From Solidity to Substrate

When? Why? Who and how?

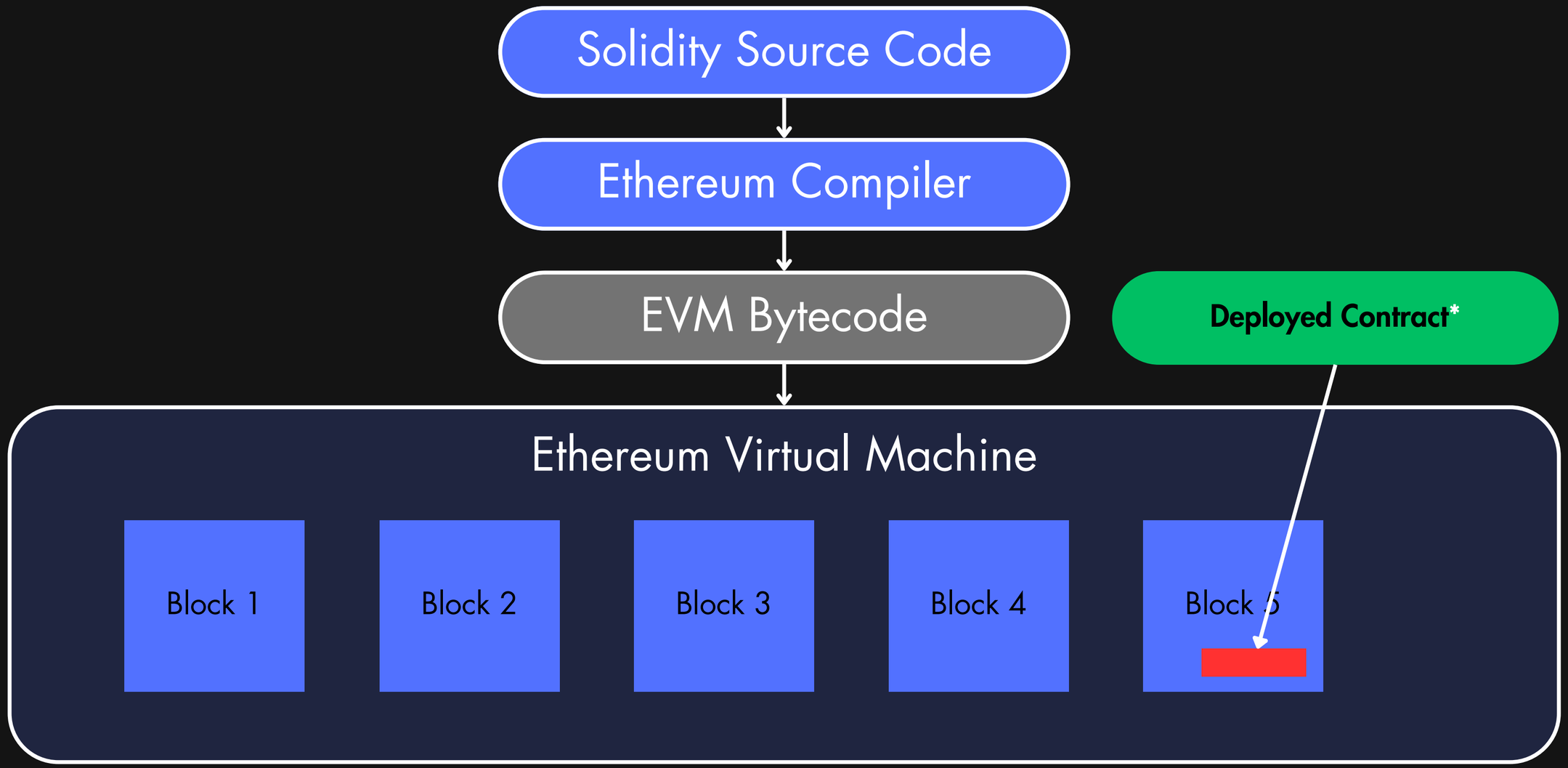
Introduction to blockchain technology

- 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



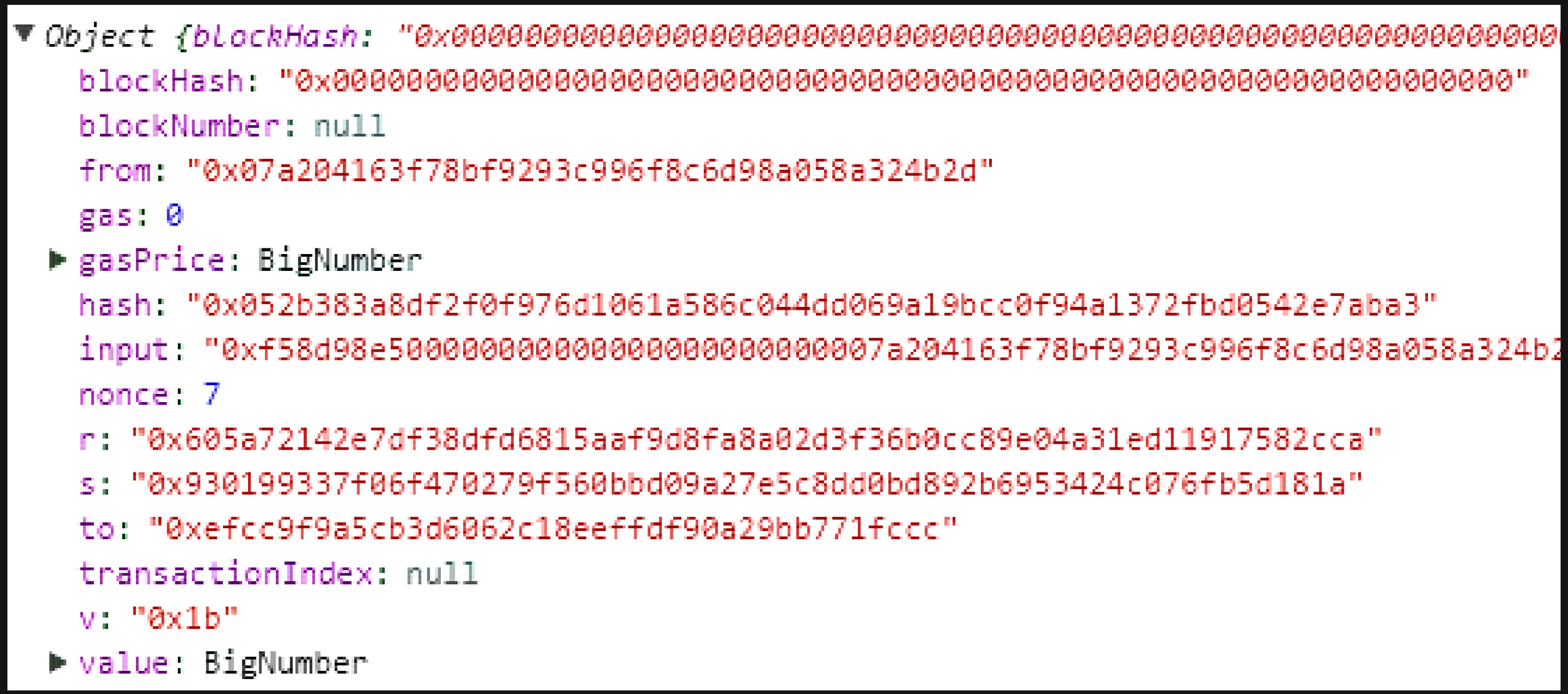
*You need ABI or source code for call or you are blind.

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

ECDSA signature in TX



Problem?

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

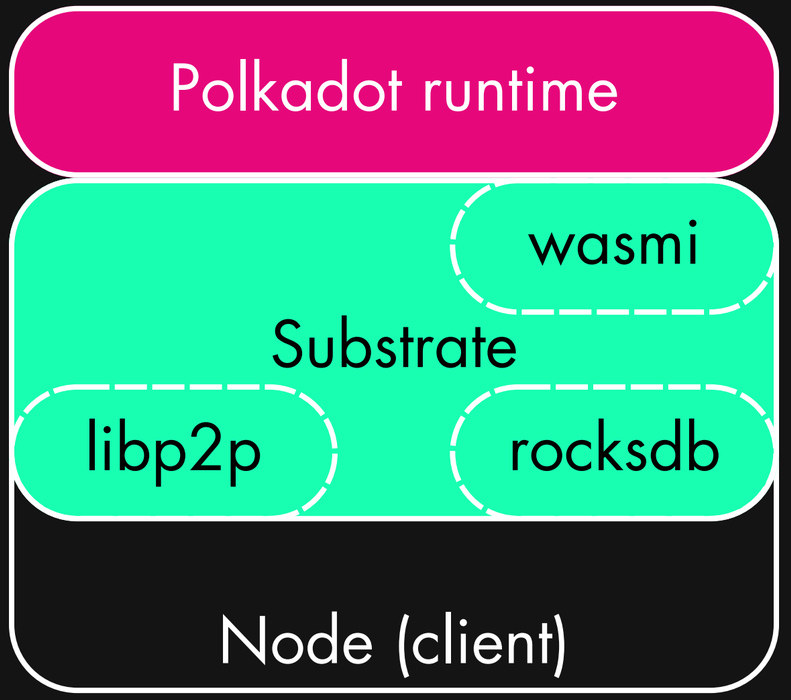
ECDSA Malleability: https://coders-errand.com/malleability-ecdsa-signatures/

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

15 mins break

Pizza & Drinks

Substrate FRAME



Substrate

- Rust programming language
  - Pretty good support for cryptography
  - Fast, Reliable, Productive. Pick Three.
  - Functional subset for pallet writing
- WASM Runtime: On-chain upgradable logic
- Democracy: Lessens the chances of a hard-fork

Substrate

- Pallets: Ready-made building blocks
- Networking built on top of libp2p
- Parachains secured by value staked on Polkadot
    - Sharding by use-cases, not just randomly

Create our own pallet - PoC

- Storage: map for account and its points
- Storage: map for challenges and their points
- Function: Submit flag
    - If valid, increase player point
- Internal function: check flag
- Function: Check my points

Bonus task: how to protect against replay attack?

Practice: Build your own blockchain

Thank you && Q&A

sixthedave.me

Polkadot

mosaic ALPHA

DCTF