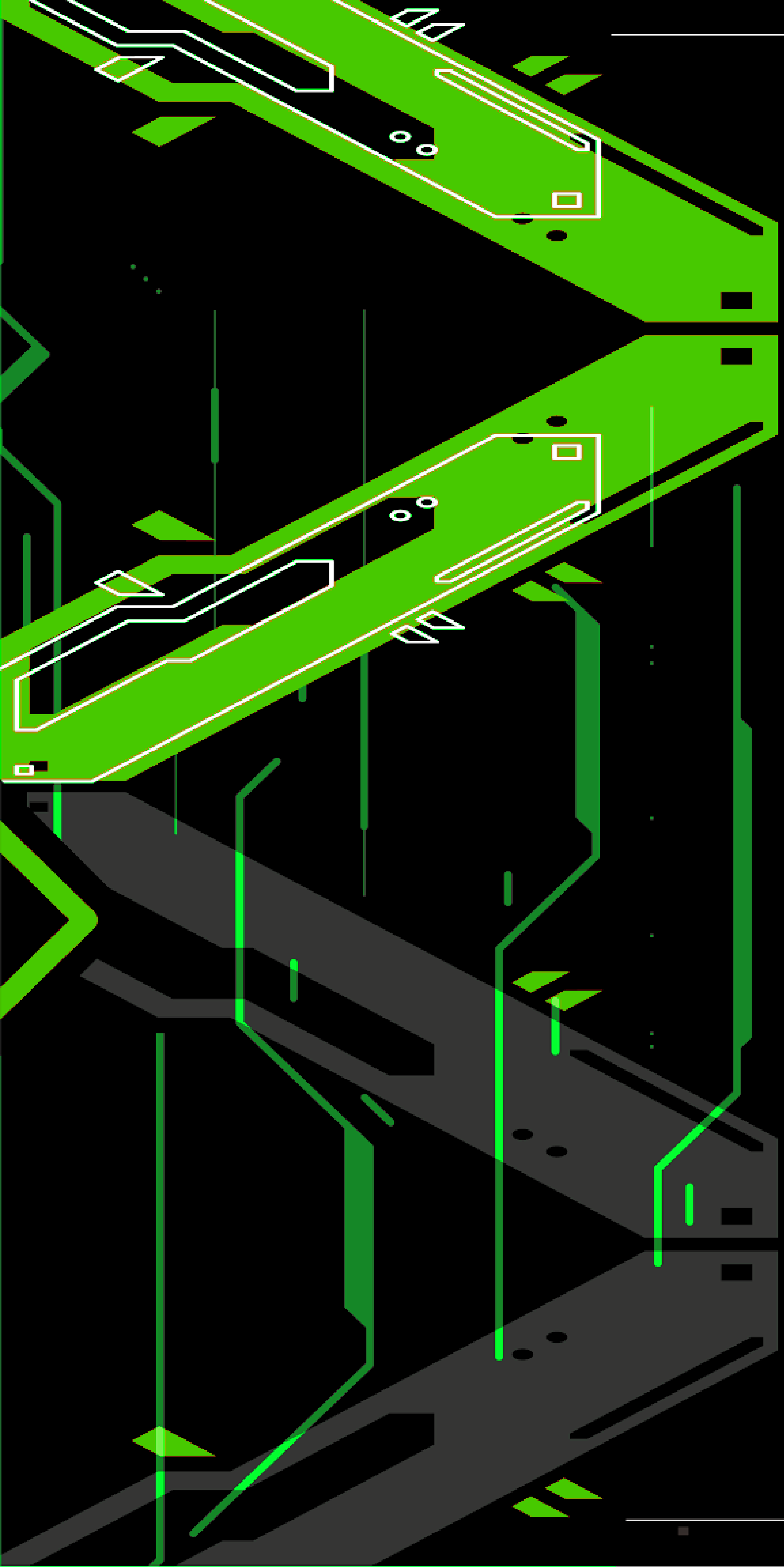


HITBSecConf
2022 Singapore

Breaking Web3

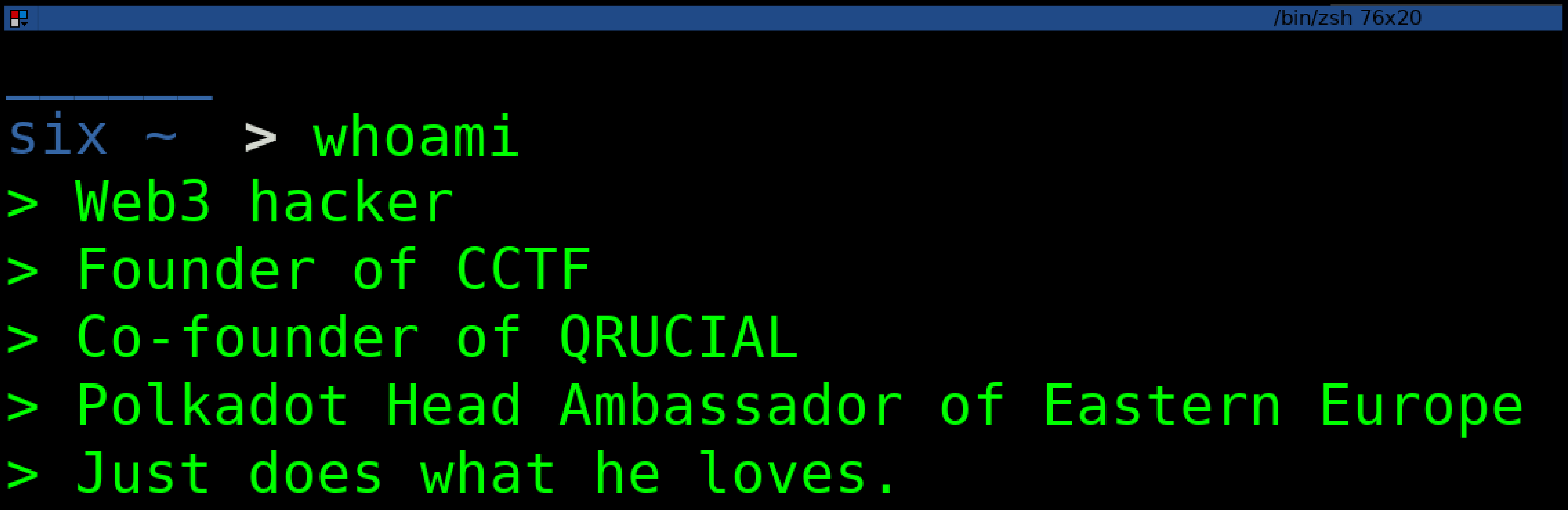
Exploitation Techniques For Cryptocurrency Hacking

author : six

Agenda

1. Introduction to web3 hacking
2. Eth Transactions
3. Tools for interacting with Eth EVM
4. Remix IDE, ERC20, Truffle, Ganace
5. Substrate/Rust, Extrinsics, PolkadotJS
6. ChaosPallet
7. From web2 to web3 -> Node keys
8. When you don't see it aka social engineering in web3
9. Spilling the Tea

author : six



/bin/zsh 76x20

```
six ~  > whoami
> Web3 hacker
> Founder of CCTF
> Co-founder of QRUCIAL
> Polkadot Head Ambassador of Eastern Europe
> Just does what he loves.
```

QRUCIAL

Polkadot

CCTF

@DaveTheSix

What the web3 aka...

Reverse engineering buzzwords

& the hype

proof of deposit

ink!

swap

remix ide

crypto

token

DeFi

dApp

decentralized

coin

crypto wallet

bridge

web3

substrate

javascript 😱

metaverse

solidity

blockchain

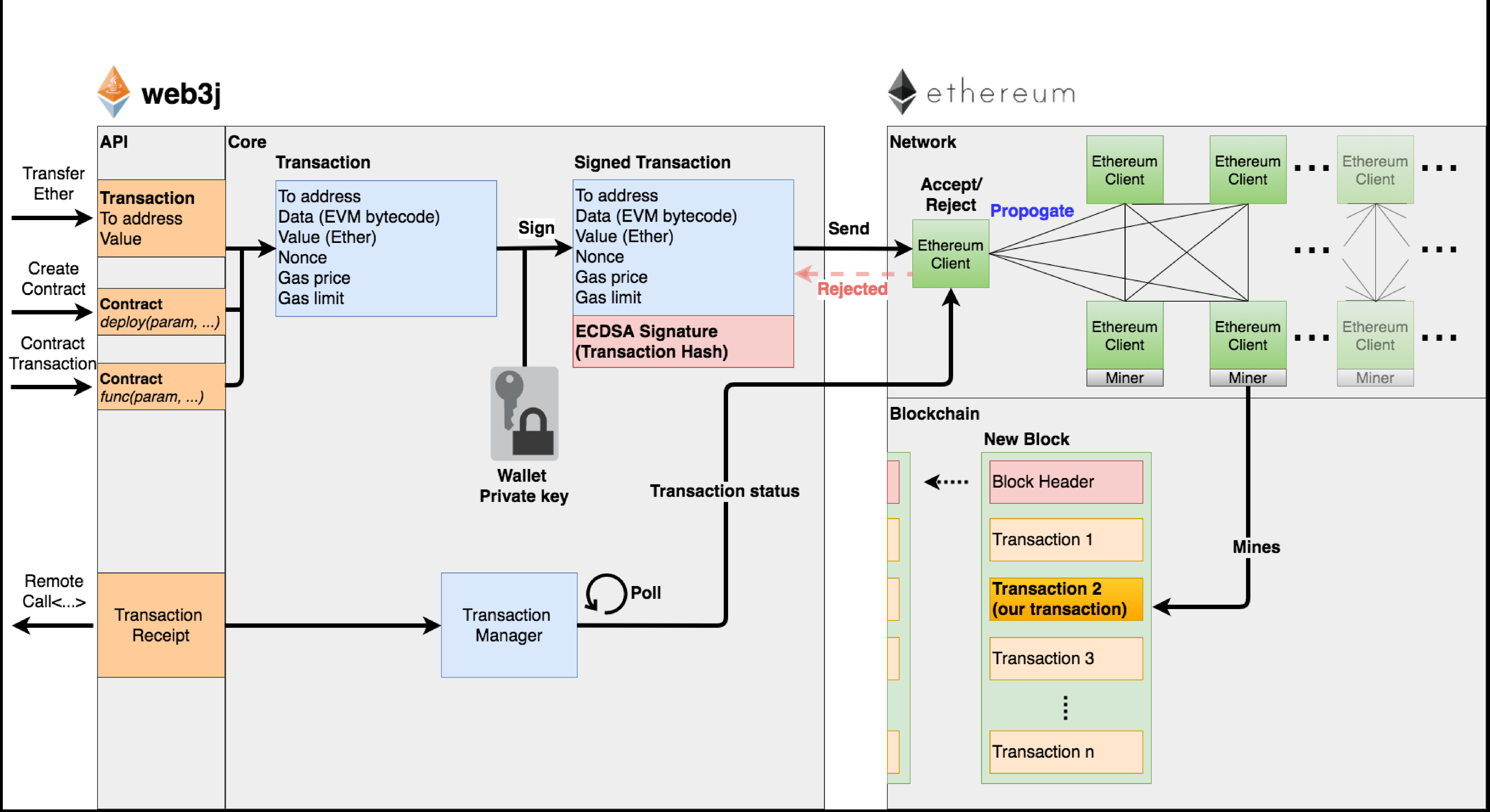
tx

wrapped coin

smart contract

signing

Basic stuff: Eth tx

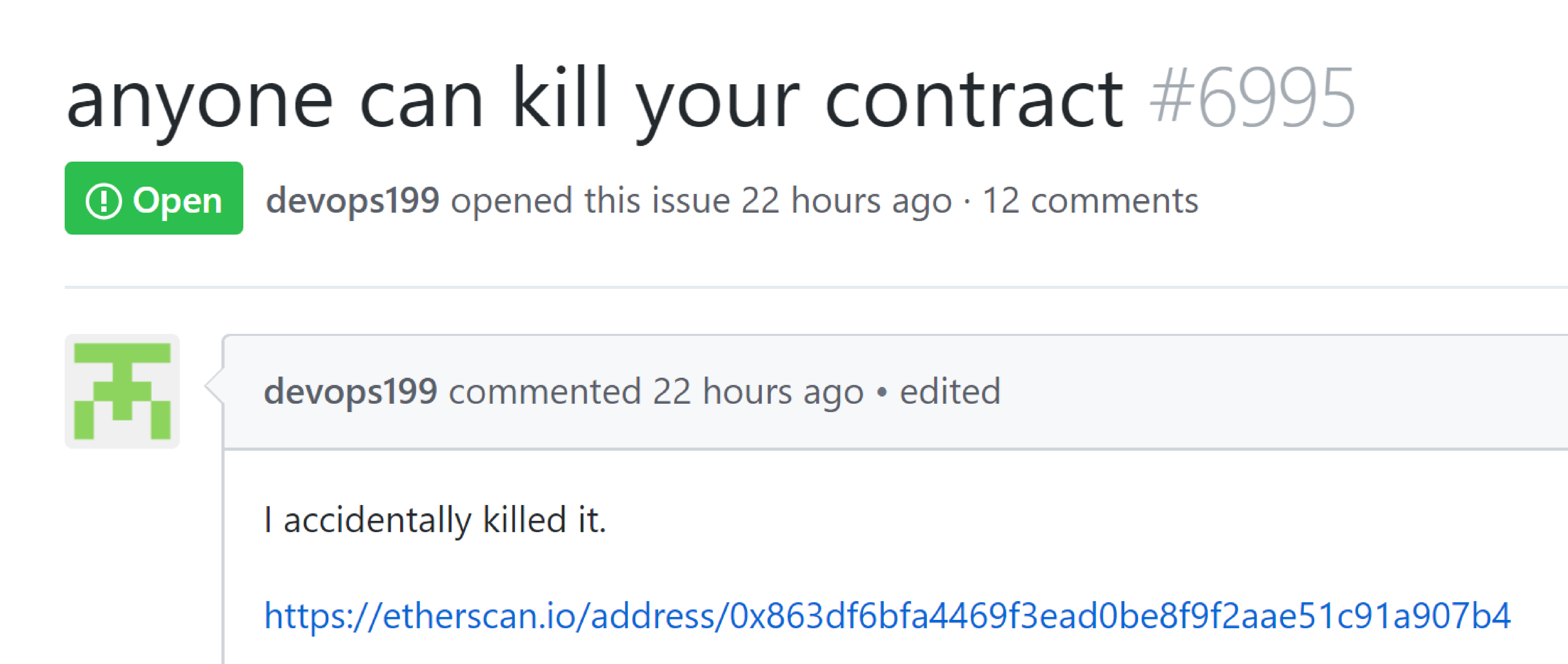


Tools to pwn all the Eth

TRUFFLE
Ganache

+ github.com/crytic/awesome-ethereum-security

Starter technique



anyone can kill your contract #6995

Open devops199 opened this issue 22 hours ago · 12 comments

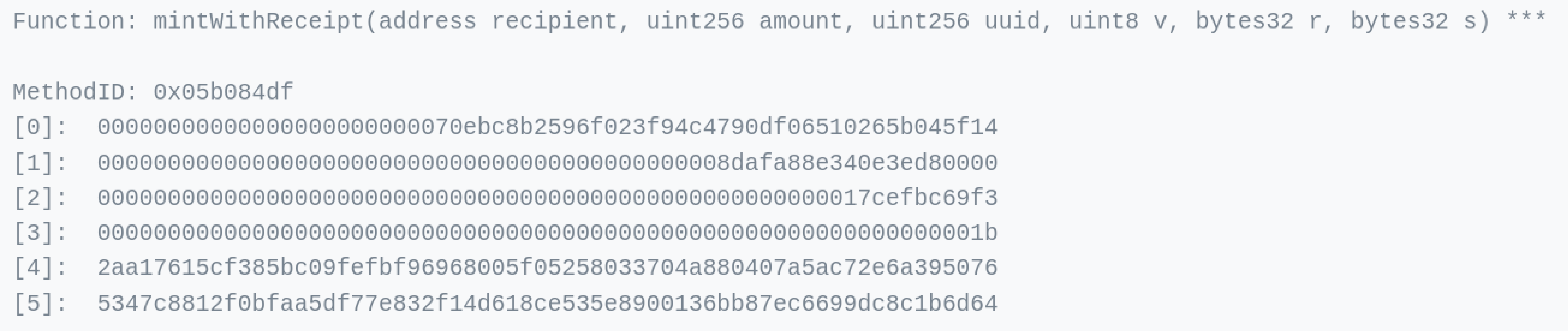
devops199 commented 22 hours ago • edited

I accidentally killed it.

https://etherscan.io/address/0x863df6bfa4469f3ead0be8f9f2aae51c91a907b4

Multisig issue: https://github.com/openethereum/parity-ethereum/issues/6995

TXDATA Replay Attack



```
Function: mintWithReceipt(address recipient, uint256 amount, uint256 uuid, uint8 v, bytes32 r, bytes32 s) ***

MethodID: 0x05b084df
[0]:  00000000000000000000000070ebc8b2596f023f94c4790df06510265b045f14
[1]:  000000000000000000000000000000000000000000008dafa88e340e3ed80000
[2]:  0000000000000000000000000000000000000000000000000000017cefbc69f3
[3]:  000000000000000000000000000000000000000000000000000000000000001b
[4]:  2aa17615cf385bc09fefbf96968005f05258033704a880407a5ac72e6a395076
[5]:  5347c8812f0bfaa5df77e832f14d618ce535e8900136bb87ec6699dc8c1b6d64
```

wBanano hack TXs:

https://polygonscan.com/tx/0xbcf3f1192d63a0d240995619b8896c406d1ba6fa7c2fc81503057d61c98bba41

https://bscscan.com/tx/0x60c3ae26d1a1d2b525a425aacdbde30bf7efdc09a125086cc7aab9b347daf684

Demo - Solidity

- Interact a smart contract (explorer)

- ERC20 in Remix

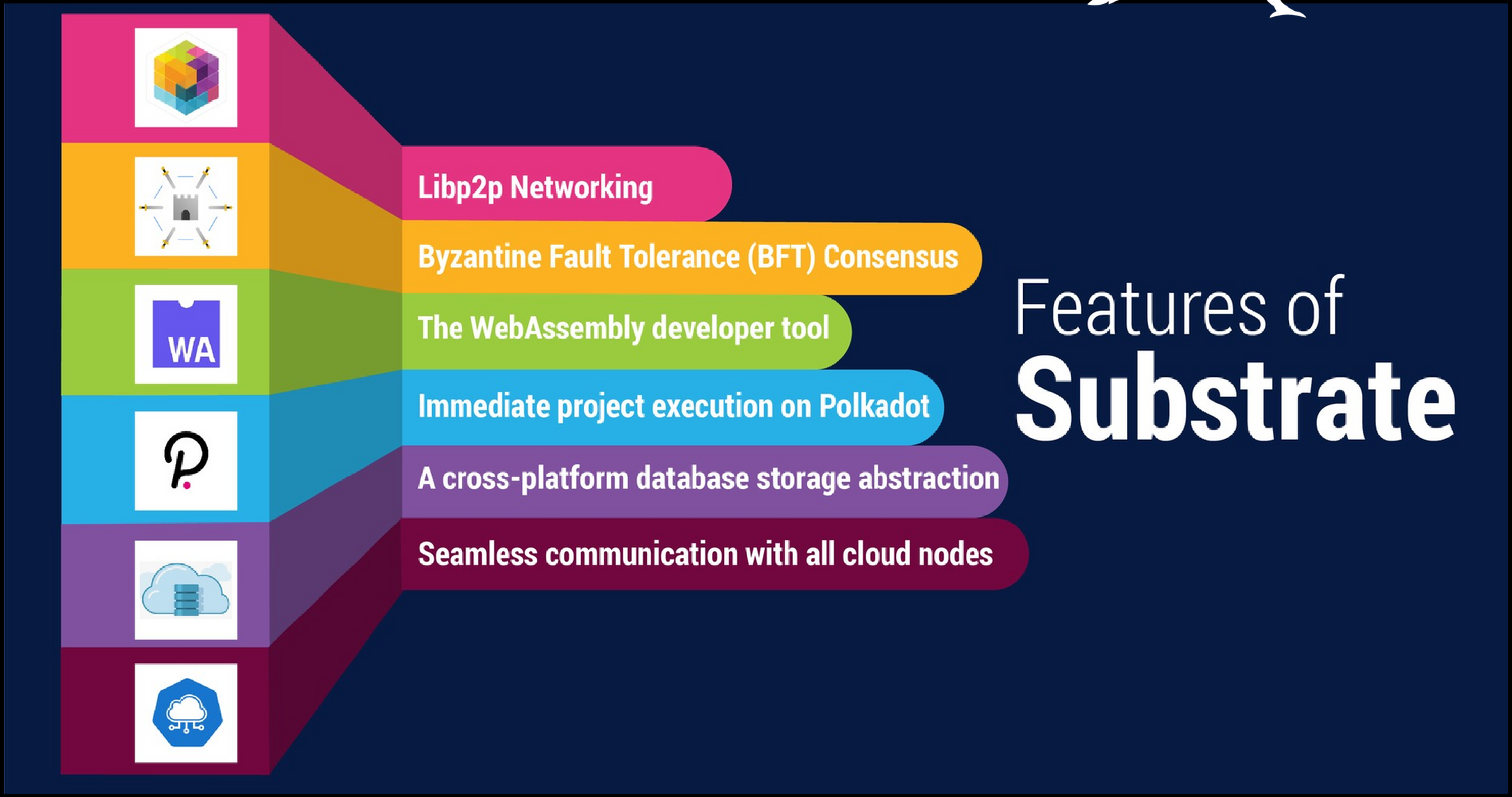
- Call from another smart contract

- Exploit reentrancy

Demo

- Ethkeygen
- Generate ECDSA keys
- Reference: wBan Hack

Hacking Substrate - Why?

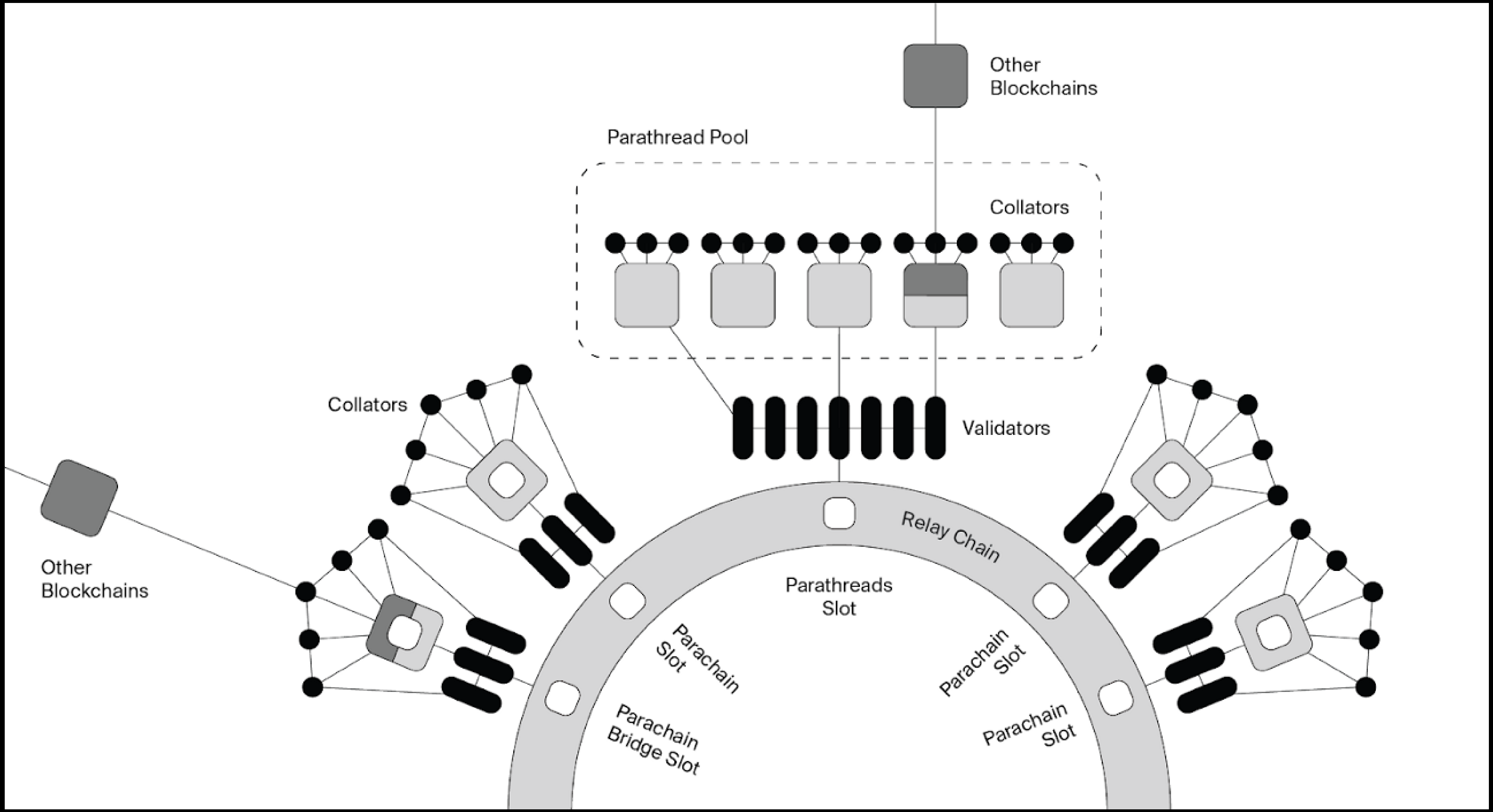


Features of **Substrate**

- Libp2p Networking
- Byzantine Fault Tolerance (BFT) Consensus
- The WebAssembly developer tool
- Immediate project execution on Polkadot
- A cross-platform database storage abstraction
- Seamless communication with all cloud nodes

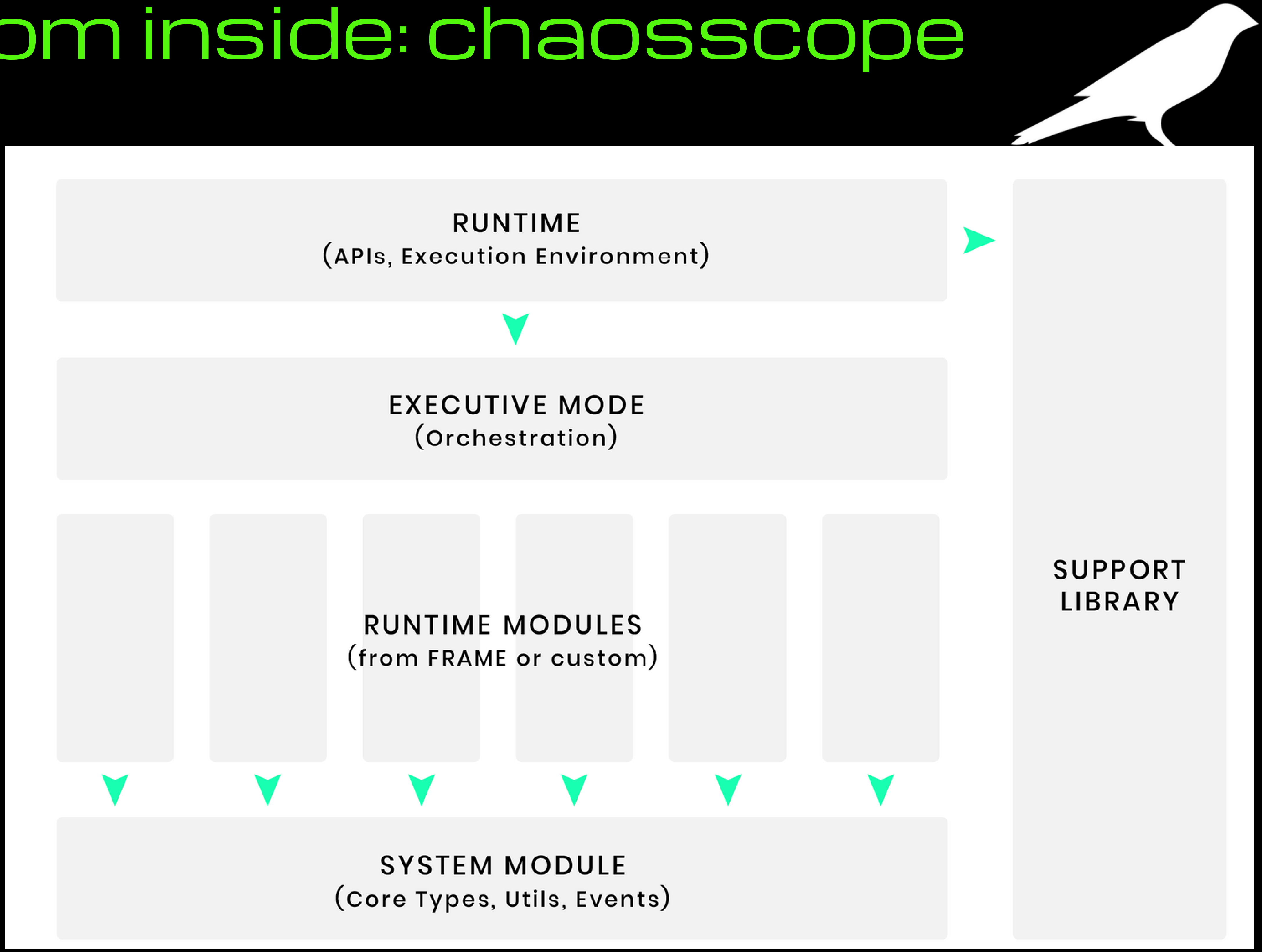
Polkadot

Polkadot targets



- Parachains -> sovereign blockchains.
- Relay chain -> Governance mechanism, Parachain auctions, NPoS
- Shared state/sec between the Relay Chain and Parachains.
- Parathread -> pay-as-you-go model.
- Governance -> in practice, through PolkadotJS !!!! $$$! :)))

Attack from inside: chaosscope



Polkadot

https://github.com/paritytech/chaoscope

Okey, but how do we hack it?

- Chaos Pallet
- Build and run Substrate -> substrate.io
- How-NOT-to-build-a-pallet (ideas)
- Lets speak about the ink! pallets too!

How not to build a pallet -> https://github.com/apopiak/how-not-to-build-a-pallet

Guide -> https://qrucial.io/hacking-substrate-with-chaos-pallet/ (mostly works)

Attacking: ink! smart contracts

- Run locally by 'substrate-contracts-node'

- Connect to the node with PolkadotJS
https://polkadot.js.org/apps/

- Execute smart contracts using ContractsUI
https://github.com/paritytech/contracts-ui
https://contracts-ui.substrate.io/

ink! VS Solidity

https://ink.substrate.io/ink-vs-solidity

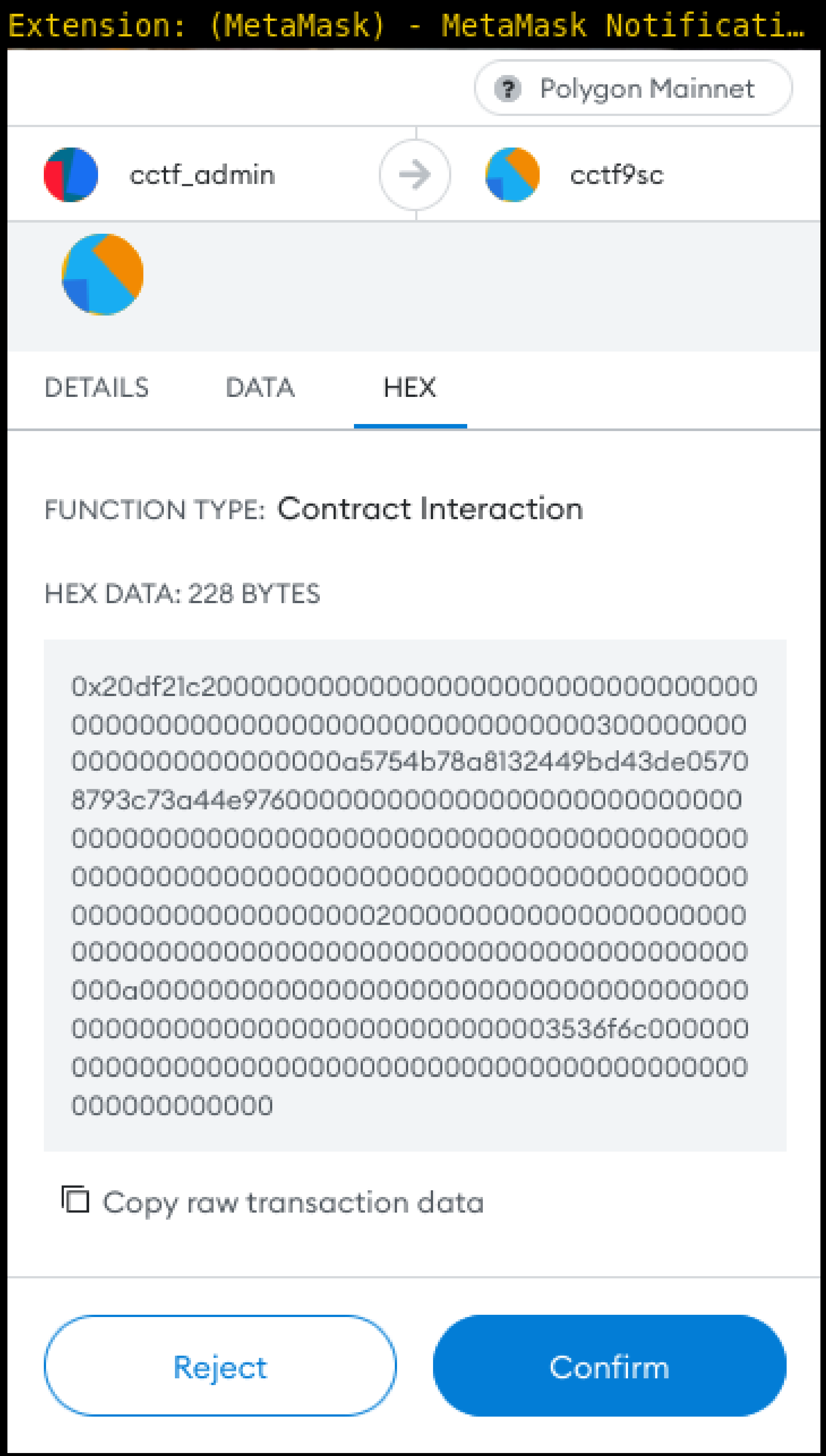
Note on what web3 is NOT meant to be:

SELL BITCOIN
WAIT TILL DUMP
BUY AGAIN
WEN CHEAP

Life of a standard MetaMask user

+

Social Engineering



Extension: (MetaMask) - MetaMask Notificati…

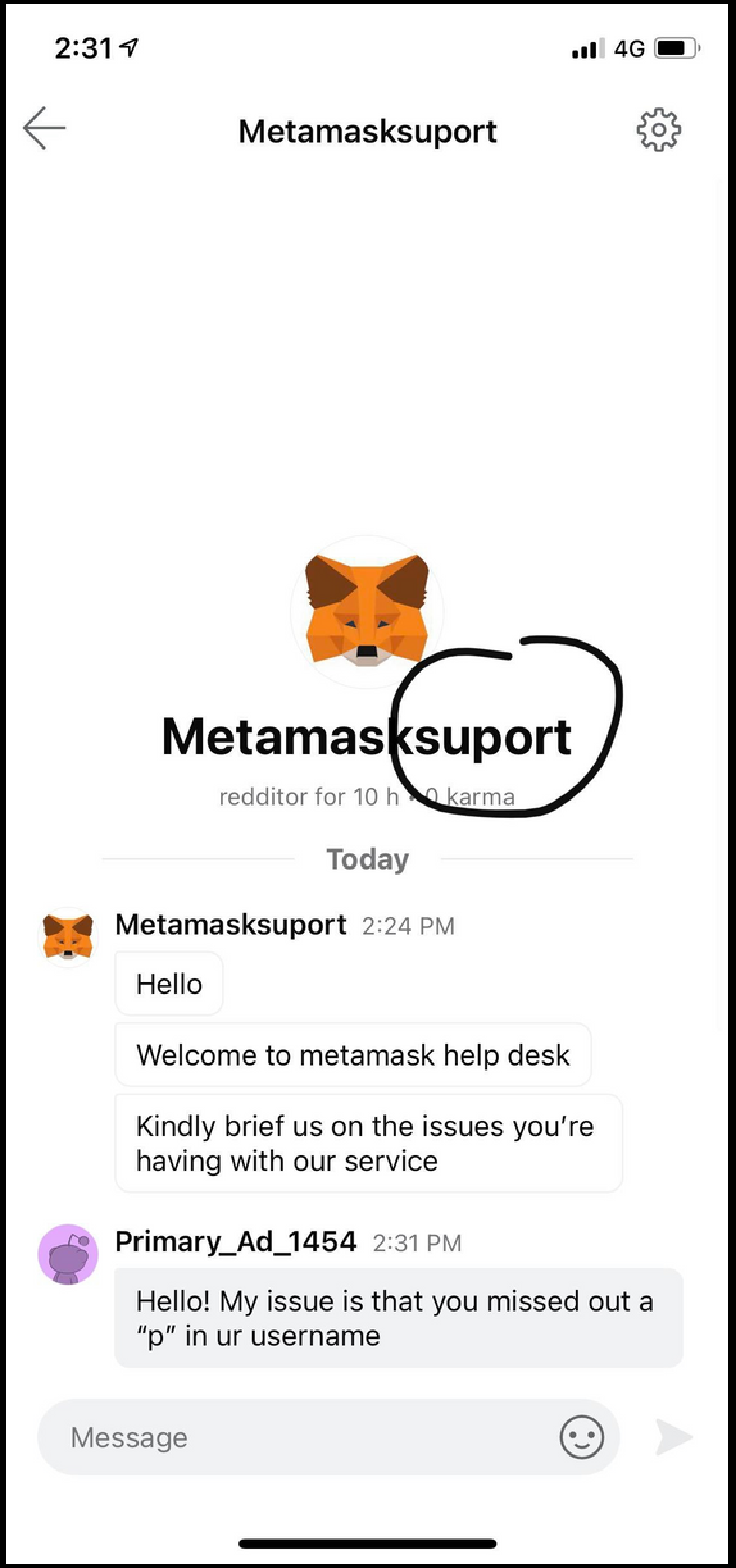
FUNCTION TYPE: Contract Interaction

HEX DATA: 228 BYTES

```
0x20df21c200000000000000000000000000000000
0000000000000000000000000000000300000000
0000000000000000a5754b78a8132449bd43de0570
8793c73a44e9760000000000000000000000000000
0000000000000000000000000000000000000000
0000000000000000000000000000000000000000
0000000000000000002000000000000000000000
0000000000000000000000000000000000000000
000a000000000000000000000000000000000000
0000000000000000000000000003536f6c000000
0000000000000000000000000000000000000000
000000000000
```

Not always the brightest attackers ->

Awareness <3



Metamasksuport

redditor for 10 h • 0 karma

Today

Metamasksuport 2:24 PM

Hello

Welcome to metamask help desk

Kindly brief us on the issues you're having with our service

Primary_Ad_1454 2:31 PM

Hello! My issue is that you missed out a "p" in ur username

Spilling the tea: advanced techniques

- Proxy contract hacking (same tools)
- Reverse engineering (octopus helps)
- Consensus and network attacks
- Flash Loan
- Logic bugs <3
- MEV
- Vulns like Uncle Maker
    -> https://eprint.iacr.org/2022/1020

Contact

Matrix: @hexff:matrix.org

Twitter: @DaveTheSix

CCTF room: #CCTF:matrix.org

Audit request: hello@qrucial.io