Global Journal of Computer Science and Technology: H Information & Technology
Volume 23 Issue 2 Version 1.0 Year 2023
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

A Smart Contract Blockchain Penetration Testing Framework

By Shyam Meshram & Isha Sood
University of Ajeenkya D.Y. Patil

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.

Keywords: smart contracts, attack vectors, cyber-security, blockchain, cyber threats.

GJCST-H Classification: LCC: QA76.9.B56

Strictly as per the compliance and regulations of:

A Smart Contract Blockchain Penetration Testing Framework

Shyam Meshram [α] & Isha Sood [σ]

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.

Keywords: smart contracts, attack vectors, cyber-security, blockchain, cyber threats.

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 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 self-enforcing [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.

Consider purchasing a new car as an illustration. The con-ventional process entails visiting a car trader (an intermediate 3rd party) and haggling over the car of your choice. Instead of involving the insurance company and the transportation department in the paperwork, as well as successful toward a bank for a car advance (yet additional 3rd party). Here is a waiting retro before the car is delivered after all formalities and payments have been made. This procedure requires patience and requires communication with numerous additional 3rd parties.

Presumptuous the similar car's information, possession, IDs, then proposal are accessible, there is not at all involvement from a 3rd party, and advanced-level 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 typically the same across all use cases, but the mitigation tactics can differ. Even though it might seem

Author α σ: Ajeenkya D.Y. Patil university. Pune, Maharashtra, India.
e-mails: shyam.meshram@adypu.edu.in, facultyit459@adypu.edu.in

like the Blockchain is the ideal answer for dealings, the skill still consumes weak points. Table 1 lists the bout courses according to the Network, Applications, Data Integrity, and End Operator heights.

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.
- *Inception Vulnerability:* Thousands of nodes must coop-erate in order for a blockchain to function properly. A bulge or else collection of bulges has switch over the blockchain outcome if they switch 51.
- *Government Control:* Cryptocurrencies have the potential to cause currencies under the control of governments to lose value or become obsolete, which would desta-bilise the global economy. Such establishments would continuously desire approximately equal of switch and regulation, which is in opposition to the decentralised nature of keen agreements.
- *3rd Party Additions:* Using non-standard 3rd-party stages can present faults smooth though the Blockchain network may be safe, for example, 400 BTCs were stolen after the Nice Hash Removal bazaar in 2017, $ 60 truckload in operator coffers were stolen from Bitcoin Gold in 2018, and $ 60 million in bitcoins were stolen from Crypto Exchange Zaif in 2018.
- *Key and Certificate Security:* As of March 2019, the Darkweb had ended 60 bazaar gateways offering SSL and TLS diplomas as well as connected facilities for $250 to $2000. Another obstacle that Blockchain keys and Smart Contracts must contend with is the criminal impersonation of righthand 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.
- Attacks utilizing the Ethereum Virtual Machine's vulner-abilities are of a low-level nature. It has been found that EVM contains unchangeable flaws. Changing blockchain blocks after they have been created, losing cryptocurrency during a transfer, or allowing hackers to control access to systems can all result in the Smart Contract's sensitive functionality being accessed.
- *Mining Pools:* To combine their computing power, miners band together. In contrast to individual miners, who hardly ever earn money or receive any Bitcoins, more blocks are mined as a result, and more rewards are obtained. Miner Pools [15] raise their reward share by delaying the transmissions of excavated chunks to other parties. When that happens, every block is suddenly free. This causes additional miners to misplace their blocks. The three companies BTC.com, ViaBTC, and AntPool are the largest Bitcoin mining pools. Only Consuming lone righthand mineworkers on the network or changing the Keen Agreement procedures to skin the difference amid incomplete and filled resistant of effort confidential the Smart Agreements are mitigation strategies against such threats [16].

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. 1 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 2. 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 growth gears, was presented by Yamashita et al. (2019) [19]. Despite the fact that Java and Go were not created

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. (2019) [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. (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 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-edge technologies similar Group, Ethereum, then LoRa. For Keen Agreements schemes, which characteristically use trustless bulges in a dispersed way for dispersed storing in Blockchain networks, the writers spoke the subjects of information storing, high availability, removal, then renunciation of facility bouts.

Cture the original architecture, Wan et al. (2019) [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.

Suliman et al.'s (2019) [30] concept for conducting trans-actions made use of the characteristics of a blockchain smart contract. In a decentralized, highly trusted network with no in-termediary, the writers deliberated the architecture, application logic, object, and communication plan. This model is based on Wood et al.'s (2016) [31] use of Ethereum smart contracts for live data exchange.

Current tendencies in investigate regarding blockchain applications for manufacturing subdivisions were presented by Alladi et al. (2019) [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.

Table 1 Attack vector classification

Attack Vectors	Process Description
DoS attack	IT infrastructures face denial of service attacks, which typically involve flooding the network pipes and applications with requests. Legitimate users are denied access to the service resources. • Blockchain Smart Contracts face service denial attacks when one or more execute and updates or creation of new blocks requests are submitted to the Blockchain, which is more than what can be handled. Transaction tampering with group routing is another such attacks. Attacker sub-divide the Blockchain network into separate groups. These are not allowed to communicate with each other. Then the transactions are sent to the peer nodes. This makes it impossible for other peers to detect the tampering. • Routing attacks involve partitioning the peer nodes with delays introduced into the network interfering the message broadcasts 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 attain around 2000 transactions per second, while Twitter achieves around 5000 transactions per second. • Low efficiency of transactions often holds back Blockchain adoption for potential nodes. This also involves greater processing and throughput efforts inside Blockchain and the miners. • 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 use of multiple iterations of Penetration Testing using secure coding, with manual and automated tools. Smart Contract can be written by any node, which then spreads in the network. Integer Overflow vulnerability was the only major flow detected in Blockchain. • Points of Failure involve use of single primary database server or one master backups can be a glaring vulnerability. IT setups typically use multiple systems and backups and plan for business continuity and disaster recovery. Being Distributed Ledger with multiple nodes involved in the network, there are no such issues visible in Blockchain. • Timejacking exploits the Bitcoin timestamp vulnerability; this is done by altering the node time counter or by adding multiple fake peers having erroneous timestamps. This forces the victim node to agree on using another Blockchain network. Eclipse Attacks has the hacker taking control of large number of distributed nodes as network bots. Once the nodes are restarted, 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, cybercriminals target user wallet credentials. • Wallet Access involves traditional hacking means like use of phishing emails, dictionary attacks as well as new-sophisticated attacks, which seek vulnerabilities in the cryptographic algorithms. Blockchain utilizes ECDSA Cryptographic algorithm, which automatically generates unique private keys. ECDSA has insufficient entropy vulnerability. This results in the same random value being utilized by more than one signatures. • Fraudulent Modifications are done by Man-in-the-middle and privilege escalation attacks. These are usually mitigated by security policy, data encryption, salting for IT Infrastructure involving databases. Since Blockchain exists in form of sequential chain of blocks, anyone trying to alter records would have to first alter all transactions leading to that specific transaction, which is complicated. However, attackers can alter transaction ID and broadcast that transaction with modified hash value to the nodes. They would try to get it confirmed before the original transaction completes. The initiator would tend to believe the initial transaction might have failed, even as funds in form of BTCs had been withdrawn from their accounts. This is termed as Transaction Malleability. The attacker tricks the victim into paying twice. In 2014, MtGox Bitcoin Exchange was bankrupt due to such a Malleability attack.
End User	• Endpoint threats: Endpoint Security is controlled by enterprise with organization wise policies and console management for monitoring and detection of end user systems and mobile devices [13]. For Blockchain, the nodes are the endpoints, which can be homogeneous, so flaw in one node can be exploited as flaw in Blockchain network systems. • Intentional Misuse: Traditional setup faces insider threats by staff and employees who can steal data and affect the setup. In Blockchain, Miners are incentivized for Proof of Work, who can group together to take control of the network. Majority attack or 51% Attack occur in Blockchain network with one group or hacker harnessing enough computing power to compromise the whole network. Hacker can gain control of network hash rates to create alternate forks and then take precedence over existing forks. • Sybil Attack: is performed by controlling multiple nodes as Bots. These surround the victim node with fake nodes transactions or take time verifying the transactions. Victim node thus becomes is vulnerable to double-spend attacks which are difficult to detect and prevent. The attackers use same coins or tokens for multiple different transactions tricking the Blockchain system to accept the fraud transaction.

Fig. 1: Table 1 Attack Vector Classification

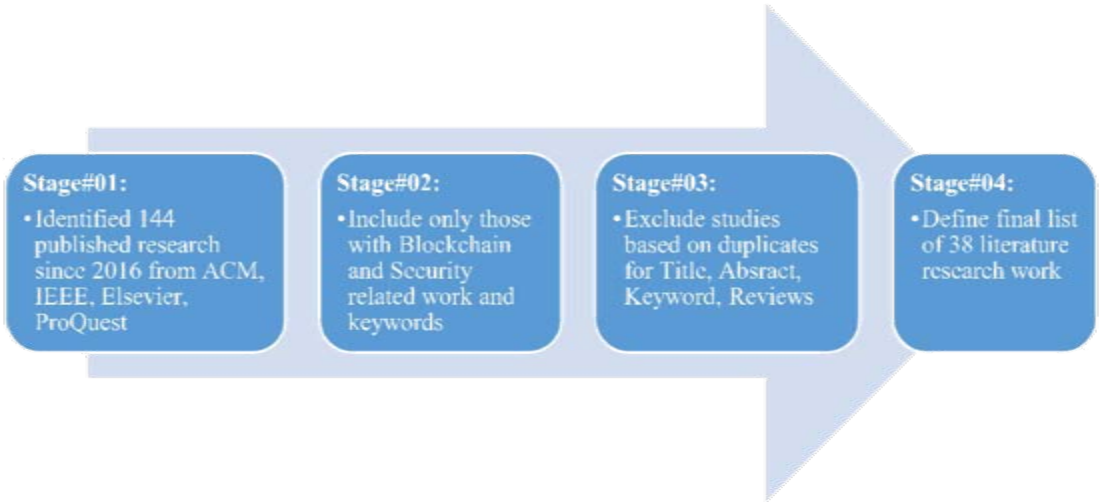

Fig. 2: Fig. 1 Staged Literature Survey Selection Criteria

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	

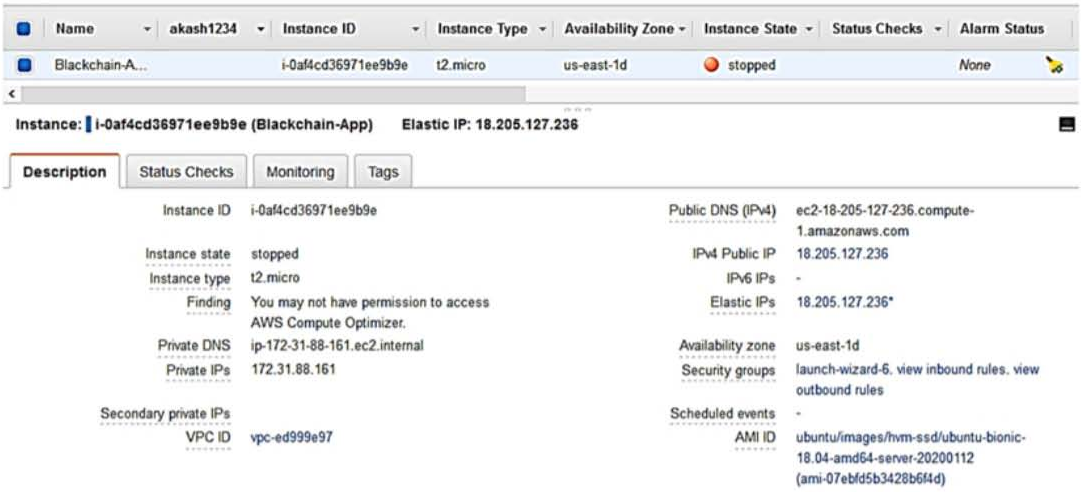

Fig. 2 AWS Node Instance setup

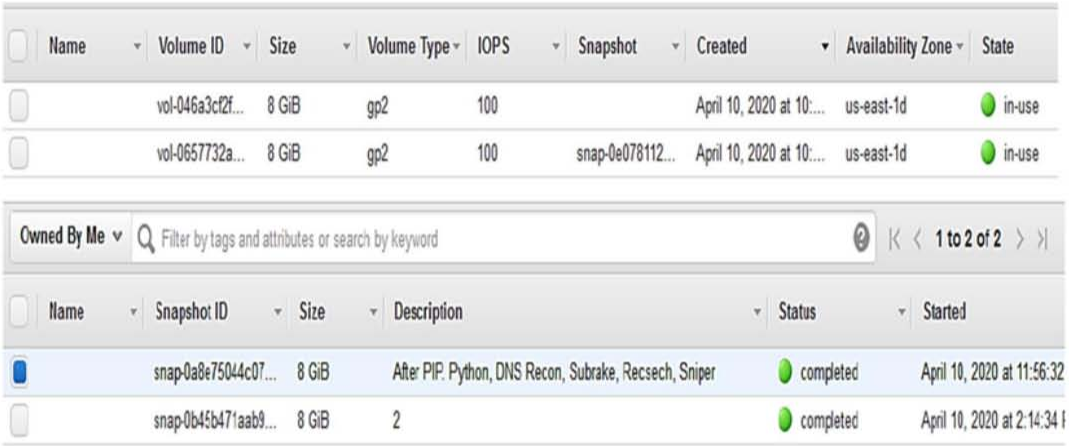

Fig. 3 AWS Node Volume and Snapshots for changes

Table 3 Blockchain environment setup prerequisite

Tool Name	Installation Steps	Tool Description

MIST Browser	$ sudo git clone https://github.com/ethereum/mist.git
	$ cd mist
	$ yarn
	$ 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 $ sudo apt install. /google-chrome-stable_current_amd64.deb	Download the Google Chrome package and then install

Nodejs & NPM	$ sudo apt install nodejs
	$ node –version
	$ sudo apt install npm
		Install JavaScript runtime for Chrome engine and node package manager

Metamask	Open https://metamask.io/ on Google Chrome Use "Get Chrome Extension" to install Metamask 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 Compiler	$ sudo npm install solc	Setup Solidity compiler

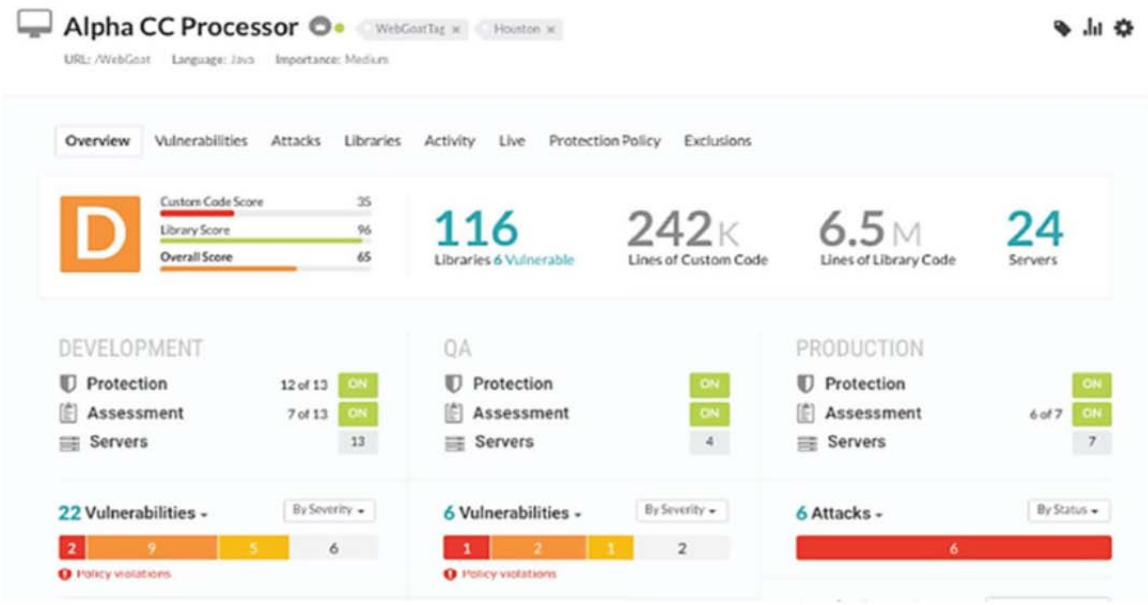

Fig. 4 AWS Setup Console for the Smart Contract Blockchain

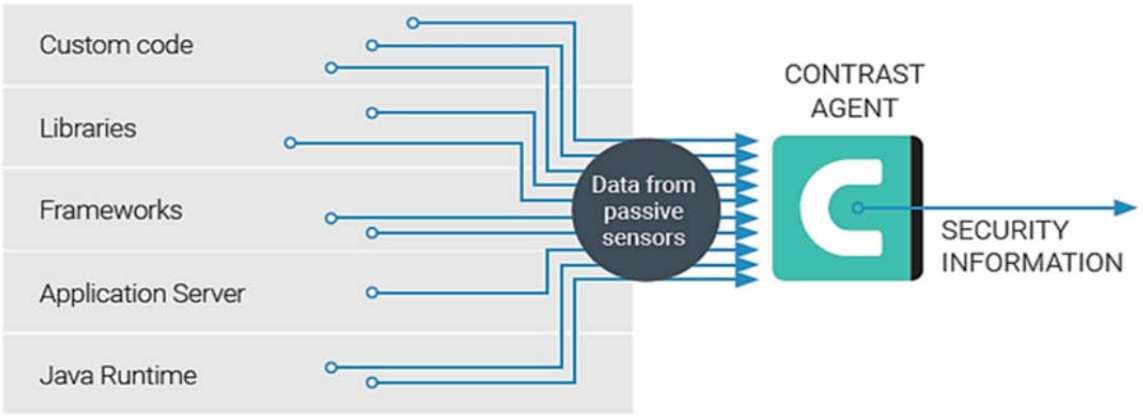

Fig. 5 Deep level application security test

III. Gaps Identified

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 dealings are totally nameless and take place deprived of 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.

IV. System Perfect

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. 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.

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. 2.

As shown in Fig. 3 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 3). 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.

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. 5 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 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.

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. 6 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. 7 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.

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

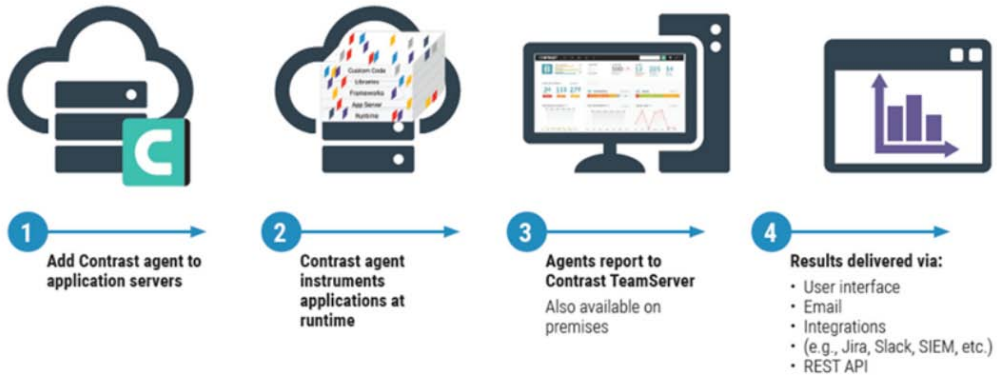

Fig. 7 Proposed architecture

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

VI. Research Performed

Danger Opinions = [Danger Opinion (All-out) * Score (Main)] + [Danger Opinion (Tall) * Score (Reasonable)] + [Danger Opinion (Little)

* Score (Slight] + [Danger Opinion (Least) * Score (Unimportant)].

Amount of Danger Opinion Amount RP

½ Received Pronunciation max*SR major ½RP high*SR moderate ¼: ½RP low*SR minor ½RP min*SR insignificant 4 Majorif Received Pronunciation ¿ HTi Severity Rating SR 3 moderate doubt Received Pronunciation HTi: 2 Minor if RP ¼ HTi 1 Insignificant doubt Received Pronunciation HTi

The challenging remained done cutting-edge 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.

Problem: 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.

1. *Vulnerability Type:* Attack Using Transaction Routing
2. *Procedure:* Drudge noble bulges toward alter the national of dealings beforehand they remain dedicated happening the net. Threat Level High.
3. *Problem:* As shown in Fig. 8, gulf the Keen net hooked happening collections cutting-edge instruction to sabotage the network's spreading mails, delay transactions, and even reroute Blockchain traffic. The underneath cypher exemplifies the NodeJS connectivity.
4. *Threat Level:* High Process: LISK Cryptocurrency's design.

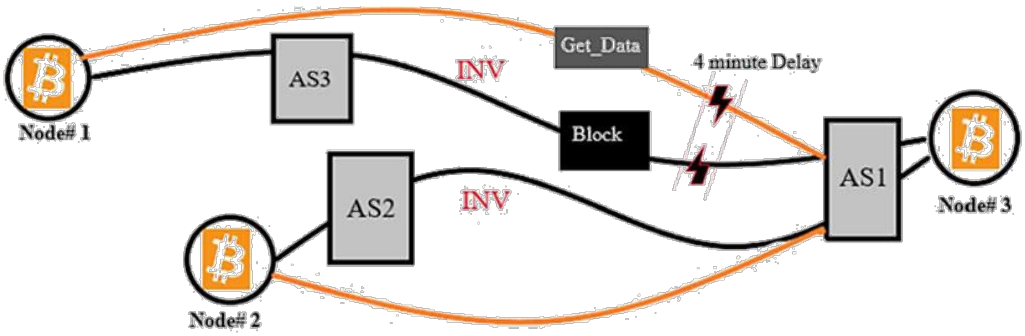

Fig. 8 Blockchain node transaction Delays

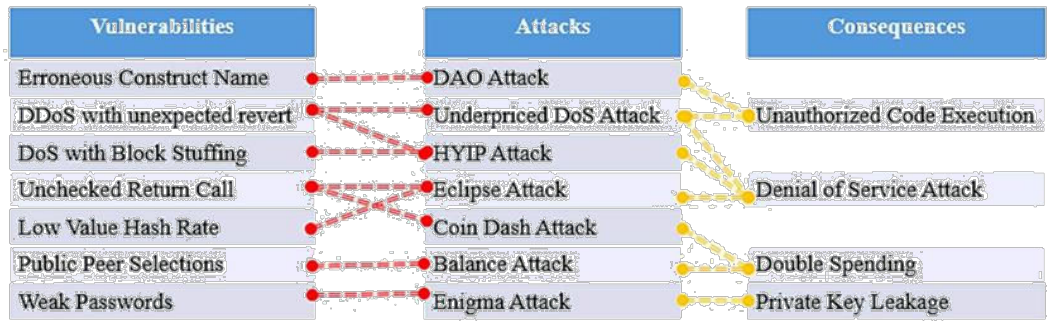

Fig. 9 Vulnerability, Attack and Consequence Relations

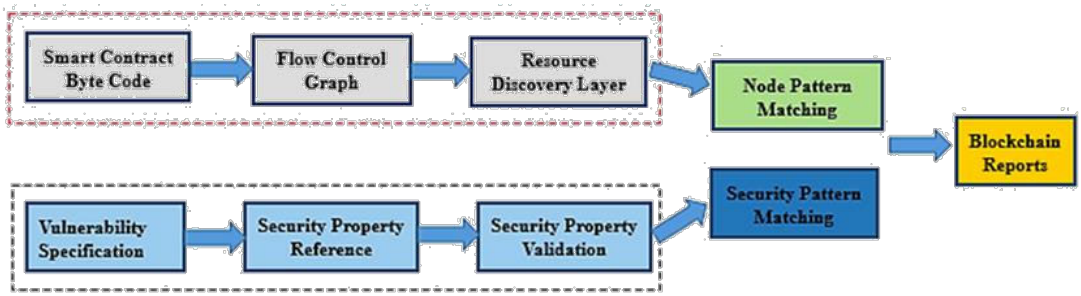

Fig. 10 Workflow for vulnerability detection

Table 5 Comparing Manual and Automated for benchmarks reported for project effectiveness

Vulnerability types	Manual V Automated	Manual – Automated	Automated – Manual
Timestamp Value	522	671	103
Reentrancy Routine	15	129	17

Table 6 Analysis of resulting rates after complete Penetration Testing for Random Samples

Benchmark	Manual FP Rate	Manual FN Rate	Automated FP Rate	Automated FN Rate
Timestamp	6%	11%	39%	31%
Reentrancy	15%	8%	44%	39%

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

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.

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 [40–43]. 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 diffusion challenging devices to understand the effectiveness of the physical still diffusion challenging achieved. The results obtained are shown in Tables 5 and 6. 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 7. 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.

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.

References Références Referencias

1. Greenspan G (2018) Why Many Smart Contract Use Cases Are Simply Impossible. Retrieved March 10, 2020, from https://www.coindesk.com/three-smart-contract-misconceptions.
2. Tsankov P (2018) Security practical security analysis of smart con-tracts. ArXiv preprint, arXiv: 1806.01143v2.
3. Wang F, Yuan Y, Rong C, Zhang J (2018) Parallel Blockchain: an architecture for CPSS-based smart societies. IEEE transactions of. Comput Soc 5 (2): 303–310.
4. Zhang Y (2018) Smart contract-based access control for internet of things (IoT). ArXiv Preprint arXiv 1802(04410): 2018.
5. Xu L, Mcardle G (2018) Internet of too many things in smart trans-port: the problem, the side effects and the solution. IEEE Access 6: 62840–62848. https://doi.org/10.1109/ACCESS.2018.2877175.
6. Li Y, Cheng X, Cao Y, Wang D, Yang Y (2018) Smart choice for the smart grid: narrowband internet of

things (NB-IoT). IEEE Internet Things J 5 (3): 1505–1515. https://doi.org/10.1109/JIOT. 2017.2781251.
7. Amani S, Begel´ M, Bortin M, Staples M (2018) Towards verifying Ethereum smart contract Bytecode in Isabelle/HOL. Proceedings of 7th ACM SIGPLAN international conference for certified program proofs (CPP), Los Angeles, 66–77.
8. Wang S (2018) A preliminary research of prediction markets based on Blockchain powered smart contracts. Proceedings of IEEE international conference of Blockchain, 1287–1293.
9. Chang T, Svetinovic D (2019) Improving Bitcoin ownership identification using transaction patterns analysis. IEEE Trans Syst Man Cyber Syst Pub 50: 9–20. https://doi.org/10.1109/TSMC.2018. 2867497.
10. Australian Securities Exchange (2018) CHESS Replacement. Retrieved February 15, 2020 from https://www.asx.com.au/services/chess-replacement.htm.
11. US Securities and Exchange Commission (2018). Investor Bulletin: Initial Coin Offerings. Retrieved February 5, 2020,
12. Zhang J (2018) Cyber-physical social systems: the state of the art and perspectives. IEEE Trans Comput Soc 5 (3): 829–840.
13. What is a DAO? (2018) Retrieved February 17, 2020, from https://blockchainhub.net/dao-decentralized-autonomous-organization.
14. Wan J, Li J, Imran M, Li M, Fazal A (2019) Blockchain-based solution for enhancing security and privacy in smart factory. IEEE transactions on industrial informatics (early access), IEEE systems, man, and cybernetics society. https://doi.org/10.1109/TII. 2019.2894573.
15. Pouttu A, Liinamaa O, Destino G (2018) 5G test network (5GTN). environment for demonstrating 5G and IoT convergence during 2018 Korean Olympics between Finland and Korea," IEEE INFOCOM 2018 - IEEE conference on computer communications workshops (INFOCOM WKSHPS), Honolulu, HI, 2018, pp. 1–2, https://doi.org/10.1109/INFCOMW. 2018.8406996.
16. Choo K, Gritzalis S, Park J (2018) Cryptographic solutions for industrial internet-of-things: research challenges and opportuni-ties. IEEE Trans Industrial Info 14 (8): 3567–3569. https://doi.org/10.1109/TII. 2018.2841049.
17. Tonelli R, Lunesu M, Pinna A, Taibi D, Marchesi M (2019) Implementing a microservices system with Blockchain smart con-tracts. IEEE international workshop on Blockchain oriented software engineering (IWBOSE), Hangzhou. https://doi.org/10.1109/ IWBOSE.2019.8666520.
18. Amoordon A, Rocha H (2019) Presenting Tendermint: Idiosyn-crasies, Weaknesses, and Good Practices. IEEE international workshop on Blockchain oriented software engineering (IWBOSE), Hangzhou. https://doi.org/10.1109/IWBOSE. 2019. 8666541.
19. Yamashita K, Nomura Y, Zhou F, Pi B, Jun S (2019) Potential risks of hyper ledger fabric smart contracts. IEEE international workshop on Blockchain oriented software engineering (IWBOSE), Hangzhou. https://doi.org/10.1109/IWBOSE.2019.8666486.
20. Al-Jaroodi J, Mohamed N (2019) Industrial applications of Blockchain. IEEE 9th annual computing and communication work-shop and conference (CCWC), Las Vegas. https://doi.org/10.1109/ CCWC.2019.8666530.
21. The Energy Web Foundation (2018) Promising Blockchain Applications for Energy: Separating the Signal from the Noise. Retrieved April 2, 2020, from http://www.coinsay.com/wp-content/uploads/2018/07/ Energy-Futures-Initiative-Promising-Blockchain-Applications-for-Energy.pdf
22. Mohamed N, Al-Jaroodi J (2019) Applying Blockchain in industry 4.0 applications. IEEE 9th annual computing and communication workshop and conference (CCWC), Las Vegas. https://doi.org/10. 1109/CCWC.2019.8666558.
23. Draper A, Familrouhani A, Cao D, Heng T, Han W (2019) Se-curity applications and challenges in Blockchain. IEEE international conference on consumer electronics (ICCE), Las Vegas, NV https://doi.org/10.1109/ICCE.2019.8661914.
24. Mahmood S, Hasan R, Ullah A, Sarker U (2019) SMART security alert system for monitoring and controlling container transportation. 4th MEC international conference on big data and Smart City (ICBDSC), Muscat. https://doi.org/10.1109/ICBDSC. 2019. 8645574.
25. Tateishi T, Yoshihama S, Sato N, Saito S (2019) Automatic smart contract generation using controlled natural language and template. IBM J Res Dev (Early Access), IBM. https://doi.org/10.1147/JRD. 2019.2900643.
26. Wang S, Ouyang L, Yuan Y, Ni X, Han X, Wang F (2019) Blockchain-enabled smart contracts: architecture, applications, and future trends. IEEE transactions on systems, man, and cybernetics: systems (early access), IEEE systems, man, and cybernetics society. https://doi.org/10.1109/TSMC. 2019.2895123.
27. Hildenbrandt E (2018) KEVM: A complete formal semantics of the Ethereum virtual machine. IEEE 31st computer Security Foundation symposium (CSF), 204–217.
28. Ozyilmaz R, Yurdakul A (2019) Designing a Blockchain-based IoT with Ethereum, swarm, and LoRa: the software solution to create high availability with minimal security risks. IEEE consumer electronics magazine, volume: 8, issue 2,

28–34. IEEE Consum Electron Soc 8: 28–34. https://doi.org/10.1109/MCE.2018.2880806.
29. Knirsch F, Unterweger A, Engel D (2018) Privacy-preserving Blockchain-based electric vehicle charging with dynamic tariff decisions. Compute. Sci. Res. Develop. 33 (1–2): 71–79
30. Suliman A, Husain Z, Abououf M, Alblooshi M, Salah K (2019) Monetization of IoT data using smart contracts. IET Networks 8 (1): 32–37. https://doi.org/10.1049/iet-net.2018.5026.
31. Wood G (2016). Ethereum: A secure decentralized generalized transaction ledger. Retrieved March 15, 2020, from https:// ethereum.github.io/yellowpaper/paper.pdf
32. Alladi T, Chamola V, Parizi R Choo R (2019) Blockchain applications for industry 4.0 and industrial IoT: a review. IEEE access, special section on distributed computing infrastructure for cyber-physical systems, volume 2019 (7). https://doi.org/10.1109/ ACCESS.2019.2956748.
33. Ch R, Gadekallu T, Abidi M, Al-Ahmari A (2020) Computational system to classify cyber crime offenses using machine learning. MDPI J Sustainability 12. https://doi.org/10.3390/su12104087.
34. Azab A, Alazab M, Aiash M (2016) Machine learning based botnet identification traffic. In 2016 IEEE Trustcom/BigDataSE/ISPA (pp 1788-1794). IEEE
35. Reddy GT, Sudheer K, Rajesh K, Lakshmanna K (2014) Employing data mining on highly secured private clouds for implementing a security-asa-service framework. J Theor Appl Inf Technol 59 (2): 317–326.
36. Qin R, Yuan Y, Wang Y (2018) Research on the selection strategies of Blockchain mining pools. IEEE Trans Comput Soc 5 (3): 748– 757.
37. Gatteschi V, Lamberti F, Demartini C, Pranteda C, Santamaria V (2018) Blockchain and smart contracts for insurance: is the technology mature enough? IEEE Future Internet 10 (2): 20–26.
38. Lin C, Wang Z, Deng J, Wang L, Ren J, Wu G (2018) mTS: temporal-and spatial-collaborative charging for wireless recharge-able sensor networks with multiple vehicles. IEEE INFOCOM 2018 - IEEE conference on computer communications. Honolulu, HI 2018:99–107. https://doi.org/10.1109/INFOCOM.2018. 8486402
39. Struye J, Braem B, Latre´ S, Marquez-Barja J (2018) The CityLab testbed — large-scale multi-technology wireless experimentation in a city environment: neural network-based interference prediction in a smart city, vol 2018. IEEE INFOCOM 2018 - IEEE conference on com-puter communications workshops (INFOCOM WKSHPS), Honolulu, pp 529–534. https://doi.org/10.1109/INFCOMW.2018.8407018.
40. Shah B, Chen Z, Yin F, Khan I, Ahmad N (2018) Energy and interoperable aware routing for throughput optimization in clustered IoT-wireless sensor networks. Futur Gener Comput Syst 81: 372–381.
41. Shah B, Zhe C, Yin F, Khan I, Begum S, Faheem M, Khan F (2018) 3D weighted centroid algorithm RSSI ranging model strategy for node localization in WSN based on smart devices. Sustain Cities Soc 39: 298–308.
42. Numan M, Subhan F, Khan WZ, Hakak S, Haider S, Reddy G, Alazab M (2020) A systematic review on clone node detection in static wireless sensor networks. IEEE Access 8:65450–65461.
43. Bhattacharya S, Kaluri R, Singh S, Alazab M, Tariq U (2020) A novel PCA-firefly based XGBoost classification model for intrusion detection in networks using GPU. Electronics 9(2): 219.