关于Ethereum智能合约中密码学实践的调研

我们希望调研您在以太坊智能合约中实现密码学任务的经验。**除了前四个问题外，其他问题都是可选的。如果有任何问题您不理解，请跳过，或选择"我不理解这个问题"选项。**

---

* 1. 您是否是一名智能合约相关领域的从业人员?

- ◯ 是
- ◯ 否

* 2. 您在智能合约相关领域的主要职责是什么?

- ◯ 开发
- ◯ 测试
- ◯ 项目管理
- ◯ 研究
- ◯ 其他

* 3. 您有多少年从事智能合约开发/测试/项目管理/研究/其他相关领域的工作经验? （请精确到小数点后一位）

* 4. 您目前所在的国家是?

5. 您使用过下面哪些以太坊密码学API？在本调查中，“以太坊密码学API”指的是当前以太坊支持的与密码学相关的字节码（Opcode）或预编译合约（Pre-compiled Contract）。【多选题】

- [ ] KECCAK256 / SHA3 (https://www.evm.codes/#20)
- [ ] ecRecover (https://www.evm.codes/precompiled#0x01)
- [ ] SHA256 (https://www.evm.codes/precompiled#0x02)
- [ ] RIPEMD160 (https://www.evm.codes/precompiled#0x03)
- [ ] ModExp (https://www.evm.codes/precompiled#0x05)
- [ ] ECADD (https://www.evm.codes/precompiled#0x06)
- [ ] ECMUL (https://www.evm.codes/precompiled#0x07)
- [ ] ECPairing (https://www.evm.codes/precompiled#0x08)
- [ ] BLAKE2 (https://www.evm.codes/precompiled#0x09)
- [ ] 以上皆无
- [ ] 我不理解这个问题
- [ ] 其他

6. 您了解下面哪些在智能合约中应用的密码学原语？【多选题】

- [ ] 哈希（如KECCAK256/SHA3, SHA2-256, RIPEMD-160等）
- [ ] 数字签名（如ECDSA等）
- [ ] 零知识证明（如Plonk等）
- [ ] 我不理解这个问题
- [ ] 其他

7. 您是否认为实现密码学任务要比实现合约的其他常见编程任务更困难?

- ◯ 是（请转到问题8）
- ◯ 他们的难度基本相同，但是难在不同方面（请转到问题8）
- ◯ 否（请转到问题9）
- ◯ 我不理解这个问题（请转到问题9）
- ◯ 其他

8. 您为什么认为实现密码学编程任务相较于实现合约中的其他编程任务更困难，或面临不同方面的困难?

9. 在您实现密码学任务的过程中，是否曾面临以下障碍？如无，请跳过这个问题。【多选题】

- ☐ 背景知识障碍：例如，我不理解密码学/区块链领域的基本概念和原理（如：数字签名）。
- ☐ 实现方式的规划障碍。例如，我不确定应该使用哪个模板/密码学API来实现任务。
- ☐ 模板的使用障碍。例如，我在尝试使用OpenZepplin的代码模板时遇到了问题。
- ☐ 密码学API的使用障碍。例如，我在直接调用以太坊密码学API(如ecRecover这一预编译合约）时遇到了问题。
- ☐ 安全障碍。例如，我难以确定我的实现是否安全。
- ☐ 以上皆无。
- ☐ 其他
- ☐ 我不理解这个问题

10. 您通常通过什么方式来获得实现合约中密码学任务所需要的知识？【多选题】

- [ ] 官方文档，例如Solidity文档/白皮书
- [ ] 模版提供方的文档，例如OpenZepplin文档
- [ ] 在线教程/博客
- [ ] Q&A网站，如Stack Overflow
- [ ] 科技书籍/论文
- [ ] 我不理解这个问题
- [ ] 其他

11. 对于目前已有可用模板的密码学任务（例如，数字签名任务已在OpenZeppelin ECDSA等模板中实现），您通常选择使用已有模板还是自己从头开始实现？【多选题】

- [ ] 我通常使用已有的模板。
- [ ] 我通常从头开始实现。
- [ ] 取决于密码学任务的复杂度。对于复杂的任务，我选择使用已有模板。
- [ ] 取决于密码学任务的复杂度。对于简单的任务，我选择使用已有模板。
- [ ] 我不理解这个问题。
- [ ] 其他

12. 是否有您希望实现的密码学任务，目前仍缺乏可用的模板？如有，请在下面列出，否则，请跳过这个问题。

13. 您是否认为当前的以太坊密码学API足够良好，足以支持您的所有密码学任务？请在功能性、易用性方面对他们进行评分。

（1）功能性：现有API是否覆盖了所有我需要的功能？
（2）易用性：现有API是否可以被轻松理解与使用，并且具有易得的文档？

	非常差	较差	一般	较好	非常好
功能性	○	○	○	○	○

易用性 ○ ○ ○ ○ ○

14. 是否有您希望实现，但当前以太坊密码学API不能支持的密码学任务？如有，请在下面列出，否则，请跳过这个问题。

15. 您是否认为保障智能合约中密码学实现的安全性相较于保障合约其他部分的安全性更具有挑战性?

- ○ 是 （请转到问题16）
- ○ 他们的难度基本相同，但是难在不同方面（请转到问题16）
- ○ 否（请转到问题17）
- ○ 我不理解这个问题（请转到问题17）
- ○ 其他

16. 您为什么认为保障密码学实现的安全相较于保障合约其他部分的安全更困难/面临不同方面的困难?

17. 您了解下面哪些在智能合约漏洞分类列表（Smart Contract Weakness Classification，SWC）中的密码学相关漏洞? 【多选题】

- ☐ SWC-117: Signature Malleability (https://swcregistry.io/docs/SWC-117)
- ☐ SWC-120: Weak Sources of Randomness from Chain Attributes (https://swcregistry.io/docs/SWC-120)
- ☐ SWC-121: Missing Protection against Signature Replay Attacks (https://swcregistry.io/docs/SWC-121)
- ☐ SWC-122: Lack of Proper Signature Verification (https://swcregistry.io/docs/SWC-122)

- [ ] SWC-133: Hash Collisions With Multiple Variable Length Arguments (https://swcregistry.io/docs/SWC-133)
- [ ] 以上皆无
- [ ] 我不理解这个问题。
- [ ] 其他

18. 您是否认为下面的工具/资源已经足够完备，可以支撑您高效与安全地实现密码学任务？请对他们进行评分。

	1（非常差）	2（较差）	3（中立）	4（较好）	5（非常好）
Ethereum官方文档	○	○	○	○	○
合约模板	○	○	○	○	○
合约测试工具	○	○	○	○	○
合约安全审计工具	○	○	○	○	○

19. 除了上述四种类型的工具/资源，是否有其他您希望得到的支持？如有，请填写在下方，否则，请跳过这个问题。

20. 如果您还有任何对本问卷的评价/问题，欢迎填写在下方。

21. 为感谢您的宝贵时间和反馈，我们将随机选取两位参与者送出$50 USDT。如果您希望参与，请输入一个您的以太坊主网地址。

提交