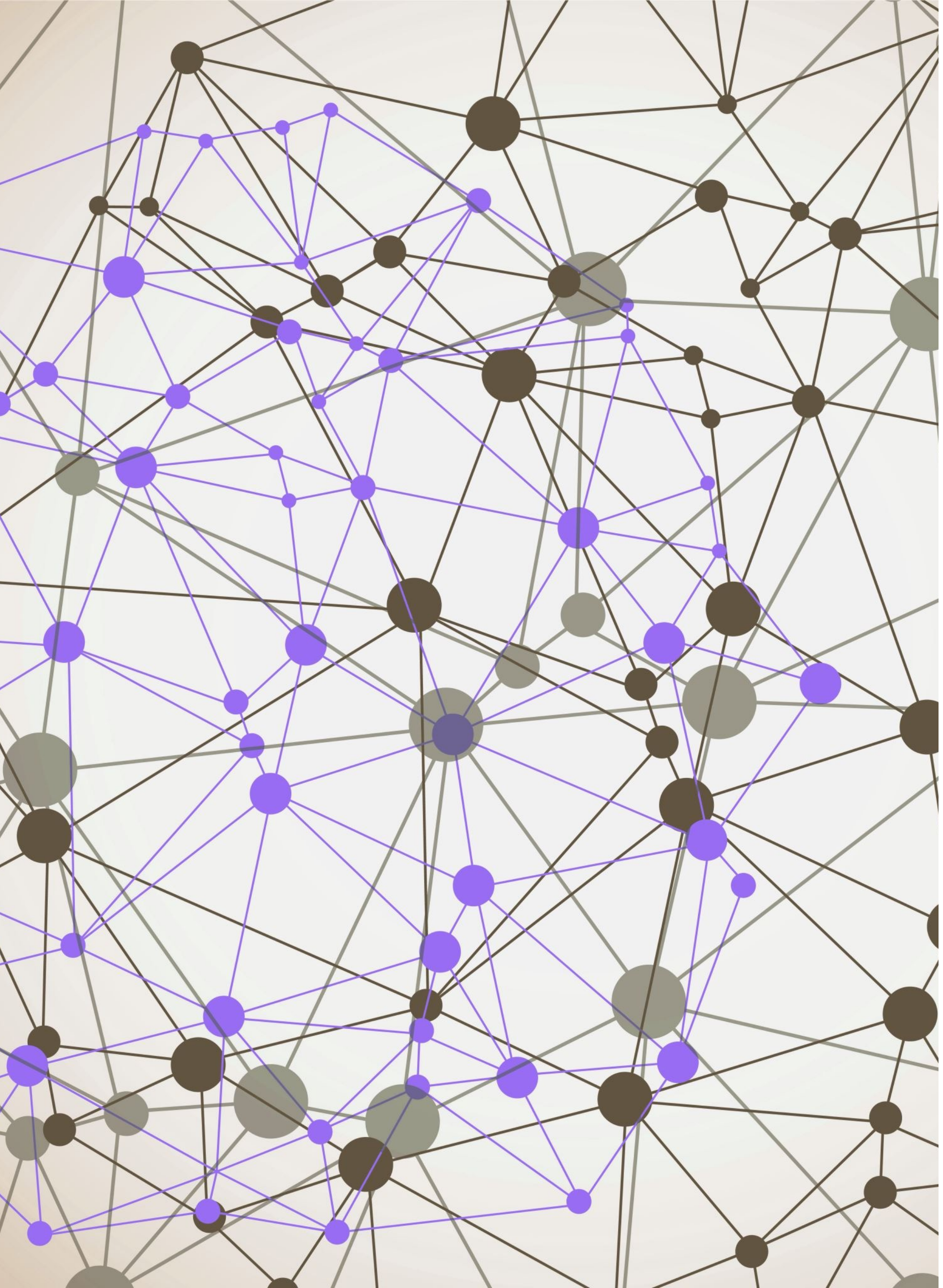
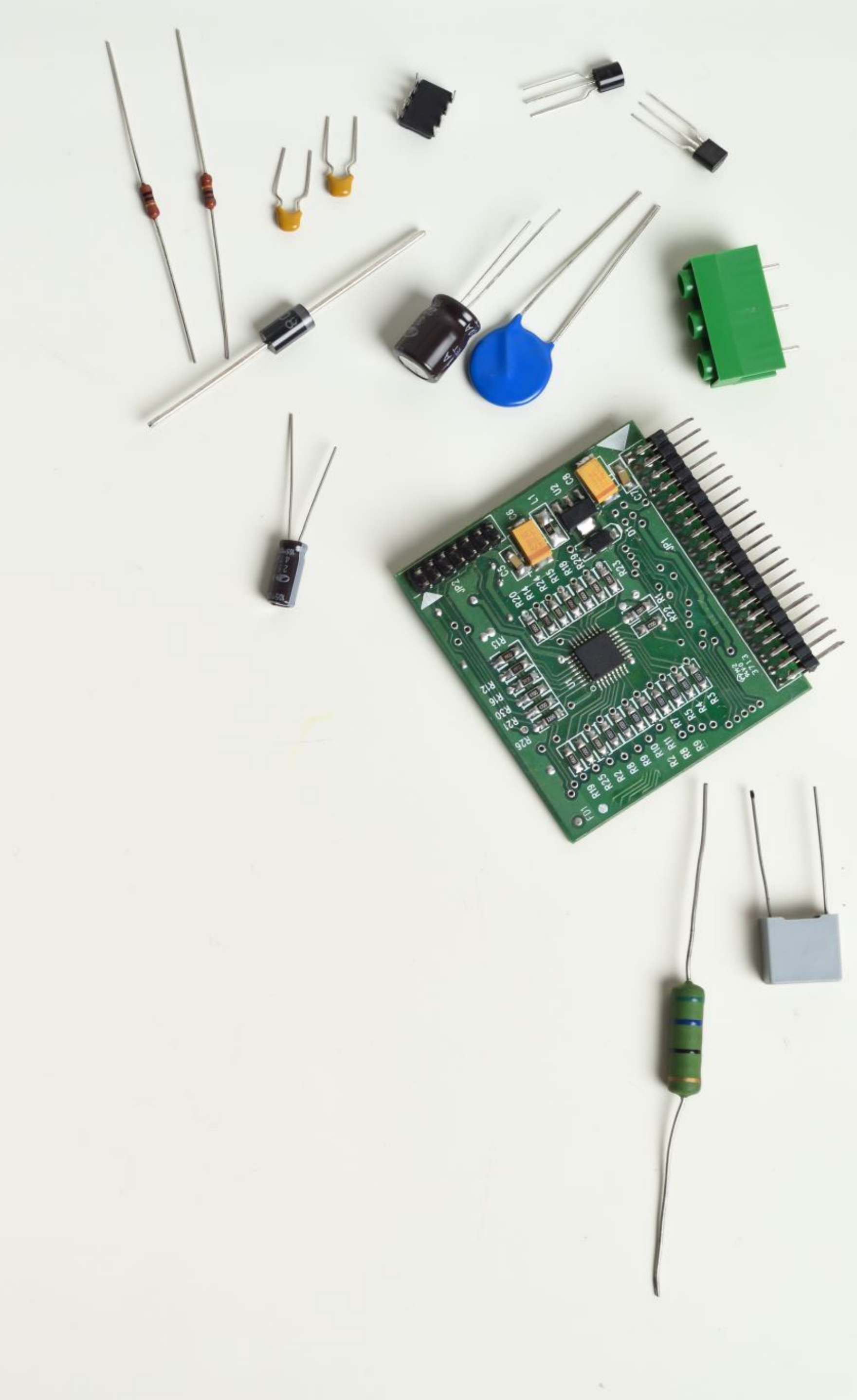


# Smart Contract Exploits and Automated Vulnerability Detection

Peter Ince <peter.ince1@monash.edu>,
Monash University



# Intro (me)

- PhD Candidate, Finding Vulnerabilities in Smart Contracts with AI
  - Blockchain Virtual Machines
  - Exploits
  - Static Analysis
  - Fuzzing
  - (toward) Fuzzing with DRL
- Request for you
  - Questions! Whether you type it in the chat or save it until the end, they are appreciated ☺

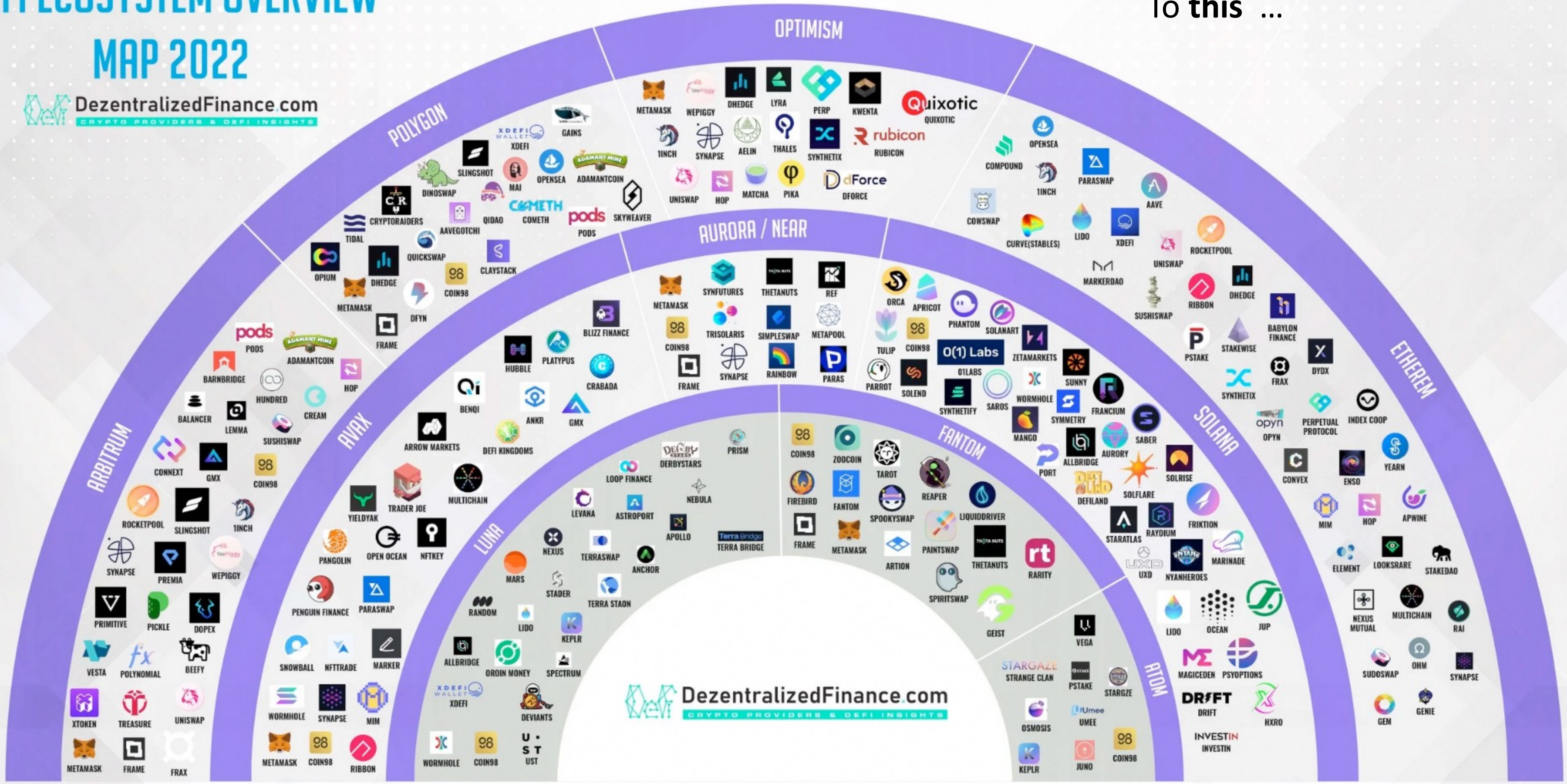
# Intro (talk)

- In a few years we have seen the growth of DeFi go from **this …**

To **this** …

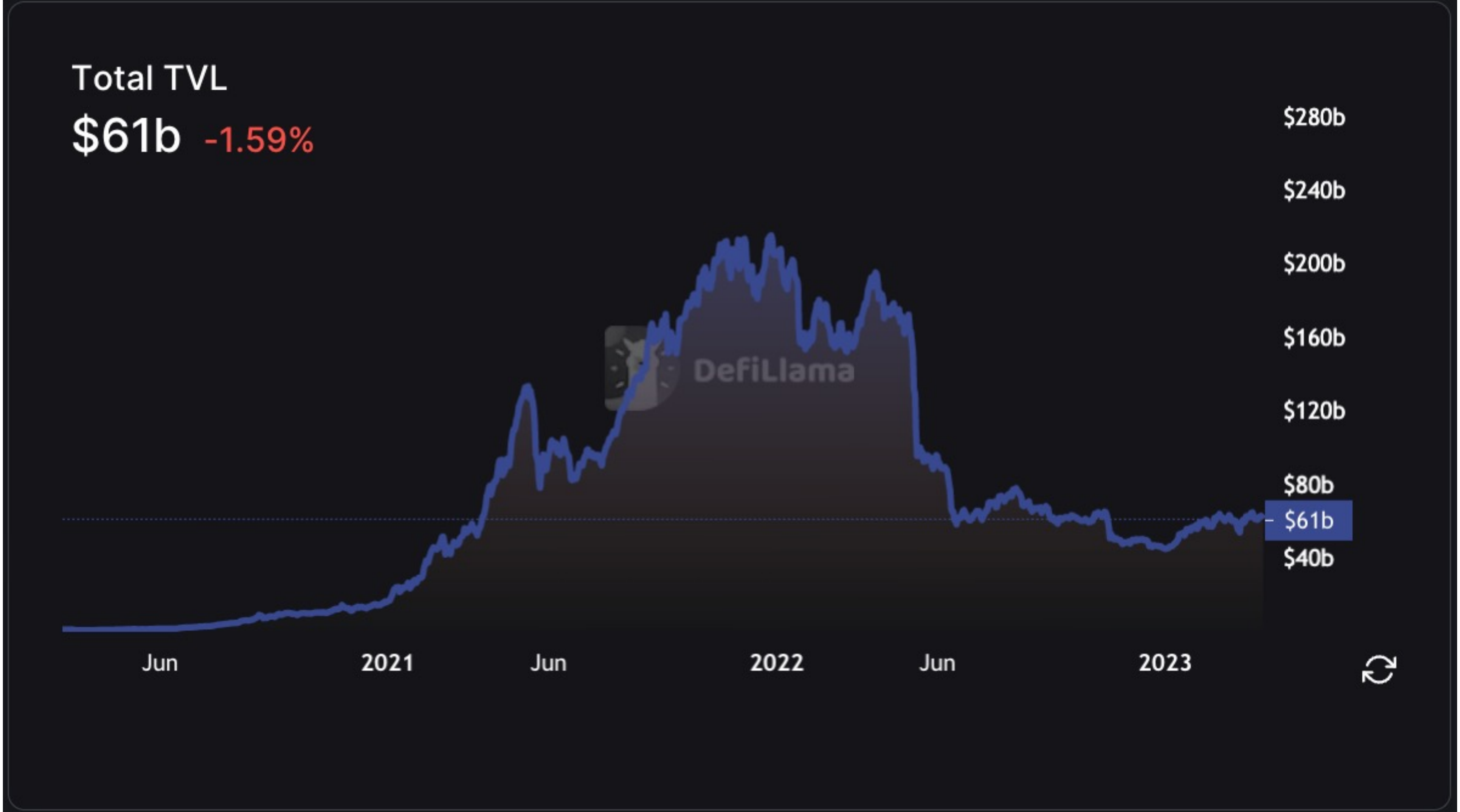
# DEFI ECOSYSTEM OVERVIEW MAP 2022

DezentralizedFinance.com
CRYPTO PROVIDERS & DEFI INSIGHTS



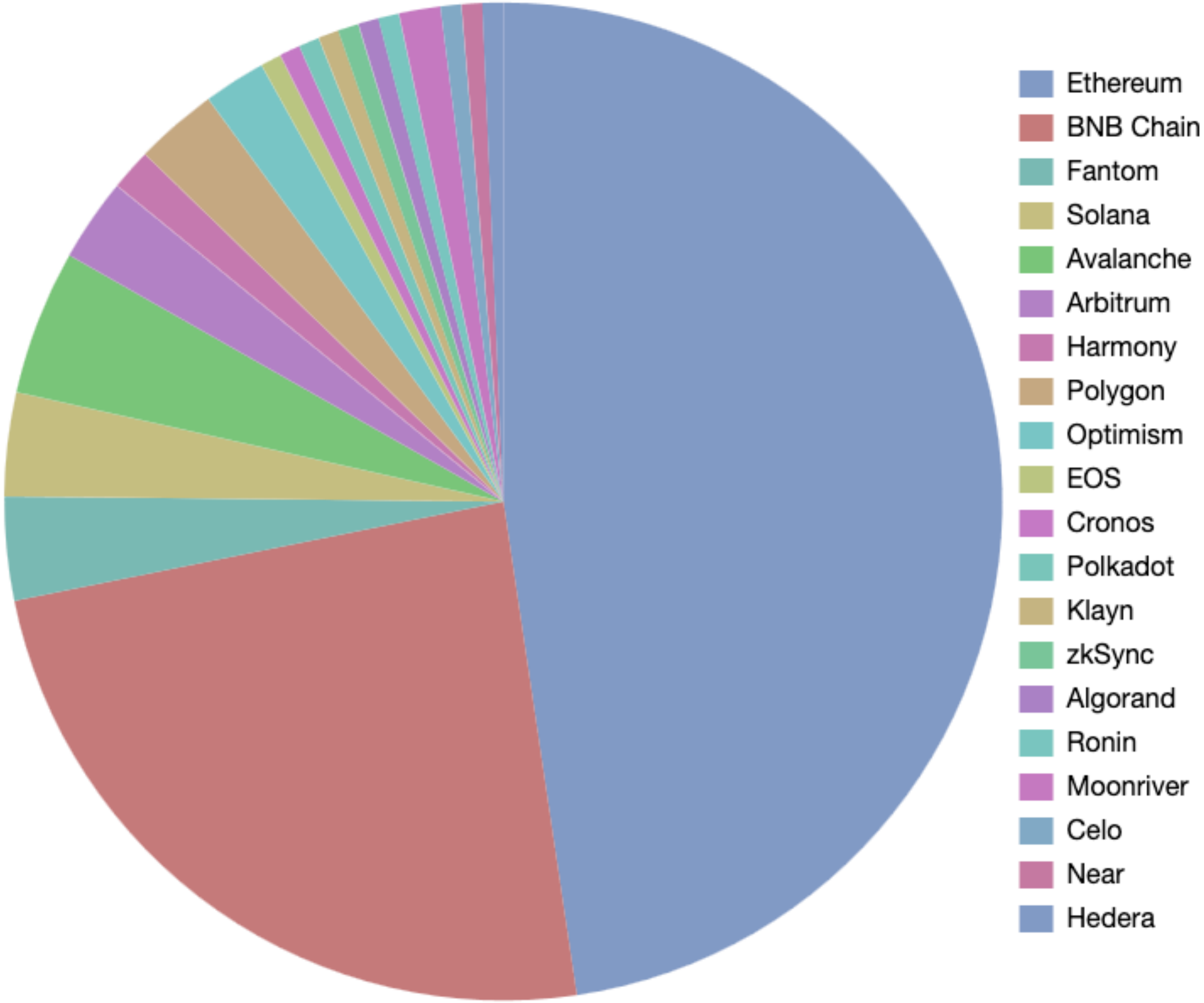
You are welcome to use this Crypto Map for free if you place a do-follow backlink onto my website as the original source.

**Contact:** info@dezentralizedfinance.com

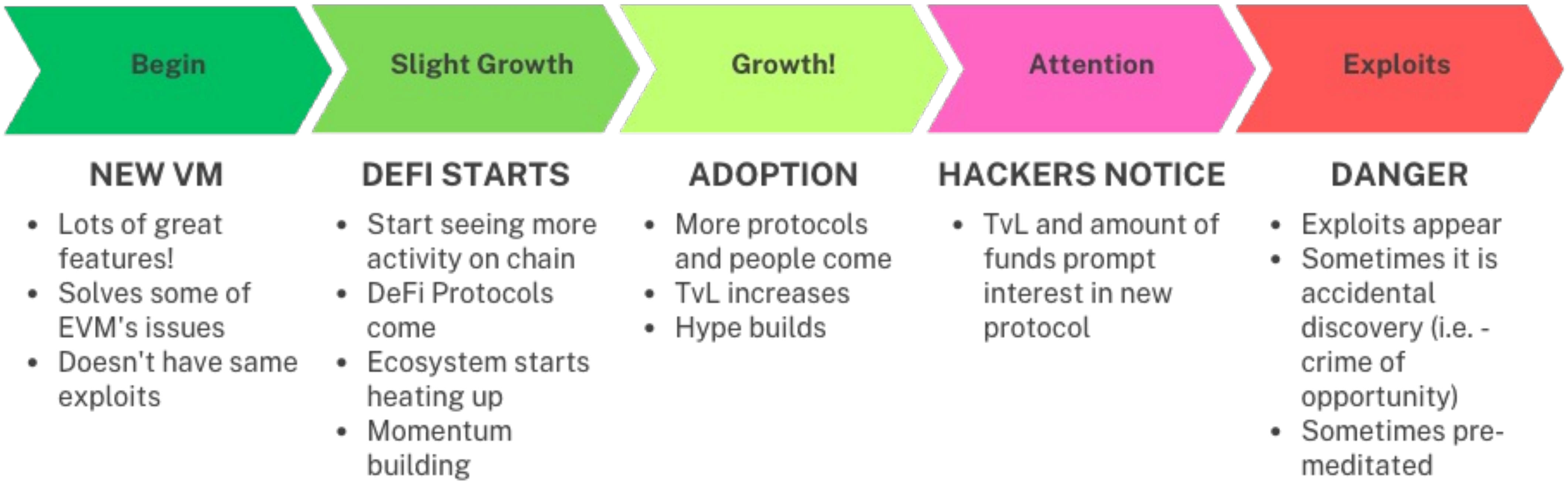

Total TVL
$61b -1.59%
$280b
$240b
$200b
$160b
$120b
$80b
$61b
$40b
DefiLlama
Jun
2021
Jun
2022
Jun
2023

# DeFi Exploits over time

- 148 Exploits[1]
- $4.28 billion



# New VM -> Exploit Pipeline



### NEW VM

- Lots of great features!
- Solves some of EVM's issues
- Doesn't have same exploits

### DEFI STARTS

- Start seeing more activity on chain
- DeFi Protocols come
- Ecosystem starts heating up
- Momentum building

### ADOPTION

- More protocols and people come
- TvL increases
- Hype builds

### HACKERS NOTICE

- TvL and amount of funds prompt interest in new protocol

### DANGER

- Exploits appear
- Sometimes it is accidental discovery (i.e. - crime of opportunity)
- Sometimes pre-meditated

# How can we find exploits before bad actors?

Auditing

Automated Vulnerability Detection

Often used together!

Trail of Bits has created some of the best tools in the space

# Background

# Blockchain Technology

You likely already have an awareness of or have seen so many great descriptions of what a blockchain is that this slide is redundant!

# Smart Contracts

(OFTEN) TURING COMPLETE PROGRAMS THAT OPERATE ON THE BLOCKCHAIN

(GENERALLY) OPEN AND TRANSPARENT

(TYPICALLY) SLOW AND EXPENSIVE COMPARED TO CENTRALIZED OPTIONS

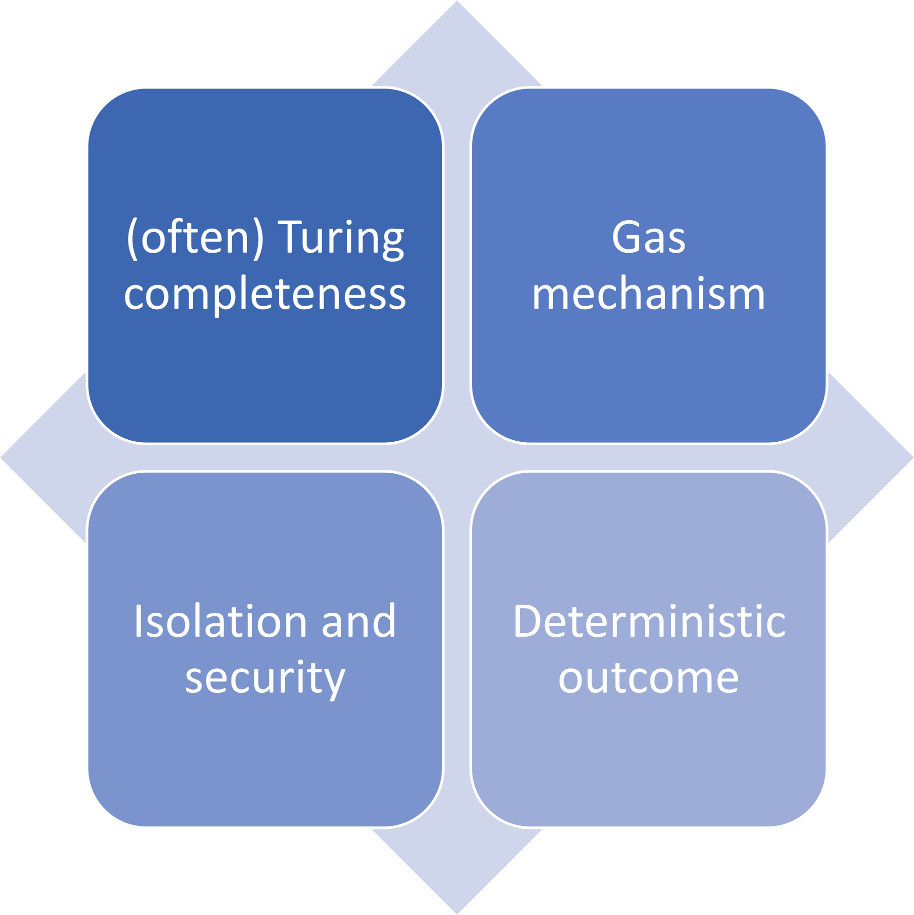
# Blockchain Virtual Machine(s)

What are Blockchain Virtual Machines?

Why are they important?

Role in executing smart contracts

# Blockchain VM Features



(often) Turing completeness

Gas mechanism

Isolation and security

Deterministic outcome

# Automated Vulnerability Detection

- Different tools are great at different things
- Static Analysis
- Dynamic Analysis
  - Fuzzing
  - Symbolic Execution
- Formal Verification

# Static Analysis Tools

- How do they work?
- Quick (relatively), cost-effective, no need for execution
- Examples
  - Slither, Smart Check, Tealer, and some of my own research

# Dynamic Analysis Tools

- How do they work?
- Key benefits: Execution-based, can identify runtime issues
- Examples
    - Echidna (Fuzzing)
    - Manticore, Mythril (Symbolic Execution)

# Formal Verification Methods

- How do they work?
- Key benefits: Mathematical proof of correctness, high confidence
- Examples
  - KEVM
  - CertiK

# Interesting approaches

- Now that we have seen the common approaches, here are some noteworthy approaches from the research.
- Please note:
  - These are just a few, there are so many great research directions and papers in this area!

# LSTM + Transfer Learning

“ESCORT: Ethereum Smart COntRacTs Vulnerability Detection using Deep Neural Network and Transfer Learning”[2]

  - Lutz et al., 2018

- Uses deep learning + transfer learning

“F1 score of 95% on six vulnerability types and the detection time is 0.02 seconds per contract”[2]

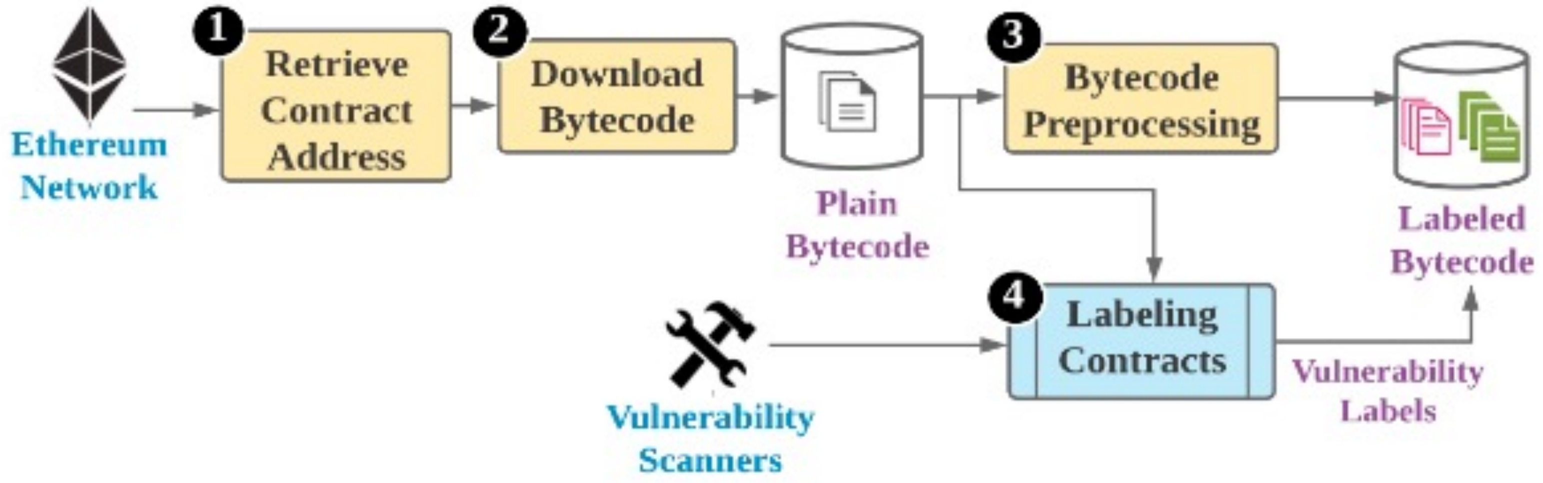


Figure 5: Generic workflow of ContractScraper for smart contract acquisition and labeling.

[2]

# Fuzzing + Deep Reinforcement Learning

“Effectively Generating Vulnerable Transaction Sequences in Smart Contracts with Reinforcement Learning-guided Fuzzing”[3]

  - Su et al., 2023

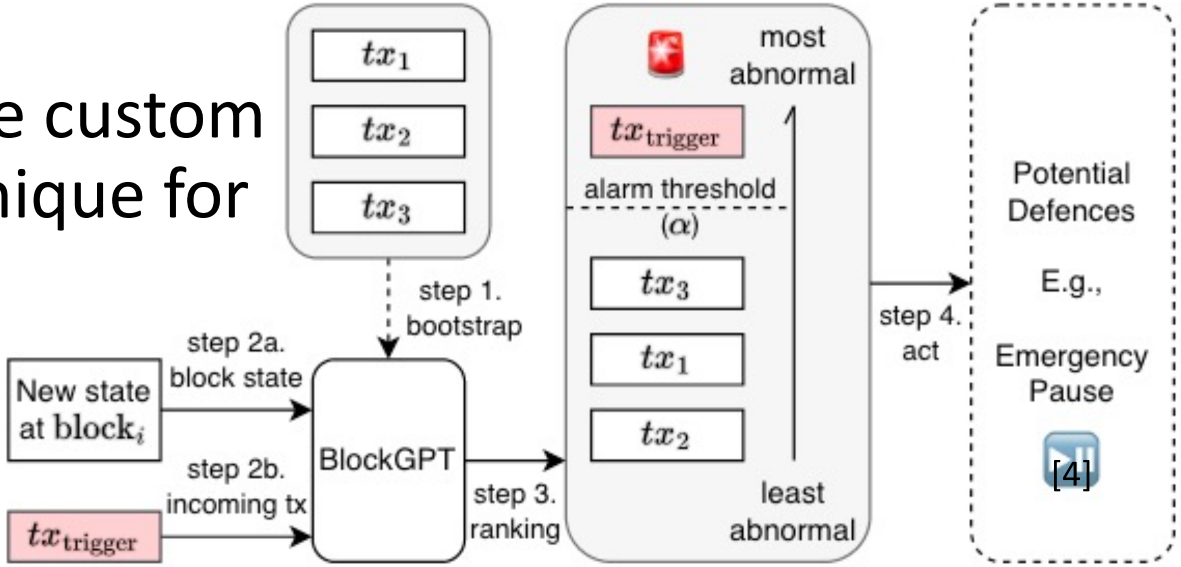
- Uses a reinforcement learning algorithm + reward functions considering both vulnerability and code coverage[3]
- Allows tool to generative effective transaction sequences faster
- Outperforms other state-of-the art tools in a 30-minute window (8-69% more vulnerabilities identified)

# LLMs for Anomaly Detection

"Blockchain Large Language Models"[4]

- Gai et al. , 2023

- BlockGPT, an LLM trained from scratch to act as a Intrusion Defense System[4]
- Meaningfully novel as they introduce custom data encoder and tokenization technique for the eco-system



[4]

# Questions?

# References

[1] - ChainSec. (n.d.). Comprehensive List of DeFi Hacks & Exploits. *ChainSec*. Retrieved 8 May 2023, from https://chainsec.io/defi-hacks/

[2] - Lutz, O., Chen, H., Fereidooni, H., Sendner, C., Dmitrienko, A., Sadeghi, A. R., & Koushanfar, F. (2021). ESCORT: Ethereum Smart COntRacTs Vulnerability Detection using Deep Neural Network and Transfer Learning. ArXiv:2103.12607 [Cs]. http://arxiv.org/abs/2103.12607

[3] - Su, J., Dai, H.-N., Zhao, L., Zheng, Z., & Luo, X. (2023). Effectively Generating Vulnerable Transaction Sequences in Smart Contracts with Reinforcement Learning-guided Fuzzing. *Proceedings of the 37th IEEE/ACM International Conference on Automated Software Engineering*, 1–12. https://doi.org/10.1145/3551349.3560429

[4] - Gai, Y., Zhou, L., Qin, K., Song, D., & Gervais, A. (2023). Blockchain Large Language Models (arXiv:2304.12749). arXiv. https://doi.org/10.48550/arXiv.2304.12749