Hypercerts: an Interoperable Data Layer for Impact-Funding Mechanisms

@davidad, June 2022 Draft

1 Introduction

This technical report proposes a new kind of ledger for tokenized certificates that are NFT-like in some dimensions, but fundamentally are fungible (like stock certificates), facilitate allocating retrospective rewards to prospective funders, and facilitate hierarchies of credit assignment and pricing mechanisms. It does all this without imposing any specific mechanisms, thereby facilitating experimentation, but provides baseline invariant guarantees such as that claims will not be forgotten as different mechanisms come into and out of fashion, and enables different kinds of mechanisms to interface naturally with each other.

2 Specification

2.1 State

A full *state* of a hypercert ledger is a tuple $S = (A, X, e, P, C, H, F)$ consisting of:

1. A finite set A of *axes*
2. For each $a \in A$, a topological space X_a whose topology is generated by a subcountable base $e_a : \mathbb{N} \rightharpoonup T_a \subseteq \mathcal{O}(X_a)$ which is closed under finite intersections and such that $\forall t \in T_a,\ t = \operatorname{int}\operatorname{cl} t$

   Definition 2.1. *$X := \prod_{a\in A} X_a$ as a product of topological spaces, and $T := \left\{\bigcap_{a\in A} t_a \middle| \forall a, t_a \in T_a\right\} \simeq \prod_{a\in A} T_a$.*

   Semantically, X is a "space of public goods."

   Theorem 2.2. *T is a subcountable base for X that is closed under finite intersections and such that $\forall t \in T,\ t = \operatorname{int}\operatorname{cl} t$.*
3. A finite set P of *people* (cryptographic identities), with a designated element $B \in P$ called the *burn address* for which signatures are impossible
4. A designated element $C \in A$ called the *contributor axis* such that $X_C = P \simeq T_C$ (i.e. X_C is P, with the discrete topology)
5. A finite subset $H \subseteq P \times T$; each element $h \in H$ is a *hypercert* (semantically, a "fractional territorial claim on a hypercubic region of public-goods space")
6. A function $F : H \to [0, 1]$ which gives the *ownership fraction* for each hypercert

2.2 Desired invariants

Definition 2.3.

$$f_S : X \to \mathbb{R} := x \mapsto \sum_{\{(p,t)\in H | x\in t\}} F(p, t)$$

$$f_{S,q} : X \to \mathbb{R} := x \mapsto \sum_{\{(p,t)\in H | p=q \wedge x\in t\}} F(p, t)$$

Note: It follows from the definitions that $0.0 \leqslant f_{S,q}(x) \leqslant f_S(x) \leqslant 1.0$.

Given two full states $S = (A, X, e, P, C, H, F)$ and $S' = (A', X', e', P', C', H', F')$, if S' is reachable from S by a (possibly empty) sequence of valid transactions signed by none other than members of $Q \subseteq P$ (written $S \xrightarrow{*}_Q S'$), then the following should hold:

1. Contributors must approve minting:
$$\forall x' \in X', \left[f_{S'}(x') > f_S(x')\right] \Rightarrow \pi_{C'}(x') \in Q$$
2. Owners must approve transfers:
$$\forall x \in X, \forall q \in P, \left[f_{S',q}(x) < f_{S,q}(x)\right] \Rightarrow q \in Q$$
3. (Almost all) claims are never forgotten:
$$\operatorname{cl}\left\{x \in X \middle| f_{S'}(x) \geqslant f_S(x)\right\} = X$$
4. All claimed points continue to have a well-defined fractional allocation:
$$\left[\forall x \in X, f_S(x) = 0 \vee f_S(x) = 1\right] \Rightarrow \left[\forall x' \in X', f_{S'}(x') = 0 \vee f_{S'}(x') = 1\right]$$
5. Axis compatibility: $A \subseteq A'$, $P \subseteq P'$, $C = C'$, and for each $a \in A$, $X_a \subseteq X'_a$ and $\forall n \in \mathbb{N}$ such that $e_a(n)$ is defined, $e_a(n) = X_a \cap e'_a(n)$

Ideally, the above invariants would be tightly characterizing in the sense that $\left[S \xrightarrow{*}_Q S'\right] \Leftrightarrow$ Invariants. This goal guides the design of the individual transactions. The much more important direction to be careful about is $\left[S \xrightarrow{*}_Q S'\right] \Rightarrow$ Invariants, but note that this direction by itself is trivially satisfied by a system that allows no transactions of any kind (i.e., that lets $S \xrightarrow{*}_Q S'$ if and only if $S = S'$).

2.3 Transaction definitions

2.3.1 Mint

If for some $c \in P$ and $t \in T$, $\pi_C(t) = \{c\}$ and $\forall (p,h) \in H_S, t \cap h = \varnothing$, then we allow the transaction

$$S \rightarrow_{\{c\}} \left(\ldots, H_S \cup \{c,t\}, F_S \left[(c,t) \mapsto 1 \right] \right)$$

2.3.2 Atomic Merge & Split

Given a finite subset $\{c_k | k < \ell\} \subseteq P$ and two finite subsets $\{Y_i | i < n\} \subseteq T$, $\left\{ Z_j \middle| j < m \right\} \subseteq T$, a number $q \in [0,1]$, for every $i < n, k < \ell$ a number $q_{i,k} \in [0,1]$, and for every $j < m, k < \ell$ a number $q'_{j,k} \in [0,1]$, then if the following conditions hold:

$$\bigcup_{i<n} \mathrm{cl} Y_i = \bigcup_{j<m} \mathrm{cl} Z_j$$

$$\forall i, i' < n, i \neq i' \Rightarrow Y_i \cap \mathrm{cl}\, Y_{i'} = \varnothing$$

$$\forall j, j' < m, j \neq j' \Rightarrow Z_j \cap \mathrm{cl}\, Z_{j'} = \varnothing$$

$$\forall i < n, \sum_k q_{i,k} = q$$

$$\forall j < m, \sum_k q_{j,k} = q$$

$$\forall i < n, \forall k < \ell, F_S(c_k, Y_i) \geqslant q_{i,k}$$

Then we allow the transaction

$$S \rightarrow_{\{c_k | k < \ell, \exists q_{i,k} > 0\}} \left(\ldots, \left(H_S \backslash \{(c_k, Y_i) | F_S(c_k, Y_i) = q\} \right) \cup \{(c_k, Z_j) | q'_{j,k} > 0\}, F_S \begin{bmatrix} (c_k, Y_i) \mapsto F_S(c_k, Y_i) - q_{i,k} \\ (c_k, Z_j) \mapsto F_S(c_k, Z_j) + q'_{j,k} \end{bmatrix} \right)$$

2.3.3 Burn

If the burn address B comes to hold hypercerts, they are considered burned. Technically this does not need a separate transaction type.

2.3.4 Modify Axes

This remains to be worked out. Without this transaction type, axis compatibility is trivially satisfied.

3 Suggested axes

- C, the contributor identities (structurally required)
- A_R, the set of included rights (beyond just bragging rights), e.g.:
  - altruistic retrospective rewards
  - reputational retrospective rewards
  - rights to toll-driven income from associated intellectual property
- W, covered scope of work (with the degenerate case being all of X_W)
- A_{TW}, covered time of work (e.g. a grant duration; degenerate cases being the entire past, entire future, or even all of time)
- A_{TF}, covered time of fruition/consumption (with the degenerate case being the entire future)

Note that fractional ownership can be thought of as an additional "shadow" axis (though I recommend against implementing it that way); if one thinks of it this way, then ownership of a particular hypercube can indeed be considered non-fungible (indivisible).

4 Algorithms

The main operations we need to check the conditions for atomic merge & split are

- To compute the intersection of ts
- To compute the intersection of t with the closure of a t'
- To compute a representation of $X_a \backslash \bigcup_{i<n} \mathrm{cl}\, t_i$ (which is an open set of $\mathcal{O}(X_a)$) as a union $\bigcup_{j<m} t'_j$

Given these operations, we can check whether $\bigcup_{i<n} \mathrm{cl} Y_i = \bigcup_{j<m} \mathrm{cl} Z_j$ by computing for each $i < n$ the intersection $Y_i \cap \left(X \backslash \bigcup_{j<m} \mathrm{cl}\, Z_j \right)$ and confirming it is $\varnothing$, then doing the converse (checking all intersections $Z_j \cap \left(X \backslash \bigcup_{i<n} \mathrm{cl}\, Y_i \right) = \varnothing$).

5 Proofs