Formal Specification of the DAI Protocol

March 4, 2021

1 Foundations

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. It may also be a constant, as it currently is in the Ethereum mainnet deployment of multi-collateral DAI.

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 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 ilk 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. All quantities are assumed to be non-negative real numbers.

Balances include collateral and DAI. There is a balance for each user in each ilk, and also a DAI balance for each user:

$$\text{ilk } i \text{ balance of user } u \equiv \text{gem}_{iu} \tag{2}$$

$$\text{dai balance of user } u \equiv \text{dai}_u \tag{3}$$

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

$$\text{position}_{iu} = (\text{ink}_{iu}, \text{dbt}_{iu}) \tag{4}$$

where ink_{iu} is the quantity of collateral backing the issued DAI, which is given by dbt_{iu}.

To complete our foundational definitions, we introduce one additional system quantity, "unbacked debt", which is debt (issued DAI) that the system has created but is not backed by a collateralized position:

$$\text{unbacked debt} \equiv \text{vice} \tag{5}$$

This quantity will be needed for accounting purposes later; for now, we are able to define the first non-trivial invariant of the system:

$$\sum_{u \in U} \text{dai}_u = \text{vice} + \sum_{i \in I, u \in U} \text{dbt}_{iu} \tag{6}$$

This relationship is sometimes called "The Fundamental Equation of DAI".

The DAI Protocol, to this point, is characterized at time t by the following data:

P_T	target price of DAI in the reference asset
I	set of ilk labels
U	set of accounts
gem_{iu}	balance of user u in ilk i
dai_u	dai balance of user u
$(\text{ink}_{iu}, \text{dbt}_{iu})$	debt position of account u in ilk i
vice	DAI not associated with a position

2 Dynamics of Balances and Positions

We now begin to introduce the protocol's dynamics, starting with the rules for balances and positions.

The ilk balances gem_{iu} can be changed by transferring assets in and out of the protocol, transfers between accounts within the protocol, or by adding or removing collateral from a position. This can be represented with a temporal change identity that holds for any ilk i between any times t_2 and t_1:

$$\sum_{i,u} (\text{gem}_{iu}(t_2) - \text{gem}_{iu}(t_1)) = \text{inflow}_i(t_2, t_1) - \text{outflow}_i(t_2, t_1) + \sum_{u} (\text{ink}_{iu}(t_2) - \text{ink}_{iu}(t_1)) \tag{7}$$

where $\text{inflow}_i(t_2, t_1)$ indicates the total amount ilk i put into the system via inbound asset transfers in the time interval $[t_1, t_2]$ and $\text{outflow}_i(t_2, t_1)$ represents the total amount of ilk i removed from the system via outbound asset transfers in the time interval $[t_1, t_2]$. A balance gem_{iu} may only decrease if the action is performed by the owning account (u) or by an account authorized by u.

DAI, on the other hand, cannot meaningfully flow into or out of the system, since it is defined by the system. The change of DAI balances over time must

respect the conservation relationship defined earlier 6. A balance dai_{iu} may only decrease if the action is performed by the owning account (u) or by an account authorized by u.

The debt of positions can be manipulated only according to certain rules. The most important is that a position's debt may only increase if the resulting values will be *safe*. For every ilk i, the system must have knowledge of some market price $P_i(t)$ for that asset (in terms of DAI). There is further a per-ilk time-varying parameter $\text{CR}_i(t)$ that expresses the minimum ratio of collateral market value to debt. A position is said to be *safe* at time t if:

$$\text{dbt}_{iu} \cdot \text{CR}_i(t) \leq \text{ink}_{iu} \cdot P_i(t) \tag{8}$$

The quantity $\text{CR}_i(t)$ is referred to as the *collateralization ratio*. A further rule that applies to the increase of a position's debt is that it can only be effected by the account that owns the postion (u), an account authorized by u, or by an account with administrative privilege (for example, another component of the system, or a governance entity).

Decreasing the debt of a position is less constrained–such an action simply requires that the fundamental equation of DAI (6) be respected, along with ownership rules.

Removing collateral from a position (i.e. decreasing ink_{iu}) is similarly constrained to adding debt–the position must be safe after the removal, and the action may only be performed by the same the owning account (u), an account authorized by u, or a priviledged account. Adding collateral to a position need only respect 7 and ownership rules.

More general actions that simultaneously modify both the collateral and debt of a position are permitted, so long as the resulting position is safe, and all permissioning rules regarding decreasing collateral and increasing debt are obeyed.

Now we come to the concept of a stability fee. This describes the time evolution of a Vault's debt. Stability fees can serve at least three different economic functions within the system: incentivizing the creation or destruction of DAI as needed to close the gap between the market price and target price, offsetting the danger posed by risky or volatile assets held as collateral, and providing financial capital necessary for the operation of the system (as well as profit to its stakeholders if income exceeds costs). The core assumption justifying this is that entities that draw DAI against collateral derive economic benefit from doing so, and are thus willing to pay the system for the service of being able to borrow in a price-stable asset. The debt of a position can of course change discontinuously whenever new DAI is generated from it or repayed; in between these discontinuous jumps, it evolves according to a differential equation for the fees:

$$\frac{d\text{dbt}_{iu}}{dt} = \alpha_i(t)\text{dbt}_{iu}(t) \tag{9}$$

The function $\alpha_i(t)$ (different, potentially, for each ilk) is determined by some combination of feedback within the system and actions by governance to set

parameters. When the stability fee equation is integrated between times t_1 and t_2, the solution obtained is:

$$\mathrm{dbt}_{iu}(t_2) = \mathrm{dbt}_{iu}(t_1) e^{\int_{t_1}^{t_2} \alpha_i(t) dt} \tag{10}$$

If a discontinuous jump due to DAI generation, repayment, or liquidation occurs at t_2 which changes the debt by a quantity Δ, then evolution continues under 9 using $\Delta + \mathrm{dbt}_{iu}(t_1) e^{\int_{t_1}^{t_2} \alpha_i(t) dt}$ as the new initial debt value from time t_2 onwards. As stability fees accumulate, the additional debt is balanced by assigning an equivalent amount of DAI to one or more accounts in a special set of accounts V which belong to the system.

The state of the protocol at time t is, with the additions of this section, given by:

P_T	target price of DAI in the reference asset
I	set of ilk labels
U	set of accounts
gem_{iu}	balance of user u in ilk i
dai_u	dai balance of user u
$(\mathrm{ink}_{iu}, \mathrm{dbt}_{iu})$	debt position of account u in ilk i
vice	DAI not associated with a position
P_i	price of each ilk in DAI
CR_i	collateralization ratio of each ilk
α_i	stability fee factor of each ilk
V	set of accounts controlled by the system that receive all stability fees