

Crypto Bridges

Motivacija

- u dosta slucaja, odgovaralo bi nam da mozemo da prebacimo nase asete sa jednog chaina na drugi
 - problem u tome je sto chainovi nisu sposobni da medjusobno komuniciraju
- Landing protokoli (AAVE) imaju bolji interes u slucaju odredenih coinova
 - ETH: 0.5%
 - Polygon 3%
- Odredjeni chainovi imaju mnogo jeftinije i brze transakcije (u vecini slucaja na ustrb bezbednosti)
 - sta mozemo uraditi sa 2\$?
 - * 1 transakcija na Ethereum
 - * 50k polygon transakcija
- Chainovi poput Bitcoina nemaju mogucnost izvršavanja smart contracta
- Razne DeFi aplikacije dostupne su samo na pojedinim chainovima

Coin wrapping

- svaki chain ima svoj native coin
 - uprkos tome, mi mozemo imati neki coin na njemu nenativnom chainu, samo u formi tokena (ERC-20)
 - * wBTC
 - da bi se mogao koristiti za DeFi
 - njime se prebacuje likvidnost sa btc chaina na ostale
 - * wETH
 - eth sam po sebi ne zadovoljava ERC-20 standard, zato se prebacuje u wETH
 - on se menja kroz contract ili metamask
- valutu koju imamo saljemo notaru/contractu koji ih zamrzavaju
- zatim oni okidaju mintovanje novih njima ekvivalentnih tokena na drugom chainu ili ih izvlace iz njihovog liquidity poola
 - kada se citava migracija izvrsi, zamrznuti tokeni na prvom chainu se unistavaju
 - * u slucaju da se tokeni reedemuju, wrapovani tokeni se spaljuju
- notar garantuje ekvivalentnost izmedju originalnog i wrapovanog tokena
 - postoje pokusaji izbegavanja ovog vida centralizacije

Gde se notar nalazi?

- Implementiran je kao:

- offchain aplikacija
- contract na trecem chainu
- ima liquidity poolove na oba chaina
- informacije o zahtevima za transakciju dobija citanjem logova ili pollingom
 - polling je ok pristup jer nam svakako nije u interesu da vrsimo migracije na svaki zahtev nego ih izvorsavamo u batchevima

Osnovna podela

- centralizovani (trust based)
 - svoj kripto dajemo pod kontrolu nekome drugom (uplatimo na neciju adresu)
 - * moramo im verovati
 - centralizovan pool
 - prednosti:
 - * brzi
 - * jeftini
 - mane:
 - * centralizacija
 - * smanjena bezbednost
 - moze se kreirati federativna verzija koja se sastoji od vise notara, ali ni to nam mnogo ne garantuje
- decentralizovani (trustless)
 - u ovom smart contract poolu ucestvuje vise korisnika
 - * nekada je implementiran i kao zeseban chain
 - skuplje, sporije, ali pouzdanije

Bridge vs Exchange

- Exchange
 - iz BTC walleta uplatim BTC na centralizovani exchange (Binance)
 - Kupim ETH
 - Posaljem ga sebi na ETH wallet
- Bridge
 - pomocu neke od metoda direktno se (peer to peer) prebacuje npr. BTC u WBTC
 - * nema posredovanja centralizovanog eniteta
- U sustini:
 - peer to peer umesto centralizovanog modela
 - autonomija i privatnost korisnika
 - siri spektar podrzanih asseta
 - nekad fee za bridge nije toliko skup ako imamo 3 “interna” chainea koji su “brzo i jeftino” povezani
 - * svaki ima neku svoju prednost, koji drugi nemaju
 - * tada im je u interesu da se bridguju

Specificne metode

Notary

Postupak

- Korisnik zaključa svoje tokene na chain A u contract
- Notary proveriti da li je on zaključao tokene i izdaje verifikaciju
- Salje se transakcija na chain B sa priloženom verifikacijom
- da nema verifikacija i notara:
 - double spending
 - * korisnik ne bi morao da zaključava svoje tokene na A vec samo da promptuje B chain
- prednosti:
 - jednostavan
 - efikasan
 - najcesce koriscen
- mane:
 - moramo da verujemo notaru da nas ne prevari
 - * pokusaj resavanja pomocu federativnih notara

Optimistic bridges

Postupak

- Korisnik zaključa svoje tokene u contract na chain A
- relay posalje info o transakciji sa A ka B
 - ALI NE proverava da li su tokeni stvarno bili zaključani na A
 - zato se zove optimisitican - pretpostavlja da je vecina transakcija validna
 - sta nas onda spreca da lazemo?
 - * ostatak peerova mreze A moze da posalje dokaz (najcesce merkle) da to nismo uradili i tada se revertuje transakcija na B i masivno slashuje maliciozni korisnik
- prednosti i mane:
 - Nemamo centralizovanog notara, vec veliki broj korisnika koji motre na bridge i detektuju maliciozne transakcije
 - * ovo su dobrovoljci

Zero knowledge bridge

- neophodna je implementacija light client protokola
 - povezuje se na full node-ove i tako omogucava interakciju sa chainom
- zaključa se token na A u contract

- bridge generise ZKP (npr: ZK snarks)
 - offchain
 - garantuje da je tx validna bez otkrivanja tajni tx
- chain B prima ZKP i verifikuje ga
- Transfer se finalizuje od strane B

Prednosti i mane

- prednosti
 - privatnost zbog ZKP
 - efikasnost
 - * umesto da se cuvaju svi detalji transakcije chainovi samo rukuju sa ZKP i headerima blokova
- mane
 - * velika kompleksnost

Bezbednost

Ronin (624M)

- Mart 2022.
- tokeni iz igrice su se prebacivali u druge valute
- pokradeni su privatni kljucevi za autentifikacije transakcija
 - slaba decentralizacija (9 validatora)
 - slab monitoring (napad primecen tek nakon 6 dana)

Poly (611M)

- 2021
- Poly mreza
- kasnije su vracene
 - napadac “je samo cuvao tudje pare da ih oni ne izgube”
 - * napa ih je iz zabave, kao neki vid izazova