Exploring Security Practices of Smart Contract Developers

Jessica Mack

Background

- Smart contracts are self-executing programs that run on blockchains
- Millions of dollars worth of digital assets are controlled by smart contracts
- There have been several cases of contracts being hacked or wallets stolen due to various security vulnerabilities

Previous Study

- Previously a semi-structured interview and a code review task was done on a group of 29 smart contract developers.
- Takeaways:
  - Early-career developer were less likely to identify security vulnerabilities than their more experienced counterparts
  - Standard documentation, reference implementations and security tools are not sufficient resources to prevent security vulnerabilities
  - Smart contract tooling is lacking in development compared to the tooling available in other development fields

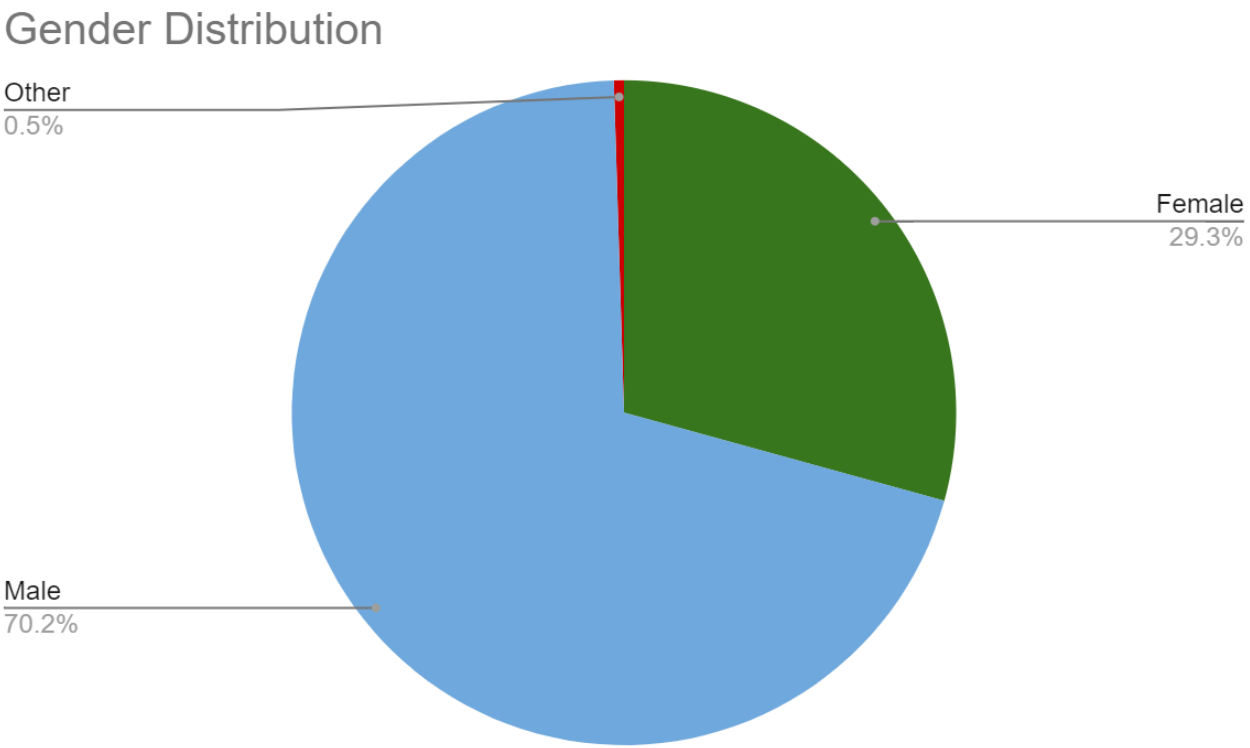
New Study Survey Design

- Multiple choice and open answer questions covering demographics, programming experience, smart contract experience, tooling preferences, and a code review challenge
- Code review challenge had 4 different options a developer could receive
- Posted to discussion boards and servers for smart contract developers

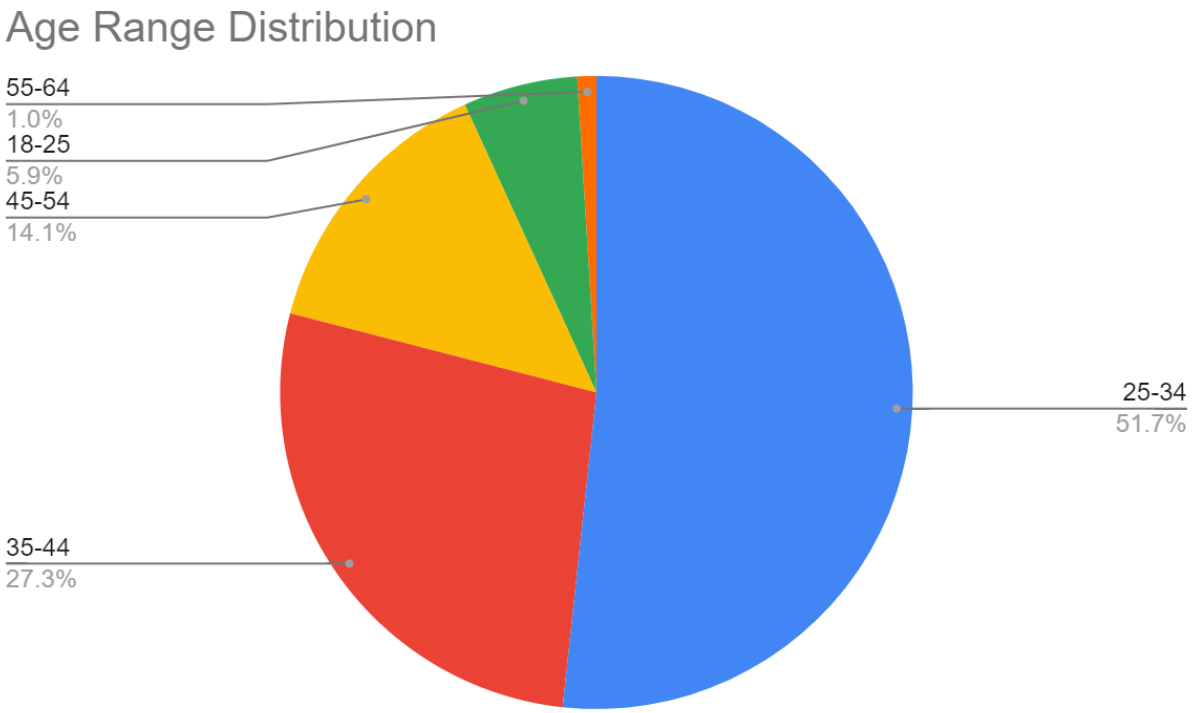
Survey Results

- Received 2400+ results. Filtered down to ~200 responses.
- Criteria
  - Duration: 5 mins or longer.
  - Years of smart contract experience: valid numerical or text description [Q9]
  - Open-Source resources used: text makes sense or is left blank [Q14]
  - Aware of security vulnerabilities: text makes sense or is left blank [Q20]
  - Imagine your dream tool: text makes sense or is left blank [Q21]
  - Code review tasks: if they answered Yes, they didn't answer No or N/A in the following fields

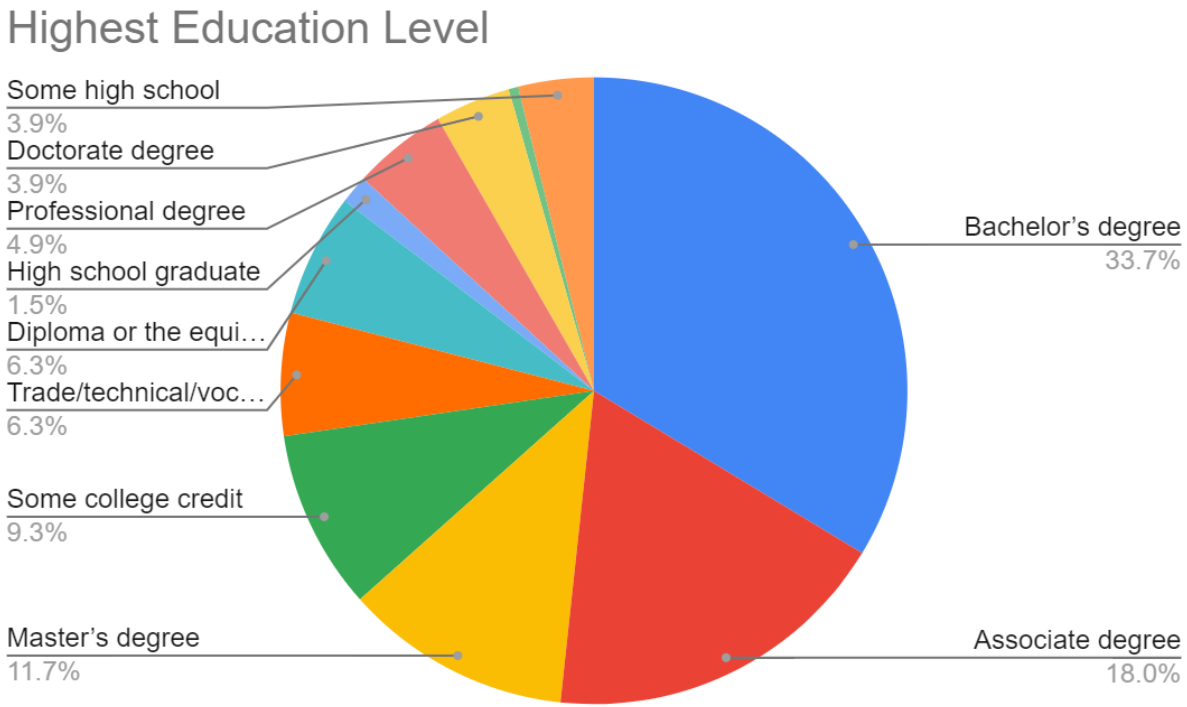
Gender



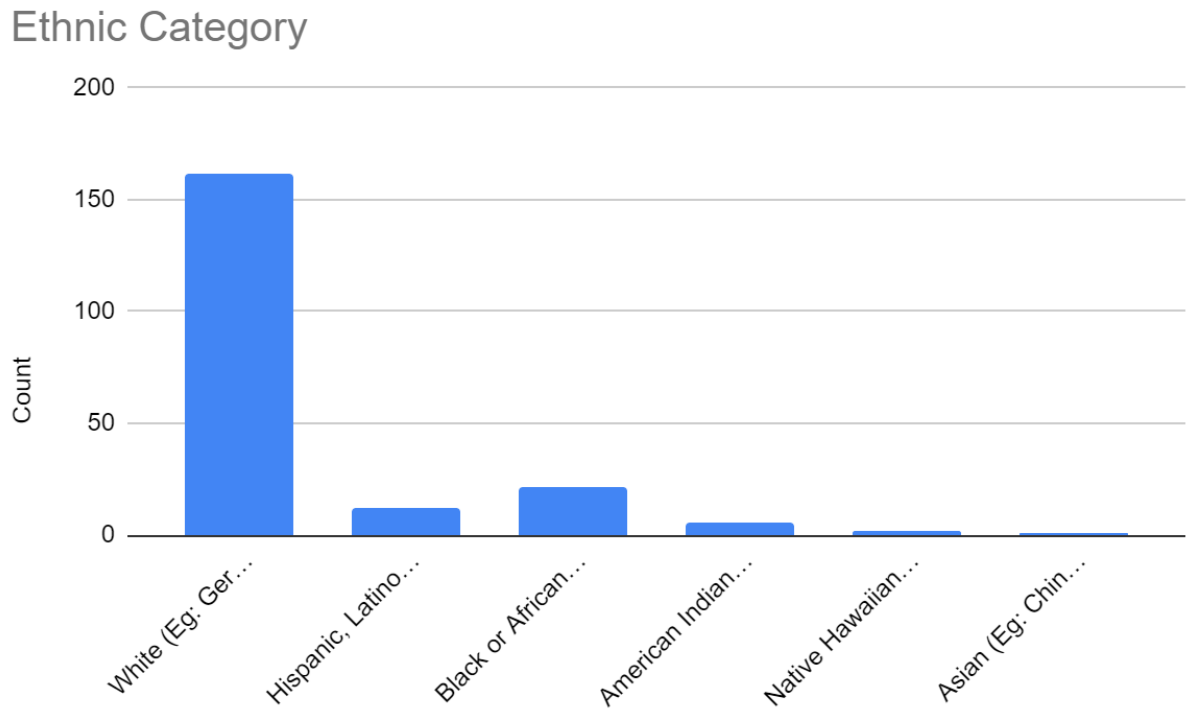
Age


Age Range Distribution
55-64
1.0%
18-25
5.9%
45-54
14.1%
25-34
51.7%
35-44
27.3%

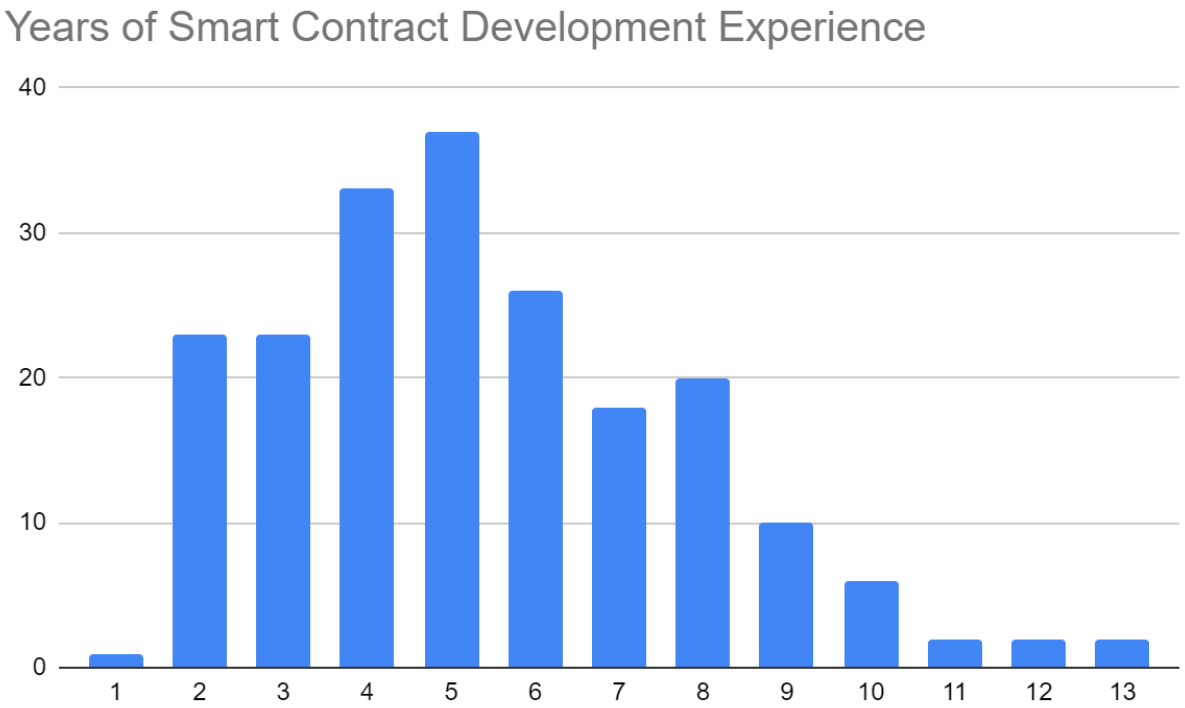
Education Level



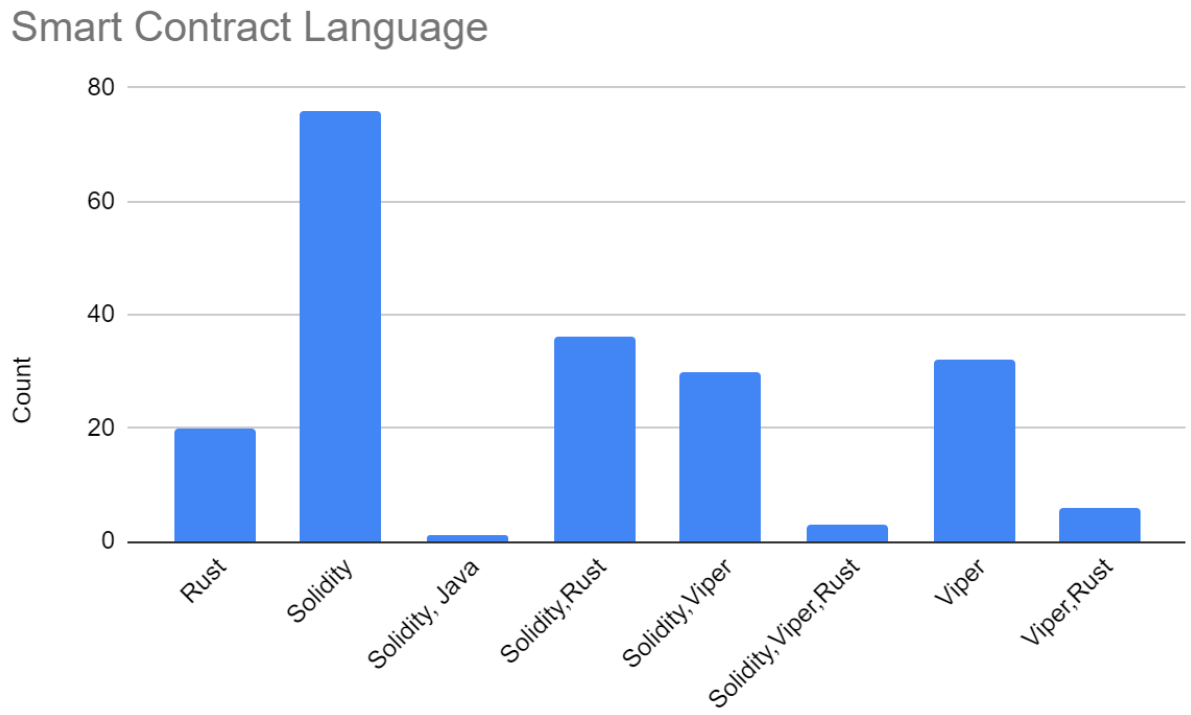
Self Identified Group



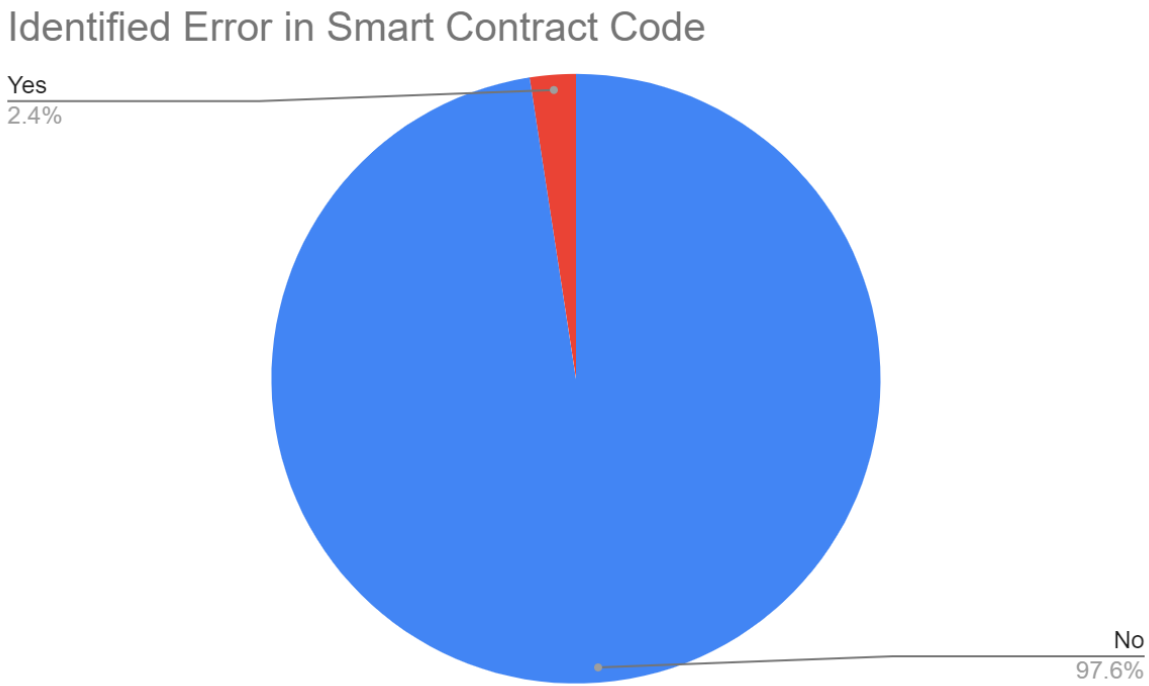
Experience in Smart Contract Development



Programming Language



Code Review Stats



Current Takeaways

- Security remains a secondary concern. Many developers were unaware of recent vulnerabilities and ranked other concerns as higher priority in developing a smart contract project
- Many developers don’t have experience with code reviews and are not able to identify security vulnerabilities
- We’ll be opening the survey again and posting to different groups to see if we can receive more detailed responses. Not being present to observe led to less detailed open answer results in code review questions