Appendices

1 Interview Protocol

1.1 Perception of Auditing

Do you know DeFi Auditing? Can you explain what is it?

Can you tell us about any audit cases you've been looking at?

What does auditing mean to you? Do you see it as something that involves responsibility, a specific process, and produces certain outcomes?

What do you think audit actually does in the audit cases you have noticed?

- What do you think the process looks like? How do you know?
- What is the cost? How do you know?
- What aspect do you think is audited, and how do you know that?
- What is the method of auditing? How do you know that?
- How long will the audit last, how many labor resources will the audit take, and where will the information be obtained?

How do you get audit-related information? Do you find it difficult to obtain? Do you think the information you get is sufficient?

During this process, how did you go about learning more about audits? What channels or sources did you use to gather different information and knowledge about audits?

What do you think about the audit results? Do you think the audit is credible?

- What risks can be mitigated by audit results?
- Will there still be significant security risks to an audited application?
- Do you think the audited vulnerabilities will be fixed?
- Do you think it is important for an application to be audited?

Do you know:

- How many applications have been audited in the market?
- Have all well-known applications been audited? Why?

Audition Firm:

Do you have an audit firm that you trust?

How do you learn about an audit firm

Do you think the audit firms are reliable, and how can you judge how reliable they are?

Will you read different audit firm reports for the same application?

Are you concerned about the independence of your audit firm?

Do you know any audit firm that is famous or reputable, and why do you think it is famous or reputable?

Have you ever followed the audit firm's social media accounts or official website?

How do you think audit firms are responsible for the audit results?

Before the audit begins, how do you think the audit firms and the applications will confirm the cooperation?

During the audit, what are the responsibilities of the audit firms, and what needs to be done?

After the audit is completed, do you feel that the audit firm has any responsibilities to bear?

Assuming that something goes wrong with an audited applications, what should the related audit firm do?

Auditor:

Have you ever noticed the auditor in charge of the audit, and how do you find out?

If yes, would you do an auditor's background check?

If not, why didn't you pay attention to the auditor's information

What do you think is the responsibility of auditors?

How do auditors work together on the same application?

What does an auditor do?

Do all the auditors belong to the firm, and do you think there is outsourcing?

How much responsibility do you think auditors have for the results of the audit?

Audit Report:

Have you read audit reports before? What content stood out to you the most?

How long do you typically invest in an audit report?

To what extent are you able to understand the content of audit reports?

What aspects of an audit report do you pay attention to?

Audit Method:

Are you familiar with automated audit tools? How did you come to know about them?

- Who do you think is using audit tools?
- How do you think audit tools implement audits?
- Do you find the audit tool reliable?
- Do you think the introduction of artificial intelligence in auditing will replace manual auditing?

Have you ever tried to conduct a personal audit using an audit tool?

- Under what circumstances would you go about using it?
- What is the reason you didn't use it?

What do you think about manual auditing?

- Who is responsible for manual audits?
- Do you find the results of the manual audit reliable?
- What do you think would be the difference between a manual audit and a tool audit?

Application:

What do you think the applications should do when applying for an audit? How do you know?

- Is there anything need to prepare?
- Will members of the application be involved in the audit process?
- Are you worried that the involvement of the application will affect the confidence in the audit results?

Do you think the application will need to do anything after the audit, and how do you know?

- Do you think the application will modify the code after the audit is over?
- Is the audit content of the audit report consistent with the final contract? Who is responsible for supervising it?

How would you define or assess an audit firm's independence when it comes to its relationship with the applications? And why is this important in your opinion?

How would you judge that an audit firm regularly serves the same application?

General Perception:

Do you find it difficult to understand the audit process?

- In terms of technical knowledge (Unable to understand technical terms, unable to understand the core of the problem, unable to understand threat rating)
- In terms of reporting (Poor legibility, lack of charts, color highlights, too long)
- In terms of Audit firms (The auditors, audit time, and audit methods are not clear, The audit standards are not uniform, and the judgment of vulnerabilities and the classification of risk levels are inconsistent)

Do you think audits have limitations?

- Are there any specific areas where you believe audits may fall short or have certain limitations?
- Do limitations affect your decision-making and attitude towards audit?

1.2 Decision Making

How much attention or importance do you personally place on audits?

- Will you only care about whether there is an audit and the results of the audit or Will you roughly/carefully read the contents of the audit report?
- Will you pay attention to whether there is an audit for most/partial/very few applications?

Could you share your previous experiences with application audits and how the results of those audits may have influenced your subsequent actions or views on the applications?

- Does whether the application has been audited affect your decision-making?
- Does the diversity of application-related audit reports (not only one firm's audit) affect your decision-making
- How will the audit results of the applications affect your decision-making?

Are you involved in unaudited applications?

- Why would you want to get involved?
- Have you considered urging an application to conduct an audit?

I just asked you about auditors, audit firms, audit methods, and audit reports. Which of these factors do you think you would pay more attention to?

Are there any ways you think can avoid or reduce the limitations of Web3 audit?

- Unified auditing standards? such as web2 audit firms
- Industry Autonomous Committees of Industry Organizations?
- External government regulation institutions?
- Audit firm's compensation services or insurance services?

1.3 Basic Information

What is your age, city, and occupation?

How are your computer skills/technical knowledge of blockchain systems?

- Can you understand the code?
- Can you write code?
- Can you propose a solution to the problem based on the code content?

How long have you been involved in Web3 or using Web3 applications?

- What Web3 applications have you used?
- Where did you know about new Web3 applications?

2 Web3 Auditing Website Investigation

2.1 Company Introduction

1. How does the audit firm introduce its services? (Multiple choice)

- **a)** Through a brief description (e.g., "We specialize in providing top-notch smart contract auditing services")
- **b)** With a mission statement or slogan (e.g., "Securing the decentralized world")
- **c)** Through an introductory video (e.g., a company overview or explainer video)
- **d)** Showcasing their team members and their expertise
- **e)** Other

2. How does the audit firm introduce its firm advantages? (Multiple choice)

- **a)** Company size (e.g., "Our team consists of 50+ experienced auditors")
- **b)** Experience (e.g., "We have audited 200+ smart contracts")
- **c)** Client base (e.g., "We have more than 500 customers")
- **d)** Unique selling points or competitive advantages (e.g., "We utilize cutting-edge automated tools and manual review for comprehensive audits")
- **e)** Other

3. How does the audit firm present its credit? (Multiple choice)

- **a)** Industry partnerships (e.g., "We collaborate with major blockchain platforms")
- **b)** Notable applications (e.g., "Our clients include Aave, Compound, and MakerDAO")
- **c)** Successful audits (e.g., "We have conducted 100% successful audits with no exploited cases")
- **d)** Awards or recognitions (e.g., "Winner of the 2022 Blockchain Security Excellence Award")
- **e)** Testimonials or endorsements from applications or industry experts
- **f)** Other

2.2 Presentation of Services

4. How does the audit firm describe its service process? (Multiple choice)

- **a)** Step-by-step description (e.g., "1. Client onboarding, 2. Code review, 3. Reporting, 4. Re-audit")

b) Flowchart or infographic (e.g., a visual representation of the auditing process)

c) Video or animation (e.g., an explanatory video detailing the service process)

d) Other

5. What is the scope of the audit firm's services? (Multiple choice)

a) Smart contract auditing (e.g., "We focus on auditing smart contracts for DeFi projects")

b) Security consulting (e.g., "We provide security consulting services to improve the overall security of your project")

c) Bug bounty programs (e.g., "We help you set up and manage bug bounty programs to crowdsource vulnerability detection")

d) Penetration testing (e.g., "We offer penetration testing services to identify potential security weaknesses")

e) Other

6. Is the distinction between various services provided by Web3 audit firms, such as Web3 auditing and exchange auditing, clearly defined without any overlapping or confusion?

a) Yes, clear and understandable.

b) Somewhat clear, but requires explanation.

c) Not very clear, vague.

d) Unclear, difficult to understand.

7. Does the audit firm provide post-audit support? (Multiple choice)

a) Yes, they offer ongoing support for bug fixes and re-audits.

b) Limited support, available only for a specific duration after the audit.

c) No, they do not provide post-audit support.

d) Other

8. Are the audit reports publicly available or accessible upon request? (Multiple choice)

a) Publicly available on the firm's website

b) Accessible upon request with application's consent

c) Not available for public access

d) Other

9. Does the audit firm have a standardized audit report format, or do they customize reports based on applications' requirements? (Multiple choice)

a) Standardized format for all audit reports

b) Customized reports based on applications' requirements

c) Combination of standardized and customized reports

d) Other

10. How does the audit firm present its pricing structure? (Multiple choice)

a) Fixed pricing based on project complexity or size

b) Customized quotes depending on specific application requirements

c) Tiered pricing with different service levels or features

d) Hourly or retainer-based pricing

e) Other

11. Does the audit firm have a strong track record of successful audits without exploited cases? (Multiple choice)

a) Yes, they have a proven history of successful audits.

b) Mostly, with only a few minor exploited cases.

c) No, they have a history of exploited cases despite their audits.

d) Other

12. Does the audit firm have a strong track record of successful audits without exploited cases? (Multiple choice)

a) Yes, they have a proven history of successful audits.

b) Mostly, with only a few minor exploited cases.

c) No, they have a history of exploited cases despite their audits.

d) Other

2.3 Additional Security Information

13. How security-related knowledge or information does the audit firm share on its homepage? (Multiple choice)

a) Blog articles (e.g., informative articles on smart contract security, industry trends, and best practices)

b) Webinars or workshops (e.g., online events discussing security topics and challenges)

c) Whitepapers or reports (e.g., in-depth research and analysis of security topics)

d) Security guides or checklists (e.g., resources to help projects improve their security)

e) Podcasts or interviews (e.g., conversations with industry experts and thought leaders)

f) Other

14. Does the audit firm have a strong presence on social media or community platforms? (Multiple choice)

a) Yes, they have an active presence on popular platforms (e.g., Twitter, LinkedIn, Telegram, Discord)

b) They have some presence, but it's not very active or engaging.

c) No, they have little to no presence on social media or community platforms.

d) Other

15. Does the audit firm provide any additional resources or tools for developers or applications? (Multiple choice)

a) Open-source tools or libraries (e.g., tools for smart contract analysis or vulnerability detection)

b) Educational materials (e.g., tutorials, guides, or courses)

c) Security frameworks or templates (e.g., resources to help projects implement security best practices)

d) Other