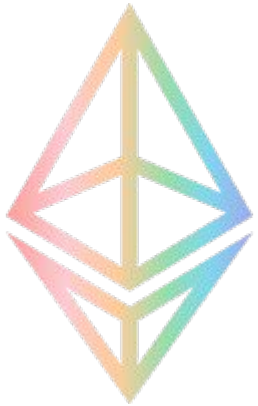


BLOCKCHAIN CHALLENGE

workshop ethereum

Adrià Massanet

twitter @adria0

SSB ZFWw+UclcUgYi081/C8lhgH+KQ9s7YJRoOYGnzxW/JQ=.ed25519

Menu

Postre : Take away  (crema catalana)

Segon : Caractéristiques de desplegament  (ànec amb peres)

Primer : Desenvolupament (browser/server/IoT)  (canelons panses i pinyons)

Vermut : Fonaments de seguretat  (vermuth)

BLOCK?HAIN CHALLENGE

Take away

- Entre iguals, donar garanties per a que puguin col·laborar
- Models criptoeconòmics, disseny de càstigs/incentius
- Tokens: minting/mining, hardcap, bounding curves, airdrop, oxidize
- Multisigs, timelocks, governance
- Harberger tax
- Democràcia líquida / consens hologràfic
- xdai / diposits
- Escalabilitat / privacitat
- Diferents blockhains per a diferents proposits / bridging
- Minimitzar codi onchain / documentar minim

BLOCK?HAIN CHALLENGE

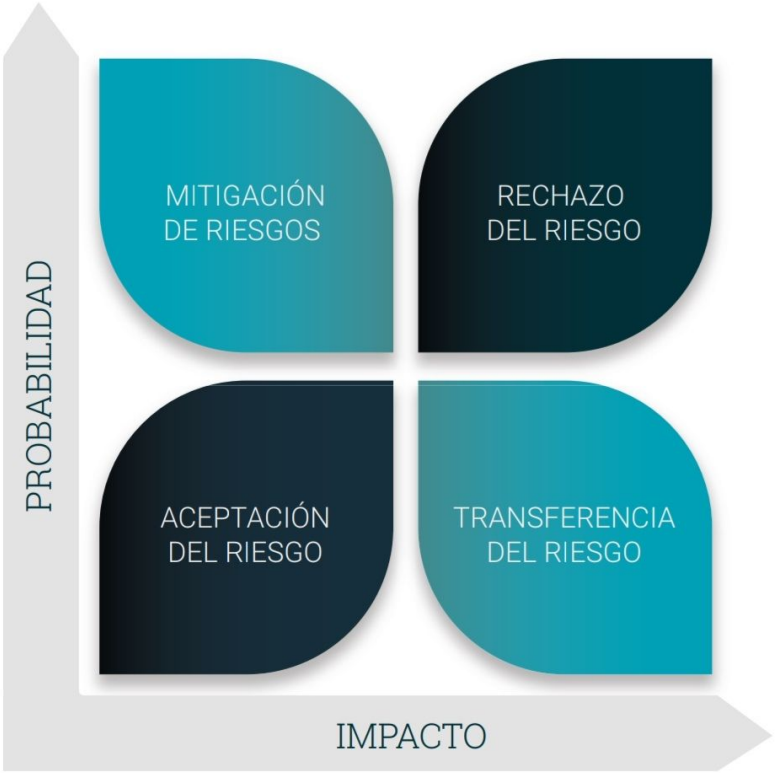
Escenaris de desplegament

Mainnet: *blockchain gobal pública genèrica*, en PoW/PoS obert i anònim

Nou.network: *blockchain barcelona, generica*, PoA en nodes reconeguts universitats, gas a demanda

Kvartalo: *blockchain de i per els veïns els sants*, la moneda kuarto i la governança amb privacitat

BLOCKCHAIN CHALLENGE



BLOCKCHAIN CHALLENGE

Capacitat de la xarxa

- Algú em pot assegurar que no es saturarà *per mi*?
- Que faré si la xarxa es satura? I si tinc transaccions pendents?
- Depenc d'altres sistemes?
- Fins quantes transaccions tinc capacitat d'escalar?

idees

- Acumuladors en arbres de merkle
- Acumuladors zk-snarks
- Sharding

BLOCKCHAIN CHALLENGE

Capacitat de la xarxa

Mainnet

Nou.network

Kvartalo

BLOCK?HAIN CHALLENGE

Cost de transacció

- Té cost variable la transacció? fins on puc assumir la pujada del cost de la transacció?

idees

- Desar menys dades, fer menys calculs
- Fer servir una altre blockchain temporalment

BLOCKCHAIN CHALLENGE

Cost de transacció

Mainnet

Nou.network

Kvartalo

BLOCKCHAIN CHALLENGE

Inmutabilitat

- Si hi ha una fallada al contracte i causa danys, he de poder arreglar-ho?
- He de complir una normativa externa que esta fora del meu control?
- He de donar garanties que cap agent extern pot alterar les dades?

idees

- Tindre clar el sistema de governança dels nodes
- Fer smartcontracts actualitzables (governança!)

BLOCK2HAIN CHALLENGE

Inmutabilitat

Mainnet

Nou.network

Kvartalo

BLOCKCHAIN CHALLENGE

Privacitat

- Algú pot saber alguna cosa de mi?
- Algú pot saber alguna cosa del meu negoci?
- Ja que el codi dels smartcontracts es public, que passa si algú ho copia?

idees

- Patentar
- Hash de les dades
- Acumuladors en arbres de merkle periodics
- Acumuladors zk-snarks

BLOCK?HAIN CHALLENGE

Privacitat

Mainnet

Nou.network

Kvartalo

BLOCKCHAIN CHALLENGE

Accés

- Qui pot llegir?
- Qui pot escriure?
- Qui té gas? Qui pot ser un code?
- Implicacions legals, privacitat, seguretat en els SCs?

idees

- Meta-transaccions
- KYC amb credencials pre-existents (idcat, etc..)

BLOCKCHAIN CHALLENGE

Accés

Mainnet

Nou.network

Kvartalo

BLOCKCHAIN CHALLENGE

Magatzem de valor

- Si hi ha desacord i algú fa un fork, que passarà?
- Hi ha col.laterals? Qui els guarda?

idees

- Cooperativa de consumidors i usuaris
- Sistemes de pagament amb lliçència

BLOCK CHAIN CHALLENGE

Magatzem de valor

Mainnet

Nou.network

Kvartalo

BLOCK?HAIN CHALLENGE

Repàs eines de desenvolupament

- Etherscan.io / ethereum gas station
- Remix
- Truffle / Ganache
- OpenZeppelin
- olidity-coverage / manticore / mythril / slither
- web3.js / metamask / wallets
- go-ethereum
- rs-web3

BLOCK2HAIN CHALLENGE

browser js (navegador)

```
// npm i web

const abi = …
const addr = …

if (window.ethereum) {
   web3Provider = window.ethereum;
   try {
     await window.ethereum.enable();
   } catch (error) {
     console.error("User denied account access")
   }
} else if (window.web3) {
  web3Provider = window.web3.currentProvider;
} else {
  web3Provider = new Web3.providers.HttpProvider('http://localhost:9545');
}
web3 = new Web3(web3Provider);


web3.eth.defaultAccount = (await web3.eth.getAccounts())[0];
let prova = new web3.eth.Contract(abi,addr);
console.log(await prova.methods.i().call());
await prova.methods.inc().send({ from : web3.eth.defaultAccount });
```

BLOCK2CHAIN CHALLENGE

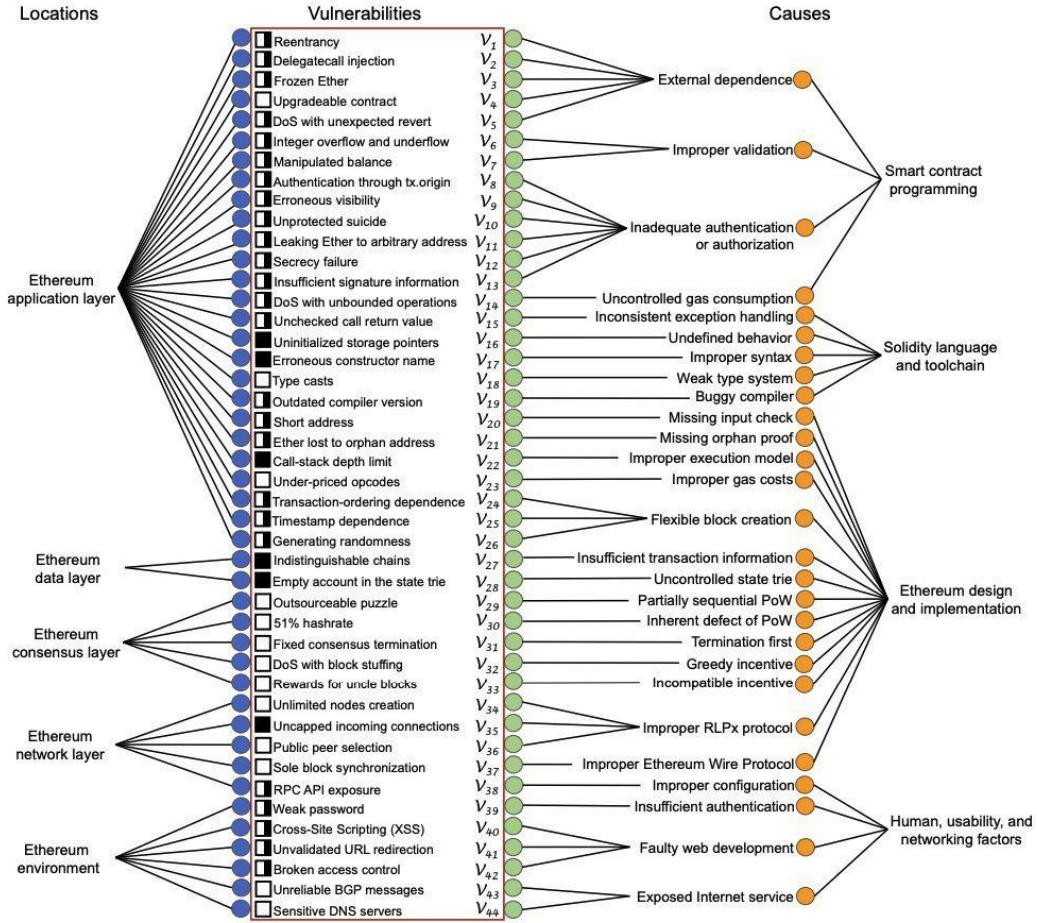
go (servidor)

```
solcjs --abi Prova.sol
docker run -v `pwd`:/contracts ethereum/client-go:alltools-latest abigen --pkg abi1  --abi
/contracts/Prova_sol_Prova.abi

package main
import (
  "github.com/ethereum/go-ethereum/accounts/abi/bind"
  "github.com/ethereum/go-ethereum/common"
  "github.com/ethereum/go-ethereum/core/types"

  addr := “...”

  client, err := ethclient.Dial("http://localhost:9545")
  key, err := crypto.HexToECDSA(“<32 bytes in hex>”)
  contractAddress := common.HexToAddress(addr)
  contract, err := abi.NewProva(contractAddress, client)
  auth := bind.NewKeyedTransactor(key)
  tx, err := acontract.Inc(auth, "hello")
}
```

BLOCK2CHAIN CHALLENGE

rust (iot)

```
// web3 = "0.8.0"
// easycontract = { git = "https://github.com/adria0/ethworkshop-rustfest" }

fn main () {

  let address = “...”

  let (eloop, transport) = web3::transports::Http::new(“http://localhost:9545”)
    .expect("cannot create web3 connector");
   eloop.into_remote();

  let web3 = web3::Web3::new(transport);
  let account  = Account::from_secret_key("<32 bytes in hex>");
  let abi_json = include_bytes!("Yeah.abi");
  let contract = EasyContract::from_json(&web3, address, abi_json)
     .expect("cannot assign to contract");

  contract.call("inc", (), &account1, U256::zero())
    .expect("cannot call inc");
}
```



g. 5: A classification of Ethereum vulnerabilities and their state-of-the-art treatments (■ means “eliminated already”, ◨ eans “can be avoided by best practice”, and □ means open (i.e., has yet to be eliminated).