

# How to Audit Smart Contract Languages: Brief Intro

Nicolas Garcia

Let's Start with a

# Quick Poll



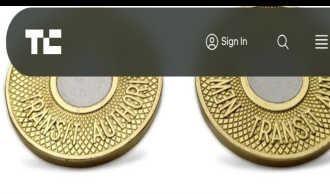
# Why Audit the Languages Themselves?



## Security Alert: Variables can be overwritten in storage

Posted by Christian Reitwiessner on November 1, 2016

SECURITY ALERTS



Overflow error shuts down token trading

John Biggs · 6:04 AM PDT · April 25, 2018

COINTELEGRAPH  
The future of money

\$ BTC \$67,981 | ETH \$2,408 | BNB \$554 >



TOM BLACKSTONE

MAY 16, 2023

**Libra-related Sui blockchain fixes critical bug that put 'billions' at risk**

COSMOS HUB FORUM [Sign Up](#) [Log In](#)

**[critical] EVM Precompiled contract bug allowing unlimited token mint**

Conversation Security

## Key Differences

- Focus Areas
- Complexity of Scope
- Severity & Risk Propagation
- Maintenance Aspects

# Some of the Things to Look For When Auditing a Smart Contract Language

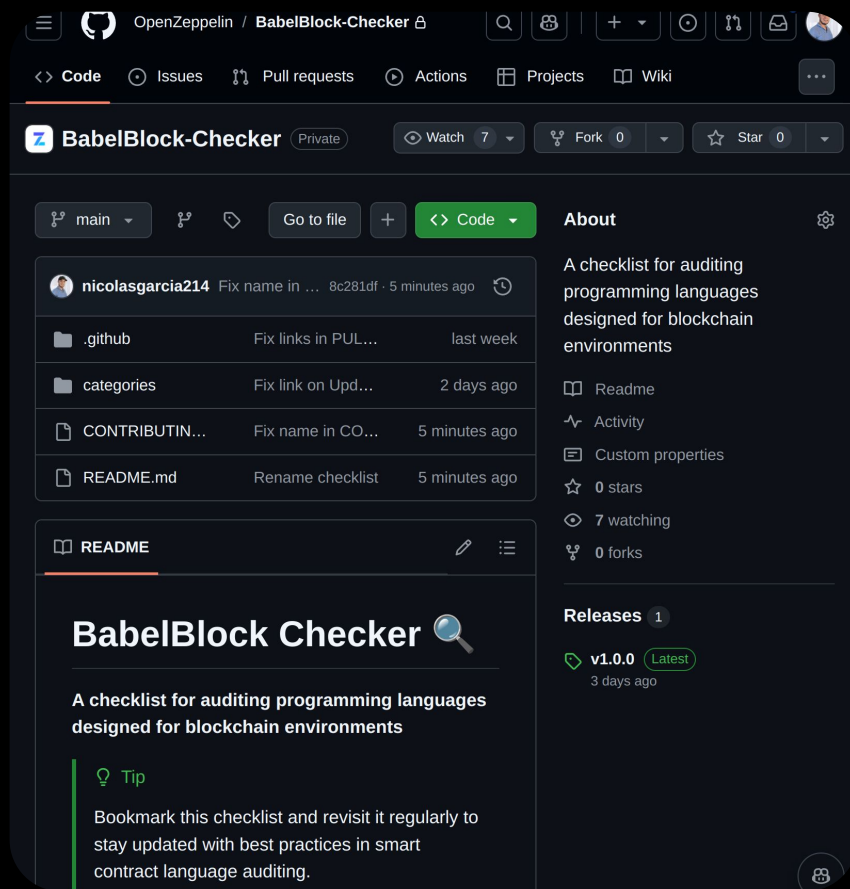
- Function Identifier Management
- Storage Layout Implementation
- Explicit State Mutability and Visibility Declarations
- Misleading or Undefined Keywords
- Undefined Behaviours
- Efficient Memory Allocation and Management
- Compiler Optimization Safety
- Integer Overflow/Underflow Protection
- Built-in Reentrancy Protection
- Non-deterministic execution
- Atomic Transactions and Error Handling
- Type system inconsistencies
- Up-to-date and Consistent Documentation

**...and many more!**

# BabelBlock Checker

## A Checklist for Auditing Smart Contract Languages

<https://github.com/OpenZeppelin/BabelBlock-Checker>



The screenshot shows the GitHub repository page for 'BabelBlock-Checker' by 'OpenZeppelin'. The repository is private and has 7 watchers, 0 forks, and 0 stars. The main content area displays the README file, which includes the title 'BabelBlock Checker' with a magnifying glass icon, a description 'A checklist for auditing programming languages designed for blockchain environments', and a 'Tip' section advising users to bookmark the checklist and revisit it regularly for updates on smart contract language auditing best practices. The right sidebar provides additional context, including the repository's description, a list of navigation links (Readme, Activity, Custom properties), statistics (0 stars, 7 watching, 0 forks), and a single release 'v1.0.0' labeled 'Latest' from 3 days ago.

File	Commit Message	Time Ago
.github	Fix links in PUL...	last week
categories	Fix link on Upd...	2 days ago
CONTRIBUTIN...	Fix name in CO...	5 minutes ago
README.md	Rename checklist	5 minutes ago

# Thank You

Nicolas Garcia  
@ngp2311

 OpenZeppelin

We're hiring! 🙋

