infrastructure manages data security using the CIA triad. This includes backups and implementation of strong security policies and processes with audits. For Blockchain systems, [illegible] wallet credentials.<br>• Wallet Access: [illegible] traditional hacking [illegible] dictionary attacks as well as [illegible] attacks, which seek vulnerabilities in the cryptographic algorithms. Blockchain utilizes ECDSA Cryptographic Algorithm, which automatically generates unique private keys. ECDSA has insufficient entropy vulnerability. [illegible] signatures.<br>• [illegible] are done by [illegible] privilege escalation attacks. These are usually [illegible] security policy, data encryption [illegible] IT infrastructure involving databases. Since Blockchain exists in form of sequential chain of blocks, anyone trying to alter records would have to [illegible] connections leading to that specific transaction, which is complicated. However, attackers can alter transaction ID and [illegible] transaction with [illegible] hash value to the nodes. [illegible] Transaction Malleability. [illegible] In 2014, Mt.Gox Bitcoin Exchange [illegible] such a Malleability attack. |
| End User | • Endpoint [illegible]: Endpoint Security is controlled by [illegible] policies and [illegible] for monitoring and detection of end user systems and mobile devices [15]. For Blockchain, the nodes are the endpoints, which [illegible] exploited [illegible] Blockchain network [illegible].<br>• Intentional Misuse: Traditional [illegible] by staff and employees who [illegible]. In Blockchain, Miners are incentivized for Proof of Work, [illegible] together to take control of the network. Majority attack or 51% Attack occurs in Blockchain network [illegible] computing power [illegible] the whole network. [illegible]<br>• Sybil Attack: [illegible] by controlling multiple nodes or Peers. [illegible] transactions [illegible] the transactions. Victim node then becomes [illegible] attacks which are difficult to detect and prevent. The attackers [illegible] the Blockchain system [illegible] transactions. |

Figure 1: Fig. 1 :Fig. 2 :



Stage#01:

- Identified 144 published research since 2016 from ACM, IEEE, Elsevier, ProQuest

Stage#02:

- Include only those with Blockchain and Security related work and keywords

Stage#03:

- Exclude studies based on duplicates for Title, Absract, Keyword, Reviews

Stage#04:

- Define final of 38 literatu research wor

Figure 2: A

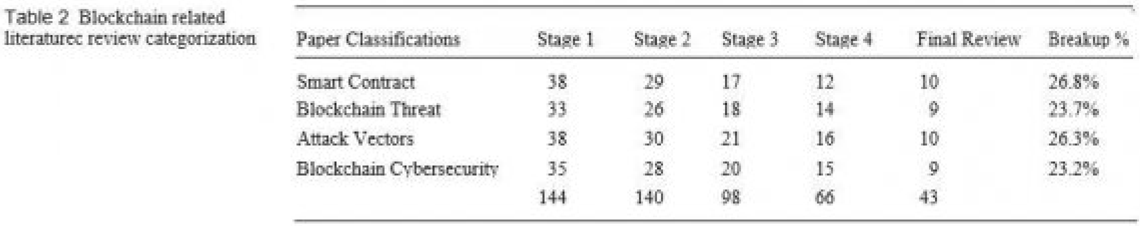
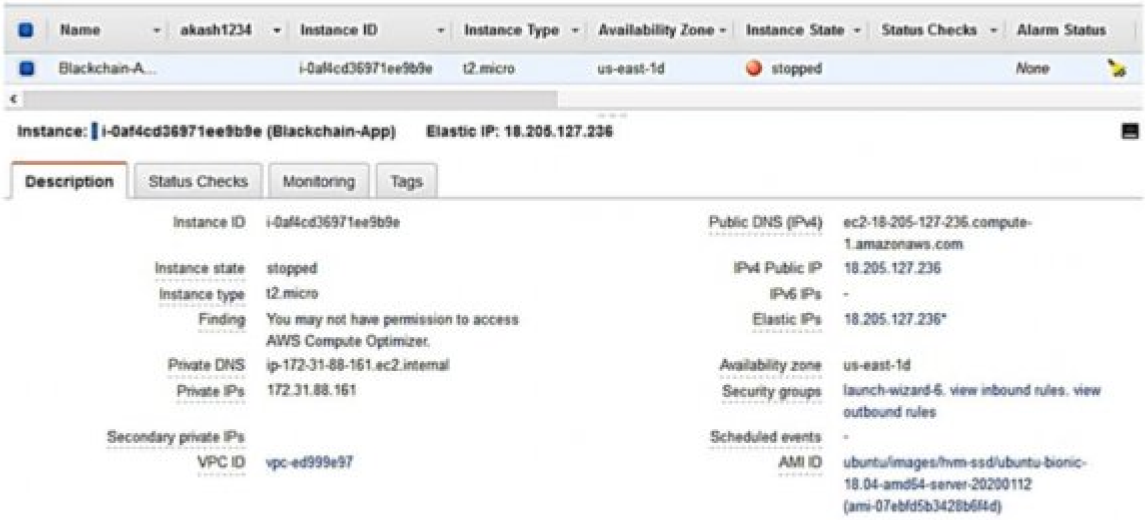


Table 2 Blockchain related literaturec review categorization

| Paper Classifications | Stage 1 | Stage 2 | Stage 3 | Stage 4 | Final Review | Breakup % |
|---|---|---|---|---|---|---|
| Smart Contract | 38 | 29 | 17 | 12 | 10 | 26.8% |
| Blockchain Threat | 33 | 26 | 18 | 14 | 9 | 23.7% |
| Attack Vectors | 38 | 30 | 21 | 16 | 10 | 26.3% |
| Blockchain Cybersecurity | 35 | 28 | 20 | 15 | 9 | 23.2% |
| | 144 | 140 | 98 | 66 | 43 | |

Figure 3:

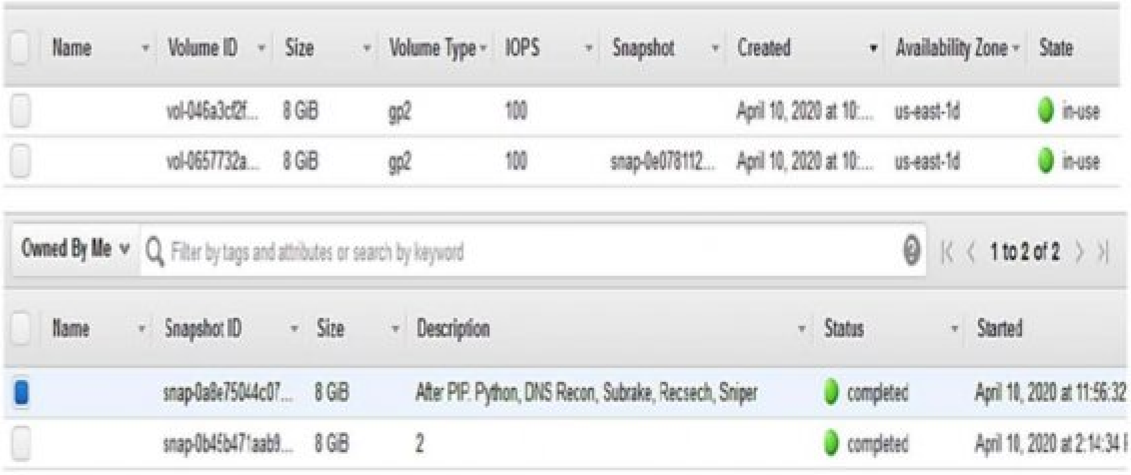


| ■ | Name | akash1234 | Instance ID | Instance Type | Availability Zone | Instance State | Status Checks | Alarm Status |
|---|---|---|---|---|---|---|---|---|
| ■ | Blackchain-A... | | i-0af4cd36971ee9b9e | t2.micro | us-east-1d | ● stopped | | None |

Instance: i-0af4cd36971ee9b9e (Blackchain-App) Elastic IP: 18.205.127.236

| | | | |
|---|---|---|---|
| Instance ID | i-0af4cd36971ee9b9e | Public DNS (IPv4) | ec2-18-205-127-236.compute-1.amazonaws.com |
| Instance state | stopped | IPv4 Public IP | 18.205.127.236 |
| Instance type | t2.micro | IPv6 IPs | - |
| Finding | You may not have permission to access AWS Compute Optimizer. | Elastic IPs | 18.205.127.236* |
| Private DNS | ip-172-31-88-161.ec2.internal | Availability zone | us-east-1d |
| Private IPs | 172.31.88.161 | Security groups | launch-wizard-6. view inbound rules. view outbound rules |
| Secondary private IPs | | Scheduled events | - |
| VPC ID | vpc-ed999e97 | AMI ID | ubuntu/images/hvm-ssd/ubuntu-bionic-18.04-amd64-server-20200112 (ami-07ebfd5b3428b6f4d) |

Fig. 2 AWS Node Instance setup



| □ | Name | Volume ID | Size | Volume Type | IOPS | Snapshot | Created | Availability Zone | State |
|---|---|---|---|---|---|---|---|---|---|
| □ | | vol-046a3cf2f... | 8 GiB | gp2 | 100 | | April 10, 2020 at 10:... | us-east-1d | ● in-use |
| □ | | vol-0657732a... | 8 GiB | gp2 | 100 | snap-0e078112... | April 10, 2020 at 10:... | us-east-1d | ● in-use |

| □ | Name | Snapshot ID | Size | Description | Status | Started |
|---|---|---|---|---|---|---|
| ■ | | snap-0a8e75044c07... | 8 GiB | After PIP. Python, DNS Recon, Subrake, Recsech, Sniper | ● completed | April 18, 2020 at 11:56:32 |
| □ | | snap-0b45b471aab9... | 8 GiB | 2 | ● completed | April 18, 2020 at 2:14:34 |

Fig. 3 AWS Node Volume and Snapshots for changes

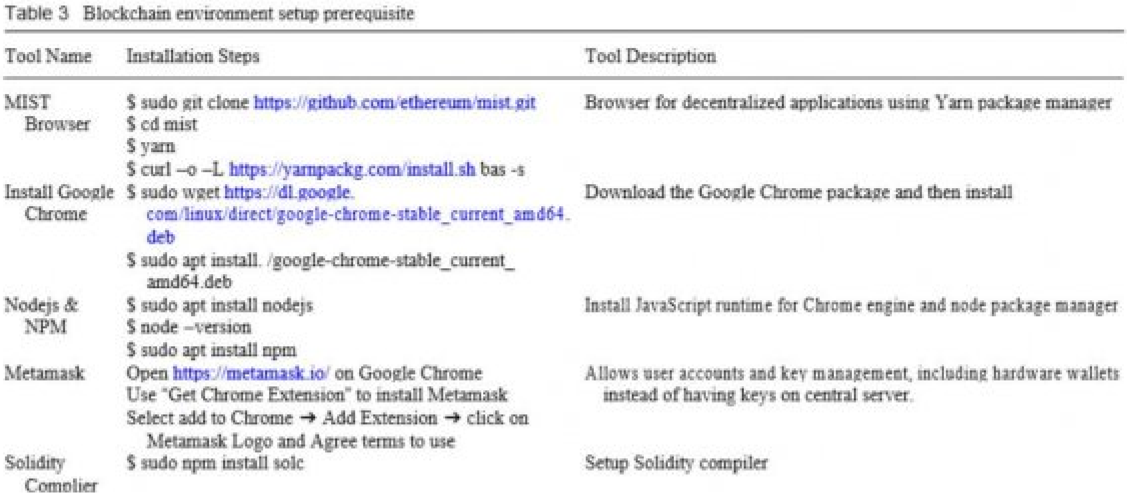
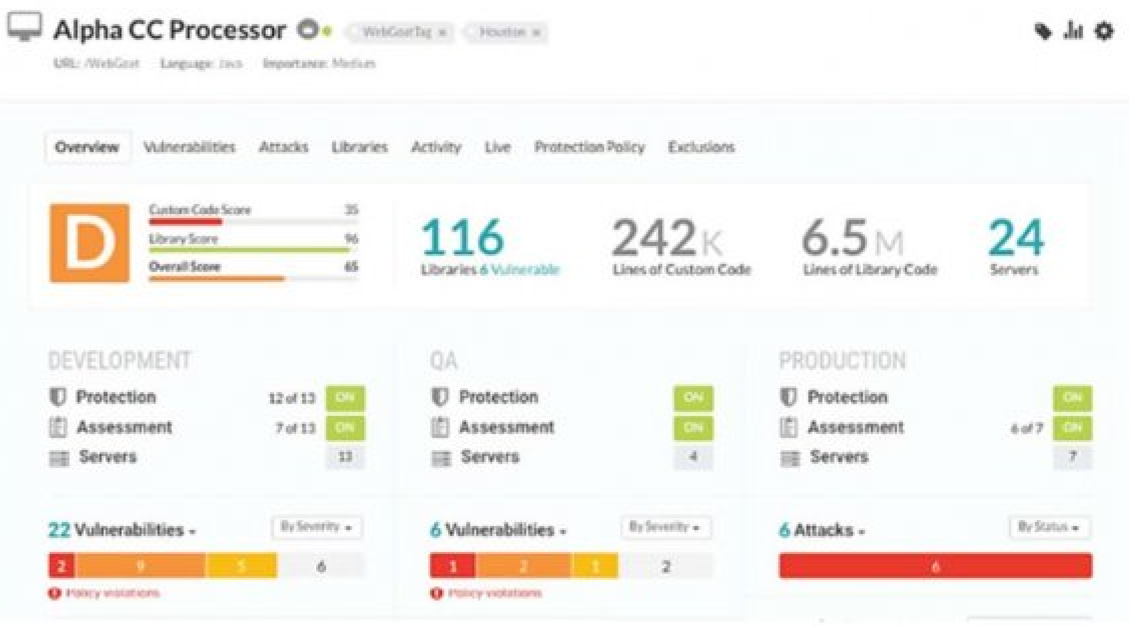


Table 3 Blockchain environment setup prerequisite

| Tool Name | Installation Steps | Tool Description |
|---|---|---|
| MIST Browser | $ sudo git clone https://github.com/ethereum/mist.git<br>$ cd mist<br>$ yarn<br>$ curl –o –L https://yarnpackg.com/install.sh bas -s | Browser for decentralized applications using Yarn package manager |
| Install Google Chrome | $ sudo wget https://dl.google.com/linux/direct/google-chrome-stable_current_amd64.deb<br>$ sudo apt install. /google-chrome-stable_current_amd64.deb | Download the Google Chrome package and then install |
| Nodejs & NPM | $ sudo apt install nodejs<br>$ node –version<br>$ sudo apt install npm | Install JavaScript runtime for Chrome engine and node package manager |
| Metamask | Open https://metamask.io/ on Google Chrome<br>Use "Get Chrome Extension" to install Metamask<br>Select add to Chrome ➔ Add Extension ➔ click on Metamask Logo and Agree terms to use | Allows user accounts and key management, including hardware wallets instead of having keys on central server. |
| Solidity Complier | $ sudo npm install solc | Setup Solidity compiler |

4

Figure 4: 4 .



Alpha CC Processor WebGoatTag × Houston ×

URL: /WebGoat Language: Java Importance: Medium

Overview Vulnerabilities Attacks Libraries Activity Live Protection Policy Exclusions

D

Custom Code Score 35

Library Score 96

Overall Score 65

116 Libraries 6 Vulnerable

242K Lines of Custom Code

6.5M Lines of Library Code

24 Servers

DEVELOPMENT

Protection 12 of 13 ON

Assessment 7 of 13 ON

Servers 13

22 Vulnerabilities By Severity

2 9 5 6

Policy violations

QA

Protection ON

Assessment ON

Servers 4

6 Vulnerabilities By Severity

1 2 1 2

Policy violations

PRODUCTION

Protection ON

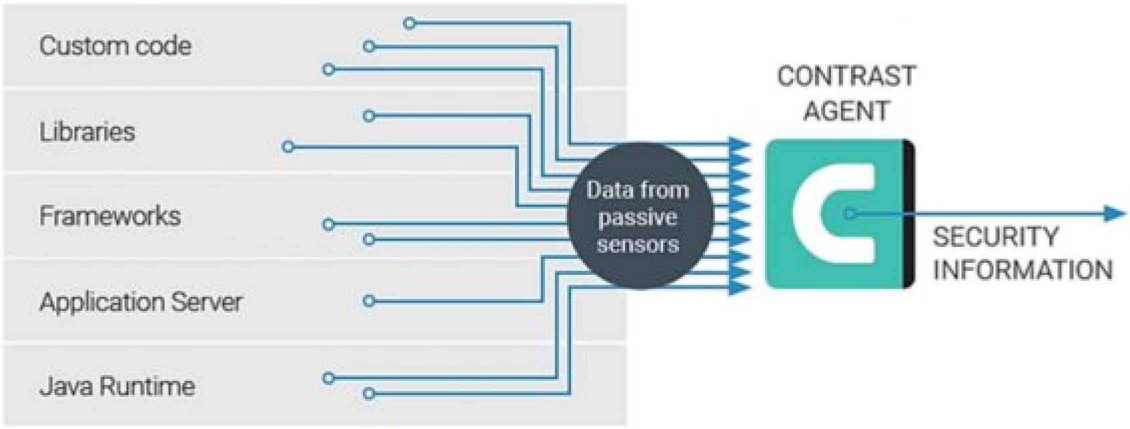
Assessment 6 of 7 ON

Servers 7

6 Attacks By Status

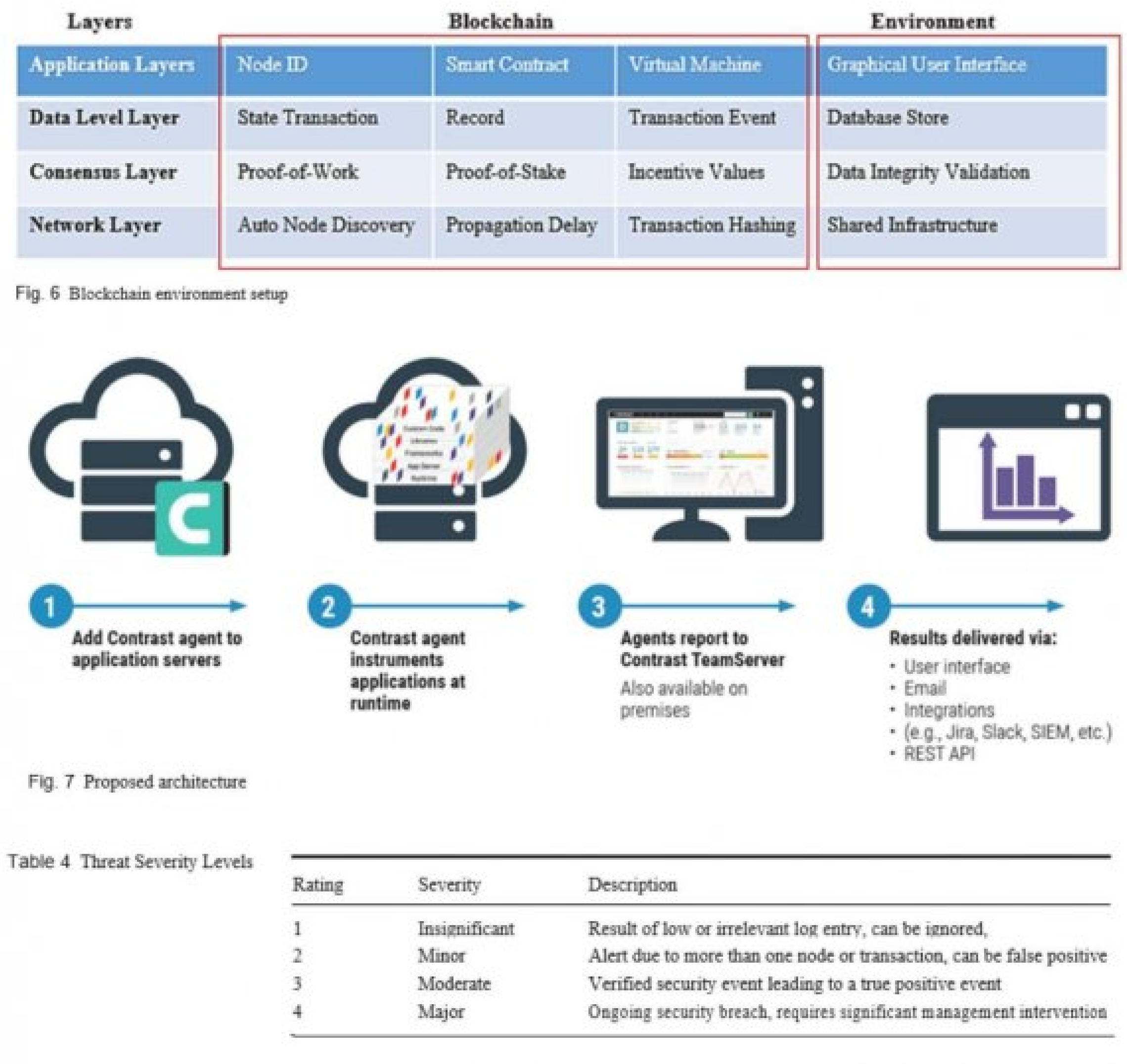
6

Fig. 4 AWS Setup Console for the Smart Contract Blockchain



**25** Fig. 5 Deep level application security test

Figure 5: 25



| Layers | Blockchain | | | Environment |
|---|---|---|---|---|
| Application Layers | Node ID | Smart Contract | Virtual Machine | Graphical User Interface |
| Data Level Layer | State Transaction | Record | Transaction Event | Database Store |
| Consensus Layer | Proof-of-Work | Proof-of-Stake | Incentive Values | Data Integrity Validation |
| Network Layer | Auto Node Discovery | Propagation Delay | Transaction Hashing | Shared Infrastructure |

Fig. 6 Blockchain environment setup

1 Add Contrast agent to application servers

2 Contrast agent instruments applications at runtime

3 Agents report to Contrast TeamServer

Also available on premises

4 Results delivered via:

- User interface
- Email
- Integrations
- (e.g., Jira, Slack, SIEM, etc.)
- REST API

Fig. 7 Proposed architecture

Table 4 Threat Severity Levels

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

Figure 6:

[Honolulu ()] , H I Honolulu . 10.1109/INFOCOM. https://doi.org/10.1109/INFOCOM 2018. 2018. p. 8486402.

[Shah et al. ()] '3D weighted centroid algorithm RSSI ranging model strategy for node localization in WSN based on smart devices'. B Shah , C Zhe , F Yin , I Khan , S Begum , M Faheem , F Khan . *Sustain Cities Soc* 2018. 39 p. .

[Pouttu et al. ()] '5G test network (5GTN). environment for demonstrating 5G and IoT convergence during 2018 Korean Olympics between Finland and Korea'. A Pouttu , O Liinamaa , G Destino . 10.1109/INFCOMW.2018.8406996. https://doi.org/10.1109/INFCOMW.2018.8406996 *IEEE INFOCOM 2018 -IEEE conference on computer communications workshops (INFOCOM WKSHPS)*, (Honolulu, HI) 2018. 2018. p. .

[Bhattacharya et al. ()] 'A novel PCA-firefly based XGBoost classification model for intrusion detection in networks using GPU'. S Bhattacharya , R Kaluri , S Singh , M Alazab , U Tariq . *Electronics* 2020. 9 (2) p. 219.

[Wang ()] 'A preliminary research of prediction markets based on Blockchain powered smart contracts'. S Wang . *Proceedings of IEEE international conference of Blockchain*, (IEEE international conference of Blockchain) 2018. p. .

[Numan et al. ()] 'A systematic review on clone node detection in static wireless sensor networks'. M Numan , F Subhan , W Z Khan , S Hakak , S Haider , G Reddy , M Alazab . *IEEE Access* 2020. 8 p. .

[Mohamed ()] 'Applying Blockchain in industry 4.0 applications'. N Mohamed , Al-Jaroodi , J . 10.1109/CCWC.2019.8666558. https://doi.org/10.1109/CCWC.2019.8666558 *IEEE 9th annual computing and communication workshop and conference (CCWC)*, (Las Vegas) 2019.

[Tateishi et al. ()] 'Automatic smart contract generation using controlled natural language and template'. T Tateishi , S Yoshihama , N Sato , S Saito . 10.1147/JRD. https://doi.org/10.1147/JRD *IBM J Res Dev (Early Access)* 2019. 2019.2900643. (IBM)

[Gatteschi et al. ()] 'Blockchain and smart contracts for insurance: is the technology mature enough?'. V Gatteschi , F Lamberti , C Demartini , C Pranteda , V Santamaria . *IEEE Future Internet* 2018. 10 (2) p. .

[Alladi et al. ()] *Blockchain applications for industry 4.0 and industrial IoT: a review. IEEE access, special section on distributed computing infrastructure for cyber-physical systems*, T Alladi , V Chamola , R Parizi , R Choo . 10.1109/ACCESS. https://doi.org/10.1109/ACCESS 2019. 2019.2956748. 2019.

[Wan et al. ()] 'Blockchain-based solution for enhancing security and privacy in smart factory'. J Wan , J Li , M Imran , M Li , A Fazal . 10.1109/TII. https://doi.org/10.1109/ICBDSC.2019.8645574 *IEEE transactions on industrial informatics (early access), IEEE systems, man, and cybernetics society*, (Muscat) 2019. 2019.2894573.

[Wang et al. ()] 'Blockchain-enabled smart contracts: architecture, applications, and future trends'. S Wang , L Ouyang , Y Yuan , X Ni , X Han , F Wang . 10.1109/TSMC. https://doi.org/10.1109/TSMC *IEEE transactions on systems, man, and cybernetics: systems (early access), IEEE systems, man, and cybernetics society*, 2019. 2019.2895123.

[CHESS Replacement (2018)] *CHESS Replacement*, https://www.asx.com.au/services/chess-replaceme-nt.htm 2018. February 15. 2020. Australian Securities Exchange.

[Ch et al. ()] 'Computational system to classify cyber crime offenses using machine learning'. R Ch , T Gadekallu , M Abidi , A Al-Ahmari . 10.3390/su12104087. https://doi.org/10.3390/su12104087 *MDPI J Sustainability* 2020. 12.

[Choo et al. ()] 'Cryptographic solutions for industrial internet-of-things: research challenges and opportunities'. K Choo , S Gritzalis , J Park . 10.1109/TII.2018.2841049. https://doi.org/10.1109/TII.2018.2841049 *IEEE Trans Industrial Info* 2018. 14 (8) p. .

[Zhang ()] 'Cyber-physical social systems: the state of the art and perspectives'. J Zhang . *IEEE Trans Comput Soc* 2018. 5 (3) p. .

[Ozyilmaz and Yurdakul ()] 'Designing a Blockchain-based IoT with Ethereum, swarm, and LoRa: the software solution to create high availability with minimal security risks'. R Ozyilmaz , A Yurdakul . 10.1109/MCE.2018.2880806. https://doi.org/10.1109/MCE.2018.2880806 *IEEE consumer electronics magazine* 2019. 8 (8) p. . (IEEE Consum Electron Soc)

[Reddy et al. ()] 'Employing data mining on highly secured private clouds for implementing a security-asaservice framework'. G T Reddy , K Sudheer , K Rajesh , K Lakshmanna . *J Theor Appl Inf Technol* 2014. 59 (2) p. .

[Shah et al. ()] 'Energy and interoperable aware routing for throughput optimization in clustered IoT-wireless sensor networks'. B Shah , Z Chen , F Yin , I Khan , N Ahmad . *Futur Gener Comput Syst* 2018. 81 p. .

[Wood (2016)] *Ethereum: A secure decentralized generalized transaction ledger*, G Wood . https://ethereum.github.io/yellowpaper/paper.pdf 2016. March 15, 2020.

[Tonelli et al. ()] ‘Implementing a microservices system with Blockchain smart con-tracts’. R Tonelli , M Lunesu , A Pinna , D Taibi , M Marchesi . 10.1109/IWBOSE.2019.8666520. https://doi.org/10.1109/IWBOSE.2019.8666520 *IEEE international workshop on Blockchain oriented software engineering (IWBOSE)*, (Hangzhou) 2019.

[Chang and Svetinovic ()] ‘Improving Bitcoin ownership identification using transaction patterns analysis’. T Chang , D Svetinovic . 10.1109/TSMC.2018.2867497. https://doi.org/10.1109/TSMC.2018.2867497 *IEEE Trans Syst Man Cyber Syst Pub* 2019. 50 p. .

[ Al-Jaroodi J ()] ‘Industrial applications of Blockchain’. Al-Jaroodi J , MohamedN . 10.1109/CCWC.2019.8666530. https://doi.org/10.1109/CCWC.2019.8666530 *IEEE 9th annual computing and communication work-shop and conference (CCWC)*, (Las Vegas) 2019.

[Xu and Mcardle ()] ‘Internet of too many things in smart trans-port: the problem, the side effects and the solution’. L Xu , G Mcardle . 10.1109/ACCESS.2018.2877175. https://doi.org/10.1109/ACCESS.2018.2877175 *IEEE Access* 2018. 6 p. .

[Investor Bulletin: Initial Coin Offerings (2018)] *Investor Bulletin: Initial Coin Offerings*, 2018. February 5, 2020. US Securities and Exchange Commission.

[Hildenbrandt ()] ‘KEVM: A complete formal semantics of the Ethereum virtual machine’. E Hildenbrandt . *IEEE 31st computer Security Foundation symposium (CSF)*, 2018. p. .

[Azab et al. ()] ‘Machine learning based botnet identification traffic’. A Azab , M Alazab , M Aiash . *IEEE Trustcom/BigDataSE/ISPA* 2016. 2016. IEEE. p. .

[Suliman et al. ()] ‘Monetization of IoT data using smart contracts’. A Suliman , Z Husain , M Abououf , M Alblooshi , K Salah . 10.1049/iet-net.2018.5026. https://doi.org/10.1049/iet-net.2018.5026 *IET Networks* 2019. 8 (1) p. .

[Lin et al. ()] *mTS: temporal-and spatial-collaborative charging for wireless recharge-able sensor networks with multiple vehicles*, C Lin , Z Wang , J Deng , L Wang , J Ren , G Wu . 2018.

[Wang et al. ()] ‘Parallel Blockchain: an architecture for CPSS-based smart societies’. F Wang , Y Yuan , C Rong , J Zhang . *IEEE transactions of. Comput Soc* 2018. 5 (2) p. .

[Yamashita et al. ()] ‘Potential risks of hyper ledger fabric smart contracts’. K Yamashita , Y Nomura , F Zhou , B Pi , S Jun . 10.1109/IWBOSE.2019.8666486. https://doi.org/10.1109/IWBOSE.2019.8666486 *IEEE international workshop on Blockchain oriented software engineering (IWBOSE)*, (Hangzhou) 2019.

[Amoordon and Rocha ()] ‘Presenting Tendermint: Idiosyn-crasies, Weaknesses, and Good Practices’. A Amoordon , H Rocha . 10.1109/IWBOSE.2019.8666541. https://doi.org/10.1109/IWBOSE.2019.8666541 *IEEE international workshop on Blockchain oriented software engineering (IWBO SE)*, (Hangzhou) 2019.

[Knirsch et al. ()] ‘Privacypreserving Blockchain-based electric vehicle charging with dynamic tariff decisions’. F Knirsch , A Unterweger , D Engel . *Compute. Sci. Res. Develop* 2018. 33 (1-2) p. .

[The Energy Web Foundation (2018)] *Promising Blockchain Applications for Energy: Separating the Signal from the Noise*, The Energy Web Foundation . http://www.coinsay.com/wp-content/uploads/2018/07/Energy-Futures-Initiative-Promising-Blockchain-Applications-for-Energy.pdf 2018. April 2, 2020.

[Qin et al. ()] ‘Research on the selection strategies of Blockchain mining pools’. R Qin , Y Yuan , Y Wang . *IEEE Trans Comput Soc* 2018. 5 (3) p. .

[Draper et al. ()] ‘Se-curity applications and challenges in Blockchain’. A Draper , A Familrouhani , D Cao , T Heng , W Han . 10.1109/ICCE.2019.8661914. https://doi.org/10.1109/ICCE.2019.8661914 *IEEE international conference on consumer electronics (ICCE)*, (Las Vegas, NV) 2019.

[Tsankov ()] *Security practical security analysis of smart con-tracts*, Tsankov . arXiv:1806.01143v2. 2018. (ArXiv preprint)

[Li et al. ()] *Smart choice for the smart grid: narrowband internet of*, Y Li , X Cheng , Y Cao , D Wang , Y Yang . 2018.

[Zhang ()] *Smart contract-based access control for internet of things (IoT)*, Zhang . arXiv 1802(04410): 2018. 2018. (ArXiv Preprint)

[Mahmood et al. ()] ‘SMART security alert system for monitoring and controlling container transportation. 4th MEC international conference on big data and Smart City things (NB-IoT)’. S Mahmood , R Hasan , A Ullah , U Sarker . 10.1109/JIOT.2017.2781251. https://doi.org/10.1109/JIOT.2017.2781251 *IEEE Internet Things J* 2019. 5 (3) p. .

[Struye et al. ()] ‘The CityLab testbed -large-scale multi-technology wireless experimentation in a city environment: neural network-based interference prediction in a smart city’. J Struye , B Braem , S Latre´ , J Marquez-Barja . 10.1109/INFCOMW.2018.8407018. https://doi.org/10.1109/INFCOMW.2018.8407018 *IEEE INFOCOM 2018 -IEEE conference on com-puter communications workshops (INFOCOM WKSHPS)*, (Honolulu) 2018. 2018. p. .

[Amani et al. ()] ‘Towards verifying Ethereum smart contract Bytecode in Isabelle/HOL’. S Amani , M Begel´ , M Bortin , M Staples . *Proceedings of 7th ACM SIGPLAN international conference for certified program proofs (CPP)*, (7th ACM SIGPLAN international conference for certified program proofs (CPP)Los Angeles) 2018. p. .

[Greenspan (2018)] *Why Many Smart Contract Use Cases Are Simply Impossible*, G Greenspan . `https://www.coindesk.com/three-smart-contract-misconceptions` 2018. March 10, 2020.