

Article

A Survey of Bug Bounty Programs in Strengthening Cybersecurity and Privacy in the Blockchain Industry

Junaid Arshad ¹, Muhammad Talha ¹ , Bilal Saleem ¹ , Zoha Shah ¹, Huzaifa Zaman ¹ and Zia Muhammad ^{2,3,*} 

¹ Department of Cyber Security, Air University, Islamabad 44000, Pakistan; 231274@students.au.edu.pk (J.A.); 231350@students.au.edu.pk (M.T.); 211096@students.au.edu.pk (B.S.); 221498@students.au.edu.pk (Z.S.); 211124@students.au.edu.pk (H.Z.)

² Department of Computer Science, North Dakota State University, Fargo, ND 58102, USA

³ Department of Computer Science and Technology, University of Jamestown, Jamestown, ND 58405, USA

* Correspondence: zia.muhammad@ndsu.edu

Abstract: The increasing reliance on computer networks and blockchain technology has led to a growing concern for cybersecurity and privacy. The emergence of zero-day vulnerabilities and unexpected exploits has highlighted the need for innovative solutions to combat these threats. Bug bounty programs have gained popularity as a cost-effective way to crowdsource the task of identifying vulnerabilities, providing a secure and efficient means of enhancing cybersecurity. This paper provides a comprehensive survey of various free and paid bug bounty programs in the computer networks and blockchain industry, evaluating their effectiveness, impact, and credibility. The study explores the structure, incentives, and nature of vulnerabilities uncovered by these programs, as well as their unique value proposition. A comparative analysis is conducted to identify advantages and disadvantages, highlighting the strengths and weaknesses of each program. The paper also examines the role of ethical hackers in bug bounty programs and their contributions to strengthening cybersecurity and privacy. Finally, the study concludes with recommendations for addressing the challenges faced by bug bounty programs and suggests potential future directions to enhance their impact on computer networks and blockchain security.



Citation: Arshad, J.; Talha, M.; Saleem, B.; Shah, Z.; Zaman, H.; Muhammad, Z. A Survey of Bug Bounty Programs in Strengthening Cybersecurity and Privacy in the Blockchain Industry. *Blockchains* **2024**, *2*, 195–216. <https://doi.org/10.3390/blockchains2030010>

Academic Editors: Jingyu Hua and Na Ruan

Received: 27 May 2024

Revised: 22 June 2024

Accepted: 2 July 2024

Published: 8 July 2024



Copyright: © 2024 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

Keywords: bug bounty programs; blockchain; cybersecurity; privacy; network security; software vulnerabilities; ethical hacking; zero-day vulnerabilities; exploits; crowdsourcing; cyber threats; vulnerability discovery; security vulnerabilities

1. Introduction

New software, websites, and web applications are being developed daily on a global scale. However, this rapid growth also brings an increased risk of security threats. Often, these vulnerabilities stem from bugs inadvertently introduced during the development process. Cyber attackers, adept at identifying and exploiting such weaknesses, can manipulate these bugs to gain unauthorized access and potentially harvest sensitive data. To get ahead of security threats, bug bounty programs have become a significant part of cybersecurity strategies for many organizations. Security researchers earned approximately USD 40 million from bug bounty programs in 2019 [1].

Bug bounty programs leverage the collective intelligence of the cybersecurity community, and have emerged as a cost-effective solution to the persistent and ubiquitous threats that exploit network vulnerabilities. They are considered effective as they enable organizations to discover and fix vulnerabilities before they can be exploited. These programs offer a proactive approach to security, helping to identify and address vulnerabilities before they are exploited. They can be more cost-effective than traditional security measures, as they tap into the collective expertise of the security community. The number of hacker-powered

security initiatives grew by at least 30% in various regions, with Latin America leading at a 41% growth rate [2].

Platforms such as Bugcrowd, HackerOne, Cobalt, Synack, and Zerocopter [3,4] have pioneered the concept of creating a user-friendly ecosystem where organizations can collaborate with numerous ethical hackers. These platforms facilitate cyber threat resolution by harnessing the collective expertise of these security professionals. Ethical hackers are incentivized to report vulnerabilities to the respective companies, often receiving rewards for their contributions. Collectively, these initiatives are known as bug bounty programs or vulnerability assessments.

Through these programs, organizations offer a structured environment where the security of their software and websites can be rigorously tested. Ethical hackers report any detected vulnerabilities and, in return, may receive monetary compensation or other forms of credit. Additionally, participants can gain recognition through ‘Hall of Fame’ listings, which also serve to enhance their reputation within these platforms. In Figure 1, a graph of domains targeted by cybercriminals provides a detailed analysis of various business sectors that are frequently targeted by hackers. This includes financial services, online service platforms, and e-commerce, which together account for up to 50% of all cyber attacks worldwide.

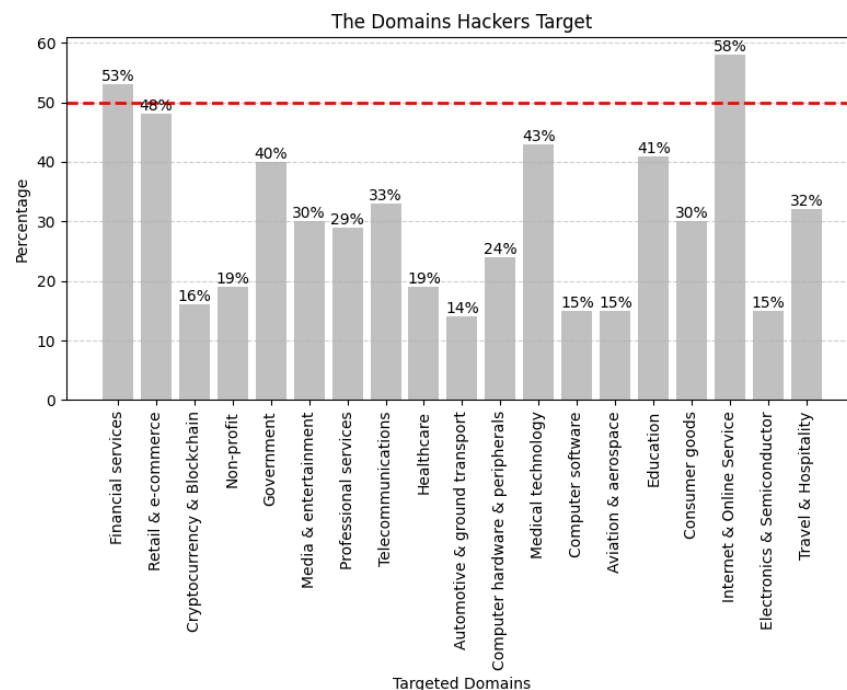


Figure 1. An overview of business domains and sectors targeted by cybercriminals.

These programs are not only used by the private sector; instead, in preparation for launching official software and web applications, governments often conduct thorough testing. To enhance this process, many have established bug bounty programs, which offer a safer and more cost-effective alternative to traditional security audits [5]. For example, Singaporean authorities initiated a bounty program for their technology company, aimed at strengthening the security of their IT infrastructure. The rewards for identifying bugs ranged from SGD 250 to SGD 5000, depending on the severity of the vulnerabilities discovered. In exceptional cases, where a bug could potentially compromise an entire government database and cause substantial harm, a special reward of up to SGD 150,000 was offered [6].

Similarly, in the United States, the Department of Defense (DoD) launched the ‘Hack the Pentagon’ initiative. This pioneering program, introduced in 2016, was designed to secure the DoD’s IT infrastructure prior to public deployment [7,8]. To date, there have

been 40 bug bounty programs, engaging over 1400 security researchers. These white hat hackers have been instrumental in identifying more than 2100 vulnerabilities within the DoD's systems [9]. On average, each program uncovered 38 vulnerabilities, with 11 deemed critical, 23 high, and 4 medium in severity. The impact of these findings has significantly enhanced the security posture of both the DoD and the Pentagon. The rewards for vulnerability assessments on platforms like HackerOne range from USD 100 to USD 15,000 [10].

The rapid emergence of blockchain technology has created a pressing need for companies to integrate it into their operations, but this integration also presents a significant cybersecurity challenge. As technology advances, security threats proliferate, prompting companies to initiate their bug bounty programs to identify and remediate vulnerabilities [11]. Bug bounty programs have evolved to become a crucial component of a company's cybersecurity strategy, with many organizations either managing them internally or leveraging third-party platforms [12]. Despite the growing popularity of bug bounty programs, there remains a conspicuous absence of comprehensive research that explores this domain. Furthermore, few studies have investigated the differences between company-based and platform-based programs or examined the latest innovations in the industry [13]. This knowledge gap highlights the need for a systematic analysis of bug bounty programs in the context of blockchain adoption, as well as the role they play in enhancing cybersecurity and ensuring the integrity of blockchain-based systems.

We realize that blockchain technology is widely used for security applications in various fields, with a significant focus on IoT, healthcare, and wireless networks. Also, smart contracts are commonly used in blockchain security solutions, and integration with other technologies is also a popular practice to enhance security [14]. Therefore, having bug bounty platforms that accommodate these platforms' security and privacy is needed.

Our research aims to fill this void by presenting an exhaustive overview of the bug bounty ecosystem and conducting an in-depth comparative study of both platform-based and company-based programs. A review of the existing literature reveals a gap in discussions surrounding the challenges and opportunities within the bug bounty landscape, as well as the emerging innovations. This presents a unique opportunity to consolidate these topics into a singular article, providing valuable insights for both bug hunters and organizations. In our study, we seek to address pivotal questions that often challenge newcomers to the bug bounty field. We will scrutinize the pros and cons of these platforms from the perspectives of hackers and the entities offering bug bounty programs. In this article, we address the following:

1. We conduct a comprehensive review of the blockchain landscape and bug bounty ecosystem, providing a detailed understanding of the current state of bug bounty programs for computer networks and blockchain-based companies.
2. We investigate the effectiveness of different bug bounty program models (platform-based and company-based) and identify the most suitable platforms for launching a bug bounty program.
3. We compare and analyze various bug bounty programs, uncovering their unique value propositions, challenges, and opportunities, as well as identifying innovations that are shaping the future of bug bounty programs and their potential applications in the blockchain space.

2. Background

This Section will review the existing studies that explore the challenges, benefits, and analysis of bug bounty programs. For the ease of the reader's understanding, Table 1 presents a comparative analysis of selected studies in an easy-to-understand manner.

Malinka et al. [15] considered that integrating bug bounty programs into cybersecurity education was a promising strategy. Their idea was to add real-world bug bounty into the curriculum of students to enhance their practical skills and contribute to the overall security infrastructure. The results were promising as they assisted students in building

practical skills and knowledge of how to tackle real-world problems, providing them with exposure to the ethical hacking industry and training them to reduce the gap between academia and practical skills. Magalhaes et al. [16] highlighted that bug bounty programs are novel approaches in cybersecurity that use a global community of ethical hackers to find vulnerabilities. Although such programs provide monetary benefits for finding vulnerabilities at a low cost, there are other moral and legal issues to consider as well. Organizational rules are intended to maintain authority and guarantee ethical behavior. Yet, legal uncertainties continue to exist, creating difficulties for regulatory frameworks and compliance. National and international authorities need to handle these challenges as bug bounty programs develop to protect legal integrity, ethical standards, and ultimately, cybersecurity performance.

Table 1. Comparative analysis of literature review.

Author	Challenges	Opportunity	Platforms Base Program	Company Base Program	Emerging Trends
Malinka et al. [15]	×	✓	×	×	×
Magalhaes et al. [16]	✓	✓	×	✓	×
Gersbach et al. [17]	×	×	×	×	✓
Wachter et al. [18]	×	✓	×	×	×
Akgul et al. [19]	✓	✓	×	✓	×
Maulani et al. [20]	✓	✓	×	×	×
Atefi et al. [21]	✓	✓	×	×	×
Melo et al. [22]	×	×	✓	×	✓
Canido et al. [23]	×	×	×	×	✓
Shafigh et al. [24]	✓	×	✓	×	✓
Walshe et al. [3]	×	✓	×	×	×
Sivagnanam et al. [25]	×	✓	×	×	×
Zhao et al. [26]	×	✓	✓	×	×
Bhushan et al. [27]	✓	✓	×	×	×
Akgul et al. [28]	✓	✓	×	✓	×
Bukangwa et al. [29]	×	×	✓	×	✓
Wachs et al. [30]	×	✓	✓	×	×
Sridhar et al. [31]	×	✓	×	×	×
This Paper	✓	✓	✓	✓	✓

Symbols: ✓—The research covers this aspect. ×—The research does not cover this aspect.

Gersbach et al. [17] highlighted the concept of artificial bug insertion which will increase the search for actual bugs. The paper suggested that only one bug is sufficient to achieve all possible efficiency gains. Artificial bugs are especially beneficial when the budget for bounties is low or when finding actual bugs is more important. The authors discussed multiple approaches for implementing artificial bugs in practice and outlined additional benefits of using them. Wachter et al. [18] addressed the challenge of encouraging software engineers to build secure code, which is made more difficult by moral hazard in teams. One suggestion was to create scored competitions involving white hat hackers or bug bounty hunters and software development teams to combat moral hazard. The study looks at a lack of investment in security caused by mismatched objectives and

compares the effectiveness of black-hat and white-hat markets, as well as the role of bug bounty programs.

Akgul et al. [19] examined the bug bounty ecosystem from the view of ethical hackers, pointing out the challenges and benefits. The research was based on different types of surveys and interviews with skilled ethical hackers to know their opinions and motivation. They found out that ethical hackers are motivated by the rewards and learning opportunities while the scope of the project is the one thing that makes a difference while choosing programs. The research concluded with the main challenge of communication between the officials and ethical hackers. Maulani et al. [20] explored the substantial impact of bug bounty hunting on company security. They highlighted the expertise of security researchers and emphasized their role in identifying complex vulnerabilities. The effectiveness and quality of their work significantly contribute to enhancing a company's security posture. Additionally, the paper delves into both the challenges and benefits associated with bug bounty hunting. The findings suggest that bug bounty programs are a cost-effective approach to improving security measures, although they need to overcome communication challenges.

Atefi et al. [21] explored the bug bounty programs of Chromium and Firefox using a data-driven approach. They introduced the concept of the probability of rediscovery as a metric to assess the difficulty of uncovering vulnerabilities. Their research indicates that following bug bounty programs, threat actors face increased challenges in exploiting vulnerabilities. Additionally, the study compared vulnerabilities identified internally with those discovered externally. These findings underscore the effectiveness of bug bounty programs in enhancing security measures. Pinto et al. [22] emphasized the pivotal role of Web3 technology within the blockchain and smart contract ecosystem, known for its secure, distributed, and decentralized applications. As Web3 evolves with ongoing innovations, it inevitably encounters security vulnerabilities. Additionally, the research evaluates tools designed to detect bugs within smart contract systems. The study also discusses the development and integration of plugins tailored for smart contracts.

Canido et al. [23] draw attention to the significance of open software vulnerability systems. Many organizations host bug bounty programs to engage a wider pool of security experts, a challenge within this ecosystem. Addressing this, the paper introduces VeriOSS, an innovative bug bounty platform designed to integrate blockchain technology. VeriOSS ensures secure transactions by providing rewards with guaranteed economic incentives. This paper advances and enriches the bug bounty program industry. Shafigh et al. [24] examine the reasons behind invalid report submissions in bug bounty programs. This paper addresses two main questions: the underlying reasons for reports being deemed invalid and the characteristics that categorize them as out-of-scope. Utilizing data from HackerOne, the study reveals that out-of-scope submissions are often considered invalid reports. The findings of this research pave the way for suggesting an automated classification technique based on vulnerability types to enhance the identification of invalid reports.

Walshe et al. [3] highlighted in their research that launching a bug bounty program is more economical than two security engineers. Their study calculates the average cost of a bug bounty program and the salary of two security engineers. Astonishingly the results suggest that launching a bug bounty has more benefits than hiring two security engineers. Bug bounty programs gather a large pool of freelance security experts. This approach not only gathers a broader pool of expertise but also reduces cost. Sivagnanam et al. [25] examined the data of bug bounty programs to prove that bug hunters' vulnerabilities are more critical than organization's security engineers. The review finds that launching a bug bounty program has more benefits for organizations in terms of the severity of vulnerabilities. High-reward bug bounty programs attract expert white hat hackers that increase the quality of vulnerabilities. Bug hunters often come with a new mindset about vulnerability discovery. These new mindsets always uncover blindspots that are overlooked by hired security engineers. Furthermore, the competitive nature of bug bounty programs forces bug hunters to invest more time and effort.

Zhao et al. [26] researched two platforms, HackerOne and Wooyun, to analyze monetary reward, which is a benefit for bug hunters. The results of the study show that monetary reward is a powerful tool to motivate bug hunters for effective investment of time and effort. The engagement of expert bug hunters in high-reward programs keeps organizations safe from false positive reports. The study does not analyze the data on challenges caused by these platforms. Bhushan et al. [27] highlighted the scope of bug bounty programs focusing on the severity of vulnerabilities. Research has also examined the quality of bugs assessment. Akgul et al. [28] conducted a survey by hiring white hat hackers to explore the challenges and opportunities they face in the realm of bug bounty programs. Most bug hunters said that rewards attract them to specific programs, though the communication gap between organizations and bug hunters makes them stop operations on a specific program. The main challenge white hat hackers face is dissatisfaction with responses.

Bukangwa et al. [29] proposed a simulation model using NetLogo to enhance the efficiency of bug bounty programs. The study suggests using an AI-based algorithm to streamline bug data analysis and optimization of reports. Further, the model integrates economic and political frameworks by reviewing monetary rewards that will attract bug hunters. This paper presents a promising step towards efficient data handling of bugs. Wachs et al. [30] highlighted the role of platforms in the transactions of rewards between organizations and white hat hackers. The study also highlights that platforms reduce frictional costs linked with payments and uncertain assets. The paper talks about HackerOne's facilitation in the report on vulnerabilities. Sridhar et al. [31] analyzed the data on bug bounty programs and how these programs are valuable for companies with limited resources. The study calculates the effect of bug bounty programs on the industry. The results suggest that the use of bug bounty programs not only enhances the security posture of an organization but is also valuable for white hat hackers.

Given the recent and rapidly evolving nature of bug bounty programs within the cybersecurity landscape, we have examined the existing literature as a foundation for our study. Our review of this literature revealed a significant research gap, with many papers focusing narrowly on specific attributes of bug bounty programs. This paper, however, seeks to bridge this gap by providing a thorough analysis that encompasses all these attributes. Furthermore, we have examined several papers as discussed in Table 1 and identified a research gap. Specifically, we found that these papers did not adequately discuss the challenges, opportunities, comparative analysis, and emerging trends of various bug bounty platforms. Our paper aims to address this gap and contribute to the body of knowledge in this area.

3. Blockchain Security Landscape

Blockchain technology is a peer-to-peer network working in chains of multiple blocks providing immutability, security, and traceability. The technology was introduced by Satoshi Nakamoto, a person or group behind cryptocurrency, bitcoin, and blockchain. Blockchain was mainly introduced for bitcoin for immutable and secure transactions and transfer of ownership. Blockchain nowadays is not just limited to cryptocurrency but its security features have caught the attention of many technology enthusiasts using technology in any industry where security is required, like supply chain, intellectual property, healthcare, real estate, etc. [32]. The benefits provided by blockchain also come with some drawbacks. Blockchain technology has security limitations. Blockchain integration can be a challenge and create particular problems if it is compromised. Blockchain has many parts and can be compromised if proper security measures are not applied to them.

3.1. Consensus Mechanism

The consensus mechanism serves an important part in blockchain technology as it makes sure that all the nodes are agreed upon and established on a single dataset. It is a protocol that engages all the nodes and aligns them with the dataset while maintaining transparency, collaboration, and cooperation [33]. The popular attack in the consensus

mechanism is a 51% attack; if an attacker or a group of attackers gains unauthorized access to more than 50% of the network it will be able to control it and reverse transactions and manipulate them [34]. A Sybil attack is another attack in which the attacker makes several identities to gain access to the network. It can disrupt the ability of decision-making, and affect transparency overall, disrupting the integrity of the consensus mechanism [35]. The "Nothing at stake" problem is caused by multiple forks—stake validators propose multiple forks and sometimes some forks are left unchecked or are unnoticed, and because of the lack of validation, it can cause a potential vulnerability for attackers to gain access to the network [36].

3.2. Smart Contracts and Security

Smart contracts are digital agreements that automatically perform actions when specific conditions are met. Smart contracts are used with blockchain technology that is immutable and transparent. These contracts operate on a decentralized platform that automates processes, making them highly valuable across various industries. In the financial sector, it enables secure automated transactions, reducing costs and increasing efficiency. Every technology has some security flaws along with benefits. Reentrancy attacks [37] exploit integer overflow attacks, denial-of-service attacks, improper exception handling, type conversion errors, and unpredictable state changes due to chain forks [38]. These are some issues that smart contracts are facing and bug bounty programs enhance the security by finding vulnerabilities.

To strengthen the network of any blockchain-enabled technology, one should consider strengthening the network and user from common attacks like DDoS and phishing. DDoS can be very effective in planning to disrupt the normal working of a network because it floods the network with unmanageable traffic ending in a damaged network and no service. However, DDoS is not a big issue for blockchain as it uses decentralization; however, if the attacker can generate fake/spam transactions forcing the network to be slow and overwhelm it overall, the normal working of the network can be disrupted [39]. Routing attacks on blockchain networks involve changing the network traffic and forcing it to partition the network and slow the transaction processes making the network distributed and vulnerable [40]. Similarly, eclipse attacks on networks monopolise the nodes controlling their paths feeding the wrong information, and completely isolating the node from the rest. This process enables connections to the fake node of the attacker. The attack will show the node separate views of the blockchain network enabling double-spending attacks [41]. Phishing and social engineering tactics can help gain sensitive data regarding the blockchain network revealing private keys which can help the attacker to gain access to the network.

3.3. Identity Management and Supply Chain

In blockchains with decentralized technology, the issue of identity theft arises because of decentralization. The lack of central authority can help attackers to impersonate the identity of the actual owner and gain access to the network—to counter this issue, a solution termed self-sovereign identity (SSI) has been proposed [42]. The solution states that users can have full control over their accounts by giving them unique credentials and checking these credentials at login allowing the user to manage their identities themselves. The account can be used on different platforms facilitating interoperability [43].

Supply chain management ensures the quality and productivity of an industry supporting the delivery of raw products through to refined end products. Reliance on a blockchain supply chain also requires security measures to ensure the integrity and confidentiality of the industry. Blockchain can help track and trace the overall progress of products ensuring proper security measures are taken. Each transaction is recorded on the blockchain for immutable records. Smart contracts can be applied to execute tasks that are predefined and executed when certain conditions are met [44].

4. Bug Bounty Life Cycle

This section provides a brief overview of the bug bounty hunting life cycle, offering a comprehensive understanding for beginners. The bug bounty hunting life cycle is a sequence of steps that hunters follow to identify and report vulnerabilities as explained in Figure 2. The first step in this process is choosing a program. Bug bounty hunters select a program based on certain criteria, with the reward offered by the company being a primary motivation. Once a program is chosen, the next step is to define the scope of the target. This includes the target website's domain, subdomains, and related sites or applications. Defining the scope ensures that no potential vulnerabilities are overlooked.

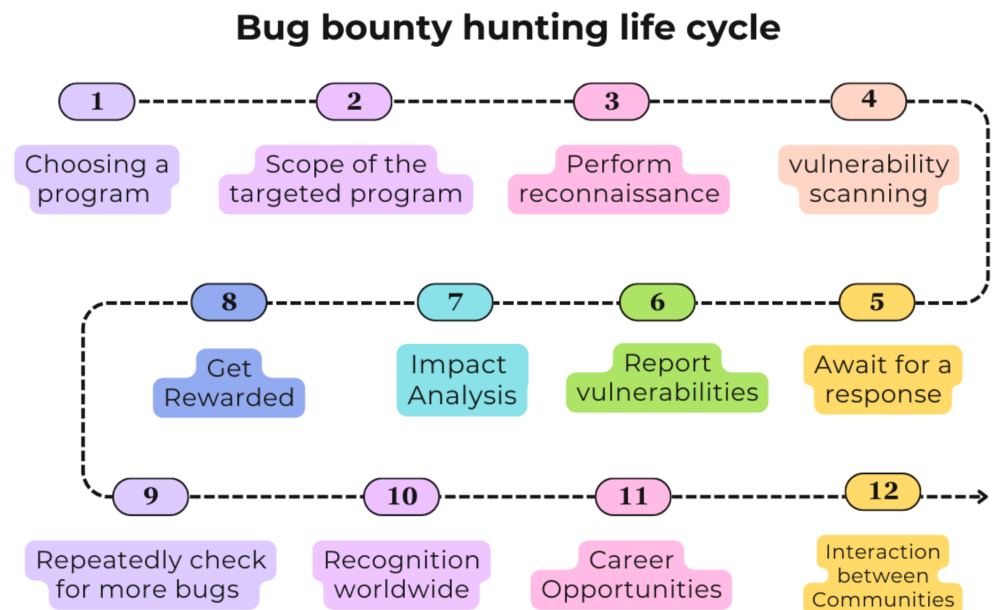


Figure 2. An overview of bug bounty hunting life cycle.

After identifying the target website's scope, hunters perform reconnaissance to gather information on its technologies, configurations, and vulnerabilities. Tools like Google Dorks, Whois Lookup, and Nmap are commonly used at this stage. Following reconnaissance, vulnerability scanning is conducted. While automated vulnerability scanning is crucial, manual testing is also essential. This involves directly checking for vulnerabilities like SQL injection, XSS, and CSRF on the target website.

Once vulnerabilities are discovered, an impact analysis is performed. This involves evaluating the potential impact of the vulnerabilities, understanding their severity, potential exploitation scenarios, and the risks they pose to the application and users. After identifying vulnerabilities, it is important to report the vulnerabilities to the owner of the bounty program. The owners are then given adequate time to validate, fix, and release patches before the information is shared publicly.

Upon successful validation and patching of the reported vulnerabilities, hunters are rewarded according to the severity of the reported vulnerability. Even after a successful bounty hunt, it is important to perform frequent checks. A system is never fully protected; many potential vulnerabilities can exist. Therefore, hunters should keep looking for them in the program frequently. Successful bounties increase the points acquired by the hunters, giving them a chance to be in the Hall of Fame, which can be seen worldwide. This recognition often leads to career opportunities as many companies will want to work with recognized hunters. During the complete process, a hunter goes through multiple obstacles. To overcome them, one often seeks help from many skilled professionals or reads blogs on different vulnerabilities to approach the target differently. This interaction between communities is a crucial part of the bug bounty hunting life cycle.

5. Programs Selection and Offered Assessments and Compliance

This section discusses various types of bug bounty programs. These programs are hosted on diverse platforms tailored to the needs of companies and white hat hackers. Each platform has its unique workspace, workflow, reward system, and scope for different vulnerabilities. The choice of platform varies among online websites and companies for crowdsourcing [45].

Figure 3 presents a detailed taxonomy of bug bounty programs and the platforms chosen for this study. The taxonomy is divided into four major segments: Platform-based Programs, Company Specific-based Programs, Assessments, and Compliance. Details of all these segments will be provided in the subsequent sections.

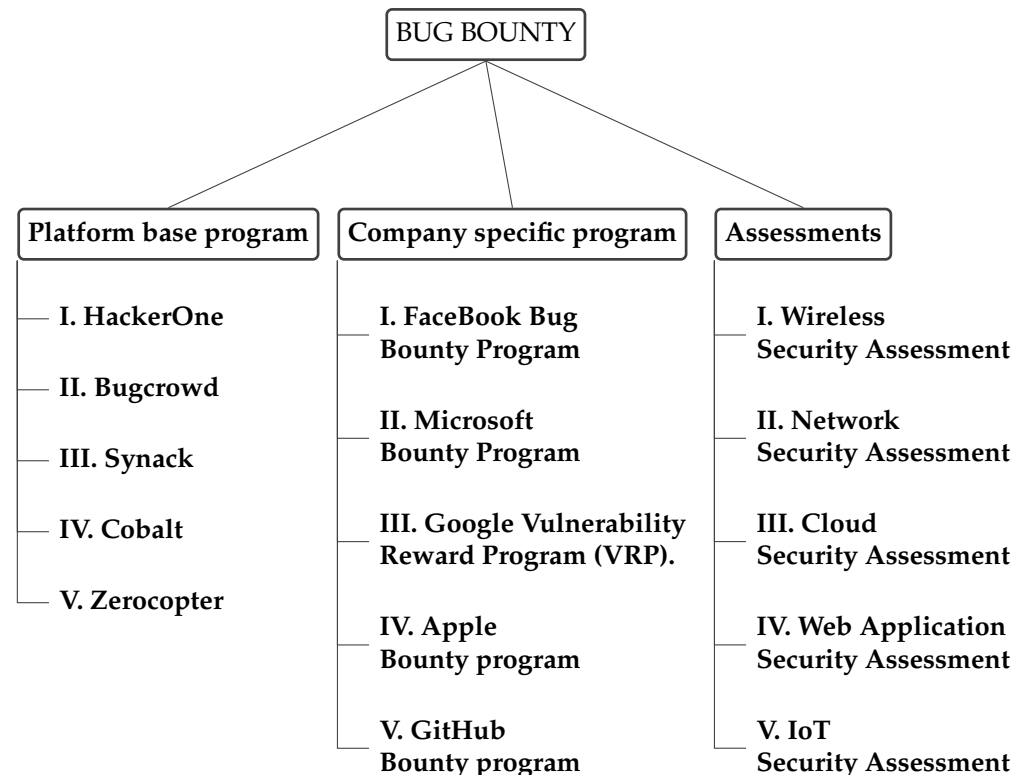


Figure 3. Bug bounty taxonomy: visualization of programs, assessments, and compliance.

5.1. Platform-Based Bug Bounty Programs

Platform-based programs are bug bounty programs hosted on platforms that connect security researchers with organizations. These platforms provide a structured environment for reporting vulnerabilities and receiving rewards. For this study, we selected five platforms: Hackerone, Bugcrowd, Synack, Cobalt, and Zerocopter.

5.1.1. Hackerone

HackerOne, a leading global platform, was established in 2012 by some of the best Dutch hackers. Their goal was to secure the internet, which they demonstrated by discovering critical bugs in high-tech companies during the “Hack-100” program. As of 2021, the platform had over a million active ethical hackers [46]. HackerOne boasts the largest community among all platforms, where ethical hackers work continuously to enhance security. The platform’s response time to a vulnerability report averages under 5 days, and the triage process takes between 5 to 10 days. HackerOne has paid out USD 230 million in bounties and counts the US Defense Department among its clients [10,47].

5.1.2. Bugcrowd

Bugcrowd, founded in the same year as HackerOne [48], provides services like SaaS and penetration testing for clients interested in vulnerability disclosures. They also offer services for APIs, Mobile apps, IoT, Networks, and Web apps. Bugcrowd hosts more than 300 programs per quarter on its website for full vulnerability disclosure, with more than 300,000 hackers registered. The monetary rewards for successful bounty programs range from USD 100 to USD 100,000, depending on the company's policy [49]. Bugcrowd offers both private and public programs, with a triage process that takes up to 48 h to validate and respond to a submitted vulnerability [50].

5.1.3. Synack

Synack, established in 2013 by former employees of the NSA and US DoD, aims to make the internet safer [51]. Synack stands out for its private bounty programs, which hire only skilled, professional, and ethical hackers [52]. Synack is not for beginners as they focus on skilled professionals. The platform provides substantial monetary rewards for authentic vulnerability reports, and their response time is the fastest among the other platforms [53].

5.1.4. Cobalt

Cobalt, founded in 2013, is based on the principle that penetration testing can be ethical [54]. They aimed to make their services in-demand by offering Penetration Testing as a Service (PTaaS), paired with Software as a Service (SaaS). They launched a successful platform for industries to test their IT infrastructure security [55]. While Cobalt may not be as well known as HackerOne or Bugcrowd, it competes with other platforms like Zerocopter and Synack. Cobalt offers three distinct packages for its clients: Standard, Premium, and Enterprise [56]. Each package varies in cost and services offered. The platform's response time to queries is average compared to other platforms [57].

5.1.5. Zerocopter

Zerocopter, established in 2016, aims to regularly monitor the confidentiality and integrity of a platform, enabling organizations to operate at their full potential without fear of cyber-attacks and critical data breaches [58]. The platform was founded by a team of security enthusiasts skilled in both defensive and offensive security, with a determination to effect positive societal changes [59]. Zerocopter offers reasonable monetary rewards to white hat hackers and provides companies with a smooth environment for crowdsourcing. Their rewards are based on the reported vulnerability, with standard rewards ranging from Low: USD 55–160, Medium: USD 160–490, High: USD 540–3250, to Critical: USD 1630–5425 [60]. However, Zerocopter is not the first choice for companies or hackers using crowdsourcing due to its policy of maintaining secrecy concerning its clients and insider data.

5.2. Company-Specific Programs

Company-specific programs are bug bounty programs run independently by individual companies, often large tech corporations. These programs allow companies to maintain more control over their vulnerability disclosure process. For this study, we chose the bug bounty programs of Facebook, Microsoft, Google, Apple, and GitHub.

5.2.1. Facebook Bug Bounty Program

Facebook, under its parent company Meta, runs a bug bounty program that rewards actual bug reports [61]. Launched in 2011, the program leverages the expertise of global security experts to identify and disclose vulnerabilities in platforms such as Facebook, Instagram, WhatsApp, and Messenger. The program has successfully fixed several vulnerabilities over the years, fostering collaboration between Facebook's security team and the global security research community. To stay ahead of emerging risks and enhance its security posture, Facebook continues to fund its Bug Bounty Program.

5.2.2. Microsoft Bug Bounty Program

Microsoft operates a bounty program that rewards successful vulnerability reports within its allowed domains [62]. Launched in 2013, the program actively identifies and fixes vulnerabilities across all Microsoft services and products, including Office, Windows, and Azure. The program has facilitated the discovery and mitigation of several vulnerabilities within Microsoft's infrastructure and encouraged responsible vulnerability disclosure. Microsoft is committed to expanding and adapting its Bug Bounty Program in response to new security risks.

5.2.3. Google Vulnerability Reward Program (VRP)

Google offers bounties for valid vulnerability reports within its allowed domains. Initiated in 2010, the Vulnerability Reward Program (VRP) encourages security researchers to find and report vulnerabilities in Google's products and services, including Google Search, Gmail, Chrome, and Android [63]. The program has significantly improved the safety and resilience of Google's products and services and fostered collaboration and trust among security research communities. Google is committed to continually developing and evolving its VRP to meet emerging security challenges and enhance its ecosystem's security posture.

5.2.4. Apple Bounty Program

Apple's Bug Bounty Program rewards users for finding vulnerabilities in any of its products, including tvOS, iOS, macOS, and iCloud. Launched officially in 2016, the program encourages security researchers to find and report vulnerabilities in Apple's software like, watchOS (version 3.0 or later) macOS Server (version 5.0 or later) hardware, and services [64]. The program has helped discover and mitigate several security vulnerabilities within Apple's infrastructure, contributing to the continuous improvement in product security and privacy features. Apple is committed to further extending and improving its Bug Bounty Program to meet evolving security threats and challenges, with a focus on fostering interactions with the security research community and prioritizing user privacy and security.

5.2.5. GitHub Bounty Program

GitHub operates a bug bounty program to find and fix security flaws within its platform [65]. Launched in 2014, the Security Bug Bounty Program detects and resolves security flaws in GitHub's code hosting platform and related technologies. The program has helped find and fix various security flaws, enabling GitHub to address security issues and implement robust security measures to protect its users and their data. GitHub continues to invest in its Bug Bounty Program to stay ahead of new threats and vulnerabilities, aiming to enhance its security architecture and foster collaboration among developers.

5.3. Assessment Variations

The assessments section focuses on the types of assessments provided on these bug bounty platforms. We evaluated all chosen platforms based on five types of assessments: Wireless Security Assessment, Network Security Assessment, Cloud Security Assessment, Web Application Vulnerability Assessment, and IoT Assessment.

1. Wireless security assessment aims to identify weak points in wireless networks. It involves examining the security of Bluetooth connections, Wi-Fi networks, and other wireless technologies. Common wireless security issues include weak encryption standards, incorrectly configured access points, rogue devices, and unauthorized access.
2. Network security assessment evaluates a network infrastructure's security. It involves scrutinizing networks for flaws, errors, and vulnerabilities in hardware, such as servers, firewalls, routers, and switches. Network segmentation gaps, unsecured protocols, and potential entry points for attackers can all be identified through network security assessments.

3. Cloud security assessment evaluates the security of cloud-based environments and services. In cloud systems like Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform, it involves checking settings, permissions, access controls, and data encryption.
4. Web application vulnerability assessment examines the security of web applications by testing known vulnerabilities like SQL injection, cross-site scripting (XSS), server-side request forgery (SSRF), and client-side request forgery (CSRF).
5. IoT vulnerability assessment identifies bugs and weaknesses in IoT devices and systems integrated with them. It aims to identify potential threats to the security of IoT devices and systems that could be exploited.
6. Blockchain security assessment evaluates the security of blockchain-based systems and applications. It involves identifying vulnerabilities in smart contracts, examining the integrity of blockchain transactions, and assessing the overall resilience of blockchain-based systems.

6. Comparative Analysis of Bug Bounty Programs

Table 2 provides a comparison of different bug bounty platforms [48]. The table has multiple columns, each providing specific insights: The first column platform lists the names of the bug bounty platforms, the second column lists the location where each platform is based and the year column shows the year established.

Table 2. A review of different bug bounty platforms based on features, rewards, and industries they serve [66].

Platform	Loc.	Year	Features	Rewards	Severity	Industry
HackerOne [67]	US	2012	Supports various industries, offers training platform for beginners, uses AI copilot (Hai) for efficient operation	\$100–\$1 M	Low–Critical	Blockchain, Cryptocurrency, E-commerce, Software, Media
Bugcrowd [48]	US	2012	Offers integrations, validation service, provides a training platform for beginners	\$125–\$3 M	Low–Critical	Blockchain, Cryptocurrency, NFTs, Automobile, Space Exploration, Network Providers, Blockchain, Security
Synack [52]	US	2013	Complies with government regulations, offers a training platform (Synack Red Team) for beginners, focuses on skilled professionals	Disclosures only to invited or selected red teamers.	Depends on severity	Blockchain Industries, Computer Networks, E-commerce, Software, Media
Cobalt [54]	US	2013	Facilitates team collaboration, offers different packages for companies	Standard, Premium, and Enterprise packages.	Any vulnerability	Computer Networks, Cybersecurity, Pen-testing, Blockchain Industries
Zerocopter [58]	Netherlands	2013	Provides triage and validation of reported vulnerabilities	\$50–\$5000	Depends on severity	IT Industries, Blockchain Industries, Computer Networks, Cybersecurity and Privacy
Facebook [61]	US	2011	Offers rewards for vulnerability in their products	\$100–\$1 M	Low–Critical	Social Media and Technology
Microsoft [62]	US	2013	Offers rewards for responsible vulnerability disclosures in Microsoft services	\$100–\$60 k	Low–Critical	IT Industries, Media, E-commerce, Cryptography
Google [63]	US	2010	Offers rewards for responsible vulnerability disclosures in Google’s products and services	\$100–\$40 k	Low–Critical	IT industries, Computer network
Apple [64]	US	2014	Offers rewards for responsible vulnerability disclosures in Apple’s products and services	\$5 k–\$2 M	Low–Critical	Consumer Electronics, IT industry, Media, Websites
GitHub [64]	US	2016	Offers rewards for responsible vulnerability disclosures in GitHub’s products	\$600–\$30 k	Low–Critical	Software development and Vulnerabilities

Similarly, unique features detail special offerings, rewards specify the monetary incentives for identifying vulnerabilities, severity refers to the levels of vulnerability, and industry describes the sectors that these platforms cater to.

Each platform mentioned offers unique benefits and drawbacks. Platform-based programs manage the bug bounty program efficiently, providing effective communication. They also ensure secure and transparent monetary rewards and define the scope of testing. On the other hand, company-based programs may lack clear scope and limitations. Company-based bug bounty programs like Google, Apple, and Microsoft offer clear benefits and internally have total control over the procedure, including setting the range for rewards, regulations, and scope. However, the success of company-provided bug bounty programs depends on the organization's ability to attract and retain highly qualified researchers, which can be challenging, particularly for smaller or less well-known companies.

Table 3 provides a comparative analysis of selected bug bounty platforms. It highlights key features including the availability of programs, fast response times, high rewards, training platforms, diversity of ethical hackers, and AI integration. Most bug bounty programs, such as HackerOne and Bugcrowd, are widely used due to their diverse pool of experienced ethical hackers. Both platforms aid in finding and mitigating security vulnerabilities in blockchain-based systems. In contrast, platforms like Google, Apple, and Microsoft offer a focused approach, with specialized testing in areas such as network, integration modes, user-side, and server-side. However, they do not specifically offer services for securing third-party blockchain technology [66]. From the table, HackerOne seems to provide several features discussed. HackerOne has private/public bounty programs, and the triage takes a standard time. It provides a quick and efficient response. In terms of monetary rewards, HackerOne is one of the platforms that provides effective rewards for successful reports. Zerocopter has security researchers and skilled professionals who test the security of a company's IT infrastructure. Zerocopter has private programs on which professionals of Zerocopter work. It seems to be the least preferred of the selected platforms.

Table 3. Comparative analysis of selected bug bounty platforms based on key features.

Platforms	Private Programs	Public Programs	Fast Response	High Reward	Training Platform	Diverse Ethical Hackers	AI Integration
Hackerone [67]	✓	✓	✓	✓	✓	✓	✓
Bugcrowd [48]	✓	✓	✓	✓	✓	✓	×
Synack [52]	✓	×	✓	✓	✓	×	×
Cobalt [54]	✓	×	×	×	×	×	×
Zerocopter [58]	✓	×	×	×	×	×	×
Facebook [61]	×	✓	✓	✓	×	✓	×
Microsoft [62]	×	✓	✓	✓	×	✓	×
Google [63]	×	✓	✓	✓	×	✓	×
Apple [64]	×	✓	✓	✓	×	✓	×
GitHub [64]	×	✓	✓	✓	×	✓	×

The analysis shows that HackerOne stands out by offering all the features listed, including both private and public programs, fast response, high rewards, a training platform, diverse ethical hackers, and AI integration. Bugcrowd also offers a wide range of features but lacks AI integration. Synack focuses on private programs, fast response, high rewards, and a training platform but does not support public programs, diverse ethical hackers, or AI integration. Cobalt and Zerocopter provide private programs but lack other features, such as fast response, high rewards, and AI integration.

In contrast, platforms like Facebook, Microsoft, Google, Apple, and GitHub offer public programs, fast response, high rewards, and support for diverse ethical hackers but do not provide private programs, training platforms, or AI integration. This comprehensive comparison highlights the strengths and limitations of each platform in terms of the features they offer.

7. Challenges, Opportunities, and Emerging Innovations

In the blockchain industry, bug bounty programs face significant challenges that hinder the strengthening of cybersecurity and privacy. Bug bounty programs encounter challenges such as unreasonable reports, limited scope, communication issues, misaligned incentives, and lack of recognition. Unreasonable reports pose a significant challenge to strengthening the security of the blockchain industry [68]. White hat hackers play a crucial role in an organization's security architecture [69], but sometimes submit invalid reports that are difficult for organizations to manage. These reports can waste time and delay responses to valid reports. Invalid reports, including out-of-scope, false positives, no proof-of-concept (POC), fixed internally, and duplicate reports, affect both organizations and hackers' profiles on bug bounty platforms. To manage these reports, organizations should implement report review phases [70].

Limited scope is another challenge. It restricts the attack surface, limiting the areas that can be tested. However, hackers prefer programs with a larger scope [19], as they offer higher chances of finding bugs. Limited-scope programs often lead to invalid reports. Organizations should consider expanding the scope of their bug bounty programs to reduce invalid reports and increase competition [71].

Communication quality significantly impacts an organization's success [72]. Poor communication and slow response times can distract hackers from a program and lead to program failure. Efficient response times are crucial for addressing critical vulnerabilities [73]. Improving communication can prevent conflicts and avoid regrettable outcomes due to late patching [20].

Misaligned incentives also pose a challenge. Incentives, based on vulnerability severity, attract hackers and recognize their expertise. However, low incentives can result in reduced participation from expert bug hunters. Therefore, incentives should be carefully adjusted based on the severity of the vulnerability [74].

Recognition, in the form of public disclosure of achievements, rewards, and special badges, motivates bug hunters. However, organizations often hesitate to disclose the technical details of the vulnerabilities found due to security concerns. This lack of recognition can lower hackers' motivation and lead to misunderstandings. A potential solution could be for organizations to disclose and discuss vulnerability findings in industry conferences or seminars, providing valuable insights to the broader cybersecurity community without compromising sensitive technical details. These challenges include dealing with unreasonable reports, navigating limited scope constraints, overcoming communication challenges, aligning incentives appropriately, and ensuring adequate recognition for ethical hackers. Each of these challenges is compounded by the technically complex landscape of blockchain platforms, where securing smart contracts, consensus mechanisms, and decentralized applications is particularly challenging. Effective bug bounty programs in blockchain must successfully address these challenges to uphold platform integrity and cultivate a robust security ecosystem.

Bug bounty programs in blockchain present unique opportunities for ethical hackers to advance their skills and reputation. These platforms not only incentivize hackers with monetary rewards for identifying critical vulnerabilities but also offer recognition through features like the Hall of Fame. This acknowledgment serves as a showcase of hackers' capabilities to leading companies in the industry. Beyond financial incentives, inclusion in the Hall of Fame can lead to career advancements and invitations to prestigious global events. These opportunities not only expand hackers' professional networks but also enable them to contribute meaningfully to cybersecurity initiatives within the blockchain ecosystem.

Ethical hackers play a crucial role in strengthening the security of blockchain ecosystems by proactively identifying and reporting critical vulnerabilities [75]. Their expertise offers valuable insights into potential security gaps helping to secure blockchain applications and platforms used by various companies [28]. By uncovering both known vulnerabilities and zero-day exploits, ethical hackers significantly boost the overall security posture of blockchain organizations [76]. Furthermore, they contribute to maintaining the integrity of the CVE database by sharing their findings and insights [77,78].

Also, bug bounty platforms offer a cost-effective alternative to hiring additional software engineers within blockchain ecosystems. On average, companies globally spend approximately USD 83,950 annually per bug bounty program, significantly less than the cost of hiring multiple software engineers to audit their IT infrastructure's security [3]. These platforms attract skilled white hat hackers from diverse backgrounds leveraging their expertise to identify and address vulnerabilities at a reduced cost compared to traditional hiring practices [79]. Unlike fixed employment costs, bug bounty programs operate on a pay-for-results basis, where companies only pay for valid vulnerabilities discovered [28]. This approach not only minimizes expenses associated with vulnerability disclosure but also enhances the overall security resilience of blockchain applications and platforms.

Moreover, harnessing diverse skill sets is a hallmark of bug bounty programs within blockchain ecosystems. These platforms attract a diverse array of ethical hackers each bringing unique expertise in various domains which enhances the program's ability to identify critical vulnerabilities effectively [28]. Ethical hackers gain diverse skills during bug bounty programs, motivating them to work hard and acquire more skills. They actively participate in various communities, sharing knowledge and insider tips, and take part in effective learning of roadmaps and collaborations. This helps them gain new approaches to a bug bounty program and encourages them to earn ethically [80]. When hackers encounter difficulties with a particular program, they explore similar vulnerability reports or blogs by other hackers to gain insight [81]. Learning through online platforms by playing CTFs and other online pen testing labs can also increase their knowledge and change their approach towards a bug bounty program.

Flexibility in the work environment allows individuals to choose when, where, and how they want to work. Bug bounty programs offer this flexibility, enabling bug hunters to work anytime, anywhere, according to their schedule. This flexibility helps bug hunters balance their work and personal lives, leading to better job satisfaction. It also increases their productivity and reduces stress, allowing them to invest quality time in finding critical vulnerabilities. Cybersecurity experts often start their careers by participating in Capture The Flag (CTF) competitions and exploring vulnerable environments. However, the real world of cybersecurity is far more complex and unpredictable [82]. Unlike CTFs, real-world testing involves navigating through a myriad of challenges and uncertainties. This transition is crucial for cybersecurity experts to hone their skills and expertise. Investing quality time in real-world testing allows bug hunters to refine their problem-solving abilities, develop a deeper understanding of complex systems, and enhance their overall cybersecurity knowledge, especially in the blockchain security ecosystem [3]. Bug bounty programs offer valuable real-world testing opportunities and provide bug hunters with earning opportunities. Successful identification and reporting of vulnerabilities can lead to monetary rewards, making bug bounty programs beneficial for cybersecurity professionals. This combination of skill enhancement and earning potential makes bug bounty programs attractive.

8. Discussion

The primary aim of this study was to evaluate the effectiveness of bug bounty programs in strengthening cybersecurity and privacy within the blockchain industry. Through a comprehensive comparison of various bug bounty programs, company-based platform-based, and open-source initiatives, we analyzed their strengths, weaknesses, and overall success in addressing vulnerabilities. This evaluation also extended to the challenges and

opportunities that these programs encounter, which can sometimes become challenges in the enhancement of blockchain security.

Our analysis revealed that while bug bounty programs play a crucial role in identifying and mitigating vulnerabilities in blockchain systems, they are not without their challenges. Unreasonable reports, limited scope, communication issues, and misaligned incentives are some of the key obstacles that these programs face. Addressing these issues is crucial for organizations to maximize the benefits of bug bounty programs and foster a robust security ecosystem.

To overcome these challenges, organizations are increasingly integrating advanced technologies, such as artificial intelligence (AI) and blockchain, to enhance transparency and implement more effective methodologies. For instance, AI can be used to filter out invalid reports and prioritize genuine threats, thereby improving the efficiency of bug bounty programs. Here, we will discuss some great innovations to address these challenges and offer proposals to enhance the bug bounty ecosystem.

8.1. AI Application

One of the most important AI applications is the integration of the GenAI copilot, Hai. Launched by HackerOne on 27 February 2024, Hai builds on extensive security knowledge and provides reviews on submission reports with strong reasoning [83]. It uses a craft nuclei template for vulnerabilities, reducing the time to submit a report. It helps in understanding the vulnerabilities, their impacts, and other related details. It also offers remediation advice on vulnerabilities and can write a response message after reading the submission report. This innovation plays a role in handling all the challenges discussed in Section 4. Organizations on HackerOne use this latest innovation to increase the efficiency of bug bounty programs. Smartretro is an example of real-world implementation of AI in which vulnerabilities are detected using algorithms that scan the devices for any retrospective vulnerability after installation to uncover any security vulnerability [84].

AI is not only used in detecting vulnerabilities but is also being used in triage. AI models like CNNs, neural networks, and word embedding are being used for automatic bug triage which helps save time and additional workforce and automates everything [85]. Nowadays, AI is doing all the tough work—machine learning and deep learning are being trained on datasets to perform automated security testing to detect common vulnerabilities that can be detected using the datasets. Some vulnerabilities are difficult to find with AI but if trained well with enough data it can detect all kinds of vulnerabilities [86].

8.2. Smart Contracts

Bug bounty programs, serve as the primary motivation for bug hunters to invest quality time and effort in discovering vulnerabilities. However, when bug hunters do not receive rewards promptly, it can lead to frustration and dissatisfaction within the community. This dissatisfaction can result in a decline in the quality of vulnerability reports submitted to the bug bounty program, ultimately compromising the program's success and effectiveness. Additionally, the lack of transparency and accountability in traditional reward systems can exacerbate these challenges, making it difficult for bug hunters to track their rewards' status and ensure fair compensation for their efforts.

To address these challenges, a blockchain-based reward system utilizing smart contracts can be introduced. Smart contracts can automatically reward bug hunters when specific conditions are met, creating a transparent and secure environment that enhances the security of the platform by leveraging a decentralized framework. These contracts are immutable and transparent, performing predefined actions without the need for manual intervention once the conditions are satisfied. Algorithm 1 presents the blockchain smart contract system that demonstrates how smart contracts can perform actions and call functions:

Algorithm 1 Blockchain-Based Smart Contracts Working Algorithm

```

1: Initialization:
2: Define a state variable bugStatus to store the status of the reported bug.
3: Initialize an event BugReported(status) to log when a bug is reported.
4: Initialize an event RewardIssued(hunter) to log when a reward is issued.
5: Define a mapping rewards to keep track of reward balances for different addresses.
6:
7: procedure REPORTBUG(status)
8:   Validate the input status: it must be either 0 (unverified) or 1 (verified).
9:   if status is valid then
10:     Update bugStatus to the new status.
11:     Emit the BugReported event with the new status.
12:   else
13:     Revert the transaction with the message "Invalid status value".
14:   end if
15: end procedure
16:
17: procedure REWARDBUGHUNTER
18:   Check if bugStatus is equal to 1 (bug is verified).
19:   if bugStatus is 1 then
20:     Increment the reward balance for the caller (msg.sender) by 1.
21:     Emit the RewardIssued event for the caller.
22:   else
23:     Revert the transaction with the message "Bug has not been validated".
24:   end if
25: end procedure
26:
27: function GETREWARDBALANCE(hunter)
28:   return the reward balance for the specified hunter.
29: end function
30:
31: procedure WITHDRAWREWARD
32:   Retrieve the reward balance for the caller (msg.sender).
33:   if reward balance is greater than 0 then
34:     Reset the caller's reward balance to 0.
35:     Transfer the reward (in Ether) to the caller.
36:   else
37:     Revert the transaction with the message "No rewards available".
38:   end if
39: end procedure
40:
41: procedure RECEIVEETHER
42:   Allow the contract to accept Ether transfers.
43: end procedure

```

The pseudo-code for Algorithm 1 defines a blockchain-based bounty reward system using smart contracts. It includes functions for reporting bugs (ReportBug), checking their status (GetBugStatus), and rewarding users who verify bugs (RewardBugHunter). The ReportBug function updates the bugStatus, while GetBugStatus provides transparency by returning the current status. The RewardBugHunter function checks if the bug is verified (bugStatus is 1) and rewards the user by updating their balance. Users can view (GetRewardBalance) and withdraw (WithdrawReward) their rewards securely. The system utilizes smart contracts for automated, decentralized reward management, ensuring secure transactions [87]. This mechanism is akin to the SmartRetro system, which also leverages blockchain to assess vulnerabilities and distribute rewards transparently [84,88]. The Hydra framework is also an excellent example of smart contracts as it enables detection

of vulnerabilities at a very low cost ensuring honest detection of vulnerabilities with less self-profit. The framework detects at run time by running the programs several times at once to detect security issues overall [89].

9. Conclusions and Future Work

Bug bounty programs play a pivotal role in enhancing cybersecurity, network security, and privacy. By identifying and addressing software vulnerabilities, they provide a cost-effective and innovative solution to the ever-evolving landscape of cyber threats. This paper serves as a guide for newcomers in the field of cybersecurity or bug bounty hunting, providing a detailed review of the best platforms available to kick-start their bug-hunting journey. Bug hunters having difficulty choosing a single platform to test their skills can refer to this paper and choose a platform that aligns with their interests and needs. This paper provided an in-depth analysis of both platform-based and company-based bug bounty programs. It explored the unique challenges and opportunities inherent in each, offering a comparative analysis. The study identified several challenges and proposed solutions to address them. Each platform and company-provided bug bounty program offers unique benefits and drawbacks. Platform-based programs manage bug bounty programs efficiently, providing an effective communication pathway, secure and transparent monetary rewards, and a defined scope of testing. They also utilize AI algorithms to handle bug bounty programs effectively. On the other hand, company-based programs may lack clear scope and have limitations, leading to potential legal issues. Based on this analysis, platform-based programs offer a better way to protect against out-of-scope testing, with their advanced AI algorithms making them more adept at managing bug bounty programs.

In analyzing company-based programs, such as the Google vulnerability reward program, GitHub bounty program, Microsoft program, Facebook bug bounty program, and the Apple bounty program, we found that these programs are not beginner-friendly. They lack proper communication channels, leading to frustration and demotivation among bug hunters. Among the programs compared, HackerOne emerged as a notable option due to its exceptional ability to overcome challenges and its extensive public reward programs. It is not only beneficial for organizations but also provides a platform for beginner enthusiasts to improve their skills. HackerOne stands out for its exceptional management in terms of submission handling and its transparent reward system. Simultaneously, Synack is recognized for its remarkably rapid response time and bounty payouts. However, it is less accessible to a broader audience due to its focus on experienced professionals. Some state-sponsored or government-funded programs remain anonymous and less transparent. Unfortunately, sufficient data were not available to include this crucial aspect in the current study due to the confidentiality of platforms and programs.

Future Research Directions

In the future, we aim to enhance our research by providing a more comprehensive comparison of bug bounty platforms and adding more platforms to the list for automated feature comparison through practical bounty hunting. We also plan to conduct surveys to gather opinions from experienced ethical hackers and bug hunters, which will help us gather the most accurate information for comparison. Additionally, future research could explore the impact of transparent bug-hunting policies and resource sharing among sectors.

Bug bounty programs face various challenges, including the inability of some platforms to handle a large number of vulnerabilities and the need for a prioritization system to address them effectively. Security teams must also perform penetration testing themselves to understand what to expect during these programs. Another challenge is lack of engagement from the hacker community, which can be due to low financial compensation for reporting bugs. It is essential to find an average cost of bounties and adjust our program accordingly.

Effective communication is also crucial to avoid misinterpretation or misunderstanding. Providing an easy and user-friendly way for bounty hunters to communicate with

the platform is necessary. Furthermore, there are regulatory issues that need to be addressed. For instance, healthcare data must adhere to regulatory compliance, such as HIPAA. Therefore, it is necessary to develop a system that ensures zero-trust blocks follow these regulations. Finally, research on motivation structures could be conducted to determine the optimal reward amount to attract top-notch bounty hunters who can identify vulnerabilities in critical blockchain structures.

Finally, future research can extend the scope of our study by exploring the application of bug bounty programs in other domains, such as healthcare and finance, where data security and privacy are critical concerns. The study can also be extended to the ZeroTrustBlock framework which leverages blockchain technology to provide a decentralized, secure, and private platform for managing health data, addressing limitations in current healthcare information systems. A comparative analysis of bug bounty programs in different industries can identify best practices, challenges, and potential solutions. Additionally, investigating the role of artificial intelligence and machine learning in enhancing bug bounty programs can improve their effectiveness and efficiency.

Author Contributions: Methodology, Z.S. and H.Z.; Supervision, Z.M.; Validation, B.S. and Z.S.; Visualization, B.S.; Writing—original draft, J.A. and M.T.; Writing—review and editing, Z.M. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Data is contained within the article.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Security Intelligence. Are Bug Bounty Programs Worth It? 2024. Available online: <https://securityintelligence.com/articles/are-bug-bounty-programs-worth-it/> (accessed on 2 March 2024).
2. Feng, N.; Zhou, T.; Feng, H.; Li, M. Optimal Launch Timing of Bug Bounty Programs for Software Products under Different Licensing Models. *J. Assoc. Inf. Syst.* **2024**, *25*, 239–266. [CrossRef]
3. Walshe, T.; Simpson, A. An empirical study of bug bounty programs. In Proceedings of the 2020 IEEE 2nd International Workshop on Intelligent Bug Fixing (IBF), London, ON, Canada, 18 February 2020; pp. 35–44.
4. Sinha, S. *Bug Bounty Hunting for Web Security*; Springer: Berlin/Heidelberg, Germany, 2019.
5. Tianlu, Z.; Ma, D.; Nan, F. The Use of Bug Bounty Programs for Software Reliability Improvement 2023. Available online: <https://aisel.aisnet.org/pacis2023/99> (accessed on 25 April 2024).
6. Tan, A. GovTech launches Vulnerability Rewards Programme: Computer Weekly. 2021. Available online: <https://www.computerweekly.com/news/252506024/GovTech-launches-vulnerability-rewards-programme> (accessed on 27 April 2024).
7. Chatfield, A.T.; Reddick, C.G. Cybersecurity Innovation in Government: A Case Study of U.S. Pentagon’s Vulnerability Reward Program. In Proceedings of the 18th Annual International Conference on Digital Government Research, DG.O’17, New York, NY, USA, 7–9 June 2017; pp. 64–73. [CrossRef]
8. Pentagon Launches the Feds’ First ‘Bug Bounty’ for Hackers. Available online: <https://www.wired.com/2016/03/pentagon-launches-feds-first-bug-bounty-hackers/> (accessed on 27 April 2024).
9. Department of Defense Expands ‘Hack the Pentagon’ Crowdsourced Digital Defense Program. Available online: <https://www.defense.gov/News/Releases/Release/Article/1671231/departments-of-defense-expands-hack-the-pentagon-crowdsourced-digital-defense-pr/> (accessed on 28 April 2024).
10. Hack-the-Pentagon. Available online: <https://www.hackerone.com/hack-the-pentagon> (accessed on 29 April 2024).
11. Zheng, Z.; Xie, S.; Dai, H.N.; Chen, X.; Wang, H. Blockchain challenges and opportunities: A survey. *Int. J. Web Grid Serv.* **2018**, *14*, 352–375. [CrossRef]
12. Thantharate, P.; Thantharate, A. ZeroTrustBlock: Enhancing Security, Privacy, and Interoperability of Sensitive Data through ZeroTrust Permissioned Blockchain. *Big Data Cogn. Comput.* **2023**, *7*, 165. [CrossRef]
13. Yli-Huumo, J.; Ko, D.; Choi, S.; Park, S.; Smolander, K. Where is current research on blockchain technology?—A systematic review. *PLoS ONE* **2016**, *11*, e0163477. [CrossRef] [PubMed]
14. Moosavi, N.; Taherdoost, H. Blockchain Technology Application in Security: A Systematic Review. *Blockchains* **2023**, *1*, 58–72. [CrossRef]
15. Malinka, K.; Firc, A.; Loutocky, P.; Vostoupal, J.; Křištofik, A.; Kasl, F. Using Real-world Bug Bounty Programs in Secure Coding Course: Experience Report. *arXiv* **2024**, arXiv:2404.12043.
16. Magalhães, J.P. Bug Bounties: Ethical and Legal Aspects. In *Legal Developments on Cybersecurity and Related Fields*; Springer: Berlin/Heidelberg, Germany, 2024; pp. 235–250.

17. Gersbach, H.; Pitsuwan, F.; Blieske, P. Artificial Bugs for Crowdsearch. *arXiv* **2024**, arXiv:2403.09484.
18. Wachter, J. Bug-Bounty Teams Contests. Available online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4695808 (accessed on 1 May 2024).
19. Akgul, O.; Eghtesad, T.; Elazari, A.; Gnawali, O.; Grossklags, J.; Mazurek, M.L.; Votipka, D.; Laszka, A. Bug {Hunters'} Perspectives on the Challenges and Benefits of the Bug Bounty Ecosystem. In Proceedings of the 32nd USENIX Security Symposium (USENIX Security 23), Anaheim, CA, USA, 9–11 August 2023; pp. 2275–2291.
20. Maulani, I.E.; Anggraeni, R. Bug Bounty Hunting: A Case Study of Successful Vulnerability Discovery and Disclosure. *Devotion J. Res. Community Serv.* **2023**, *4*, 1735–1740. [\[CrossRef\]](#)
21. Atefi, S.; Sivagnanam, A.; Ayman, A.; Grossklags, J.; Laszka, A. The Benefits of Vulnerability Discovery and Bug Bounty Programs: Case Studies of Chromium and Firefox. In Proceedings of the ACM Web Conference 2023, WWW '23, Austin, TX, USA, 30 April–4 May 2023; pp. 2209–2219. [\[CrossRef\]](#)
22. Melo, A.R.A. State of Web3 Security: Analysis of Vulnerabilities in Bug Bounty Reports. Master's Thesis, Polytechnic Institute of Viana do Castelo, Viana do Castelo, Portugal, 2023.
23. Canidio, A.; Costa, G.; Galletta, L. VeriOSS: Using the blockchain to foster bug bounty programs. *Open Access Ser. Inform.* **2021**, *82*, 1–14.
24. Shafigh, S.; Benatallah, B.; Rodríguez, C.; Al-Banna, M. Why some bug-bounty vulnerability reports are invalid? Study of bug-bounty reports and developing an out-of-scope taxonomy model. In Proceedings of the 15th ACM/IEEE International Symposium on Empirical Software Engineering and Measurement (ESEM), Bari, Italy, 11–15 October 2021; pp. 1–6.
25. Sivagnanam, A.; Atefi, S.; Ayman, A.; Grossklags, J.; Laszka, A. On the benefits of bug bounty programs: A study of chromium vulnerabilities. In Proceedings of the Workshop on the Economics of Information Security (WEIS), Online, 28–29 June 2021; Volume 10.
26. Zhao, M.; Grossklags, J.; Liu, P. An empirical study of web vulnerability discovery ecosystems. In Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, Denver, CO, USA, 12–16 October 2015; pp. 1105–1117.
27. Bhushan, A.; Billa, V.; Sonkar, M.; Chavan, V. The Dynamics of a Bug Bounty Platform. In Proceedings of the 2022 5th International Conference on Advances in Science and Technology (ICAST), Mumbai, India, 2–3 December 2022; pp. 399–405. [\[CrossRef\]](#)
28. Akgul, O.; Eghtesad, T.; Elazari, A.; Gnawali, O.; Grossklags, J.; Votipka, D.; Laszka, A. The hackers' viewpoint: Exploring challenges and benefits of bug-bounty programs. In Proceedings of the 2020 Workshop on Security Information Workers, ser. WSIW 2020, Santa Clara, CA, USA, 11 August 2020; Volume 20.
29. Bukangwa, A.; Uehara, T. An Agent-Based Modeling Approach to Designing and Optimizing Bug Bounty Programs for Cybersecurity in Developing Countries. In Proceedings of the 2023 IEEE 23rd International Conference on Software Quality, Reliability, and Security Companion (QRS-C), Chiang Mai, Thailand, 22–26 October 2023.
30. Wachs, J. Making markets for information security: The role of online platforms in bug bounty programs. *arXiv* **2022**, arXiv:2204.06905.
31. Sridhar, K.; Ng, M. Hacking for good: Leveraging HackerOne data to develop an economic model of Bug Bounties. *J. Cybersecur.* **2021**, *7*, tyab007. [\[CrossRef\]](#)
32. Kriptomat. A Brief History of Blockchain Technology That Everyone Should Read. Available online: <https://kriptomat.io/blockchain/history-of-blockchain/> (accessed on 17 March 2024).
33. Geekforgeeks. Consensus Algorithms in Blockchain. Available online: <https://www.geeksforgeeks.org/consensus-algorithms-in-blockchain/> (accessed on 10 February 2024).
34. Investopedia. 51% Attack: Definition, Who Is At Risk, Example, and Cost. Available online: <https://www.investopedia.com/terms/1/51-attack.asp> (accessed on 15 March 2024).
35. Wikipedia. Sybil Attack. Available online: https://en.wikipedia.org/wiki/Sybil_attack (accessed on 30 March 2024).
36. Golden. Nothing-at-Stake Problem. Available online: https://golden.com/wiki/Nothing-at-stake_problem-639PVZA (accessed on 2 March 2024).
37. Alkhalifah, A.; Ng, A.; Watters, P.A.; Kayes, A. A mechanism to detect and prevent Ethereum blockchain smart contract reentrancy attacks. *Front. Comput. Sci.* **2021**, *3*, 598780. [\[CrossRef\]](#)
38. Alaba, F.A.; Sulaimon, H.A.; Marisa, M.I.; Najeem, O. Smart Contracts Security Application and Challenges: A Review. *Cloud Comput. Data Sci.* **2024**, *5*, 15–41.
39. Cointelegraph. DDoS Attacks in Blockchain Networks. Available online: <https://cointelegraph.com/explained/ddos-attacks-in-blockchain-networks-explained> (accessed on 23 May 2024).
40. Apostolaki, M.; Zohar, A.; Vanbever, L. Hijacking Bitcoin: Routing Attacks on Cryptocurrencies. In Proceedings of the 2017 IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA, 22–26 May 2017; pp. 375–392. [\[CrossRef\]](#)
41. Heilman, E.; Kendler, A.; Zohar, A.; Goldberg, S. Eclipse Attacks on Bitcoin's Peer-to-Peer Network. In Proceedings of the 24th USENIX Security Symposium (USENIX Security 15), Washington, DC, USA, 12–14 August 2015; pp. 129–144.
42. Fiaz, F.; Sajjad, S.M.; Iqbal, Z.; Yousaf, M.; Muhammad, Z. MetaSSI: A Framework for Personal Data Protection, Enhanced Cybersecurity and Privacy in Metaverse Virtual Reality Platforms. *Future Internet* **2024**, *16*, 176. [\[CrossRef\]](#)
43. Avellaneda, O.; Bachmann, A.; Barbir, A.; Brennan, J.; Dingle, P.; Duffy, K.H.; Maler, E.; Reed, D.; Sporny, M. Decentralized Identity: Where Did It Come From and Where Is It Going? *IEEE Commun. Stand. Mag.* **2019**, *3*, 10–13. [\[CrossRef\]](#)
44. Casino, F.; Dasaklis, T.K.; Patsakis, C. A systematic literature review of blockchain-based applications: Current status, classification and open issues. *Telemat. Inform.* **2019**, *36*, 55–81. [\[CrossRef\]](#)

45. Wu, S.; Aaltonen, A.; Thatcher, J.B. Are Bug Bounty Programs Equally Beneficial to All Companies? An Empirical Analysis of Cybersecurity and Crowdsourcing. 2022. Available online: https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1082&context=treos_icis2022 (accessed on 21 May 2024).
46. 2021 Annual Hacker Report HackerOne. Available online: <https://www.hackerone.com/sites/default/files/2021-03/the-2021-hacker-report.pdf> (accessed on 15 Jan 2024).
47. HackerOne. HackerOne. 2024. Available online: <https://www.brighttalk.com/channel/13109/> (accessed on 25 May 2024).
48. Bugcrowd Official Site. Available online: <https://www.bugcrowd.com/> (accessed on 4 January 2024).
49. Bugcrowd. Inside the Platform: Bugcrowd's Vulnerability Trends Report. 2024. Available online: <https://www.bugcrowd.com/blog/inside-the-platform-bugcrowds-vulnerability-trends-report/> (accessed on 22 May 2024).
50. Bugcrowd. Inside the Platform: Bugcrowd's Vulnerability Disclosure. 2024. Available online: <https://www.bugcrowd.com/products/vulnerability-disclosure/> (accessed on 17 February 2024).
51. Synack. Synack inside the Company/Platform. 2024. Available online: <https://www.synack.com/about/> (accessed on 19 May 2024).
52. Synack Official Site. Available online: <https://www.synack.com/> (accessed on 4 January 2024).
53. Synack. The Synack Red Team. 2024. Available online: <https://www.synack.com/red-team/> (accessed on 5 May 2024).
54. Cobalt Official Site. Available online: <https://www.cobalt.io/> (accessed on 4 January 2024).
55. Cobalt. Cobalt Inside the Company. 2024. Available online: <https://www.cobalt.io/about> (accessed on 13 March 2024).
56. Cobalt. Cobalt Pentest Pricing. 2024. Available online: <https://www.cobalt.io/pentest-pricing> (accessed on 19 March 2024).
57. Cobalt. Cobalt Quality Control and Response Rate/Time. 2024. Available online: <https://www.cobalt.io/blog/new-features-quality-control-and-response-rate-time> (accessed on 23 March 2024).
58. Zerocopter Official Site. Available online: <https://www.zerocopter.com/> (accessed on 4 January 2024).
59. Zerocopter. Zerocopter Inside the Company. 2024. Available online: <https://www.zerocopter.com/about/our-story> (accessed on 15 February 2024).
60. Zerocopter. Zerocopter Bug Bounty. 2024. Available online: <https://www.zerocopter.com/products/bb> (accessed on 2 February 2024).
61. Facebook. Meta Bug Bounty Program. 2024. Available online: https://web.facebook.com/whitehat?_rdc=1&_rdr (accessed on 4 May 2024).
62. Microsoft. Microsoft Bug Bounty Program. 2024. Available online: <https://www.microsoft.com/en-us/msrc/bounty> (accessed on 15 March 2024).
63. Bughunters. Google Vulnerability Reward Program (VRP). 2024. Available online: <https://bughunters.google.com/> (accessed on 13 March 2024).
64. Apple. Apple Security Bounty. 2024. Available online: <https://security.apple.com/bounty/> (accessed on 7 May 2024).
65. Github. GitHub Bug Bounty. 2024. Available online: <https://bounty.github.com/> (accessed on 7 May 2024).
66. Sosnowski, K.; Sepczuk, M. SURE: A smart failover blockchain-based solution for the recycling reuse process. *Electronics* **2023**, *12*, 2201. [CrossRef]
67. HackerOne Official Site. Available online: <https://www.hackerone.com/> (accessed on 4 January 2024).
68. Huang, C.; Liu, J.; Fang, Y.; Zuo, Z. A study on Web security incidents in China by analyzing vulnerability disclosure platforms. *Comput. Secur.* **2016**, *58*, 47–62. [CrossRef]
69. HackerOne Vulnerability Management. Available online: <https://www.hackerone.com/solutions/vulnerability-management-system> (accessed on 14 January 2024).
70. Kannan, K.; Telang, R. Market for software vulnerabilities? Think again. *Manag. Sci.* **2005**, *51*, 726–740. [CrossRef]
71. The Problem with Limited Scope. Blog. Available online: <https://www.bugcrowd.com/blog/the-impact-of-limited-scope/> (accessed on 4 March 2024).
72. Boholm, Å. Lessons of success and failure: Practicing risk communication at government agencies. *Saf. Sci.* **2019**, *118*, 158–167. [CrossRef]
73. Finifter, M.; Akhawe, D.; Wagner, D. An empirical study of vulnerability rewards programs. In Proceedings of the 22nd USENIX Security Symposium (USENIX Security 13), Washington, DC, USA, 14–16 August 2013; pp. 273–288.
74. Hackerone. Common Mistakes When Running a Bug Bounty Program. 2024. Available online: <https://www.hackerone.com/vulnerability-management/common-bug-bounty-program-mistakes> (accessed on 2 May 2024).
75. Munjal, M.N. Ethical hacking: An impact on society. *Cyber Times Int. J. Technol. Manag.* **2014**, *7*, 922–931.
76. Walshe, T.; Simpson, A. A longitudinal study of hacker behavior. In Proceedings of the 37th ACM/SIGAPP Symposium on Applied Computing, Brno, Czech Republic, 25–29 April 2022; pp. 1465–1474.
77. Martin, R.; Christey, S.; Baker, D.; Corporation, M. *The Common Vulnerabilities and Exposures (CVE) Initiative*; Tehnical Report AD1125343; MITRE Corporation: Bedford, MA, USA, 2002.
78. What Is A CVE Vulnerability And Why Are They Important? Available online: <https://www.roboshadow.com/blog/what-are-cve-vulnerabilites> (accessed on 13 March 2024).
79. Luna, D.; Allodi, L.; Cremonini, M. Productivity and patterns of activity in bug bounty programs: Analysis of HackerOne and Google vulnerability research. In Proceedings of the 14th International Conference on Availability, Reliability and Security, Canterbury, UK, 26–29 August 2019; pp. 1–10.

80. Thackray, H. Hackers Gonna Hack: Investigating the Effect of Group Processes and Social Identities within Online Hacking Communities. Ph.D. Thesis, Bournemouth University, Poole, UK, 2019.
81. What to Do When Stuck Bug Hunting or, Some Ideas to Get Out of That Rut. Available online: <https://medium.com/@vuk.ivanovic9000/what-to-do-when-stuck-bug-hunting-5aad9759f697> (accessed on 14 May 2024).
82. Votipka, D.; Stevens, R.; Redmiles, E.; Hu, J.; Mazurek, M. Hackers vs. testers: A comparison of software vulnerability discovery processes. In Proceedings of the 2018 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 20–24 May 2018; pp. 374–391.
83. Hackerone. Hai: The AI Assistant for Vulnerability Intelligence. 2024. Available online: <https://www.hackerone.com/ai/hai-ai-assistant-vulnerability-intelligence> (accessed on 29 March 2024).
84. Wu, B.; Li, Q.; Xu, K.; Li, R.; Liu, Z. Smartretro: Blockchain-based incentives for distributed iot retrospective detection. In Proceedings of the 2018 IEEE 15th International Conference on Mobile Ad Hoc and Sensor Systems (MASS), Chengdu, China, 9–12 October 2018; pp. 308–316.
85. Lee, S.R.; Heo, M.J.; Lee, C.G.; Kim, M.; Jeong, G. Applying deep learning based automatic bug triager to industrial projects. In Proceedings of the 2017 11th Joint Meeting on Foundations of Software Engineering, Paderborn, Germany, 4–8 September 2017; pp. 926–931.
86. Harzevili, N.S.; Belle, A.B.; Wang, J.; Wang, S.; Ming, Z.; Nagappan, N.; et al. A Survey on Automated Software Vulnerability Detection Using Machine Learning and Deep Learning. *arXiv* **2023**, arXiv:2306.11673.
87. Gao, Z.; Xu, L.; Chen, L.; Shah, N.; Lu, Y.; Shi, W. Scalable blockchain based smart contract execution. In Proceedings of the 2017 IEEE 23rd International Conference on Parallel and Distributed Systems (ICPADS), Shenzhen, China, 15–17 December 2017; pp. 352–359.
88. Agrawal, T.K.; Angelis, J.; Khilji, W.A.; Kalaiarasan, R.; Wiktorsson, M. Demonstration of a blockchain-based framework using smart contracts for supply chain collaboration. *Int. J. Prod. Res.* **2023**, *61*, 1497–1516. [[CrossRef](#)]
89. Singh, A.; Parizi, R.M.; Zhang, Q.; Choo, K.K.R.; Dehghantanha, A. Blockchain smart contracts formalization: Approaches and challenges to address vulnerabilities. *Comput. Secur.* **2020**, *88*, 101654. [[CrossRef](#)]

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.