Web3 Audits

[] The current State of Audits

Crypto projects have long depended on external smart contract auditing firms. There is no doubt that has helped secure a lot of the ecosystem from a variety of exploits and vulnerabilities.

The realm of crypto security has only just begun shedding some of its Web2 persona. Large firms and startups alike are trying to embrace and aim for “smart contract monitoring” among other new approaches like post audit commitments, SECaaS, periodical bounty audits, etc.

[] The vulnerable + their remedies (by value capture)

] Project driven opsec

Just like there is high awareness on wallet security and self custody for individuals, there seems to be a lack of it in the most important part of crypto, the projects themselves. A majority of hacks in value (2b) per Defillama, happened by project private key, cloudflare, and DNS compromises.

Projects like Shieldxyz are trying to solve this problem, where they put in place standard best practices for projects to adhere to. This approach would help founders explore the different attack vectors that may be a risk to their projects, outside of their siloed and often lacking skills in this category. Even the largest projects, both centralised and decentralised, have been susceptible to opsec weaknesses.

] Protocol logic + Smart Contract Language

Coming in second is your standard code vulnerabilities that are susceptible to all coloured hat attacks. The bread and butter of audit firms. The usual suspects of web3 security come in the following styles:

Standard audit
Contest audit
Bounty (passive or campaign)
Monitoring
SECaaS

The last two are the most nascent from the list but do have a lot of room for potential as that pocket of the space matures from a technical standpoint. Contest audits also have the reward dilution issue, which is being tackled by limiting the number to vetted devs.

] Ecosystem (Interactions)

This includes the infamous flashloan oracle, governance, and reentrancy manipulation hacks. Focus here on external calls has to do with a variety of factors, mostly not enough

] Rugpulls et wallet hacks

Degenland
The focus in this section is user driven security. From rugpulls to slowpulls (token unlocks). There are tools that help in detecting liquidity locks, honeypots, and the likes for the uber degens scouring dextools/screener, which use Team finance, Tokensniffer and the likes.

Token unlocks
As for the more established projects that as we've seen earlier last week with SUI's staking rewards that they refuted. This has been a very prevalent issue in crypto with vague unlock schedules using low jpeg images and schedules that don't take into account project progression. Many decent projects have a joke of a marketcap because of early aggressive unlocks. Hop and CoW are the first that come to mind. Projects tackling this are Token unlocks + dropstabs.

User wallet
Another big market coming up is user wallet security. This happens to amateurs and long-time crypto users alike. There is a plethora of projects working on social login via on-chain 2FA, AA, MPC, and social recovery. List

[] What’s to come

Credentials will also play a big role in this new wave of web3 style audits, where collectives or individuals will have their developer skills shown on-chain, via zkp, badges, etc. (examples like gitpoap + gateway).

The emergence of AI is also becoming a type of means but not a solution, essentially making human auditing more efficient. It will most likely play a larger role as it improves but so will its archnemesis hackerAI.

As all new solutions converge for security a Moore’s law effect will lessen a constraint that projects have: cost. Many projects juggle their budget balances among many expenses, and sometimes this is where security budget is sacrificed. The JDPowers of sec firms are a little too many. Another interesting issue floating around blogs and at Devcon here is full dependence on auditor purview, also lack of awareness and education in opsec.

[] Conclusion

One cannot claim any right direction towards this or any field for that matter, and even there each of the “alternative” auditing methods have their pros and cons. In the case here it is pertinent to consider the many methods emerging in the space. Aside from the non-human tools mentioned, the approach of a more open-source and decentralized way of auditing better fits the space.

The same way project best practices include multiple security tools, like toolkits, fuzzing, formal verification, simulations, and static analysis to supplement standard audits. All the above solutions will ideally become part of a holistic standard for projects. So, we may see smart contract monitoring, AI, SECaaS becoming a more common practice.

*No AI was used in this writeup