Wrapped tokeni

- imamo custodiana koji uzme nase tokene zamrzne ih u vaultu i izmintuje nove tokene na mrezi za koju wrapujemo nas token
- inverzna operacija je burnovanje gde se unisti wrapovani token, a iz vaulta odmrzne nas provbitni token
- custodian garantuje ekvivalenciju izmedju originalnog i wrapovanog tokena
  - sto je ujedno i problem

Primeri

- 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

Bridges

- svaki chain ima svoj native coin
  - uprkos tome, mi mozemo imati neki coin na njemu nenativnom chainu, samo u formi tokena
- neki landing prootkoli imaju bolje ponude za neke coine i zato je nekad bolje da npr eth prebacimo u polygon i onda landujemo polygon jer je njegov interest veci

Motivi

```
- vecina ERC-20 tokena je nativana Eth
    - Npr: ako na coinbase uzmemo polygon, dobicemo eht verziju poligona
- Na nekim ch su transakcije mnogo jeftinije
    - 2$
        - 1 eth transakcija
        - 50k polygon transakcija (ali placa se bezbednoscu :()
- Napredak
    - razni ch imaju razlicite prednosti i mane
        - njihovim povezivanjem mozemo iskoristiti prednosti svakog od ch da bi zadovoljili
```

Mane

```
- ne moze im se 100% verovati
    - iza svakog bridgea se nalazi neka organizacija -> vecinski su centralizovani
- jako spori (minuti, sati, dani)
```

Tipovi

- centralizovani (trust based)
  - bukvalno dajes svoj kripto u kontrolu nekom drugom
  - centralizovan pool
  - spori
  - mora im se verovati
  - radi samo ako ga ljudi konstatno koriste
  - sad ovaj batica kaze da su brzi i jeftiniji po cenu poverenja(i sled batica je to rekao)
- smart contract (trustless) - decentralizovani
  - asset koji saljes se zamrzne u contractu
  - smart contract ti izminta kopiju tog tokena na zeljenoj mrezi
  - koristi se na ch koji nemaaju mogucnost smart contracta
    - npr btc ne moze da se koristi na aave pa se onda prebaci na eth da bi mogao
    - daje npr brc mogucnost da komunicira i koristi dapp-ove koji postoje samo na odredjenim ch
  - skuplje, sporije i manje se mozemo osloniti na njih
  - na drugu stranu, uvek imamo kontrolu nad nasim assetima

Specificne metode

Notary

- jednostavan
- efikasan
- najcesce koriscen
- moramo da verujemo notaru da nas ne prevari
  - pokusaj resavanja pomocu federated bridges
    - imamo grupu validatora, ali ne notara

Postupak

- korisnik zakljuca svoje tokene na prvom chainu
- Notary proveri da li je on zakljucao tokene i izdaje verifikaciju za to
- Salje se transakcija na drugi chain sa prilozenom verifikacijom (to radi notary)(?)
- da nema verifikacija i notara:
  - double spending
    - korisnik ne bi morao da zakljucava svoje tokene na 1. vec samo da promptuje 2. chain i tjt

Optimistic bridges

Postupak

- Korisnik zakljuca svoje tokene u contract na ch A
- realyer posalje info o transakciji na A ka B
  - ALI ne proverava da li su tokeni stvarno bili zakjucani na A
  - zato se zove optimsitican - pretpostavlja da je vacina transakcija validna
  - sta nas onda sprecava da lazemo?
    - ostatak mreze A moze da posalje dokaz (pomocu merkle) da to nismo uradili i tada se revertuje transakcija na B

Prednosti i mane

- Nemamo centralizovanog notara, vec veliki broj korisnika koji motre na bridge i detektuju maliciozne transakcije
  - ovo je i mana sto to moraju da budu dobrovoljci

Hash time locked bridges (HTLC)

Postupak

- Bob i Alice (chain A i B)
- Bob smisli tajnu i hashuje je
- Bob salje tokene na contract, zajedno sa hashovanom tajnom
  - contract je takav da ce osloboditi kes samo ako alice obezbedi tajnu i ako dokaze da je ona alice
- Alice postavi contract na B svoje tokene i prgramira ga tako da oslobdi tokene bobu, samo ako on zna tajnu,
- znaci oba kontrakta znaju samo haseve ne i same tajne
- Bob salje transakciju na B zajedno sa tajnom i skida kes
  - tada se i tajna javno objavljuje i stavlja na chain
- Alice onda vidi tajnu i iskoristi je da oslobodi tokene sa A
- postoji ograniceno vreme za koje oboje moraju da dignu tokene, inace se transakcija revertuje oboma, da se ne bi desilo da se neciji tokeni zaglave u contractu

Prednosti i mane

- Prednosti
  - potpuno decentralizovani
  - ili oboje dobijaju ili niko
- Mane
  - kompleksan za korisenje
  - spor
  - mogu se koristiti samo ako oba chaina imaju mogucnost rada sa contractima

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 finalizuj od strane B

Prednosti i mane

- prednosti
  - privatnost zbog ZKP
  - efikasnost
    - umesto da se cuvaju svi detalji transakcije chainovi samo rukuja sa ZKP
  - interoperabilnost
    - detalji transakcije aptrahuju se u ZKP kojem se razlicite tehnologije lakse prilagodjavaju
- mane
  - velika kompleksnost

Realne implementacije

- neki dozvoljavaju transakcije samo izmedju dva chaina
  - polygon bridge
  - arbitrum bridge
  - WBTC bridge
- stargate npr dozovoljava konektovanje mnogo vise chainova
- **CCIIP**

Primeri

- xpollinate
- binance bridge
- polugon bridge

Bridge vs Exchange

Koraci za BTC -> ETH

Exchange

- uplatim BTC na centralizovani exchange
- konverujem 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
- Using a blockchain bridge instead of a centralized exchange offers several advantages. Bridges enable direct, peer-to-peer transactions between different blockchains, reducing reliance on central intermediaries. This enhances the autonomy and privacy of users. They also support a wider range of tokens and assets.

Napadi

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")

Pitanja

- Da li se notary nalazi na nekom chainu ili je offchain/oracle
- Sta se desi kada se potrose novoizmintani tokeni, da li eth ostane zamzrznut contractu zauvek
- Kod liquidity poola, da li se i dalje dobija WETH u Polygonu ili se dobija Polygon native coin
- Bridge vs DeX