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
- sus tions 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

- blockNumber: null
 - from: "0x07a204163f78bf9293c996f8c6d98a058a324b2d" gas: 0
 - gasPrice: BigNumber hash: "0x052b383a8df2f0f976d1061a586c044dd069a19bcc0f94a1372fbd0542e7aba3" input: "0xf58d98e5000000000000000000000000000007a204163f78bf9293c996f8c6d98a058a324b2 nonce: 7
 - r: "0x605a72142e7df38dfd6815aaf9d8fa8a02d3f36b0cc89e04a31ed11917582cca"
 - s: "0x930199337f06f470279f560bbd09a27e5c8dd0bd892b6953424c076fb5d181a"
 - to: "0xefcc9f9a5cb3d6062c18eeffdf90a29bb771fccc" transactionIndex: null
 - v: "0x1b"
 - value: BigNumber

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

- 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
- ography k Three. riting dable logic 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











