Formal Specification of the DAI Protocol

March 2, 2021

1   Introduction

The DAI Protocol is a complex system with a specific primary purpose: to create an asset ("DAI") that has a particular economic value in terms of some reference asset (for example, the US dollar).

Let the market price of DAI at a time t be given by $P_D(t)$ and the protocol's target price at t be given by $P_T(t)$. Then the system's goal is to equate these values:

$$P_D(t) = P_T(t) \tag{1}$$

In the above equation, $P_D(t)$ is measured value, whereas $P_T(t)$ is a function computed by the protocol. It may implicitly depend on any other time-varying quantity, such as the state of the rest of the DAI protocol.

The DAI asset is created by locking assets with economic value inside the protocol, and the system issues DAI as debt against such assets. The assets cannot be retrieved by their owner without repaying the debt they back. Each asset has various associated parameters (to be discussed later). The same asset market asset can have multiple representation within the system, corresponding to different parameters.

Asset and parameter combinations that determine collateral types are referred to as "ilks" and each is given a unique label. The set I denotes the set of all valid labels.

The system recognizes separation between accounts to which balances and positions are assigned. Accounts are drawn from a set U. A single external entity (for example, a person) may control multiple accounts simultaneously.

We are now ready to describe the basic balance and position structures.

Balances include collateral and DAI.

A position requires an ilk $i \in I$ and an account $u \in U$. It is given by:

$$\text{position}_{iu} = (\text{ink}, \text{debt}) \tag{2}$$