Bridge pregled

Motivacija

- u dosta slucaja, odgovaralo bi nam da mozemo da prebacimo nase assete sa jednog chaina na drugi
  - problem u tome je sto chainovi nisu sposobni da medjusobno komuniciraju
- Landing protokoli (AAVE) imaju bolji interest u slucaju odredjenih coina
  - ETH: 0.5%
  - Polygon 3%
- Odredjeni chainovi imaju mnogo jeftinije i brze transakcije (u vecini slucaja u ustrb bezbednosti)
  - sta mozemo uraditi sa 2$?
    - 1 transakcija na Etherium
    - 50k polygon transakcija
- Chainovi poput Bitcoina nemaju mogucnost izvrsavanja 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 likvindost sa btc chaina na ostale
    - wETH
      - eth sam po se bi 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
  - kada se citava migracija izvrsi, zamrznuti tokeni na prvom chainu se unistavaju ???
    - ???postoji li mogucnost ipak da se reedemuju???
- 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 ??? ??? Kod liquidity poola, da li se i dalje dobija WETH u Polygonu ili se dobija Polygon native coin??? ???Kako radi ta liquidity pool metoda???
- 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 izvrsavamo u batchevima

Osnovna podela

- centralizovani (trust based)
  - svoj kripto dajemo pod kontrolu nekome drugom ???bukvalno uplatimo ili ti verifikatori samo motre na adresu na koju smo uuplatili - dali su moguce obe opcije, da li ova druga opcija prelazi u smart contract tip???
    - 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)
  - ???koristi se smart contract u kome se zamrzavaju asseti i on minta ekvivalentne tokene na drugom chainu ???
  - (nekad) skuplje, sporije
  - uvek imamo kontrolu nad nasim assetima

Bridge vs Exchange

- Exchange
  - uplatim BTC na centralizovani exchange
  - konvertujem ga u fiat valutu (stable coin)
  - Kupim ETH
  - ???Posaljem ga sebi na ETH wallet???
- Bridge
  - Preskace se medjukorak kupovine stablecoina
  - pomocu neke od metoda ???(wrappovanje ili pool)??? direktno se prebacuje BTC to WBTC
- U sustini:
  - peer to peer umesto centrailizovanog modela
  - autonomija i privatnost korisnika

  - siri spektar podrzanih asseta
  - kompleksniji
  - 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 zakljuca svoje tokene na chain A u contract
- Notary proveri da li je on zakljucao tokene i izdaje verifikaciju
- Salje se transakcija na chain B sa prilozenom verifikacijom
- da nema verifikacija i notara:
  - double spending
    * korisnik ne bi morao da zakljucava 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 federated bridges
      · imamo grupu validatora, ali ne notara

Optimistic bridges

Postupak

- Korisnik zakljuca 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 zakjucani na A
  - zato se zove optimsitican - pretpostavlja da je vecina transakcija validna
  - sta nas onda sprecava 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???

- zakljuca se token na A u contract
- bridge generise ZKP (npr: ZK snarks)
  - 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
  - interoperabilnost
    * detalji transakcije aptrahuju se u ZKP kojem se razlicite tehnologije lakse prilagodjavaju
- mane
  - velika kompleksnost

Bezbednost

Ronin (614M)

- tokeni iz igrice su se prebacivali u druge valute
- pokradeni su privatni kljucevi za autentifikacije transakcija

(611M)

- 2021
- kasnije su vracene (napadac “je samo cuvao tudje pare da ih oni ne izgube”)