10 / 01 / 2024

p l a i n t e x t

feat. Princeton Blockchain

#4 - Introduction to Web3 Security

Introductions!

Join the SIGNAL! -->

Introduce yourself:

- Name
- Where are you from
- Major and class year
- 1 other club/activity u do

Before we begin

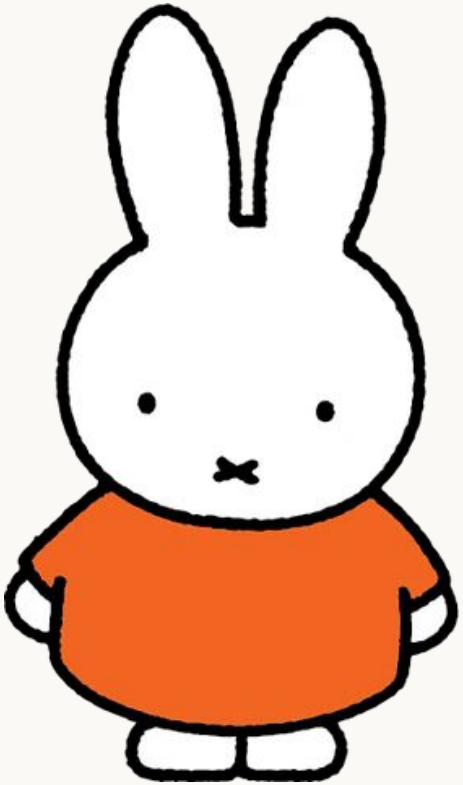
DeCenter Seminar: Towards Cryptographically Verifiable Randomness

Abstract: Public randomness has many important applications, from games and state lotteries to allocation of visas and public housing or assignment of judges to legal cases. Yet today, most of these applications provide little or no public verifiability. This talk will survey nearly ten years of work by the author on using cryptography to generate publicly verifiable randomness, including the development of verifiable delay functions and modern randomness beacon protocols based on them. It will also discuss the practical challenges in bringing these protocols into common use.

Tomorrow 4:30pm, Friend Center 113

Outline

- What is the blockchain?
- Ethernaut Intro
- Level 0 and 1 Demo
- Tips & Tricks
- Summary & Closing
- (just setup and a taster)



Blockchain? Huh?

Forget about blocks, mining, transactions

Blockchain is just **1 huge computer** in cloud

That belongs to no one - **decentralized**

Can upload programs to this computer,

and run other people’s programs

Wait Really? What about Bitcoin?

Bitcoin (2009) was just the beginning

Limited to sending bitcoin (money)

Ethereum (2015) is what's hot now.

Can send ether (money), but can

do so so so much more!

DogeCoin is just a blockchain program!

Blockchain Details

Can upload programs to this computer

= these are called **smart contracts (Solidity)**

Run other people's contracts, and

send ether to these contracts, and to other people!

Costs **ether** to run and upload! (Gas fee - important!)

Why is Web3 security so important?

Smart contracts are:

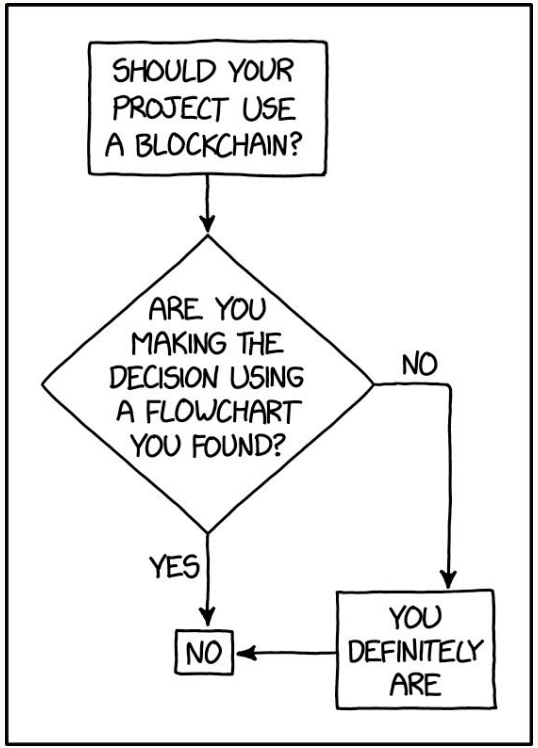
- **NOT SMART!** If programmer makes mistake *you're doomed*!
- binding contracts (can't remove it from blockchain)

Most contracts implement financial tools / systems,

so being able to hack them => 🤑🤑🤑

DPRK nuclear funding (600 million in 2023)

Any questions before we move on?



Ethernaut Intro

https://ethernaut.openzeppelin.com/

Series of vulnerable contracts (31)

To be able to learn about Web3 Security

Goes like this:

Read the Solidity code, find the bug,

steal the money, repeat!

Let’s get started!

1) Need Metamask Chrome extension

(to interact with blockchain)

2) Need some **testchain** (?) ether!

(to pay gas fees for interacting with blockchain)

Metamask

(◢_◣)

MetaMask account not connected

1) Download Metamask
2) Open Ethernaut and connect it to Metamask

ヽ(￣(ɪ)￣)ﾉ

Game not deployed

Currently the game supports only these networks:

- SEPOLIA
- OPTIMISM_SEPOLIA
- ARBITRUM_SEPOLIA
- HOLESKY
- AMOY

3) Make sure Ethernaut deploys on **sepolia-arbitrum**
4) Okay, now we just need some ether!

Getting TestChain Sepolia Ether

Try this faucet:

https://faucets.chain.link/

or Search “Chainlink Faucet”

Choose the right faucet!!!!!!

DRIPS 0.1 ETH

You need a Github account tho.

Now we can play! Any questions?

Tips and Tricks!

- Need help? Use help()!
- Numbers are strings for precision issues.
- Read the code very carefully and closely
- Google a lot!
- Think for a while before you look at solution!
- Solidity is hard? Try https://cryptozombies.io/

Summary

- What is the blockchain?
- Ethernaut Intro
- Level 0 and 1 Demo
- Tips & Tricks
- Summary & Closing

References and Resources

- https://rekt.news/ (Blockchain security news)
- https://www.damnvulnerabledefi.xyz/ (Harder challenges)
- https://code4rena.com/ (competitive Web3 security)

Thanks for coming :)