W3B Ecosystem

Status	Doing

1. Distribution Layer
   a. Main portion of the application serves as a e-commerce marketplace for the physical redemption of Goldbacks asset class. Connects standard e-commerce flows with Web3 payment settlement layer

Two distinct purchase flows:

1. Direct Cart Purchase: Users redeem a physical goldback by player to player purchase via web3 settlement layer
2. SP3N/Amazon Integration: Allows users to spend crypto(USDC) to buy real-world items.

Onramp layer: integrates deeper purchase options if funds are low(Coinbase Onramp)

Tokenization logic:
A digital token can only come into existence if a cryptographic proof demonstrates that a unique, physical Goldback serial number has been locked in the registry.
The Blockchain shall not mint a token unless the Vault proves it has the asset

Layer 1: Physicality Of Items

- Input: Physical Goldbacks.
- Every Goldback has a unique Serial Number.
- Action: API services hashes these serials using SHA-256.
- The Merkel Tree; These hashes are organized into a Binary Merkel Tree. The “Root” of this tree is an single 32 byte fingerprint that uniquely represents the

entire vaults inventory.

Layer 2:

- Problem: How do you prove we have 1k unique items without revealing the entire database to competitors?
- Solution: Zero-Knowlege Proofs (Noir Circuits)
- Logic: ZK Circuit acts as an “Digital Notary”: It takes the list of serial hashes(Private input) and performs three checks:
    1. Solvency Check: Does Count(Serials) ⇒ Total Supply?
    2. Integrity Check: Do these serials actually generate the public Merkle Root?
    3. Uniqueness Check: Are there any duplicates in the list(Prevents double counting)

Output: A ZK Proof. This is a small cryptographic receipt that says. “I have checked the private list. It is sorted, unique, and valid. It matches the Root.”

Layer 3: On Chain Truth

- Enforcing: Solona Smart Contract
- Instructions: Mint
    - The contract looks at its internal state: proven reserves vs total supply.
    - If you try to mint 100 tokens , but the ZK proof only shows 99 items, the transactions fails automatically.
    - Code is Law here: No admin key can override this. The math prevents inflation

This proposed architecture approach converts Goldbacks from a physical collectible into a programmable trust-minimized financial layer