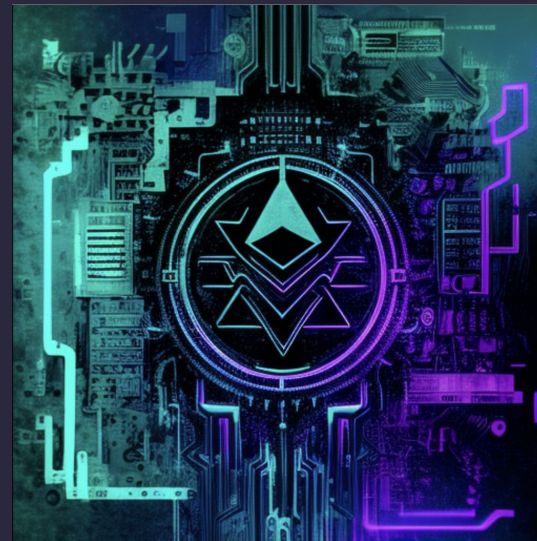




So what is an audit anyway?

Martinet Lee





Martinet Lee

Senior Research Engineer / Auditor
Head of Developer Relations
@ Quantstamp

Experience

Audited more than 50+ projects, from Defi, NFT, to Layer 1s including Yearn, ETH2, Avalanche.

Served as Audit PM and standardizing various processes that improves audit quality and communication with clients.



/Content

- Audit may not be what you think it is
- Goal of an audit
- For the devs: What is the process of an audit?
- How to reduce your auditing cost?
- Murmurs about an auditor's life

Audit may not be what you think it is

“安全審計對我來說直覺上像是公司找會計事務所簽核財報做意見表示。因為投資人與消費者不一定有能力分辨財報真實性，所以需要專業會計師這樣的角色站在兩者之間做一定程度的背書。”

“安全審計跟加密協議（甲方）彼此有什麼樣的權利義務？如果審計結果與後續發生的事實不符時，會怎麼處理？”

By Nathan Yu

Audit may not be what you think it is

- Audit in **Accounting**:
 - “independent examination of financial information of any entity, whether profit **oriented** or not, irrespective of its size or legal form when such an examination is conducted with a view to express an opinion thereon.”
 - “Auditing also attempts to ensure that the books of accounts are properly maintained by the concern **as required by law.**”

Audit may not be what you think it is

- Audit in **Accounting**:
 - “Auditors consider **the propositions before them**, obtain evidence, and evaluate the propositions in their auditing report.”
 - “Audits provide third-party assurance to various stakeholders that the subject matter is **free from material misstatement**.”

Audit may not be what you think it is

- Audit in **Web3**:

- “independent examination of **security** information of a part of project defined by the developers, whether **security oriented** or not, irrespective of its size or ~~legal form~~ when such an examination is conducted with a view to express an opinion thereon.”

- ~~◦ “Auditing attempts to ensure that the books of accounts code are properly maintained by the concern **as required by law.**”~~ ⇒ there is no “law” and it will be challenging for “law” to restrict how you implement code.

Audit may not be what you think it is

- Audit in **Web3**:
 - “Auditors consider the propositions (**User documentation**) before them, obtain evidence (**Code**), and evaluate the propositions in their auditing report.”
 - ~~“Audits provide third party assurance to various stakeholders that the subject matter is free from material misstatement.”~~ ⇒ there can only be a misstatement if there’s a requirement of some sort, like law.

Audit may not be what you think it is

- Security experts actually **DISLIKE** the term **Audit**
- Some would like to call it **Security Review** instead as this is more accurate.

Goal of an security audit - high level

(X) “Hiring experts to make sure there is **NO bug** in my protocol”

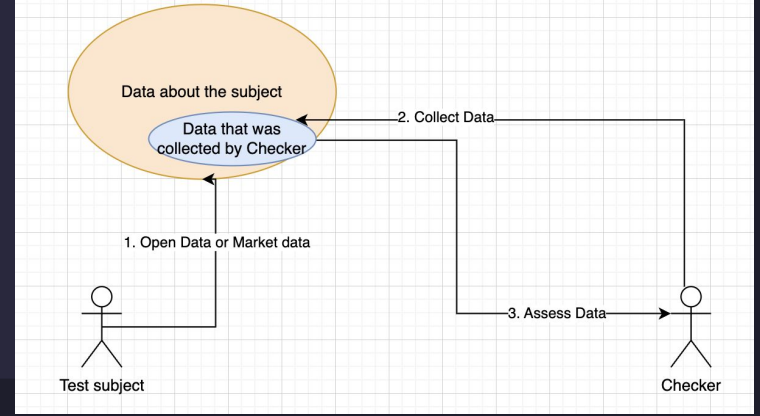
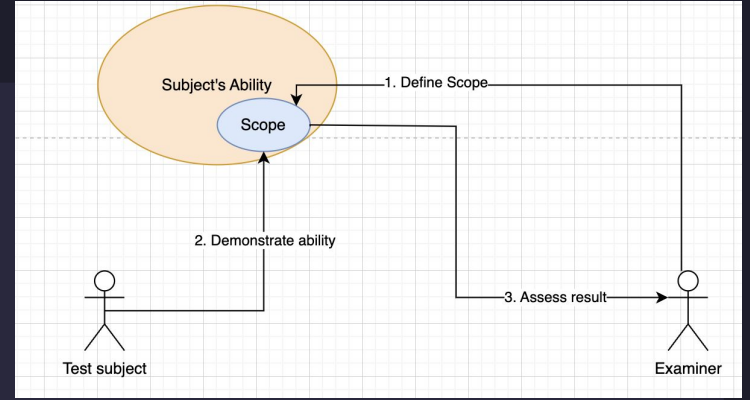
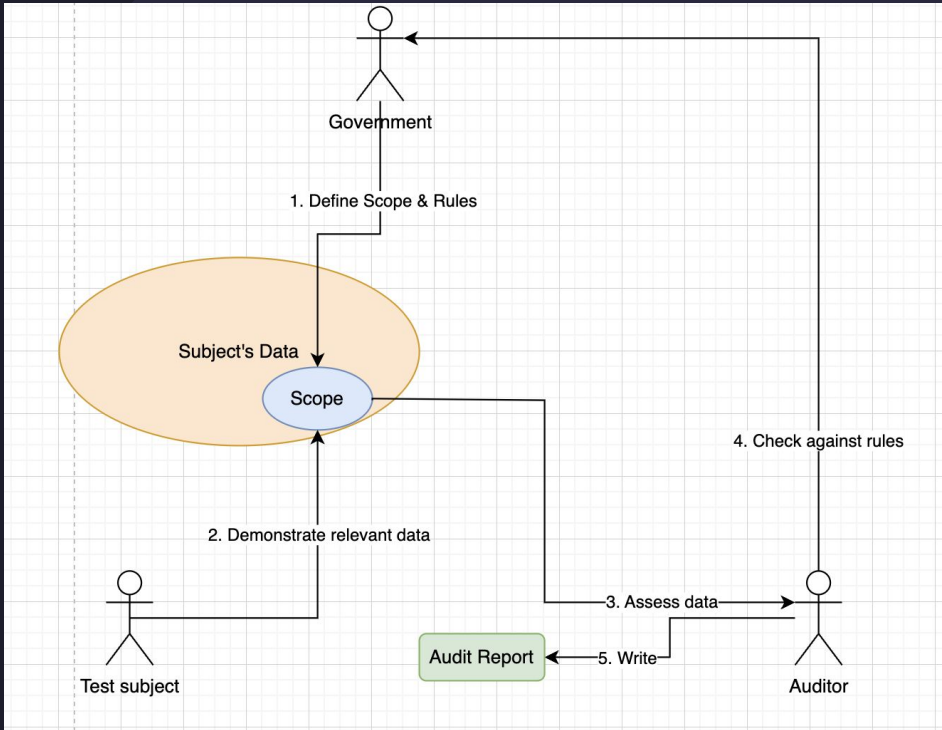
This is the wrong mindset!

Goal of an security audit - high level

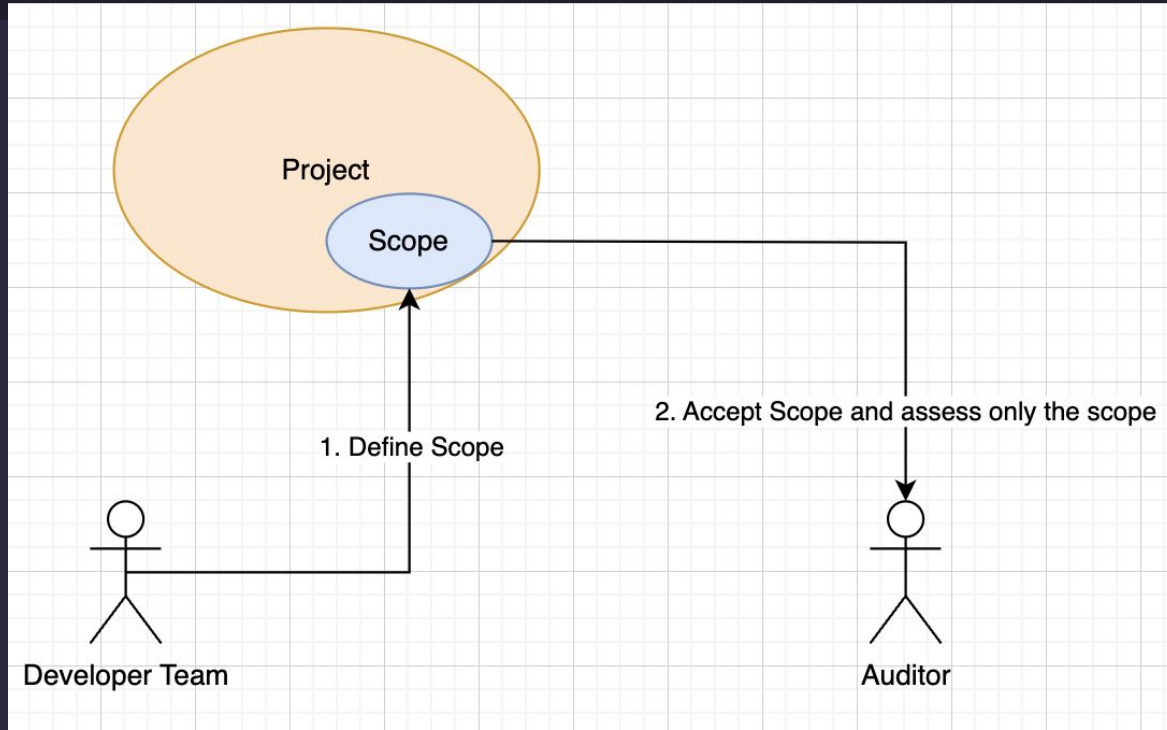
Hiring experts in a time-limited fashion and have them provide assessments, and see if they are able to find vulnerabilities or inconsistencies of your defined scope of your protocol. **Improve the codebase with the findings.**

- **Vulnerabilities:** Implementation or design flaws that leads to unintended consequences.
- **Inconsistencies:** Implementation that is different from what was intended.

A visual comparison



A visual comparison



Holy Grail - “There is no bug, it is SECURE”

- Formal verification? Symbolic execution?

“If you think technology can solve your security problems, then you don’t understand the problems and you don’t understand the technology.” – Bruce Schneier

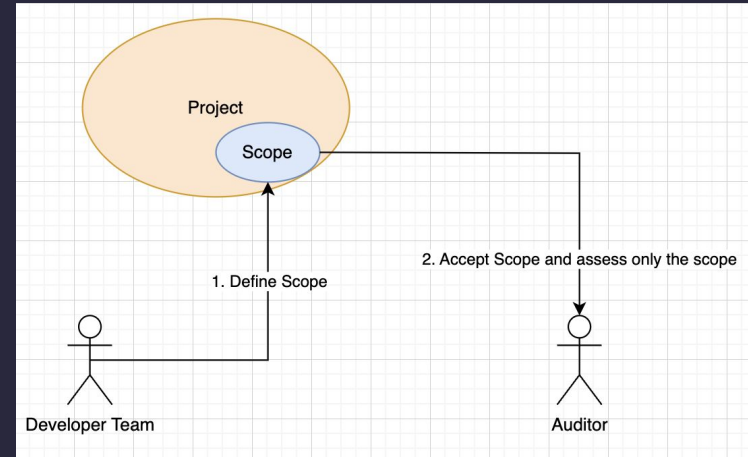
- **Challenges:**
 - Complexity
 - Composability
 - Bug in the verifying program?
 - Configuration error
 - Other human errors

“Protocol A is being Audited, is it absolutely bug-free?”

- **Unfortunately, no.**
- Getting an audit is like taking a test - if a protocol saying they got audited, it does not necessarily mean that their security is great.
- It just means that they have got an audit - It's like saying “I got an SAT, GRE, or IELTS”. **The important part is the assessment!**

“The audit presented a good assessment, is it absolutely bug-free?”

- Unfortunately, no.
- An important aspect of an audit is the “scope” of the audit.
- In security auditing, this is more tricky as scope is something the project team defines and not something the audit team defines.
- Even if everything is in scope... the fundamental challenge is still there.



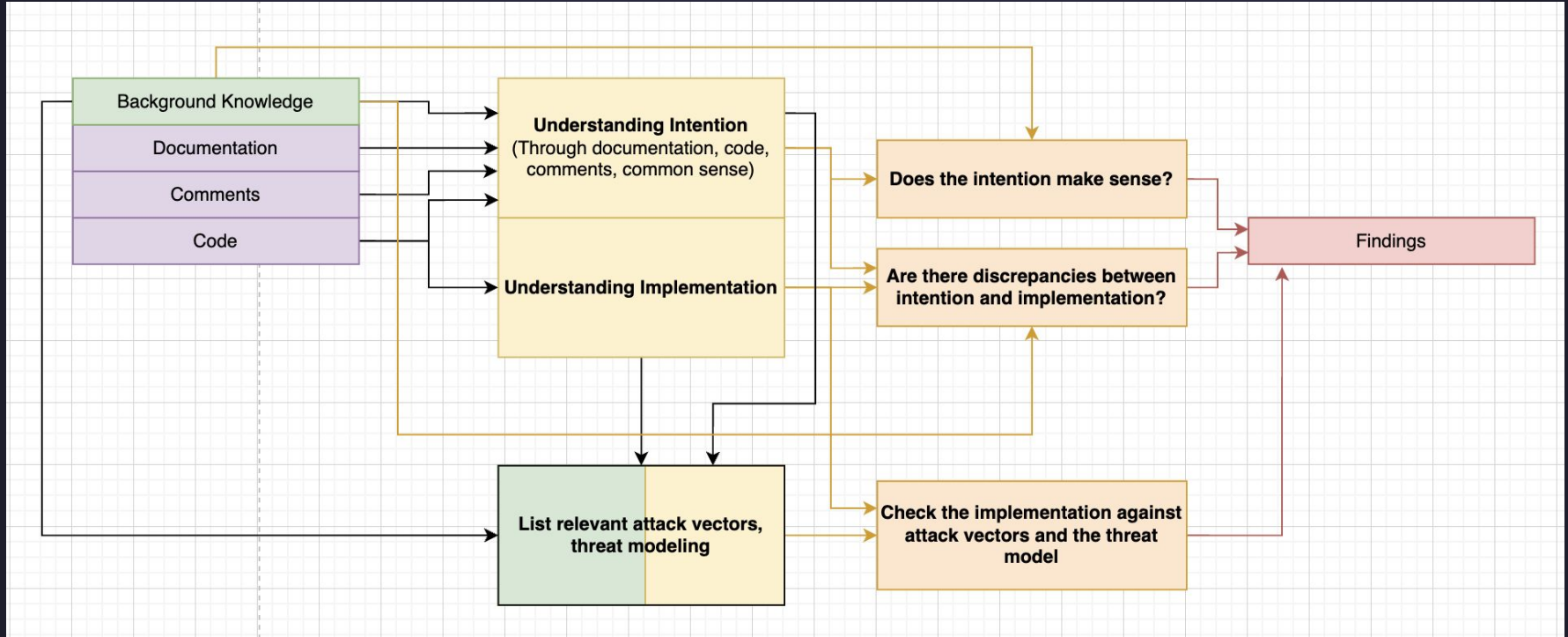
“There are not much high severity issues found, is it more or less secure?”

- This depends.
- Given that an audit is “**time-limited**” security review by nature, it depends on the complexity of the project, the clarity of the documentation, how readable is the code, etc.
- This demands a bit of explanation on how an auditor generally tries to audit a codebase...

Roughly...

- An auditor tries to **understand the project first**
 - Intention
 - Implementation
- An auditor attacks it later
 - Does the intention make sense?
 - Does the intention matches the implementation?
 - What kind of attacks may be employed on it, and do they work or not? If not, why?

An auditor's thought process (roughly)



It depends on whether there is enough “Time to attack”

- Audit is *time-limited*
- **IF** the “understanding” phase took too long, then **there is little or even just no time in performing the actual attack**. This will lead to little issues found, but does not indicate that the auditors feel safe about the project.
- This is *sometimes* being reported in the Summary section of a report to indicate auditors’ confidence on their understanding and the project. (*Not industry standard*)

Review of the question

“安全審計對我來說直覺上像是公司找會計事務所簽核財報做意見表示。因為投資人與消費者不一定有能力分辨財報真實性，所以需要專業會計師這樣的角色站在兩者之間做一定程度的背書。”

“安全審計跟加密協議（甲方）彼此有什麼樣的權利義務？如果審計結果與後續發生的事實不符時，會怎麼處理？”

By Nathan Yu

Current status of audits

- An audit is not being enforced, hence the project is typically the sole requester of an audit.
- The project receives the report, and it's up to them to publish the report or not.
- Audit firms write a report to present the findings they discovered **to improve Dev team's code.**
- Audit firms write fairly as they know sometimes these reports can be presented as marketing materials to the third party.

Quick Question

- When Auditors have critical findings, should the dev team fix them?
- Hint: How the development team responded to the issues are essential!

For 3rd parties / Users

- Read the report summary
- Understand the scope of the audit
- Read how the team addressed issues
- Also, is the audit up-to-date with the latest deployment?

For the dev team: Typical process of an Audit

- Contact
- Quote
- Audit
 - Code freeze!
 - Number of auditors?
- Report
- Fixes
- Final report

Question:

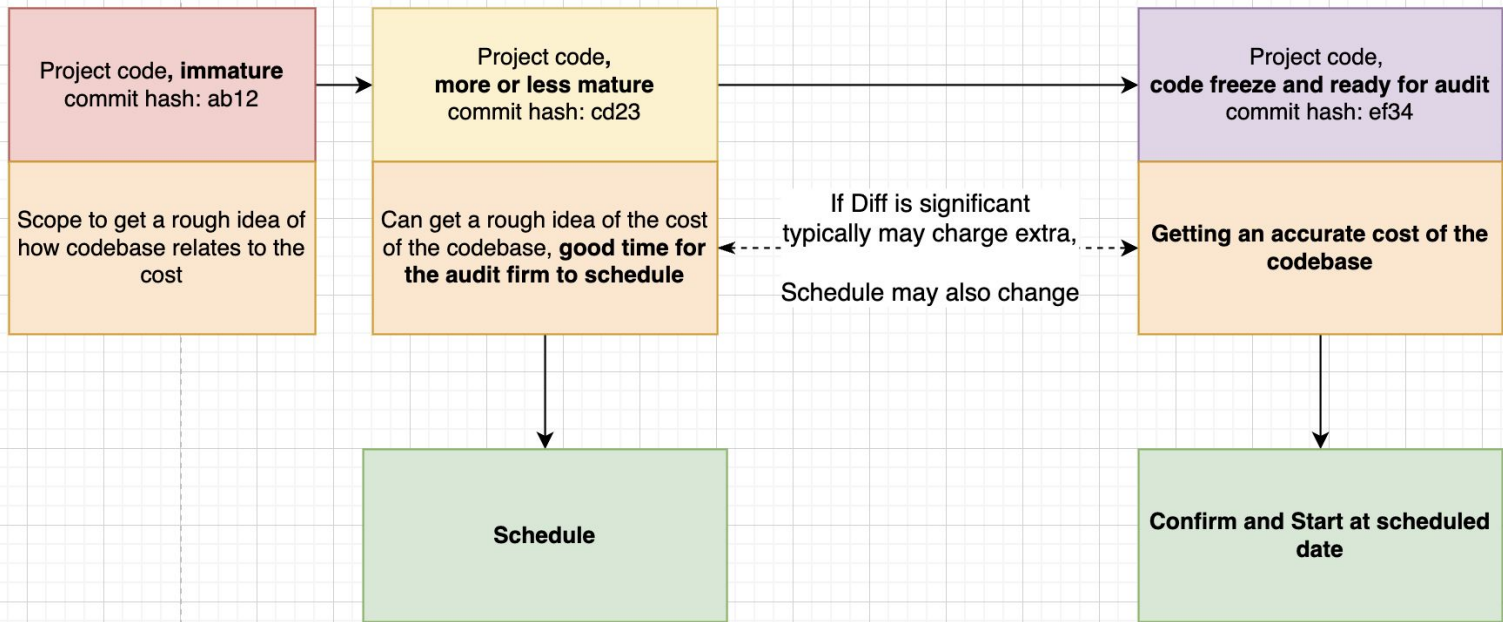
defi 項目非常多種審計公司接到一個新的項目時會怎樣評估項目內容以及時間報價呢？合約的安全漏洞會去尋找。以及項目未來的合約內容修改重新審計時會如何評估成本

By wiwi

Quote

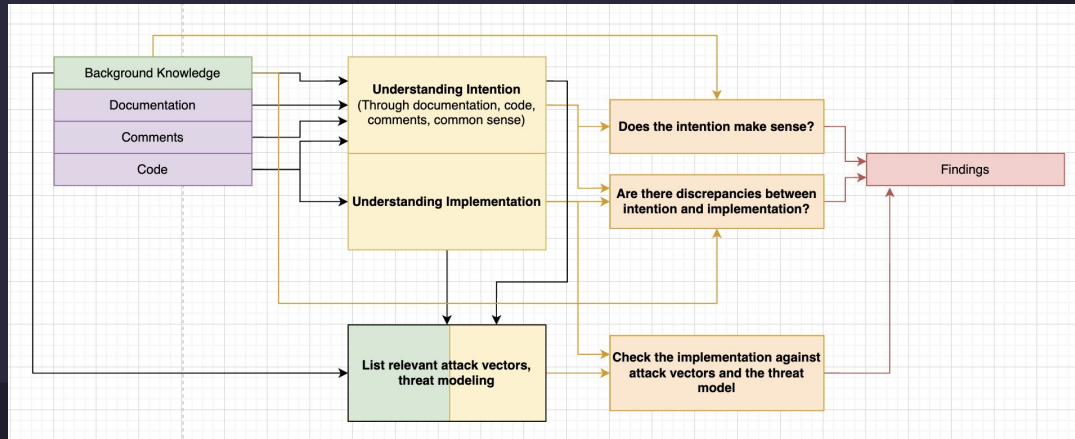
- Auditors will **need to see the code** and estimate how long it takes for us to audit it, according to our experience.
- More or less “Time” based. *But this can be optimized!*
- Auditors’ estimation on how long they need for the codebase and scope.
 - Does not matter if it is Defi or NFT marketplace or a L1.
- There is no standard here, as auditors would have different estimations based on their prior experience.

Time to ask for quote



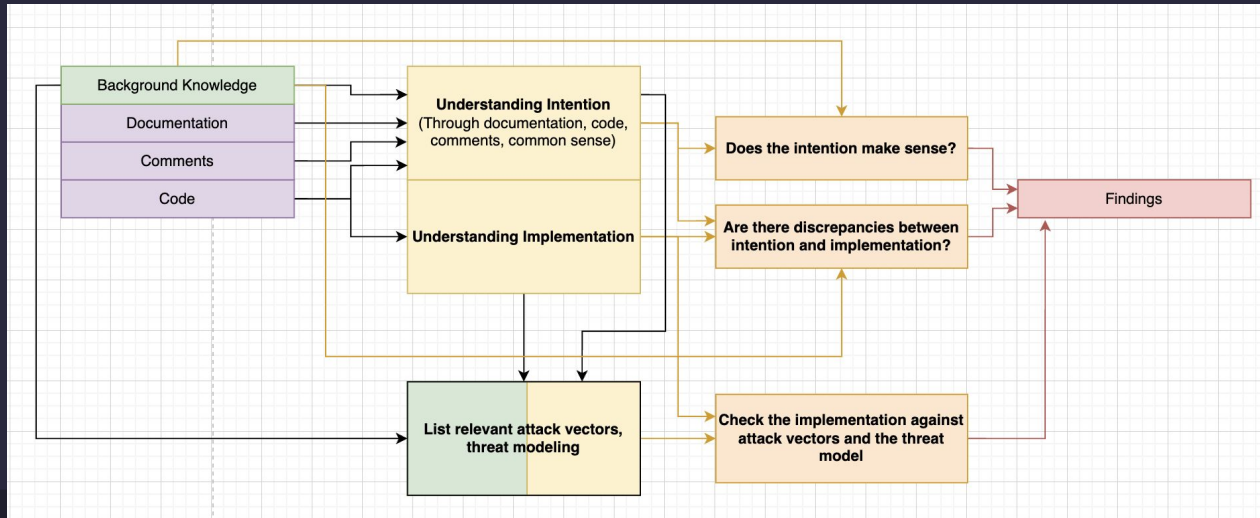
Reducing your audit cost!

- Auditors judge these things from the codebase that affects the time needed for their understanding:
 - Code quality
 - Documentation Quality
 - Design Pattern
 - Coding style
 - Test quality
 - Code readability
 - Over-optimization



Code Freeze..

- If code is not frozen, then the understanding that the auditors are building may change a lot. Resulting in longer time needed to understand and lost / mixing context.



When a project comes back..

- Same process, but audit firms would try allocate the exact same team to be on the project.
- This will reduce the time to understand the project - but they still need some time to regain the context.
- Tricky part:
 - “I just changed one line of code : D how much should it cost me?”

**Good news: the ways to optimize for
Quote are the ways to optimize for
Security!**

How a security review may help you:

- Auditors are trained in `adversarial thinking` and testing.
- Familiar with `different sets of tooling`
- Have experience / knowledge in different kinds of vulnerabilities that happened to different systems in the past. Researched to generalize these patterns and have `inhouse tools` to detect some of them.

Defense in Depth

- While developing Dapp, all of these improves your security stance.
- If one layer fails, then other layers can mitigate the issues.



Monitoring (Proactive risk detection and mitigation)



HypernativeLabs @HypernativeLabs · Aug 18
Hypernative detected the attack on @ExactlyProtocol earlier today, the malicious contract was detected 25 minutes *before* the first hack transaction
contact us to learn more about Hypernative: contact@hypernative.io

Risk Type	Severity	Details	Category	Other	Asset	Before	Reference
Exploit suspected (M2)	High	Exploit detected (216055) from wallet 0x3747dbu65a07786ac5983e473a2a38971a99. Suspected Victim ...			exactly WETH b...	High	Hack transactions 2023-08-18 09:11:39
Exploit suspected (M2)	High	Exploit detected (223762) from wallet 0x3747dbu65a07786ac5983e473a2a38971a99. Suspected Victim ...			exactly USDC (a...	High	2023-08-18 09:11:35
Exploit suspected (M2)	High	Exploit detected (224361) from wallet 0x3747dbu65a07786ac5983e473a2a38971a99. Suspected Victim ...			exactly USDC (e...	High	2023-08-18 09:11:24
Unusual contract - High mali...	High	ML model HIGH maliciveness score (0.997) for contract 0x682c09415fbc0b36480007435e0d1c0b4d			0x68_5044 + 1	High	2023-08-18 08:46:15
Unusual contract (M2)	Medium	Contract 0x682c09415fbc0b36480007435e0d1c0b4d was deployed by a suspicious wallet 0x4f84726...			0x4_f042 + 1	High	2023-08-18 08:46:13
Potential targets in unusual co...	Medium	Potential target addresses in an unusual contract 0x682c09415fbc0b36480007435e0d1c0b4d (score=0...			0x68_5044 + 2	High	2023-08-18 08:46:10

First detection 25 minutes *before* first hack transaction

Insurance

The Chainproof Blog: Your source of information of all things Chainproof



ETHEREUM SMART CONTRACTS



Regulated Non-Custodial Smart Contract Insurance

Chainproof is the world's first regulated smart contract insurer, and it brings several advantages that make it a standout choice for DeFi insurance. In this blog post, we'll explo...

Monday, April 24th, 2023

Investors & Partners




















Chainproof is backed by Quantstamp and Sompo and is reinsured by Munich Re.




Murmur: Life on an Auditor

- Leaderboard of Code4rena

2023 ▼ All

#	Competitor	USD ▼	Total	High	(Solo)	Med	(Solo)	Gas
1	 rvierdiev 	\$126,022.64	159	48	1	90	11	1
2	 Trust	\$124,688.88	40	10	4	26	11	0
3	 hansfriese 	\$105,669.70	76	23	2	44	9	0
4	 MiloTruck 	\$101,168.83	47	13	0	29	5	0
5	 bin2chen 	\$99,973.73	152	55	1	83	7	0
6	 ronnyx2017	\$87,502.43	17	7	1	6	0	1
7	 Oxsomeone	\$73,232.36	10	4	0	3	1	1
8	 cccz 	\$72,983.23	87	28	3	50	5	0
9	 AkshaySrivastav 	\$61,479.30	58	15	0	35	3	4
10	 HollaDieWaldfee 	\$59,772.70	56	18	0	31	4	0
11	 Jeiwan 	\$57,392.06	68	27	1	31	1	0



Anton Cheng 

Martinet | Quantstamp, Cohost of ETHTaipei

大家對安全審計有什麼想要問 & 好奇的東西嗎？我週一會大概聊一下，但想說看一下大家感覺也可以比較...
安全審計員薪水大公開



Murmur: Life on an Auditor

- Independent & Collaborative
- Flexible & Freedom
- Responsible to yourself
- Can be fully remote & (fully lonely lmao)

Murmur: Life on an Auditor

- **Greatest happiness:** client succeeded and appreciate your high severity findings. They launched and went smoothly - no more issues were uncovered and we share the happiness of client's success.
- **Some annoyance:**
 - Sometimes doing your job too good may lead to client disliking you. Some clients do not have the right mindset and consider smart contract audit as a rubber stamp for marketing. Sometimes they simply don't publish your report.
 - Found bugs that can drain 20M. Informed the protocol and they fixed it. The protocol offer to write a blog post LOL
 - ...

Discussions



/THAT'S A WRAP!  (mic drop)



CREDITS: This presentation template was created by **Slidesgo**, and includes icons by **Flaticon**, and infographics & images by **Freepik**

