Pwn with CCTF

author : six

$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

crypto

token

DeFi

dApp

decentralized

coin

crypto wallet

bridge

web3

substrate

javascript 😱

metaverse

solidity

blockchain

tx

wrapped coin

smart contract

signing

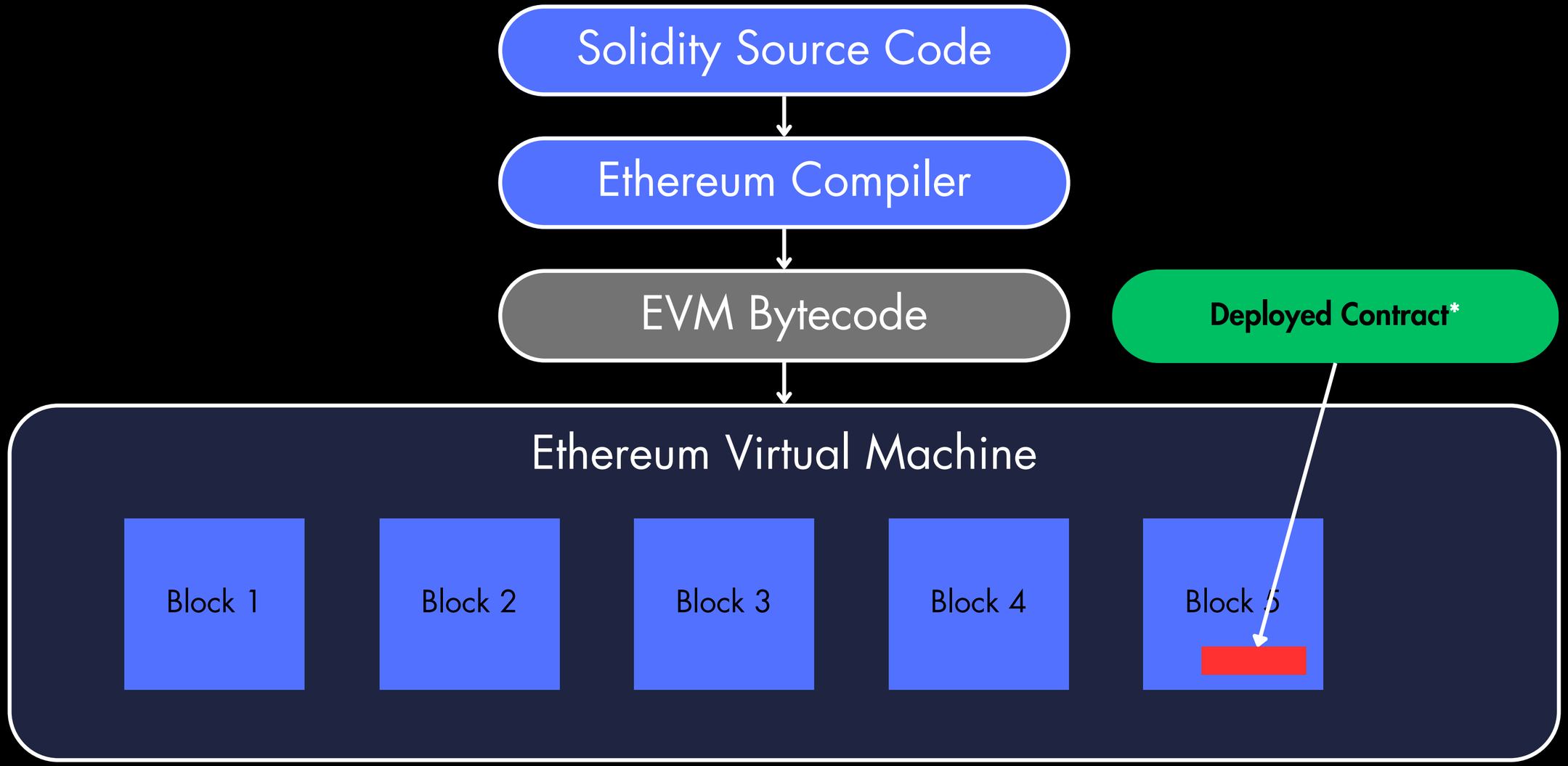
Introduction to blockchain technology

- Cryptography
- CryptoCurrency
- Private and public keys
- Wallets

- Consensus
- Transactions
- PoW vs PoS

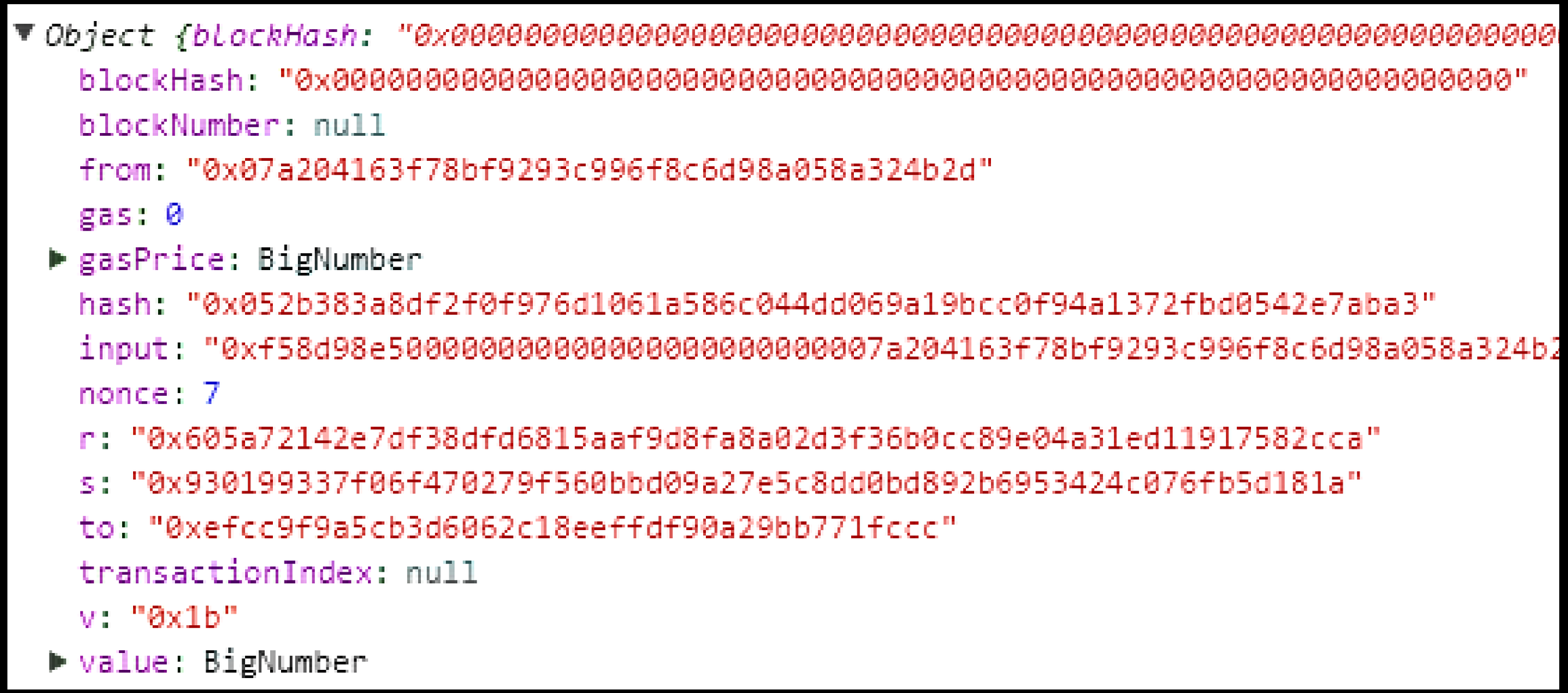
Introduction to blockchain technology

- 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



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

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