



# \$whoami

- > Background: infosec & Bitcoin <3
- > CCTF founder -> CTFs, audits, hackathons
- > Polkadot Head Ambassador -> Onboarding Project
- > Does what he loves.



What the web3 aka...

Reverse engineering buzzwords

& the hype

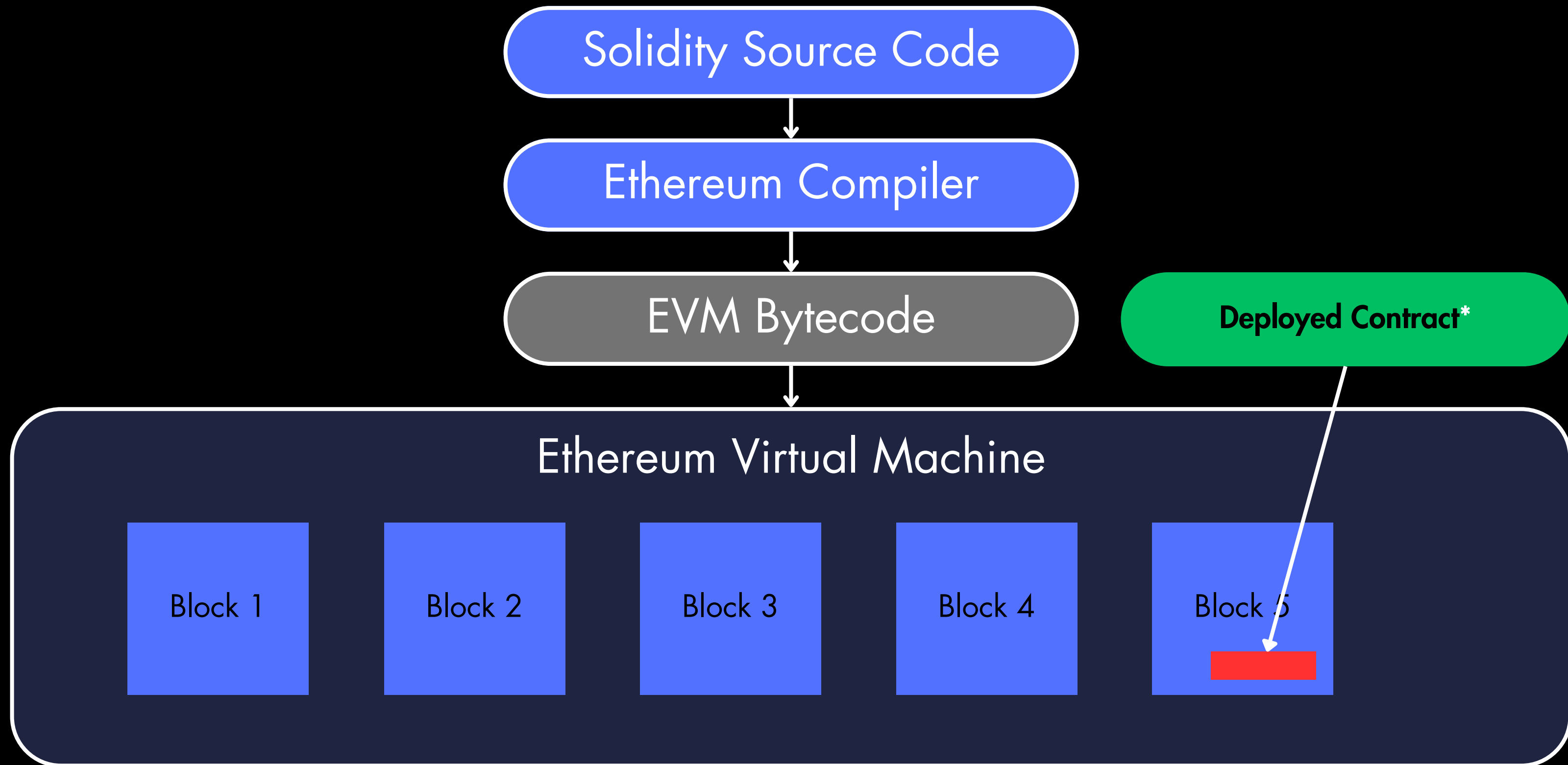
proof of deposit bridge swap remix ide  
token DeFi crypto dApp decentralized  
bridge web3 coin crypto wallet substrate  
blockchain metaverse solidity. javascript 🤖  
smart contract tx wrapped coin  
signing

# Introduction to blockchain technology

- Cryptography
- CryptoCurrency
- Private and public keys
- Wallets
- Consensus
- Transactions
- PoW vs PoS

# Introduction to blockchain technology

- Transparency and security
- Web2 API vs Substrate connect
- EVM
- Substrate FRAME



\*You need ABI or source code for call or you are blind.

# ECDSA signature in TX

```
▼ Object {blockHash: "0x0000000000000000000000000000000000000000000000000000000000000000"
  blockHash: "0x0000000000000000000000000000000000000000000000000000000000000000"
  blockNumber: null
  from: "0x07a204163f78bf9293c996f8c6d98a058a324b2d"
  gas: 0
  ► gasPrice: BigNumber
  hash: "0x052b383a8df2f0f976d1061a586c044dd069a19bcc0f94a1372fbd0542e7aba3"
  input: "0xf58d98e5000000000000000000000000000000000000000000000000000000000000000007a204163f78bf9293c996f8c6d98a058a324b2d"
  nonce: 7
  r: "0x605a72142e7df38dfd6815aaf9d8fa8a02d3f36b0cc89e04a31ed11917582cca"
  s: "0x930199337f06f470279f560bbd09a27e5c8dd0bd892b6953424c076fb5d181a"
  to: "0xefcc9f9a5cb3d6062c18eefdf90a29bb771fccc"
  transactionIndex: null
  v: "0x1b"
  ► value: BigNumber
```

# Practice with Solidity

- What is this? How?
- Remix IDE
- Deploy code in browser
- Explanation of code
- Visibility
- Security
- Interact with the functions

DCTF: <https://git.hsbp.org/CCTF/DCTF>

EthKeygen: [https://git.hsbp.org/six/eth\\_keygen](https://git.hsbp.org/six/eth_keygen)



# Problem?

CCTF article and PoC: <https://cryptoctf.org/2022/09/11/writeup-of-flag-submission-forgery-by-si/>

ECDSA Malleability: <https://coders-errand.com/malleability-ecdsa-signatures/>

Note: valid for not just ECDSA, but for ElGamal-type digital signatures generally.

# Challenge for CCTF entry

**Contract:** On Moonbase Alpha from Polkadot

<https://moonbase.moonscan.io/address/0x70f0cec3c99103113d96ed8ad82ae6a8d9a735a0>

**Contest ID:** 2023

**Challenge ID:** 0

**Flag pub key:** 0x7E5F4552091A69125d5DfCb7b8C2659029395Bdf

**Q & A**

~~Pizza & Drinks~~

# Thank you && Q&A



sixthedave.me

six@cryptoctf.org

