ChainBounty:

A Decentralized Cryptocurrency Crime Bounty Platform

Table of contents

1. Overview

A New Financial Paradigm in the Digital Age: Challenges of Virtual Assets and Web3

Virtual assets have fundamentally transformed the financial paradigm in the digital age. This revolutionary technology has brought significant changes to the financial industry through decentralized systems, and the advancement of Web3 has further accelerated the evolution of virtual assets and blockchain technology. Web3 offers a decentralized internet environment, providing users with autonomy and transparency, but the technological advancements also come with increased risks of cybercrime.

The inherent characteristics of decentralized systems mean the absence of central governing bodies, shifting the security responsibilities onto individuals and businesses. Consequently, cybercriminals exploit anonymity to attack virtual assets in increasingly sophisticated and bold ways. In such an environment, traditional centralized security models show limitations in effectively addressing evolving criminal behaviors.

To address these challenges, a new security paradigm is needed—one that is based on community collaboration and participation, creating an environment where both security experts and ordinary users can actively engage in cybersecurity and combat cybercrime.

To meet this need, Uppsala Security introduces ChainBounty, an innovative platform. ChainBounty is a decentralized bounty platform for virtual asset crimes utilizing Layer 2 technology, providing the global community with opportunities to actively participate in cybercrime prevention and response. Based on the principles of Web3, ChainBounty aims to maximize the advantages of decentralization and establish a transparent and efficient security system.

ChainBounty incentivizes users who provide information about cybercrimes through a decentralized bounty system, encouraging more participants to contribute to crime prevention and criminal tracking. Additionally, utilizing Layer 2 technology enables fast and efficient transaction processing, supporting rapid response and effective prevention of cybercrime. By leveraging the collective intelligence of the global Web3 community, ChainBounty seeks to build a robust and effective security system.

ChainBounty is expected to elevate the security level of the virtual asset market and make significant contributions to cybercrime prevention. By addressing the security issues of decentralized systems and presenting a new security paradigm, it will serve as a crucial foundation for the continued growth and development of the virtual asset market. As the virtual asset market evolves, so do cybercrimes. Uppsala Security’s ChainBounty offers new possibilities for effectively addressing cybercrime through global community collaboration in the Web3 era. ChainBounty will play a pivotal role in ensuring a safe and transparent virtual asset market.

2. Introduction

Innovation and Challenges in Virtual Assets: The Need for a New Security Paradigm

With the advent of the digital age, virtual assets have brought about revolutionary changes in the financial sector. The combination of decentralized systems and cutting-edge technology has redefined the financial industry's paradigm, with its potential and possibilities being widely recognized. However, these technological advancements also bring serious challenges.

The core characteristics of virtual assets, such as anonymity and decentralization, present attractive targets for cybercriminals. They exploit these features to threaten the virtual asset ecosystem with increasingly sophisticated and bold methods. Various forms of virtual asset crimes, including hacking, fraud, money laundering, and ransomware attacks, are occurring, and the scale of damage is rapidly expanding. Notably, criminals operate across borders based on anonymity, making it challenging for traditional centralized security systems to effectively address these global criminal networks. Jurisdictional constraints, resource shortages, and difficulties in rapid response highlight the fundamental limitations of centralized systems, posing critical weaknesses in the fight against virtual asset crime.

To resolve these issues, a new security paradigm is necessary. An approach utilizing the collective intelligence of decentralized communities can facilitate more rapid and comprehensive responses through global cooperation, overcoming the limitations of centralized systems.

In response to this need, ChainBounty has been designed as an innovative decentralized platform. ChainBounty provides a collaborative environment where global security experts, white hat hackers, and ordinary users can work together to address cybercrime, ensuring the safety of the virtual asset ecosystem and promoting healthy growth. ChainBounty's decentralized collaboration model offers a new solution to virtual asset crimes and plays a crucial role in enhancing the security of financial systems.

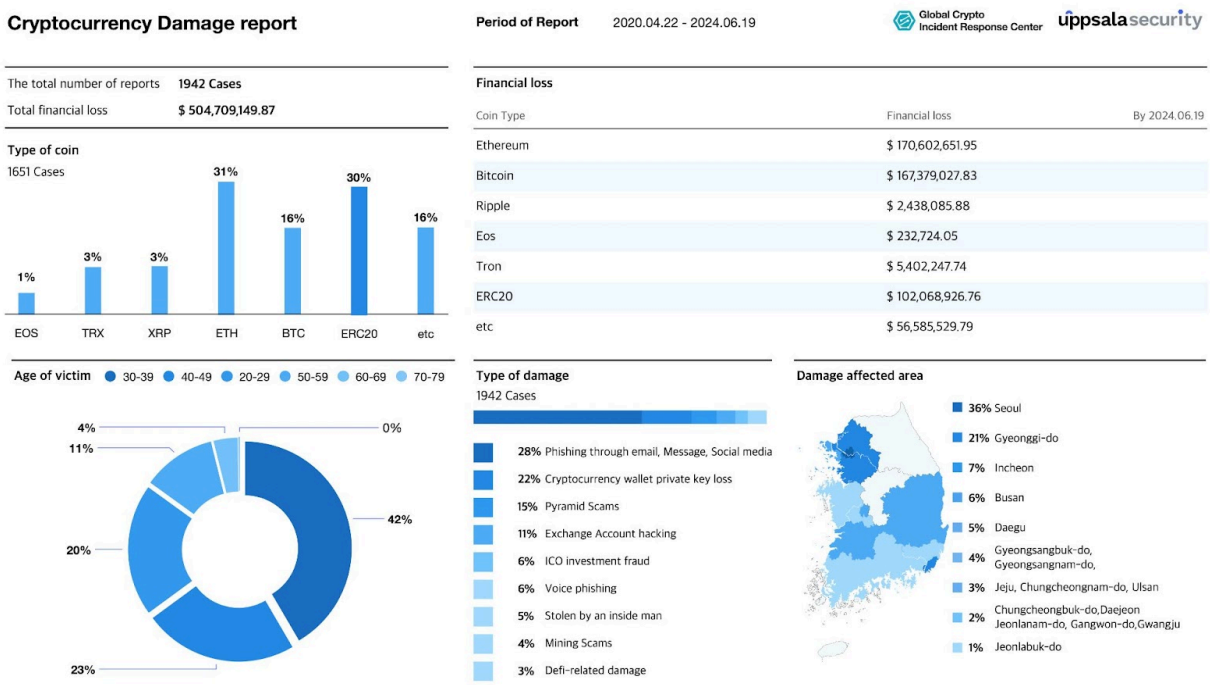
Going forward, we must solve the security problems of the virtual asset era and leverage the benefits of decentralization to build a safer and more transparent financial ecosystem. ChainBounty is expected to play a central role in this process.

3. Background and Legacy of Sentinel Protocol

Six Years of Achievements and Legacy: Sentinel Protocol and CIRC's Global Journey

In 2018, the rapid growth of the virtual asset market intensified the threats of cybercrime. Against this backdrop, Uppsala Security introduced the Sentinel Protocol, an innovative solution. Sentinel Protocol was the first threat detection platform based on collective intelligence, setting a significant milestone in the security field through a decentralized approach to addressing virtual asset crimes.

Over the past six years, Sentinel Protocol has provided practical support to thousands of victims of various forms of virtual asset crimes, including hacking, fraud, and money laundering. It has offered asset recovery opportunities to victims and provided threat intelligence to government agencies and businesses to strengthen their prevention and response capabilities. These achievements are the result of collaboration among global security experts, white hat hackers, and ordinary users, demonstrating that a decentralized collaboration model can overcome the limitations of centralized systems and offer a new paradigm in virtual asset security.



CIRC: A Trusted Guardian of the Korean Virtual Asset Market

In Korea, the Virtual Asset Reporting Center (CIRC), established in 2020, has played a crucial role in maximizing the effectiveness of the Sentinel Protocol. CIRC provides comprehensive services to victims of virtual asset crimes, including counseling, reporting, and asset recovery support.

Since April 2020, CIRC has assisted approximately 2,000 victims, with reported losses amounting to around 700 billion KRW. This figure highlights the severity of virtual asset crimes and underscores the importance of Uppsala Security and CIRC in reducing the damage caused by such crimes.

CIRC not only processes and handles reports but also provides legal advice and support to help victims recover their assets through legal procedures. It actively promotes security awareness through education and campaigns on virtual asset crime prevention.

ChainBounty: A Global Security Innovation

Uppsala Security now aims to further enhance the security level of the global virtual asset market through ChainBounty. ChainBounty is a decentralized bounty platform for virtual asset crimes that introduces a new global security model, enabling security experts, white hat hackers, and ordinary users worldwide to collaborate in addressing cybercrime.

ChainBounty offers rewards to those providing information about cybercrimes through its decentralized bounty system, creating opportunities for more people to participate in crime prevention and criminal tracking. Utilizing Layer 2 technology, ChainBounty improves transaction speed and efficiency, supporting effective prevention and response to cybercrime.

Building on the successful legacy of Sentinel Protocol, ChainBounty aims to advance its technology and global community collaboration to raise the security level of the virtual asset market. This platform will serve as a central component for the safe and sustainable growth of the virtual asset market, contributing to solving security issues.

ChainBounty's innovative approach will create a safer and more transparent environment for the global virtual asset ecosystem, extending beyond the Korean market. Uppsala Security and ChainBounty will play a pivotal role in fostering sustainable growth in the virtual asset market, effectively responding to evolving cybercrime, and collaborating with the global community to build a more secure and transparent virtual asset ecosystem.

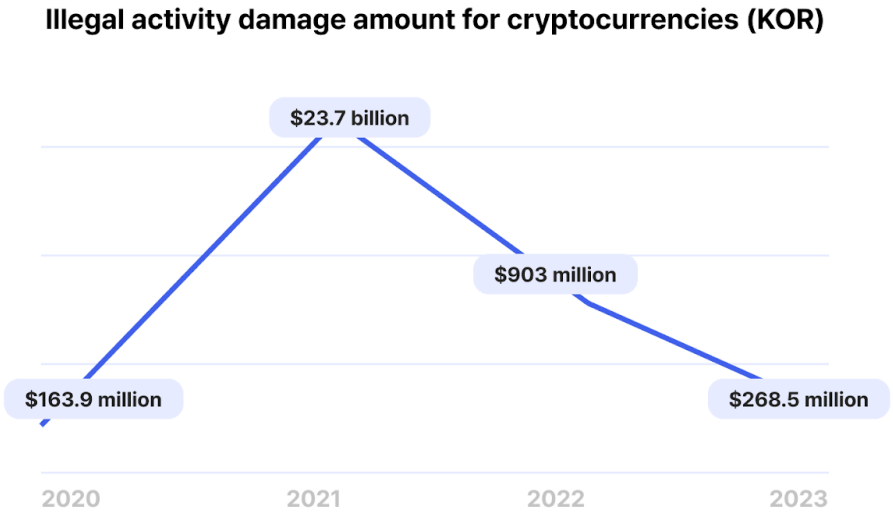
4. Increasing Threat Environment

Escalating Threats: The Increase in Virtual Asset Crimes and the Limitations of Existing Solutions

Surge in Crimes and Significant Economic Impact

From 2017 to 2021, Korea's virtual asset market experienced explosive growth, accompanied by a sharp increase in crimes targeting virtual assets. According to statistics from the National Police Agency in 2022, the total damage from virtual asset crimes during this period amounted to approximately 4.74 trillion KRW, with 12,157 victims. This clearly indicates that virtual assets have become major targets for crime, highlighting the increased risks in the virtual asset market.

Virtual asset crimes occur in various forms, including hacking, phishing, ransomware, and multi-level fraud, with the scale and scope of damage growing continuously. The decentralized nature and anonymity of virtual assets provide a favorable environment for criminals, complicating crime tracking and intensifying the suffering of victims. These crimes impede the healthy growth of the virtual asset market and create significant societal anxiety.



Limitations of Existing Solutions: Challenges in the Private and Public Sectors

Private Sector Limitations

Private companies, such as security firms like Uppsala Security, invest significant efforts in preventing virtual asset crimes. However, the complexity and extensive range of these crimes pose severe challenges. The decentralized nature and global network of virtual asset crimes make it too complex for a single company to address effectively. While innovative solutions like

Sentinel Protocol have achieved some success, the continuous evolution of crime methods and the expansion of criminal networks reveal their limitations. It is difficult for the private sector alone to effectively block such crimes.

Public Sector Constraints

Government agencies also face significant challenges in effectively addressing virtual asset crimes. The decentralized nature of virtual assets presents problems that traditional law enforcement methods cannot resolve. In particular, cross-border criminal activities expose the limitations of law enforcement agencies in tracking and responding to all crimes. Additionally, legal and regulatory systems struggling to keep up with the rapid pace of technological advancements fail to address new crime methods appropriately. This results in a lack of systematic response for crime prevention and victim recovery.

Need for New Solutions: Decentralized Collaboration Models

Given the severity of virtual asset crimes and the limitations of existing solutions, a new approach is required. An integrated and innovative environment where private companies, government agencies, and the global community collaborate to address crimes is essential. Utilizing collective intelligence to share and analyze threat information in real time and establishing rapid and effective response systems is critical.

Decentralized collaboration models offer a new breakthrough in the fight against virtual asset crimes. These models provide flexibility in responding to continuously evolving crime methods, effectively tracking global criminal networks, and protecting victims. Particularly, leveraging the collective intelligence of the global community can overcome the limitations of individual countries or companies, offering more comprehensive and effective solutions.

ChainBounty is designed to be a new solution to these problems. By creating a decentralized bounty platform that encourages global participation, ChainBounty leverages collective intelligence and collaborative efforts to address the challenges of virtual asset crimes.

5. The Necessity and Vision of ChainBounty

The Necessity of ChainBounty: Addressing the Security Gap

The virtual asset market, marked by rapid growth and increasing complexity, is grappling with persistent and evolving security threats. Traditional cybersecurity measures, while foundational, are proving inadequate against the sophisticated tactics employed by modern cybercriminals. To address these challenges effectively, a more dynamic and resilient approach is necessary. ChainBounty emerges as a critical innovation in this landscape, addressing several key issues.

1. The Growing Complexity of Cybercrime

Cybercrime in the realm of virtual assets is continually advancing. For instance, traditional phishing attacks have evolved from simple email scams to highly sophisticated spear-phishing campaigns targeting key personnel within organizations. Ransomware attacks, once confined to desktop environments, now threaten entire blockchain networks, demanding substantial ransoms paid in cryptocurrencies. Such developments highlight the inadequacy of conventional security measures, which often rely on static defense mechanisms.

ChainBounty counters these advanced threats by harnessing decentralized, collective intelligence. Through its platform, users from around the world can report suspicious activities and vulnerabilities. For example, if a new phishing scam targeting a popular cryptocurrency exchange emerges, ChainBounty allows users to report these threats in real-time. This collective vigilance enables a rapid, coordinated response, significantly enhancing the effectiveness of the security system.

2. The Limitations of Centralized Security Models

Centralized security models, which rely on a single point of control, have inherent vulnerabilities. A notable example is the 2020 Twitter hack, where attackers gained access to internal tools through compromised employee accounts. This breach underscores the risks associated with centralized control and highlights the limitations of traditional security approaches.

ChainBounty's decentralized framework addresses these vulnerabilities by distributing security responsibilities across a global network of participants. This decentralized model reduces the risk of a single point of failure. Instead of relying on a central authority, ChainBounty leverages the collective expertise of its network. For instance, if a vulnerability in a blockchain protocol is discovered, multiple independent validators within the ChainBounty network can verify and address the issue, making it much harder for malicious actors to exploit the system.

3. The Need for Community Engagement

Effective cybersecurity in the virtual asset space requires active community engagement. Traditional security measures often lack mechanisms for widespread participation. For instance, many bug bounty programs offer limited incentives and do not reach out to the broader community of security researchers and enthusiasts.

ChainBounty addresses this gap by creating a decentralized reward system that incentivizes global participation. Consider the case of a newly discovered smart contract vulnerability. ChainBounty enables users to report this vulnerability and receive rewards based on the severity and impact of their findings. This decentralized approach not only encourages more individuals to participate but also taps into a diverse pool of knowledge and expertise, enhancing the overall effectiveness of the security network.

4. The Expansion of Threat Environments

The expansion of threat environments necessitates security solutions that can adapt swiftly. For example, decentralized finance (DeFi) platforms are particularly susceptible to new types of attacks, such as flash loan exploits. These attacks leverage rapid, large-scale transactions to exploit vulnerabilities in smart contracts, demanding a responsive and scalable security solution.

ChainBounty's use of Layer 2 technologies provides a solution to this challenge. By processing transactions off the main blockchain and then consolidating them, ChainBounty can handle high volumes of data and respond to threats in real-time. This technological capability ensures that the platform can effectively manage and mitigate emerging threats, such as those targeting DeFi protocols.

The Vision of ChainBounty: Building a Safer Virtual Asset Ecosystem

ChainBounty's vision extends beyond merely addressing current security gaps; it aims to revolutionize the virtual asset ecosystem by fostering a more secure, transparent, and collaborative environment. This vision encompasses several key elements:

1. A Decentralized Crime Reporting and Reward Platform

ChainBounty introduces a decentralized platform where users can report virtual asset crimes and receive rewards. For instance, if an individual uncovers a new type of scam targeting cryptocurrency users, they can submit a report through ChainBounty's platform. The decentralized nature of this system ensures that reports are reviewed by a broad network of participants, enhancing the reliability and accuracy of the responses.

2. Collective Intelligence and Global Participation

ChainBounty harnesses the power of collective intelligence through global participation. For example, a complex scam involving multiple cryptocurrencies might require insights from experts in different areas. ChainBounty's platform facilitates collaboration among cybersecurity professionals, white-hat hackers, and everyday users, pooling their knowledge to address intricate security issues effectively.

3. Enhanced Speed and Efficiency through Layer 2 Technology

The implementation of Layer 2 technologies allows ChainBounty to process transactions quickly and efficiently. For instance, during a high-volume event like a major cryptocurrency exchange

hack, ChainBounty can utilize Layer 2 solutions to process and analyze data in real-time, ensuring a prompt and effective response to the incident.

4. Transparent and Fair Reward System

ChainBounty's reward system is designed to be transparent and fair, ensuring that contributors are compensated based on the impact and significance of their contributions. This transparent approach builds trust within the community and encourages more active participation. For example, a researcher who discovers a critical vulnerability in a widely used blockchain protocol would receive a substantial reward, reflecting the importance of their finding.

5. Building a Sustainable and Secure Ecosystem

Ultimately, ChainBounty aims to create a sustainable and secure virtual asset ecosystem. By addressing existing security gaps and fostering a collaborative, decentralized approach, ChainBounty contributes to the long-term stability and growth of the virtual asset market. This vision includes ongoing improvements to the platform and adapting to emerging threats, ensuring that the ecosystem remains resilient and secure.

In summary, ChainBounty represents a significant advancement in the field of cybersecurity for virtual assets. By combining decentralization, community engagement, and cutting-edge technology, ChainBounty offers a transformative solution to the challenges of cybercrime and plays a pivotal role in building a safer and more secure virtual asset ecosystem.

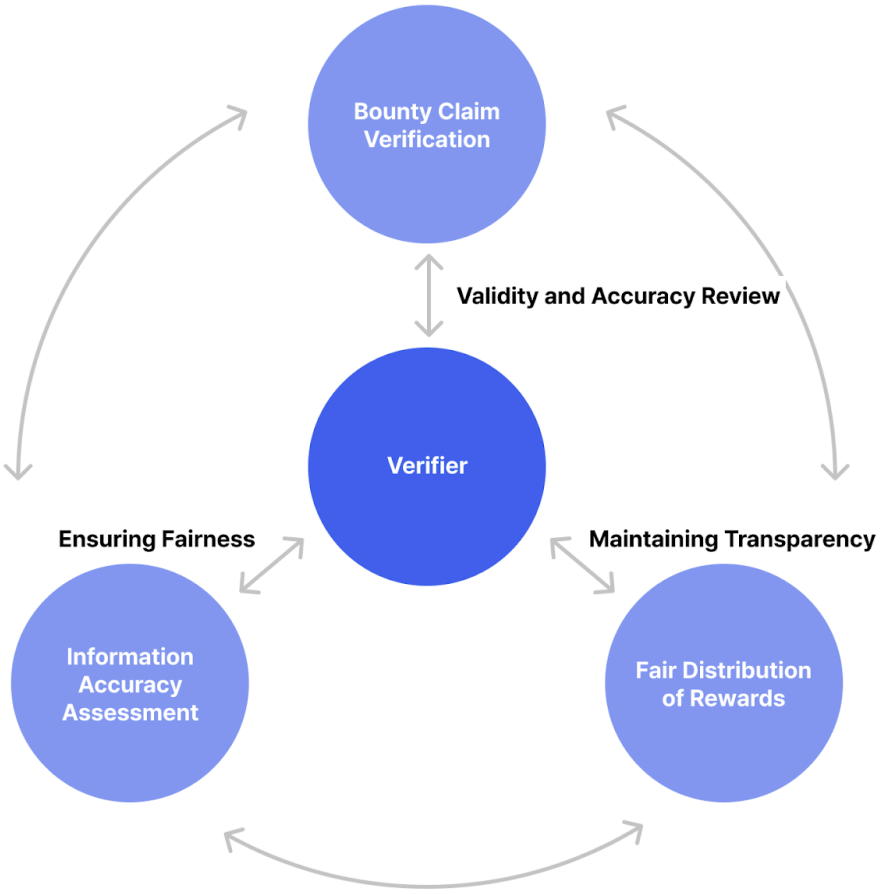
6. The Role of Validators in ChainBounty

The Importance of Validators in the ChainBounty Ecosystem

Validators in the ChainBounty ecosystem are crucial members responsible for maintaining the platform's stability and reliability. Their role extends beyond mere technical validation, leveraging extensive experience and exceptional technical expertise within the security industry. Validators ensure the transparency and fairness of the bounty process and play an essential role in enhancing ChainBounty's credibility.

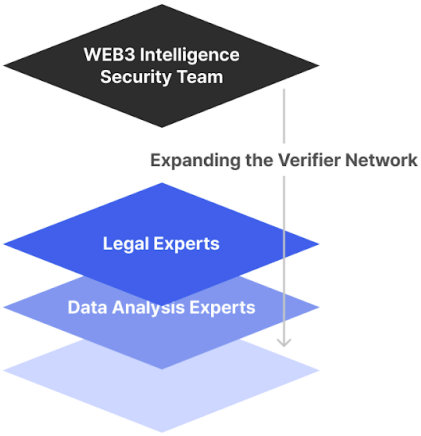
Key Roles of Validators

1. **Bounty Claim Verification**:
   Validators thoroughly review the validity and accuracy of submitted bounty claims. This process involves verifying the credibility of claims and preventing fraud or errors, thereby bolstering the platform's trustworthiness. Validators quickly and accurately assess the legitimacy of claims, effectively preventing unnecessary disputes.
2. **Accuracy of Information Assessment**:
   Validators evaluate the reliability and accuracy of submitted information to ensure the fairness of reward distribution. This helps guarantee fair transactions between information providers and beneficiaries, maintaining the system's transparency. Validators meticulously review the sources and accuracy of the information to ensure that rewards are distributed justly.
3. **Fair Reward Distribution**:
   Based on the verification results, validators distribute rewards fairly, motivating participants and enhancing the platform's sustainability. A fair reward system increases user trust and serves as a crucial factor in boosting platform engagement. Validators contribute to earning users' trust by maintaining transparency and fairness throughout the reward process.



Security Experts: The First Validator of ChainBounty, Symbolizing Trust and Safety

The first validator of ChainBounty, symbolizing trust and safety, is a leading security team in Web3. The team members, each with over 10 years of experience in Web2 and Web3 security, are expanding their expertise into the Web3 security business. They provide various intelligence data related to virtual assets in Web3 security services and play a critical role in strengthening the trust and safety of the ChainBounty platform. This involvement is expected to increase user trust in the ChainBounty platform and encourage greater participation. Additionally, their expertise and experience are vital in improving the security level of the ChainBounty platform by identifying and responding to potential vulnerabilities in advance. The team will be revealed when the validator operations begin.



Expanding the Validator Network: A Harmony of Diversity and Expertise

ChainBounty plans to secure additional validators with diverse backgrounds and expertise, including the Web3 specialist community. Each validator will contribute in their own field of expertise, further enhancing the security and efficiency of the platform.

- Legal experts will contribute to regulatory compliance and legal issue resolution.
- Data analytics specialists will be involved in analyzing crime patterns and developing predictive models.

By collaborating with validators who possess a wide range of expertise, ChainBounty can maintain high levels of security and transparency across the global virtual asset ecosystem. The expansion of the validator network reinforces ChainBounty’s core values of decentralization and collective intelligence, providing a robust foundation for the platform's continuous growth and development.

ChainBounty’s validators are not merely overseers but are key partners in safeguarding the platform’s security and trustworthiness. Their dedication and expertise will significantly contribute to fostering the healthy growth of the virtual asset market, creating an environment where users can engage with virtual assets with confidence and peace of mind.

7. ChainBounty's Technological Stack

ChainBounty's Technological Stack: Maximizing Scalability and Efficiency through Layer 2 Technology

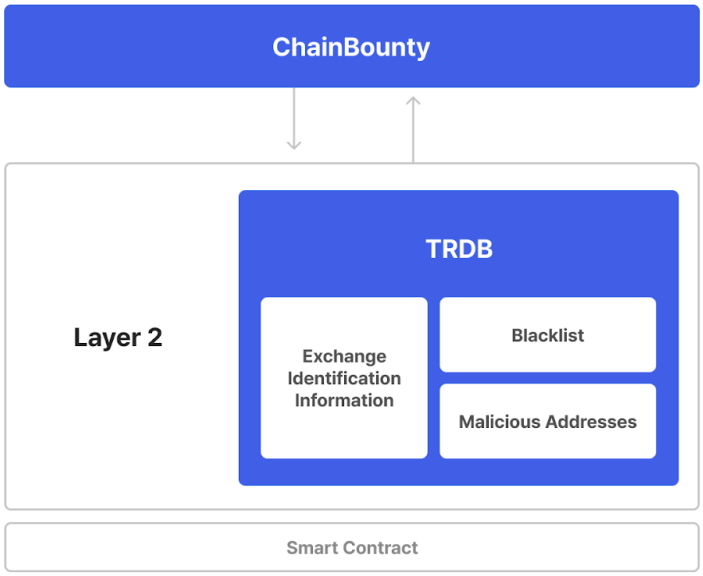
The Need for Layer 2: Overcoming the Limitations of Sentinel Protocol TRDB

The core asset of Sentinel Protocol, its Threat Reputation Database (TRDB), houses over 93 million pieces of data, including essential information for the security of the cryptocurrency ecosystem, such as exchange identification details, blacklists, and malicious addresses. However, managing and utilizing such a vast amount of data on the existing main blockchain network presents several challenges. High gas fees, slow processing speeds, and network congestion are major obstacles to effective data management and utilization.

To address these issues, ChainBounty adopts Layer 2 technology. Layer 2 is a scalability solution that allows for the efficient processing of large-scale data and transactions without overloading the main blockchain network. Through this technology, ChainBounty can expand the functionality of the Sentinel Protocol and dramatically enhance the speed and efficiency of data processing and interaction.

Benefits of Layer 2 for ChainBounty

1. **Improved Scalability:** ChainBounty employs a Layer 2 solution to efficiently handle large-scale transactions and data interactions. This solution processes most transactions off-chain, recording only the final results on the main blockchain network. This approach improves processing speed and reduces network congestion, enabling ChainBounty to handle more users and data, thereby supporting the platform's growth.
2. **Cost Reduction:** Layer 2 technology significantly reduces the high gas fees associated with storing and accessing large-scale data on the main chain. Since most transactions are processed off-chain, users can utilize the platform at lower costs, increasing accessibility and encouraging greater participation.
3. **Real-Time Data Processing:** For effective crime prevention and response, data must be processed and updated in real time. Layer 2 technology meets these real-time data processing requirements, allowing all participants to quickly access and utilize the latest information. This capability enables ChainBounty to respond swiftly to the rapidly changing landscape of cryptocurrency crime and protect its users effectively.



Efficient Data Storage and Transaction Management with Layer 2

1. **Data Stored Directly on Layer 2:** ChainBounty directly stores labeling information for over 100 million wallet addresses on the Layer 2 network. Each transaction includes specific labeling information, securely recorded on the Layer 2 blockchain. This method ensures data integrity and enhances the efficiency of data access and utilization.
2. **Transaction Generation:** Each wallet address and its corresponding label information are recorded as transactions on the Layer 2 network. This approach allows for the efficient management of large-scale data while maintaining the security features of the blockchain. The fast processing speed of Layer 2 enables real-time data updates.
3. **Integration with Smart Contracts:** Data stored on Layer 2 can be accessed through smart contracts. This capability allows various applications to utilize the data in real time and supports data-driven decision-making.

Efficient Data Access and Indexing: Fast and Accurate Information Retrieval

1. **Query via Smart Contracts:** Users can query specific data through smart contracts. For example, they can search for label information corresponding to a particular wallet address or specific types of threat information.
2. **Real-Time Synchronization:** Data stored on Layer 2 is continuously updated and synchronized, ensuring that all participants can quickly access and utilize the latest information. This feature allows ChainBounty to always provide the most up-to-date threat information, enabling users to proactively respond to criminal activities.

Through the adoption of Layer 2 technology, ChainBounty is leading innovation in the field of cryptocurrency security. By maximizing scalability, cost efficiency, and real-time data processing capabilities, the platform contributes to building a safer and more transparent cryptocurrency ecosystem.

8. Market Potential and Impact

The virtual asset market, encompassing cryptocurrencies, tokens, and blockchain-based assets, is experiencing unprecedented growth. This expansion is driven by increasing adoption across various sectors, including finance, technology, and entertainment. As more businesses and individuals engage with virtual assets, the market's total capitalization and user base continue to rise at an impressive rate. For instance, the total market capitalization of cryptocurrencies surged from under $200 billion in early 2020 to over $2 trillion by mid-2024. This explosive growth signifies not only the expanding value and importance of virtual assets but also the growing opportunities for cybercriminals targeting these assets.

In this rapidly evolving landscape, effective security solutions have become more critical than ever. Traditional security measures, while foundational, often fall short in addressing the sophisticated tactics employed by contemporary cybercriminals. ChainBounty emerges as a timely and essential solution, addressing the pressing need for enhanced security in the virtual asset ecosystem. The market potential for ChainBounty is substantial due to several factors:

1. Expansion of the Virtual Asset Market

The virtual asset market's rapid growth presents ChainBounty with significant opportunities. With more users and assets entering the market, there is an increasing demand for robust security solutions. ChainBounty's innovative approach to decentralized security positions it to capitalize on this expanding market. For example, as new cryptocurrencies and blockchain platforms emerge, they often face security challenges that ChainBounty is uniquely equipped to address.

2. Rising Cybercrime Threats

The increasing sophistication and frequency of cyberattacks in the virtual asset space underscore the urgent need for advanced security measures. High-profile incidents, such as the $600 million hack of the Poly Network in 2021, illustrate the vulnerabilities present in the current security landscape. ChainBounty’s decentralized model offers a proactive and adaptive solution, positioning itself as a valuable player in mitigating these threats. By leveraging a global network of participants to identify and respond to security issues, ChainBounty addresses the critical need for effective and scalable security solutions.

3. Global Reach and Scalability

ChainBounty’s global and decentralized framework allows it to scale effectively and adapt to diverse markets and regions. Unlike traditional security models that may be constrained by geographical or organizational limitations, ChainBounty operates across borders, engaging a wide range of participants. This global reach ensures that ChainBounty can address the complexities and varying security needs of different regions. For instance, ChainBounty’s ability to operate in emerging markets, where virtual asset adoption is rapidly increasing, enhances its potential for impact and growth.

Impact of ChainBounty

1. Enhanced Security for Virtual Assets

ChainBounty's impact on the virtual asset market is profound, contributing to a safer and more secure ecosystem. By leveraging decentralized collaboration and cutting-edge technology, ChainBounty improves the detection, prevention, and resolution of virtual asset crimes. For example, its decentralized platform allows users to report and address vulnerabilities in real-time, significantly enhancing the overall market security. This proactive approach helps to safeguard assets and protect users from emerging threats.

2. Empowering the Global Community

ChainBounty's decentralized model empowers individuals and organizations worldwide to actively participate in combating cybercrime. By creating a platform where users can contribute to security efforts and receive rewards for their contributions, ChainBounty fosters a sense of shared responsibility. This collaborative effort strengthens the collective defense against virtual asset threats, encouraging a more engaged and proactive global community.

3. Promoting Market Confidence

The successful implementation of ChainBounty has the potential to significantly boost confidence in the virtual asset market. Addressing security concerns and demonstrating a commitment to protecting users and assets can enhance market confidence. For example, as ChainBounty successfully mitigates high-profile security incidents, it reassures users and investors of the market's integrity. Increased confidence can drive further adoption and growth in the virtual asset space, benefiting the broader ecosystem.

4. Driving Innovation in Cybersecurity

ChainBounty represents a significant innovation in cybersecurity, setting a new standard for virtual asset security. Its decentralized and transparent model introduces a novel approach to addressing security challenges, influencing future developments in the industry. By demonstrating the effectiveness of its approach, ChainBounty encourages other players in the cybersecurity and virtual asset sectors to explore new and effective solutions. This drive for innovation fosters a more dynamic and resilient security landscape, ultimately benefiting the entire market.

In conclusion, ChainBounty's market potential and impact are significant. As the virtual asset market continues to expand and evolve, ChainBounty offers a crucial solution to the pressing security challenges facing the industry. Its innovative approach, global reach, and emphasis on community involvement position it as a transformative force in the virtual asset ecosystem. By enhancing security, empowering the global community, promoting market confidence, and driving innovation, ChainBounty is poised to play a pivotal role in shaping the future of virtual asset security.

9. Bounty Tokenomics

Token Supply and Inflation

The BOUNTY token economy of ChainBounty is based on the existing UPP token economy of Sentinel Protocol, adjusted to fit the new system. As outlined in the Sentinel Protocol whitepaper, a total of 500 million UPP tokens were issued, which were used as rewards for the platform's community and validators. ChainBounty introduces the new BOUNTY token based on this issuance and applies the following inflation plan**.**

Inflation Plan

- **Launch Date**: Inflation issuance begins in October 2024, coinciding with the testnet launch of ChainBounty. The official mainnet launch will take place at the end of December 2024.
- **Initial Inflation Rate:** The initial inflation rate is set at 7% in the first year.
- **Inflation Vesting Period:** There will be 20 vesting periods, with each vesting period lasting one year. This means the inflation rate spans over 20 years.
- Gradual Decrease: The inflation rate will decrease each year, reaching approximately 0.1% by the 20th year.

Yearly Expected Issuance

Year	Start Supply (BOUNTY)	Inflation Rate (%)	Inflation Amount (BOUNTY)	End Supply (BOUNTY)
Year 1 (2024 - 2025)	500000000	7.0	35000000.0	535000000
Year 2 (2025 - 2026)	535000000	6.6368	35506880.0	570506880
Year 3 (2026 - 2027)	570506880	6.2737	35791890.13	606298770
Year 4 (2027 - 2028)	606298770	5.9105	35835288.81	642134059
Year 5 (2028 - 2029)	642134059	5.5474	35621744.79	677755804
Year 6 (2029 - 2030)	677755804	5.1842	35136216.38	712892020
Year 7 (2030 - 2031)	712892020	4.8211	34369237.18	747261257
Year 8 (2031 - 2032)	747261257	4.4579	33312159.59	780573417
Year 9 (2032 - 2033)	780573417	4.0947	31962139.7	812535557
Year 10 (2033 - 2034)	812535557	3.7316	30320576.83	842856133
Year 11 (2034 - 2035)	842856133	3.3684	28390766.0	871246899
Year 12 (2035 - 2036)	871246899	3.0053	26183583.07	897430482
Year 13 (2036 - 2037)	897430482	2.6421	23711010.78	921141493
Year 14 (2037 - 2038)	921141493	2.2789	20991893.49	942133387
Year 15 (2038 - 2039)	942133387	1.9158	18049391.42	960182778
Year 16 (2039 - 2040)	960182778	1.5526	14907797.81	975090576
Year 17 (2040 - 2041)	975090576	1.1895	11598702.4	986689278
Year 18 (2041 - 2042)	986689278	0.8263	8153013.51	994842292
Year 19 (2042 - 2043)	994842292	0.4632	4608109.5	994842292
Year 20 (2043 - 2044)	999450401	0.1	999450.4	1000449852

- **October 2024 - September 2025**: In the first year after the mainnet launch, a 7% inflation rate is applied, adding **35,000,000 BOUNTY** tokens. The supply at the end of this period is **535,000,000 BOUNTY**.
- **October 2025 - September 2026**: In the second year, the inflation rate is **6.6368%**, adding **35,506,880 BOUNTY** tokens. The total supply at the end of this period is **570,506,880 BOUNTY**.

- **October 2026 - September 2027**: In the third year, the inflation rate decreases to **6.2737%**, adding **35,791,880.13 BOUNTY** tokens. The supply at the end of this period is **606,298,770 BOUNTY**.
- **October 2027 - September 2028**: In the fourth year, the inflation rate is set at **5.9105%**, adding **35,853,528.81 BOUNTY** tokens. The supply at the end of this period is **642,134,059 BOUNTY**.
- **October 2028 - September 2029**: In the fifth year, the inflation rate decreases to **5.5474%**, adding **35,621,744.79 BOUNTY** tokens. The supply at the end of this period is **677,755,804 BOUNTY**.

In this way, the inflation rate gradually decreases each year, reaching approximately 0.1% by the 20th year. This plan is designed to ensure the long-term stability and sustainability of the BOUNTY token economy of ChainBounty.

Token Usage Plan

The BOUNTY tokens issued during the first three months from October to December 2024 will primarily be used for platform development. The ChainBounty platform will be publicly launched in December 2024, following the completion of Layer 2 technology development. From January 2025 onwards, the issued BOUNTY tokens will be used for validators and bounty programs. Essentially, 50% of the issued tokens will be reserved for community bounties, while the remaining 50% will be allocated to validators.

Inflation Details

- Launch Date: Inflation issuance begins in October 2024, coinciding with the launch of the ChainBounty mainnet.
- Annual Inflation Rate: The initial inflation rate is set at 7% in the first year, decreasing each year. In the second year, the rate drops to 6.6%, followed by 6.3% in the third year, 5.9% in the fourth year, and 5.5% in the fifth year. By the 20th year, the rate reaches approximately 0.1%.
- This inflation structure ensures the long-term stability of ChainBounty's ecosystem while providing continuous rewards to the community and validators.

10. Conclusion

The adoption of cryptocurrencies and Web3 technologies has brought revolutionary changes to the financial industry, but it has also marked the advent of new forms of cybercrime. Traditional centralized security systems struggle to effectively respond to the complex and diverse criminal activities emerging within the decentralized cryptocurrency ecosystem. Cybercriminals are increasingly leveraging anonymity to carry out sophisticated and covert attacks, leaving individuals and organizations vulnerable to security threats.

To address these challenges, ChainBounty presents an innovative approach by leveraging the collective intelligence of the global community through a decentralized cryptocurrency crime bounty system. Built on Layer 2 technology, ChainBounty supports fast and efficient transaction processing while encouraging active participation through a transparent and fair reward system. By doing so, ChainBounty aims to maximize the advantages of decentralization and elevate the security standards of the cryptocurrency market.

ChainBounty is a platform that inherits and advances the successful legacy of Sentinel Protocol. As a decentralized threat detection platform, Sentinel Protocol has set significant milestones in effectively combating cryptocurrency crime. Notably, it has strengthened the security of the cryptocurrency market, particularly in South Korea, by providing tangible support to many victims through collaboration with the Cyber Incident Response Center (CIRC). Building on this success, ChainBounty seeks to deliver robust and efficient security solutions to the global cryptocurrency ecosystem through enhanced technology and a decentralized collaborative model.

As the cryptocurrency market experiences rapid growth, cybercrime is on the rise, and existing solutions from both the private and public sectors are showing limitations in effectively addressing these crimes. Therefore, an integrated approach through a decentralized collaboration model is essential. It is crucial to work together with the global community to share threat information in real-time and respond swiftly to emerging threats. ChainBounty is a platform designed to meet this need.

By adopting Layer 2 technology, ChainBounty maximizes scalability, efficiency, and real-time processing capabilities. This ensures the secure storage of TRDB data and provides real-time access while maintaining data integrity and reducing costs. Additionally, through a decentralized bounty process, ChainBounty harnesses collective intelligence, and a transparent and fair reward system fosters active participation.

The validators of ChainBounty play a crucial role as the core members of the platform. Drawing on their experience and technical expertise in the security industry, they maintain the platform’s stability and reliability. Validators assess the accuracy of bounty claims, ensure fair distribution of rewards, and enhance the platform's credibility. Professional validators, contribute to raising ChainBounty’s security standards and increasing user trust.

In summary, ChainBounty presents an innovative approach to strengthening the security of the cryptocurrency market and effectively combating cybercrime. Through a decentralized system and global community collaboration, ChainBounty will play a critical role in building a safe and transparent ecosystem for the cryptocurrency market, fostering sustainable growth. More than just a technological platform, ChainBounty stands as a powerful vision for the future of the cryptocurrency market, contributing to the creation of a safer and more transparent digital asset environment.