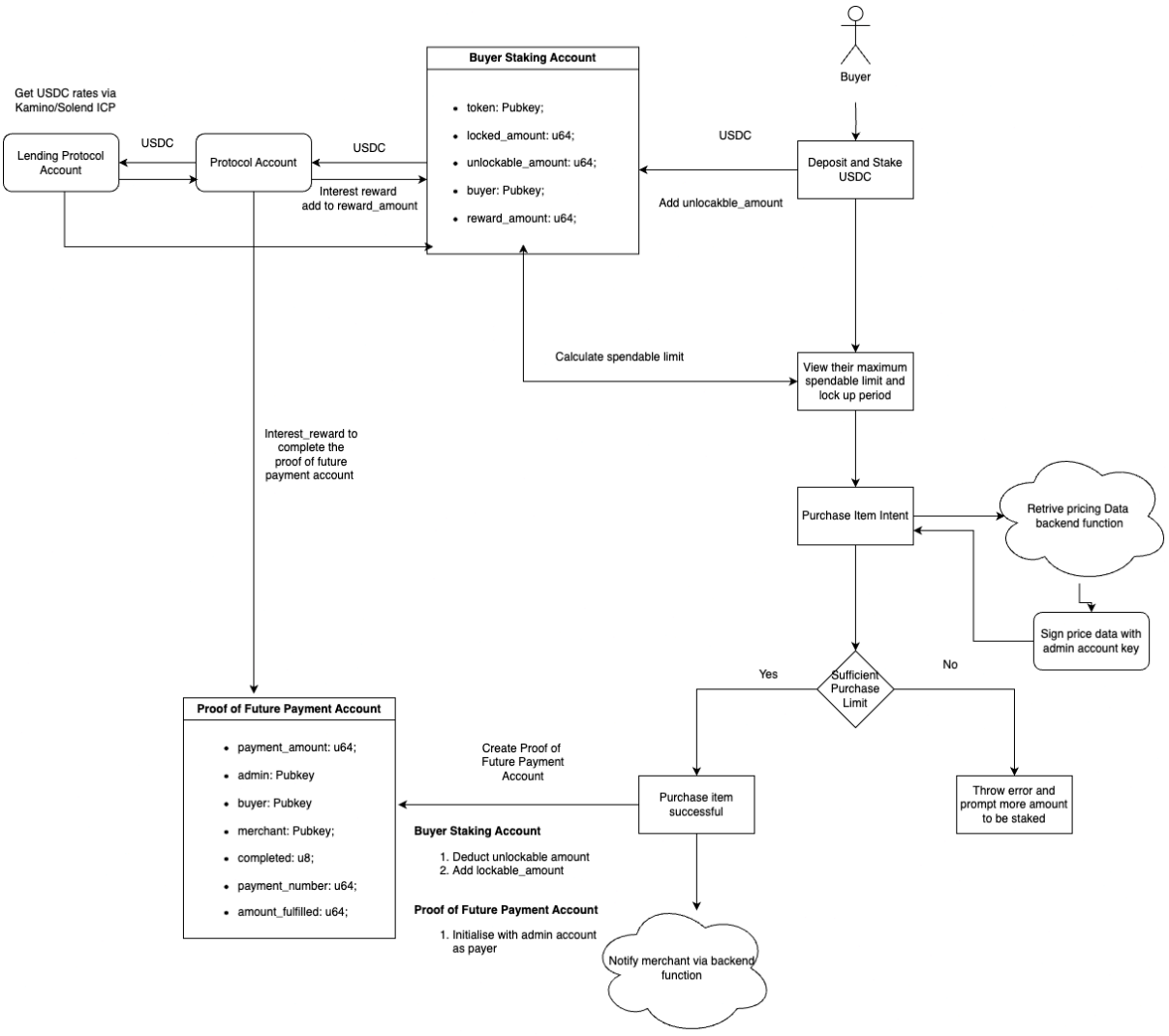
Architecture Design for FreeLunch (BNPN Protocol)

1. Protocol Requirement

- The protocol shall allow buyer to deposit / stake USDC tokens
- The protocol shall interact with other lending protocol (Solend/Kamino) to stake and earn interest from the staked USDC.
- The protocol shall provide buyer an estimation of the purchase limit based on staked asset and staking duration. The general rule is the proof of payment should be fulfilled within 1 year.
- The protocol shall allow merchant to initialise their payment address to track proof of future payments transparently.
- The protocol shall allow merchant to view their incoming payment and date of receiving the payment

2. Flowchart

2.1 Buyer Deposit and Stake



User will stake via our protocol and our protocol will interact with Kamino/Solend via their ICP so we would stake and compound the amount earned to pay back merchant for every payment. The payer for the Proof of Future Payment Account would be admin, while the Staking Contract Account would be by the Buyer.

Staking Contract Account (For Buyer Deposit/Staking & Withdraw/Unstaking)

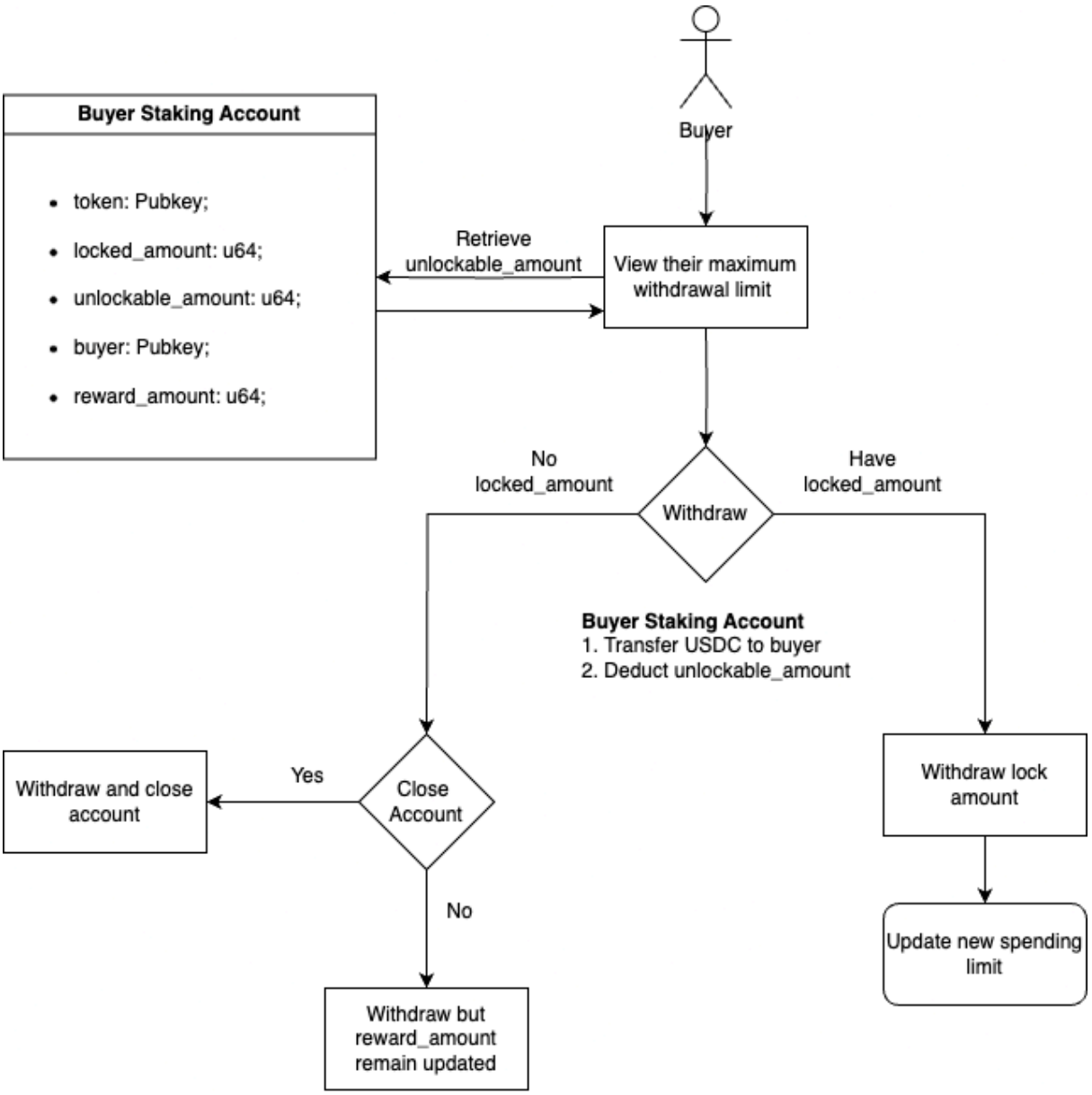
- token: Pubkey;
- locked_amount: u64;
- unlockable_amount: u64;
- buyer: Pubkey;

- reward_amount: u64;

Proof of Future Payment Account (For Merchant to keep track of their incoming payment)

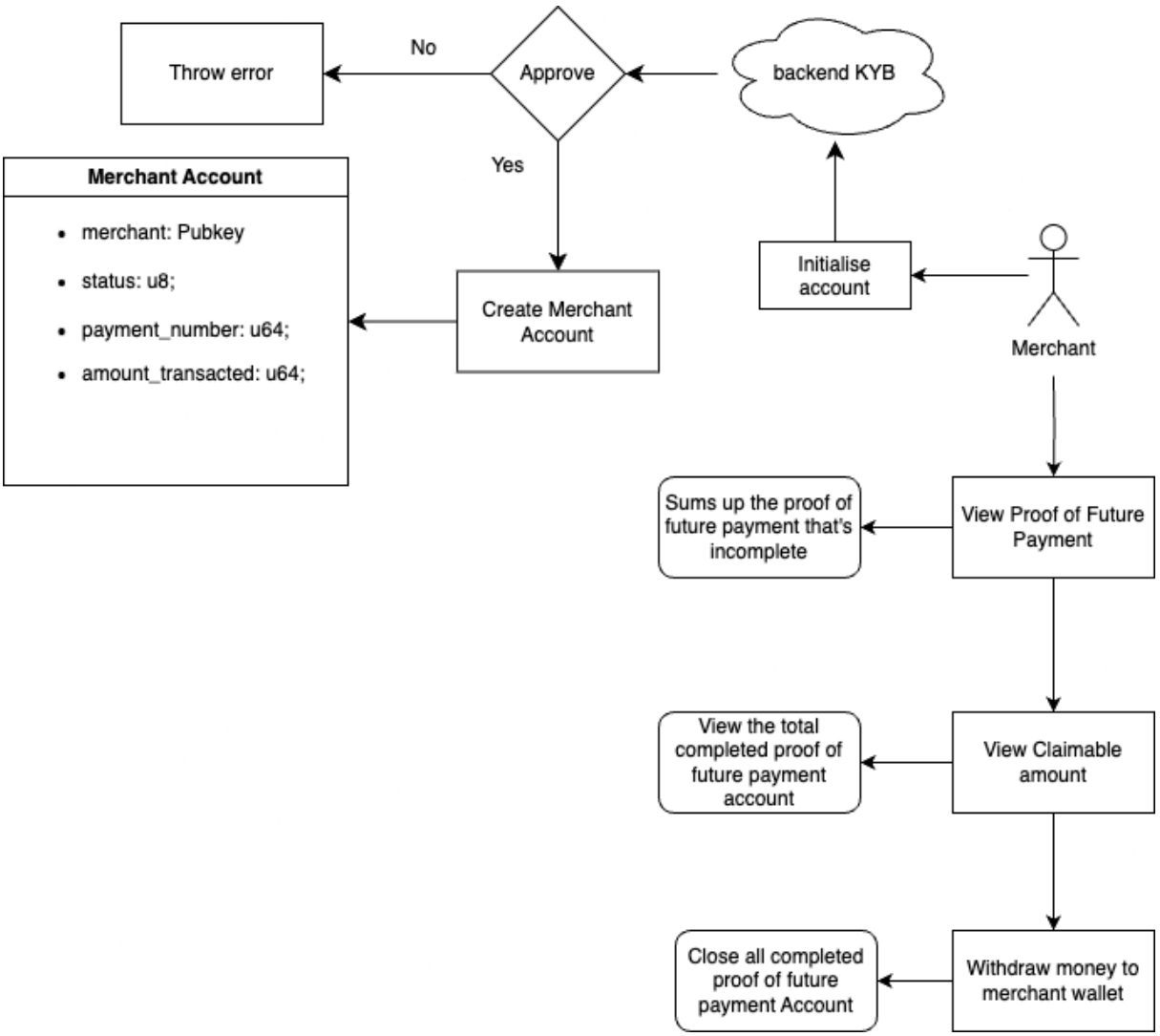
- payment_amount: u64;
- admin: Pubkey
- buyer: Pubkey
- merchant: Pubkey;
- completed: u8;
- payment_number: u64;
- amount_fulfilled: u64;

2.2 Buyer Unstake



2.3 Merchant Initialise and View

Merchant will need to initialise and register their wallet with us. A KYB Process will be in place to ensure that the business is legitimate.



Merchant Account State

- merchant: Pubkey
- status: u8;
- payment_number: u64;
- amount_transacted: u64;

3. Overview

1. User Deposit/Stake

- Initialised Buyer’s account on protocol
- Deposited USDC will be added to the unlockable_amount.
- Token will be staked with transferred to the Protocol account then to Lending Protocol account which interact with Kamino/Solend and the interest transferred will be added back into the unlockable_amount and reward_amount..

2. User can view their reward
    - User can also see their respective APY and amount earned through their reward_amount
3. User can purchase an item with one of our merchant that support our protocol
    - Once the transaction is verified off-chain along with the correct item and price, an admin signature will be used to create a Proof of future payment account. The proof of payment_number will be an identification with the same proof of payment_number on merchant and for identification, and after every new proof of future payment account creation, the merchant payment_number will increase by 1.
    - The unlockable_amount will be reduced based on the purchase amount and locked_amount will be increase to ensure the payment to be paid to their respective proof of future payment.
4. Merchant can receive payment from their proof of payment.
    - The protocol account will periodically check the lowest payment_number & incompleted proof of future payment account and transfer reward to them first instead of the staking contract account if there’s outstanding proof of future payment to be paid by the buyer.
    - Once the proof of future payment is fulfilled and completed, the staking account locked_amount will be reduced and added to unlockable_amount.
    - the completed proof of future payment will be closed.
5. User can withdraw their reward and locked amount
    - If user decide to withdraw their fund, they can partially or fully withdraw from the unlocakable_amount and rewards

- For full refund, the user can choose to close the account and fully receive back their fund for the space.

Summary of USDC Flow Between Accounts

Main Flow of Funds

1. Buyer deposits USDC → Protocol Vault → Lending Protocol
2. Interest generated → Protocol Vault → Buyer’s Staking Account
3. Buyer makes a purchase → Initiate Proof of Future Payment
4. Interest generated → Protocol Vault → Proof of Future Payment
5. Merchant’s payment → Protocol Vault → Merchant Wallet
6. Buyer unstakes/withdraws → Protocol Vault → Buyer Wallet