Skeleton Framework – Technical Development Plan

*Audience: **Keymaker** (co-developer) & core engineering team*

---

0 · Mission Statement

Build a **pilot-agnostic Web3 framework** that can power VCAN, SAM, and Reparations without hard-coding social logic. Contracts should be upgrade-safe, oracle-extensible, and portable across Ethereum mainnet, Arbitrum Orbit, and Polygon CDK.

---

1 · Repository Blueprint

```
monorepo/
├ packages/
│  ├ contracts-core/        # base libs & abstract modules
│  ├ contracts-modules/     # plug-in supply/oracle/escrow logic
│  ├ contracts-pilots/      # thin adapters (VCAN.sol, SAM.sol, RBA.sol)
│  ├ subgraph/              # Graph schema & mappings
│  ├ sdk/                   # TypeScript client (ethers v6 + viem)
│  ├ api/                   # Next.js /app router + Supabase adapters
│  └ ui/                    # React (shadcn/ui + Tailwind) components
└ infra/
   ├ hardhat.config.ts      # tests, local node
   ├ foundry.toml           # invariant & fuzz tests
   ├ github/                # Actions workflows
   └ cloud/terraform/       # optional k8s / Cartesi (oracle)
```

---

2 · Core Solidity Libraries

Purpose	Library	Version	Notes
ERC standards	**OpenZeppelin Contracts**	^5.0	ERC-721, 1155, 20, AccessControl, Governor, UUPS.
Upgrades proxy	**OpenZeppelin Upgrades Plugin (Hardhat)**	^2	UUPS proxy deploy + admin CLI.

Purpose	Library	Version	Notes
Cross-chain	**LayerZero Endpoint**	^1 (testnet)	Non-blocking messaging for Governor sync.
Oracle verify	**Chainlink Functions** & **OCR**	latest	Sensor batch + appraisal digest proofs.
Math / utils	**Solmate**, **PRB-Math**	latest	Gas-efficiency in Fractionalizer & SupplyController.
Payment split	**0xSplits** or OZ `PaymentSplitter`	latest	Revenue flow to fractional share holders.
Security testing	**OpenZeppelin Defender + Sentinels**	latest	Auto-pause triggers on oracle faults.

3 · TypeScript / Off-Chain Libraries

Layer	Lib / Tool	Version	Use
Build / node	**pnpm**	^8	workspace monorepo manager
EVM dev	**Hardhat**	^2.21	compile, local node, scripting
Fuzz / invariants	**Foundry** (`forge`, `cast`)	nightly	property tests, gas reports
Codegen types	**TypeChain**	latest	typed contract wrappers
Wallet hooks	**wagmi** + **viem**	v2-beta	React wallet & transaction flows
UI kit	**shadcn/ui** + **TailwindCSS**	latest	design-system alignment
Data store	**Supabase JS**	^2	KYC, POAP attendance, contributor db
Indexer	**@graphprotocol/graph-cli**	latest	deploy sub-graph to Hosted Service
Cross-chain	**@layerzerolabs/viem-plugin**	soon	messaging hooks in SDK
Lint / format	**eslint**, **prettier**, **husky**	latest	repo hygiene

4 · Module-by-Module Build Spec

4.1 TokenFactory (contracts-core)

- UUPS proxy; emits ERC-721, ERC-1155, and stores {pilotId, idRange} mapping.
- Emits `TokenFamilyCreated(pilotId, baseId, standard)` event.
- Guards: only `Governor` or `PilotAdmin` can call.

4.2 Registry (contracts-core)

- Mapping `pilotId → Config` (treasury, governor, oracleRouter, paramsHash).
- `setConfig` gated by 2-of-3 root multisig.

4.3 Fractionalizer (contracts-modules)

- `deposit721(tokenId, supply, shareName)` locks NFT, clones MinimalProxy ERC-20.
- `defractionalize()` burns all shares, releases NFT.
- Events feed sub-graph for share price charts.

4.4 SupplyController (contracts-modules)

- Strategy pattern: `ISupplyPolicy` interface → VCANSensorPolicy, AppraisalPolicy.
- Each pilot adapter inherits & plugs its policy.

4.5 OracleRouter (contracts-core + infra/cloud)

- Thin contract verifies EIP-712 signed payloads.
- Off-chain node (TypeScript) fetches sensors/appraisals, runs consensus via Chainlink OCR, signs batch.
- Fallback manual signer (`ReportManual`) emits same event schema.

4.6 EscrowSplitter / Streamer

- Pull-payment using OZ `PaymentSplitter` OR LlamaPay stream.
- Upgrade-safe via proxy.

4.7 Governor Suite

- OZ governor w/ module for weight multiplier (e.g., CAC 1x, RN 10x).
- LayerZero sync adapter for cross-domain proposals.

4.8 Sub-graph Schema (packages/subgraph)

```
entity Pilot { id: ID!, chainId: Int, name: String }
entity Asset { id: ID!, pilot: Pilot!, type: String, metadataURI: String }
entity Share { id: ID!, asset: Asset!, holder: Bytes!, amount: BigInt }
entity OracleReport { id: ID!, pilot: Pilot!, payloadHash: Bytes, tx: Bytes }
entity Vote { id: ID!, pilot: Pilot!, proposalId: BigInt, voter: Bytes, weight:
BigInt }
```

4.9 SDK-TS

- Wraps ethers-v6 + viem for chain calls.
- Generates React hooks: `useMintSFT` , `useLockNFT` , `useClaimRevenue` .

---

5 · DevOps & Security

- **GitHub Actions** – lint → compile → test → slither → forge fuzz → deploy to `(chain)_preview`.
- **Slither** CI severity gate (no high / medium on `main`).
- **Echidna** invariants: non-reentrant, totalSupply benches.
- **Immunefi** bug bounty opens post testnet.
- **OZ Defender Sentinel** monitors oracle lapse, auto-pauses SupplyController.

---

6 · Milestone Roadmap (detail)

Sprint	Modules & Infra	Deliverables	Demo & Review
0 **Kick**	Repo skeleton, CI, pnpm workspaces	green CI on empty contracts	walk-through with Keymaker
1 **Fabric**	TokenFactory + Registry + tests	deploy on Base Sepolia; `deploy.ts` script	K meets CLI deploy
2 **Pulse**	OracleRouter stub + off-chain node mock	emit `OracleReport` events unit test	tx decode in sub-graph
3 **Slice**	Fractionalizer + share ERC-20 factory	lock dummy NFT, mint shares	UI pop–up shows balances
4 **Flow**	SupplyController α (VCAN sensor math)	fuzz tests pass; faucet UI	Keymaker + Free sign sensor JSON
5 **Govern**	Governor module + cross-chain adapter	proposal passes on testnet	LayerZero log check
6 **Graph**	Sub-graph root, SDK codegen	React table lists assets	Keymaker code review
7 **Pilot-Adapters**	VCAN.sol, SAM.sol, RBA.sol	smoke tests mint/pledge	internal demo call
8 **Security Freeze**	Slither + Echidna full run	0 high / medium issues	external audit kickoff

---

7 · On-Boarding for Keymaker

1. Clone: `git clone git@github.com:demeter-dao/monorepo.git`
2. `pnpm i` (root) → installs all workspaces.
3. `pnpm dev` (infra local node + UI hot-reload + sub-graph)
4. `forge test` – run invariants.
5. Open `/docs/CONTRIBUTING.md` for branching rules and commit lint.

Keymaker's initial focus ➜ **Sprint 1 TokenFactory + Registry tests**. When ready, open PR labeled `core`.

End of technical development plan v1 • 28 Jun 2025