Welcome & Opening

Solidity Summit

Franziska Heintel
Solidity Team, Ethereum Foundation

Welcome to the Solidity Summit!

Welcome & Opening

#SoliditySummit

The Solidity Summit is a collaborative event focusing on the future of Solidity

- Get up to speed with the latest language proposals and new features
- Hear updates from Solidity tooling and security experts
- Learn from Solidity power users

Meet advanced Solidity users and other stakeholders of the Solidity ecosystem

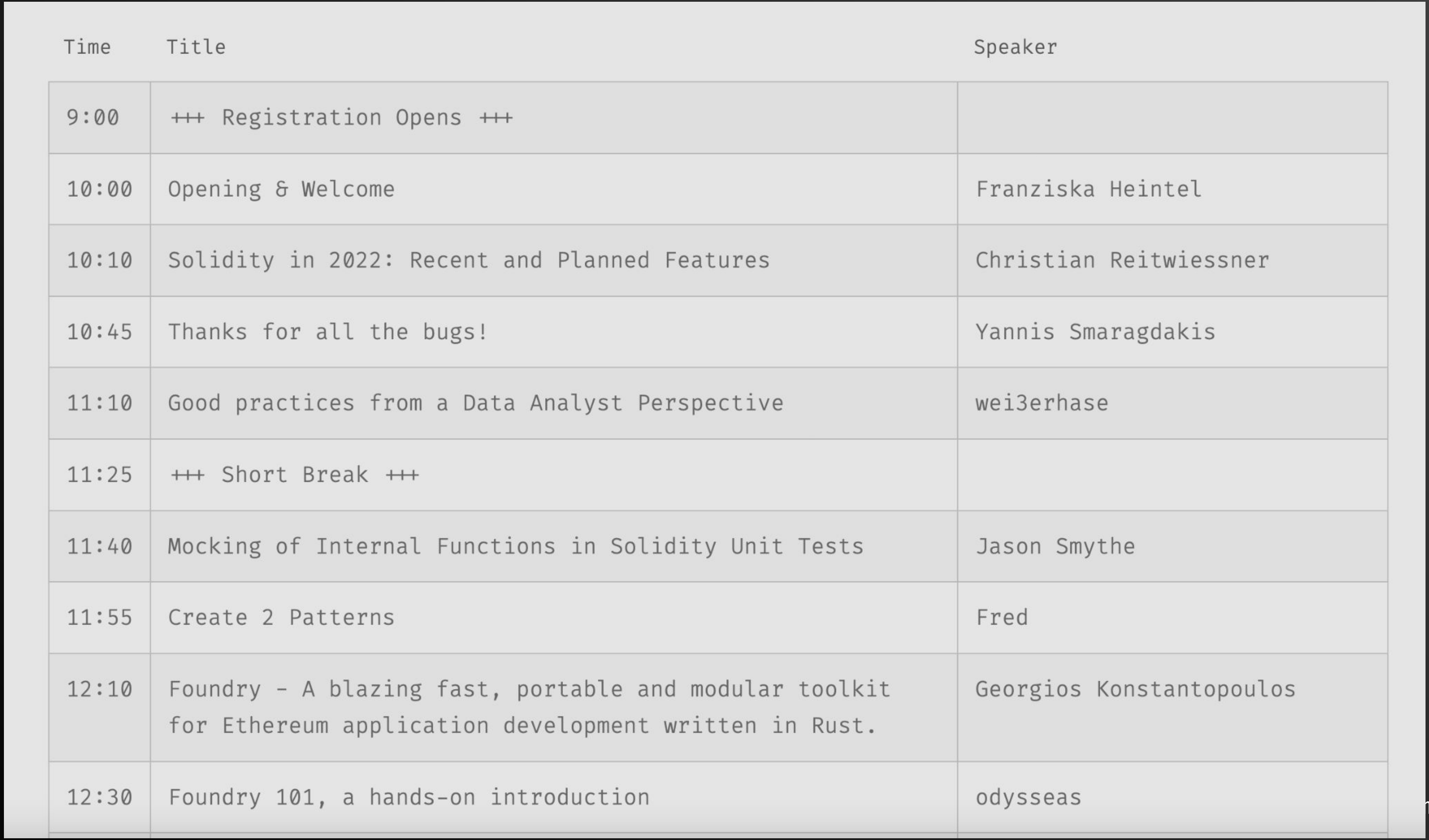
- **Solidity Language Shapers:** Present language improvement proposals and exchange ideas.
- **Tooling Builders & Auditors:** Use the opportunity to share your tools and what you've been working on with the audience.
- **Solidity Enthusiasts & Power Users:** Join, learn, network and share their best Solidity tips.

summit.soliditylang.org/agenda

→ schedule

→ speaker info

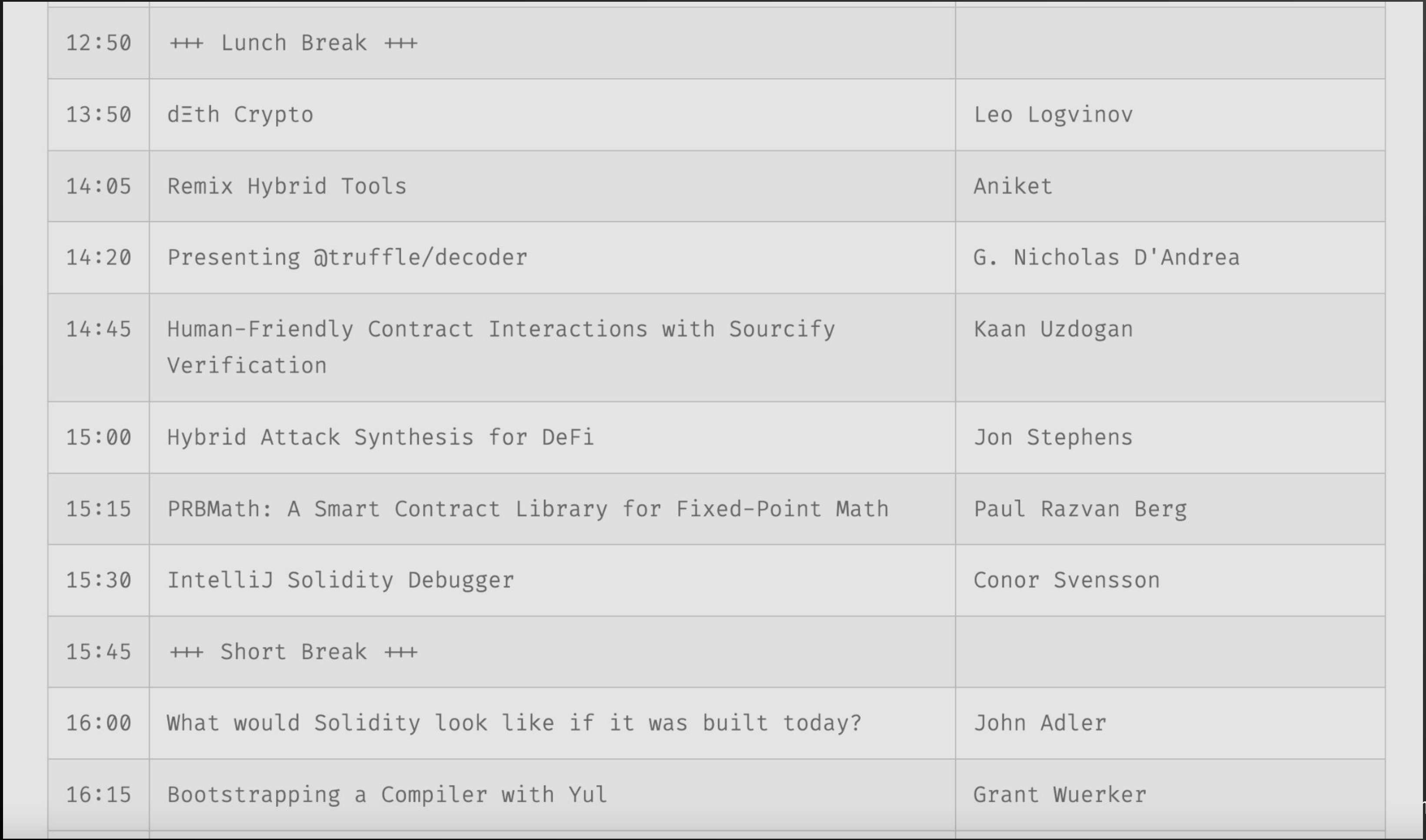
→ talk details



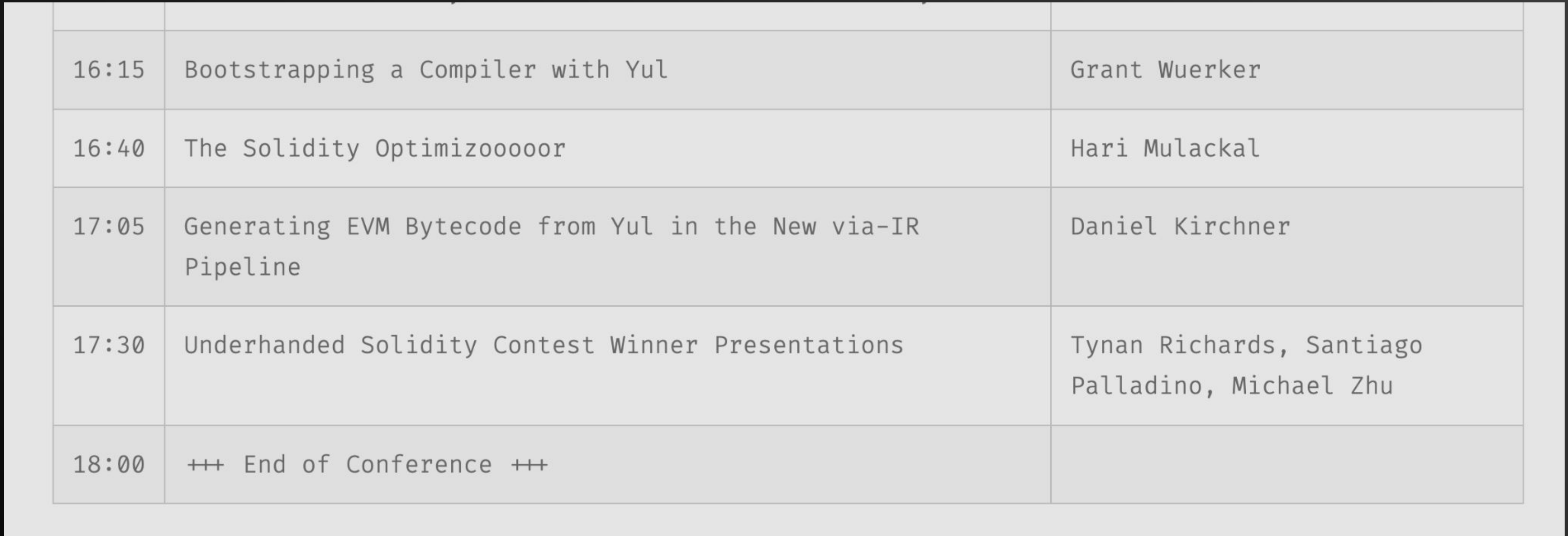
Time	Title	Speaker
9:00	+++ Registration Opens +++	
10:00	Opening & Welcome	Franziska Heintel
10:10	Solidity in 2022: Recent and Planned Features	Christian Reitwiessner
10:45	Thanks for all the bugs!	Yannis Smaragdakis
11:10	Good practices from a Data Analyst Perspective	wei3erhase
11:25	+++ Short Break +++	
11:40	Mocking of Internal Functions in Solidity Unit Tests	Jason Smythe
11:55	Create 2 Patterns	Fred
12:10	Foundry - A blazing fast, portable and modular toolkit for Ethereum application development written in Rust.	Georgios Konstantopoulos
12:30	Foundry 101, a hands-on introduction	odysseas

Solidity Summit

mmit



12:50	+++ Lunch Break +++	
13:50	dΞth Crypto	Leo Logvinov
14:05	Remix Hybrid Tools	Aniket
14:20	Presenting @truffle/decoder	G. Nicholas D'Andrea
14:45	Human-Friendly Contract Interactions with Sourcify Verification	Kaan Uzdogan
15:00	Hybrid Attack Synthesis for DeFi	Jon Stephens
15:15	PRBMath: A Smart Contract Library for Fixed-Point Math	Paul Razvan Berg
15:30	IntelliJ Solidity Debugger	Conor Svensson
15:45	+++ Short Break +++	
16:00	What would Solidity look like if it was built today?	John Adler
16:15	Bootstrapping a Compiler with Yul	Grant Wuerker



16:15	Bootstrapping a Compiler with Yul	Grant Wuerker
16:40	The Solidity Optimizooooor	Hari Mulackal
17:05	Generating EVM Bytecode from Yul in the New via-IR Pipeline	Daniel Kirchner
17:30	Underhanded Solidity Contest Winner Presentations	Tynan Richards, Santiago Palladino, Michael Zhu
18:00	+++ End of Conference +++	

A few do’s and don’ts @ Solidity Summit

DO!

- Respect the presenters and listen to their talks. :)
- Go to the second conference room to have discussions
- Wear a name badge
- Use the opportunity to have interesting convos and talk with as many bright minds as possible!
- Have a great time

PLEASE DON’T

- Talk in the main conference room, also no talks in the back please!
- Shill your project or token to people unsolicitedly. This is a technical conference not a networking event.
- Sit in the restaurant area.

POAP time!

- Find the QR code for the Solidity Summit 2022 POAP on the walls of the two conference rooms.

Have a **great day** and enjoy the upcoming talks and conversations!

Feel free to share any **feedback** you might have with me.

@_franzihei on Twitter
@franzihei on GitHub/Telegram/Matrix

Underhanded Solidity Contest Winners

Solidity Summit

Tynan Richards
Santiago Palladino
Michael Zhu

Seemingly innocent Solidity code which contains malicious behavior/backdoors

The Underhanded Solidity Contest aims to…

- Raise awareness about smart contract security.
- Uncover language design faults.
- Battle-test recently introduced language features and restrictions.
- Highlight anti-patterns in smart contact development.
- Establish new best practices for secure smart contract development.

Seemingly innocent Solidity code which contains malicious behavior/backdoors

- Each contest has a different theme or topic.
- This year, the task was to build a **decentralized exchange** that looks fair, but can be “manipulated”.
- In total, we received 19 submissions
- All submissions are at github.com/ethereum/solidity-underhanded-contest/tree/master/2022/submissions_2022
- Judges are presented with anonymized submissions

Huge thanks to our 2022 Judges

- Alex Beregszaszi, Solidity Co-Lead at Ethereum Foundation.
- Anton Permenev, Senior Engineer at ChainSecurity.
- Duncan Townsend, CTO at Immunefi.
- Gonçalo Sá, Security Engineer at ConsenSys Diligence.
- Harikrishnan Mulackal, C++ Engineer Solidity at Ethereum Foundation.
- Josselin Feist, Principal Security Engineer at Trail of Bits.
- samczsun, Research Partner at Paradigm.
- Stefan Beyer, Lead Auditor at Solidified.

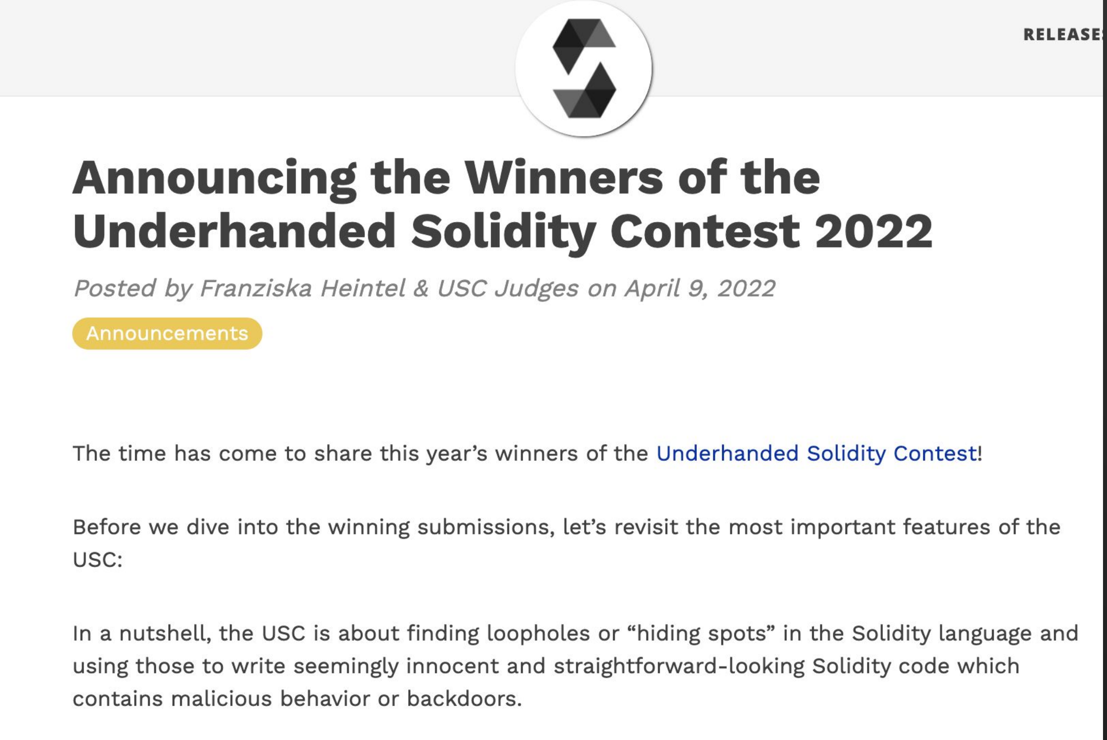
2022 Winners

Underhanded Solidity Contest

[1] Tynan Richards

[2] Santiago Palladino

[3] Michael Zhu



Announcing the Winners of the Underhanded Solidity Contest 2022

Posted by Franziska Heintel & USC Judges on April 9, 2022

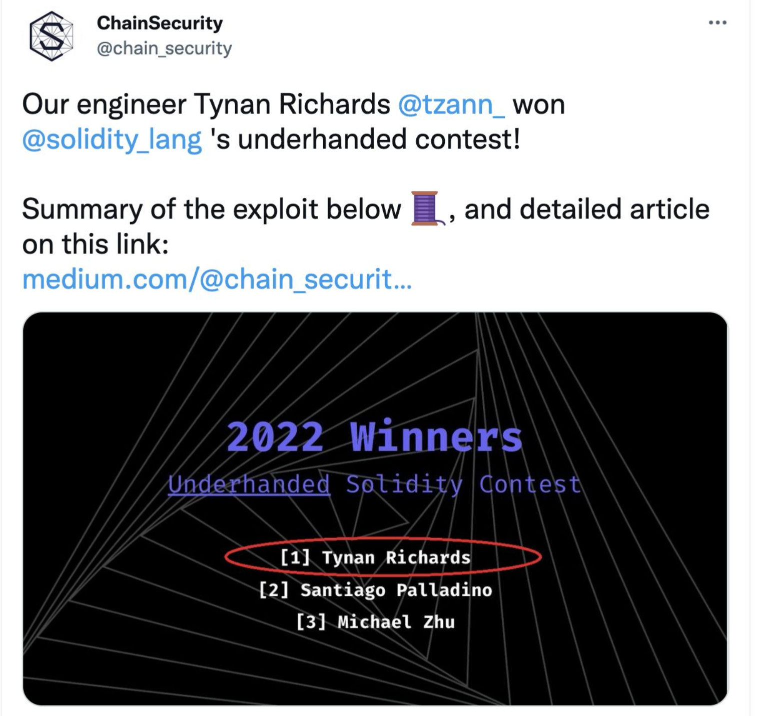
Announcements

The time has come to share this year's winners of the Underhanded Solidity Contest!

Before we dive into the winning submissions, let's revisit the most important features of the USC:

In a nutshell, the USC is about finding loopholes or "hiding spots" in the Solidity language and using those to write seemingly innocent and straightforward-looking Solidity code which contains malicious behavior or backdoors.

Underhanded Solidity Contest Winners



ChainSecurity
@chain_security

Our engineer Tynan Richards @tzann_ won @solidity_lang 's underhanded contest!

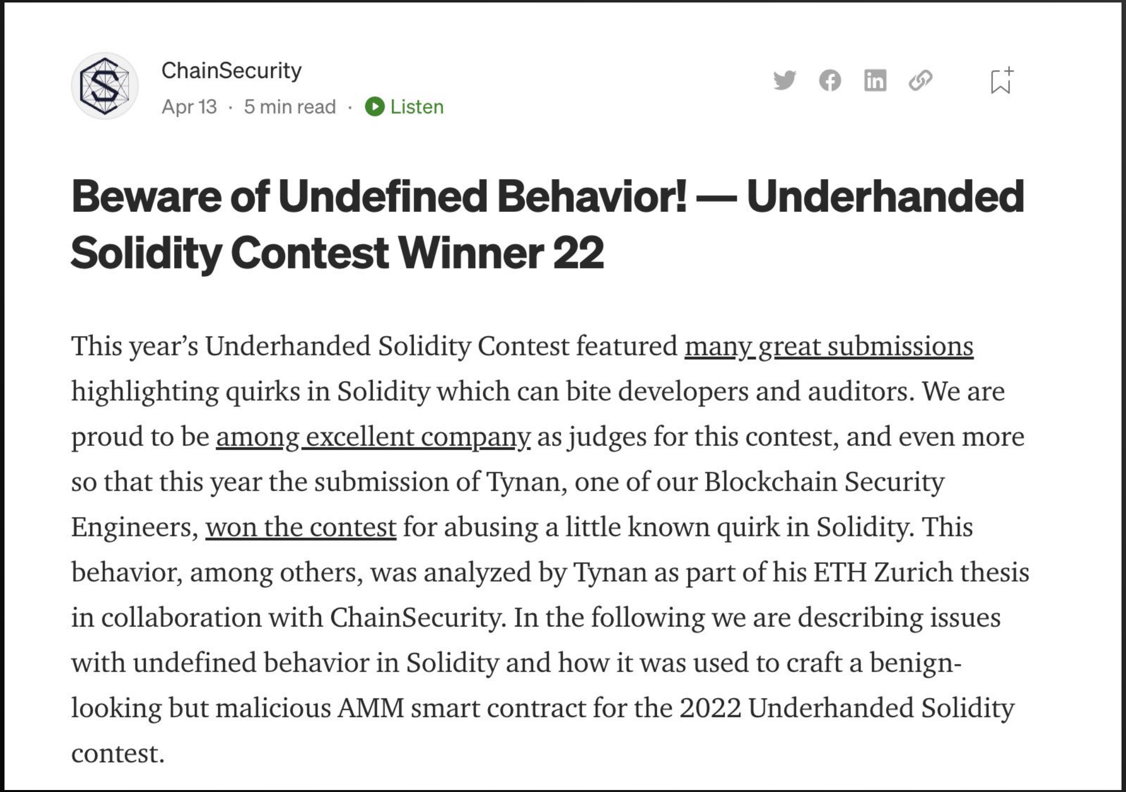
Summary of the exploit below 🧵, and detailed article on this link:
medium.com/@chain_securit...

2022 Winners

Underhanded Solidity Contest

[1] Tynan Richards
[2] Santiago Palladino
[3] Michael Zhu

- Order of evaluation is used to trick liquidity providers of a DEX.



ChainSecurity

Apr 13 · 5 min read · Listen

Beware of Undefined Behavior! — Underhanded Solidity Contest Winner 22

This year's Underhanded Solidity Contest featured many great submissions highlighting quirks in Solidity which can bite developers and auditors. We are proud to be among excellent company as judges for this contest, and even more so that this year the submission of Tynan, one of our Blockchain Security Engineers, won the contest for abusing a little known quirk in Solidity. This behavior, among others, was analyzed by Tynan as part of his ETH Zurich thesis in collaboration with ChainSecurity. In the following we are describing issues with undefined behavior in Solidity and how it was used to craft a benign-looking but malicious AMM smart contract for the 2022 Underhanded Solidity contest.