zkvalidator cosmos+zkp showcase

2021-03-26

@hdevalence

privacy + proof of stake?

private transactions
private delegation
private governance
private swaps

private transactions

transaction model

sapling-style “shielded utxo” model records value in *notes*

unlike utxos, notes are not part of the public chain state

chain state includes a *note commitment tree* instead

spending a note involves proving inclusion and revealing a nullifier

transactions consist of *descriptions* that add or subtract value balance

no accounts, no long-term identity

shielding ibc assets

sapling design can be extended to support multiple asset types

zcash design (“user defined assets”) needs issuance, absorption, naming

cosmos already provides standardized inter-blockchain communication

inbound ibc transfers provide issuance

outbound ibc transfers provide absorption

naming is standardized in adr001

direct shielding of ibc transfers

ics20 specifies `FungibleTokenPacketData` that describes a token transfer

contains `denomination`, `amount`, `sender`, `receiver`

`sender`/`receiver` specifies accounts on source/destination chain

problem: penumbra has no accounts and no concept of user identity

instead, `receiver` encodes output description creating a new shielded note

prerequisites

homomorphic threshold decryption

need a homomorphic encryption scheme operating on `i64` values

validators share control of a threshold decryption key for this scheme

used to aggregate encrypted values and decrypt only the sum

epoch system

organize blocks into epochs, duration approximately 1 day

validator set and voting power is determined per-epoch

distributed key generation is performed in the first block of each epoch

private delegation

challenges for private staking

in tendermint proof-of-stake, stakeholders delegate stake to validators

validators perform consensus with voting power according to delegations

delegators get staking rewards for taking on risk of validator misbehavior

if delegations are public, stakeholders choose privacy xor staking rewards

if delegations are private, how can the chain pay out staking rewards?

eliminating staking rewards

treat unbonded stake `PEN` and bonded stake `PENb` as distinct assets

`PENb` is a first-class staking derivative with delegation fungibility

each validator's risk is different, so `PENb` is really a class of assets `PENb(v)`

bonding `PEN` to `PENb` discounts by the cumulative rewards from genesis

unbonding `PENb` to `PEN` inflates by the cumulative rewards from genesis

delegators realize a capital gain (or loss) on unbonding, not income

delegation parameters

base reward rate is r_e indexed by epoch

per-validator commission $c_{v,e}$

per-validator reward rate $r_{v,e} = (1 - c_{v,e})r_e$

base exchange rate between `PEN` and `PENb` is

$$\psi(e) = \prod_{0 \leq i < e} (1 + r_i)$$

delegation mechanics

delegating x unbonded `PEN` to validator v at epoch e_1 results in $x/\psi_v(e_1)$ `PENb(v)`

undelegating y `PENb(v)` from validator v at epoch e_2 results in $y\psi_v(e_2)$ `PEN`

total return is

$$\psi_v(e_2)/\psi_v(e_1) = \prod_{e_1 \le e < e_2} (1 + r_{v,e}),$$

private governance

on-chain secret-ballot voting

holders of bonded stake can vote privately with special descriptions

spend an existing note, create a new note, encrypt vote to validators

prove the existing note was included before voting began

validators aggregate and decrypt votes

delegated voting is also possible

private swaps

swap mechanics

users create a swap description revealing only the asset pair

input amounts are encrypted to validators and burned

creates a *swap commitment* analogous to a note commitment

validators aggregate encrypted inputs and decrypt the net flow

clearing price and updated liquidity reserves are included in the block

later, users mint new funds, using the swap commitment to prove consistency

ongoing
design
research

https://penumbra.zone

discord link on website

@hdevalence