DeFi remains the prime target for hackers and bad actors, and it's no surprise. With millions secured in DeFi protocols, the temptation for malicious actors to attack these protocols is huge. Unfortunately, this led to

[Q3 2023 becoming the

](https://cointelegraph.com/news/700-m-loss-crypto-hacks-exploits-scams-q3-certik)

[worst quarter

](https://cointelegraph.com/news/700-m-loss-crypto-hacks-exploits-scams-q3-certik)of 2023, with reported losses of $700M.

So, does anyone still question the importance of audits?

They are a crucial safeguard in the space, all protocols must undergo an audit during their development. With the rapidly increasing availability of security offers and options, one question arises:

Should you opt for a competitive or private audit?

In summary, the answer is "Both," with some considerations though. In this blog post, we will thoroughly examine both options and explore their respective benefits based on your business requirements and the development stage of your protocol.

Competitive Vs Private audits - How to choose the right solution

Choosing the most suitable type of smart contract audit for a company

is like a chef choosing the right ingredients for their signature dish.

From an outsider's perspective, it may seem logical to recommend the most expensive ingredients or the ones with the most popular appeal, but only the chef truly understands the nuances of the dish. They know the precise flavor profiles that need to be achieved, the balance of textures that need to be maintained, and the dietary considerations that need to be considered. Likewise, only the team that has built the protocol, understood its complexities, and envisioned its use cases, can accurately determine the type and extent of audit that it needs.

However, having a helping hand in the decision-making process is always appreciated. So, let's delve into it and hopefully provide you with a clearer perspective on the best option for you.

- Private Audits

: A private firm provides a thorough review with a dedicated team, resulting in more comprehensive and detailed reports, best practices assistance, education for your team, and a close partner who can help you throughout your development and deployment process. The added benefit is the assurance that a group of experts exclusively focuses on auditing your smart contracts.

- Competitive audit platforms:

on the other hand, competitive audits allow multiple auditors to compete in auditing your company's smart contracts, potentially leading to a more diverse range of issues being identified. These platforms like CodeHawks are an attractive option for companies of all sizes.

However, there are many other factors to consider, such as:

- Time constraints
- Development status
- Codebase complexity
- Budget limitations
- Potential quality issues

that may arise from the audit

Therefore, you and your protocol must carefully weigh these factors, fully understanding that cutting corners on expenses might be extremely dangerous

. The cost of the auditing process is a small price to pay when compared to the potential damages that can result from a security breach.

Let's delve into the crucial key points of the comparison, starting with private audits, to then compare competitive vs private audits

.

Private audits: prioritizing trust as the paramount metric

There are numerous companies, such as Cyfrin, that offer specialized services focused on security reviews, static and dynamic analysis, and manual penetration testing of smart contracts. Their main goal is to ensure the security and hacker-proofing of your smart contracts. With a wide range of options available, choosing the best company for private audits can be challenging and subjective based on personal preferences.

The most crucial aspect here is trust

- the extent to which you can rely on a company to deliver the highest quality audit. While acknowledging the inherent bias in this trust metric and the impossibility of guaranteeing 100% accuracy, there are certain key factors to consider when evaluating your level of trust:
- The number of past audits conducted and the size of the protocols audited

.

- The quality of the reports and the number of issues found in previous audits.
- The investment made by the company in research and knowledge dissemination.

Private Audits Costs: Solo Auditors and Auditing Firms

It is worth noting that neither companies nor solo auditors provide a fixed fee for each audit

, as each case is distinct and the pricing reflects the complexity of the smart contracts, theSLOC, and the specific requirements of your company. However, we can use some reference numbers to provide a rough estimate and give you an idea of the potential costs involved.

There are two main types of private auditors: solo auditors and auditing firms.

Solo auditors:

usually offer a cost-effective option, charging around $2K per day for a solo audit or $5-10K per week. This price reflects their service, as well as their expertise in auditing smart contracts. However, most auditors are usually more flexible in adapting themselves to the protocol's budget, striking a balance between their perceived expertise and the allotted budget for the auditing process.

Private auditing firms:

with their larger teams, broader range of expertise, and more extensive support, typically charge higher fees. A two-week audit from an auditing firm can range anywhere from $40K to $60K

. The increased cost is justified by the comprehensive nature of the services provided. This often involves multiple levels of review, a thorough examination of the smart contract's functionality, multiple auditors, a detailed and comprehensive final report, as well as assistance to your team.

According to Cointelegraph, the cost of audits can reach up to $500K for larger projects with more complex and extensive code. The price depends on the size of your protocol and the level of difficulty in fully auditing your code base. While the affordability of a solo auditor is attractive, it is important to consider the limitations of having only one person reviewing the code and the time constraints involved in thoroughly examining an entire code base.

Private Audit: how much do they get hacked?

Now that we have a broad overview of what private audits provide, and how they aim at enhancing the security of your protocol, let's explore the data of over a hundred compromised projects since late 2020, as shown in the REKT leaderboard.

These projects range from simple meme coins to complex DeFi protocols, and they all share one common factor - insufficient security measures. Out of the 137 compromised projects, nearly half had undergone audits.

- Unaudited Projects

: 79 (approximately 57.7%)

- Audited Projects

: 58 (approximately 42.3%)

Source:

[rekt news

](https://rekt.news/leaderboard/)

Then what is the purpose of private auditing if nearly half of the compromised protocols still end up being hacked? The importance becomes apparent when we consider the tremendous increase in lost amounts over the past years and the size of the exploits.

Source:

[rekt news

](https://rekt.news/leaderboard/)

The total amount lost is approximately $4.99 Billion and the data shows, as expected, that unaudited projects have experienced a significantly

larger proportion of losses compared to Audited ones.

- Audited Projects

: 26.1% of the total amount lost, approximately $1.30 Billion

- Unaudited Projects

: 73.9% of the total amount lost, approximately $3.69 Billion

It is crucial to recognize that auditors, like anyone else, are fallible and may overlook potential errors or bugs. To ensure a comprehensive examination, we argue that involving multiple reviewers as well as multi-phase audits is the right way to go.

Now, let us delve into the other side of the coin and explore the valuable insights that competitive audits can offer.

Competitive Audits: the more eyes the better?

The premise of competitive auditing revolves around the concept that the more eyes scrutinizing the smart contract, the higher the likelihood of

[detecting vulnerabilities and flaws

](https://www.youtube.com/watch?v=O1rKwDv5kLQ). High level: in a competitive audit, several auditors review the same protocol's code base independently and then compare notes, allowing for a broader perspective.

Competitive audits take a different approach, operating on a model of collaboration and competition between independent auditors. They offer, on average, a much more comprehensive and rigorous examination of contracts as they open the code to multiple auditors concurrently. It's not uncommon for one auditor to spot an issue missed by others, enhancing the robustness of the review process.

It's worth noting, though, that while the collaborative nature of competitive audits may result in a more diversified review, they also don't come with the added benefits of having a team of auditors, helping your team of engineers throughout the development and mitigation process, educating and assisting when it comes to implementing best practices and bringing your protocol to mainnet.

Thus, the decision to opt for a competitive audit should factor in not just the financial implications, but also the administrative and strategic overhead.

Bug Bounty & Competitive Audits

On a side, similarly to competitive audits, bug bounty platforms play distinct roles in ensuring the security of smart contracts.

Bug bounty platforms

are typically used after deployment, offering rewards to individuals who can find and report vulnerabilities in the deployed code. This "pay-to-find" model encourages ongoing scrutiny of the code, even after it's launched.

Competitive audit platforms

, on the other hand, primarily operate before deployment. They engage a community of security researchers to audit the code prior to its deployment, identifying and fixing potential security issues before the product launch. This proactive approach, with a flat fee for the audit, acts as a safety net, catching vulnerabilities that may have otherwise slipped through traditional auditing processes.

The choice between bug bounty platforms and competitive audit platforms primarily depends on the stage of development:

- Pre-deployment:

competitive audits

- Post-deployment:

bug bounty platform

Pricing and Results of Competitive Audits

Code4Arena has recently released a remarkable record of approximately 154 contests held on their platform. This information provides intriguing insights into what we can anticipate from competitive audits.

First, it answers the crucial question: Do competitively audited protocols get hacked?

The answer is, yes but tremendously less than unaudited protocols - a significant majority, 60.0%, of contests audited in competitive audits remained uncompromised, on the other hand, 11.7%, of contests were hacked, once again indicating the importance of undergoing multiple audit stages to try and uncover the highest possible number of vulnerabilities.

Another 27.7% of contests in the Code4rena report, fall under the "Duplicate/Other" category, which suggests duplicate records or alternative categorization. Unfortunately, the C4 report does not include more info on this one.

Source

[code4rena

](https://docs.google.com/spreadsheets/d/1RIJCK3_9RHvtNPObsDRTAqkP9IbyutZMsqIKNnZCO00/edit#gid=0)

The other questions you're probably looking to answer: how much does a Competitive Audit cost?

Simply put: where most contests offer prize pools ranging from $0 to $100,000, there are a few contests with much higher prize pools, reaching nearly $800,000+.

By analyzing these numbers, we can observe how the prize pool changes over time, depending on the contest's start date. This information can provide valuable insights into the variations and trends of the prize pool as well as their average rewards.

Source

[code4rena

](https://docs.google.com/spreadsheets/d/1RIJCK3_9RHvtNPObsDRTAqkP9IbyutZMsqIKNnZCO00/edit#gid=0)

This tells us one thing, prize pool amounts in contests are merely references

, as they can vary greatly depending on project complexity. With an average prize pool of $60k to $100k, some protocols even host smaller competitions with prizes up to $15k.

Moreover, the high cost is a valuable investment when balanced against the potential risks associated with compromised contracts.

Critical Points of Competitive Audits:

- Financial Consideration:

Competitive audits cost between 60k to 100k, depending on project complexity. This includes platform fees.

- Comprehensive Analysis:

Competitive audits involve multiple auditors for a thorough investigation, enhancing audit quality.

- Spotting Inconsistencies:

A competitive environment helps auditors identify overlooked issues, strengthening the review process.

Conclusions

In conclusion, we hope that this comprehensive walkthrough of the differences and advantages of competitive audits vs private audits has provided you with valuable insights. As we've seen, there's not a one-catch-all type of solution, and at Cyfrin we'll always suggest our customers go through multiple audit rounds involving both private and competitive audits to strike a balance between engineering support, accountability, thoroughness, and reaching higher security coverage.

By gaining a deeper understanding of these distinct types of audits, our goal is to empower auditors and individuals who are in need of audits to make well-informed decisions that align perfectly with their unique goals and available resources. With this knowledge, you can confidently navigate the auditing landscape and optimize the outcomes of your auditing efforts.

To schedule a call with an expert who will help you decide which solution is the best for you and your protocol, fill up our form.

Reference List:

Blockchain Auditing Companies (no date) Alchemy.com. Available at:https://www.alchemy.com/best/blockchain-auditing-companies (Accessed: October 29, 2023).

Jones, C. (no date) Solana and Ethereum smart contract audits, explained, Cointelegraph. Available at: https://cointelegraph.com/explained/solana-and-ethereum-smart-contract-audits-explained (Accessed: October 29, 2023).Livestream, [ethcc] (2021)

Sebastian Banescu - Lessons learned from over 300 security audits. Youtube. Available at: https://www.youtube.com/watch?v=O1rKwDv5kLQ (Accessed: October 29, 2023).

[public] C4 exploit data (no date) Google Docs. Available at: https://docs.google.com/spreadsheets/d/1RIJCK3_9RHvtNPObsDRTAqkP9IbyutZMsqlKNnZCO00/edit (Accessed: October 29, 2023).Reguerra, E. (2023)

Q3 2023 crowned most ‘damaging’ quarter for crypto amid $700M losses: Report, Cointelegraph. Available at: https://cointelegraph.com/news/700-m-loss-crypto-hacks-exploits-scams-q3-certik (Accessed: October 29, 2023).Rekt - leaderboard (no date) rekt. Available at: https://rekt.news/leaderboard/ (Accessed: October 29, 2023).Xiao, R. (2023)

The wisdom of the crowd: Community driven security - ray Xiao, Medium. Available at: https://medium.com/@ray_xiao/the-wisdom-of-the-crowd-community-driven-security-1da010a35378 (Accessed: October 29, 2023).