Escrows are optics

Daniele Palombi

We provide a categorical interpretation for *escrows*, i.e. trading protocols in a trustless environment, where the exchange between two agents is mediated by a third party where the buyer locks the money until they receive the goods they want from the seller. A simplified escrow system can be modelled as a certain kind of *optic* in a monoidal category $\mathcal{M}$ (e.g. the category of sets with the cartesian product).

Escrows can be regarded as morphisms of a category $\mathcal{E}(\mathcal{M})$ with the same objects of $\mathcal{M}$, and where the hom-objects are $\langle X, Y\rangle = \mathsf{Opt}_{\mathcal{M}}(\left[\begin{smallmatrix} Y \\ X \end{smallmatrix}\right], \left[\begin{smallmatrix} X \\ Y \end{smallmatrix}\right])$. When X is a comonoid and Y is a monoid in $\mathcal{M}$, $\langle X, Y\rangle$ is a monoid in Set (or in the base of enrichment chosen to model one's specific problem), acting on the set of optics $\left[\begin{smallmatrix} B \\ B \end{smallmatrix}\right] \to \left[\begin{smallmatrix} X \\ Y \end{smallmatrix}\right]$. Moreover, we define a map

$$\lhd : \langle Y, X\rangle \times \mathsf{Opt}(\left[\begin{smallmatrix} Y \\ X \end{smallmatrix}\right], \left[\begin{smallmatrix} B \\ B \end{smallmatrix}\right]) \to \mathsf{Opt}(\left[\begin{smallmatrix} Y \\ X \end{smallmatrix}\right], \left[\begin{smallmatrix} X \otimes B \\ Y \otimes B \end{smallmatrix}\right])$$

having action-like properties. This has the following interpretation: the object B acts as an intermediary in a transaction between X and Y, modeled by an escrow in $\langle Y, X\rangle$.