zkBridge: The XRP Ledger

Aanchal Malhotra, Mayukha Vadari
Ripple
What is the XRP Ledger?

- One of the first decentralized blockchains (est. 2012)
- High performance (>1500 tps)
- Low latency (ledgers close every 4 seconds)
- Low fees (<$0.001 per transaction)
- Carbon-neutral
- Native DEX (no smart contracts needed)
- Native NFTs (no smart contracts needed)
Python Demo

- Connect to the ledger
- Send requests
- Create & send transactions
- Check if transactions were successful
What is a transactor?

- General term for specific features on the XRPL
- Usually they involve a ledger object and a handful of transaction types
- Examples:
  - Escrows
  - Payment Channels
What is a transaction, really?

A transaction:

- Is the only way to modify the XRP Ledger state
- Creates, modifies, or deletes ledger objects
- Commits data to the ledger that users and servers have access to
- Is submitted by an account

```json
{
    "TransactionType": "...",
    "Account": "r....",
    "Fee": "12",
    "Flags": "0",
    "Sequence": 0,
    ...
    "SigningPubKey": "033....",
    "TxnSignature": "3045....",
}
```
Ledger Objects

- How the XRP Ledger stores on-ledger data
- Must be owned by an account (exception: Amendments)

```json
{
    "TransactionType": "...",
    "Account": "r....",
    "Fee": "12",
    "Flags": "0",
    "Sequence": 0,
    ...
    "SigningPubKey": "033....",
    "TxnSignature": "3045....",
}
```
The Parts of a Transaction

- **preflight**
  - what is literally everything that you can check about the validity of the transaction without needing to check the current ledger state?

- **preclaim**
  - what is everything that you can check about the validity of the transaction with read-only access to the ledger state?

- **doApply**
  - do a few sanity checks, and actually try to apply the transaction (if it fails, then you can throw another error)

- **calculateBaseFee**
  - calculate the fee that the transaction needs to pay (usually this is just inherited from the base transactor, but e.g. escrows need higher fees)

- **makeTxConsequences**
  - used when an account has multiple transactions queued to estimate whether it'll be able to pay the fees for all of them
Current Bridge Design

1. XChainCreateClaimID
2. XChainCommit
3. XChainAddClaimAttestation * N
4. XChainClaim (optional)
Resources

For more info visit: https://xrpl.org/docs.html