Hedera Consensus Stablecoin

Software Design Description

Version 0.1.0

Prepared by Hedera Hashgraph

Updated 2020-08-24

Change History

Date	Revision	Contributors	Comment
2020-08-24	0.1	Ken ANDERSON	Initial Version

Table of Contents

1. Introduction

This Software Design Description ("SDD") provides the details for how a stablecoin should be built on Hedera's Consensus Service ("HCS"). The details are represented using UML notation and diagrams. This SDD is written to align with IEEE Std 1016-2009 "IEEE Standard for Information Technology - System Design - Software Design Descriptions".

1.1 Purpose

The purpose of this SDD is to provide context to stakeholders about the design decisions for a stablecoin on HCS. This document should also be used by:

- software developers to direct the development of the stablecoin source code
- devops to inform the configuration of development, continuous integration, and deployment environments
- test writers to guide testing boundaries and assertions to be included in the testing

1.2 Scope

The SDD will be used to develop a framework for implementing the InterWork Alliance (IWA) specification for a stablecoin, which has been thoroughly reviewed and formally modeled. This framework will include:

- a token contract written in Java and running on a token node, which will receive token messages from an HCS topic, validate the message, and mutate the state according to the logic of the IWA specification,
- a state API interface for reading the state from a token node,
- a payment API interface for facilitating payment of HCS messages,
- a token bridge service that will facilitate movement of the stablecoin between the HCS stablecoin and a matching Ethereum stablecoin smart contract,
- a sample client for buying, transferring, and selling stablecoins,
- and an administrative interface for monitoring the network and managing compliance-related functions on the network.

This framework **will not** address network governance, collateral management, or pre-issuance logic.

1.3 Context

A stablecoin is a type of digital token that is backed by another stable currency like fiat currency. The stablecoin token network will be used by client users to convert their fiat currency to a stablecoin. A stablecoin is valuable in a number of ways. It has the benefit of carrying the value of the underlying currency, having lower transaction costs relative to the underlying currency, can be transferred quickly with finality and a certain level of autonomy.

Stablecoins may be subject to regulatory oversight. They should provide certain functions that allow for compliance monitoring, evaluation, and enforcement.

2. References

Anderson, K., Bąk, K., Gorzny, J., Leckey, R., Thibeau, D., & Zulkoski, E. (2020, July). *Hedera High-Level Specification.* Retrieved August 2020, from https://docs.google.com/document/d/1-HC5G08X_f4qIxLVhrLn7NXQZyw10eErfgzrZunZJ9s

Software & Systems Engineering Standards Committee of the IEEE Computer Society. (2009, March 19). *1016-2009 - IEEE Standard for Information Technology - System Design - Software Design Descriptions.* Retrieved August 2020, from IEEE Explorer: https://ieeexplore.ieee.org/document/5167255

3. Glossary

Term	Definition
Hedera Consensus Service ("HCS")	One of four current services offered on the Hedera public network. This service accepts messages directed at a pre-defined topic, orders all messages globally, and outputs a fair ordered stream of messages.
InterWork Alliance ("IWA")	Organization that is the maintainer of the Token Taxonomy Framework, which is a collection of use-case specific token specifications.
Stablecoin	A digital currency of which the value is derived by its relationship to a fiat currency. An example is a stablecoin that is pegged to USD, ensuring that the coin is as stable as USD.
Token Node	A node that runs the token contract code, listens to state updates via the Hedera Consensus Service, validates and applies state updates to a persistent layer. Token nodes may be permissionless or permissioned per the requirements of the implementation.

4. Body

4.1 Identified stakeholders and design concerns

The stakeholders for this stablecoin include, but are not limited to:

- **token holders** who desire to have a more portable, secure, and financially stable mechanism for transacting real value through a trusted network.
- **token issuers** who seek to make financial interactions with their consumers and partners seamless and trusted.
- **regulators** who act to protect the network from malicious activity that may impact those they serve.
- **service providers** who provide a function of the system such as compliance monitoring, infrastructure hosting, liquidity, and custody.

4.1.1 Design Concerns

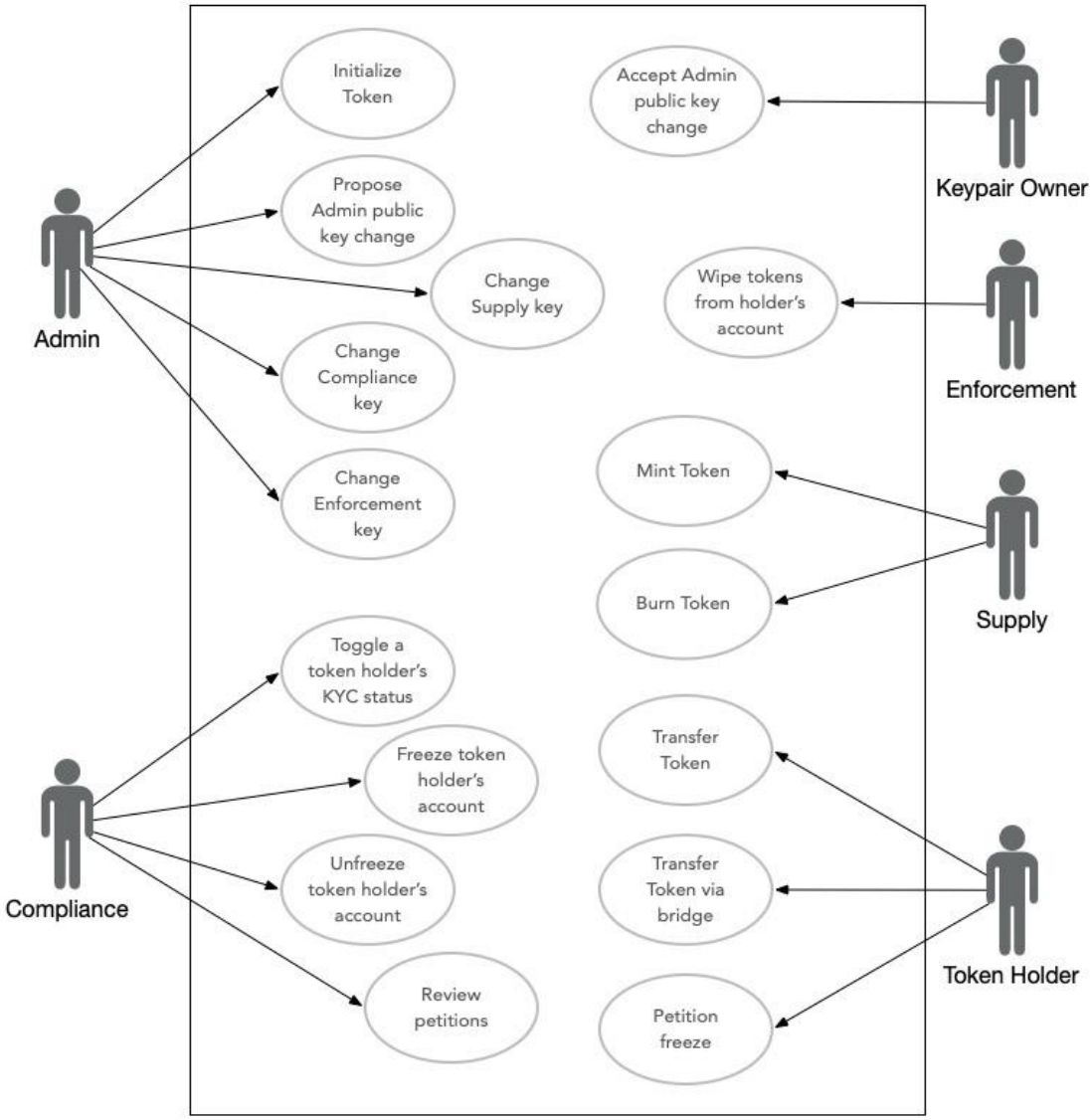
	Token Holder	Token Issuer	Regulator	Service Provider
System Services & Users				
Composition & Modularity				
Persistence				
Object Communication				

4.2 Context

4.2.1 Design Concerns

System services and users. The core actors in a stablecoin network are: administrator, token holder, compliance, supply, and enforcement. The administrator is also the owner of the stablecoin token and is responsible for the overall operation of the token and network. A token holder is a user of an application which interfaces with the token network and is the owner of tokens. Compliance monitors and evaluates network activity to identify suspicious or malicious token holders, freezing those who are not in compliance with the relevant regulation. Supply is responsible for the functions of minting and burning tokens on the network to maintain stability as it relates to the necessary collateral.

4.2.2 Use Case Diagram

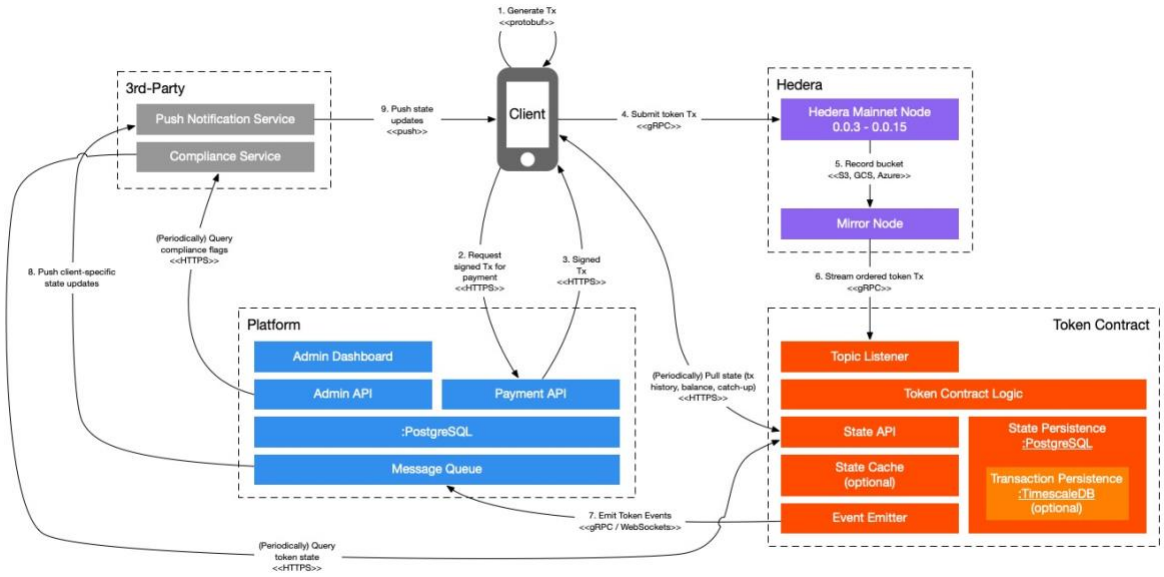


4.3 Composition

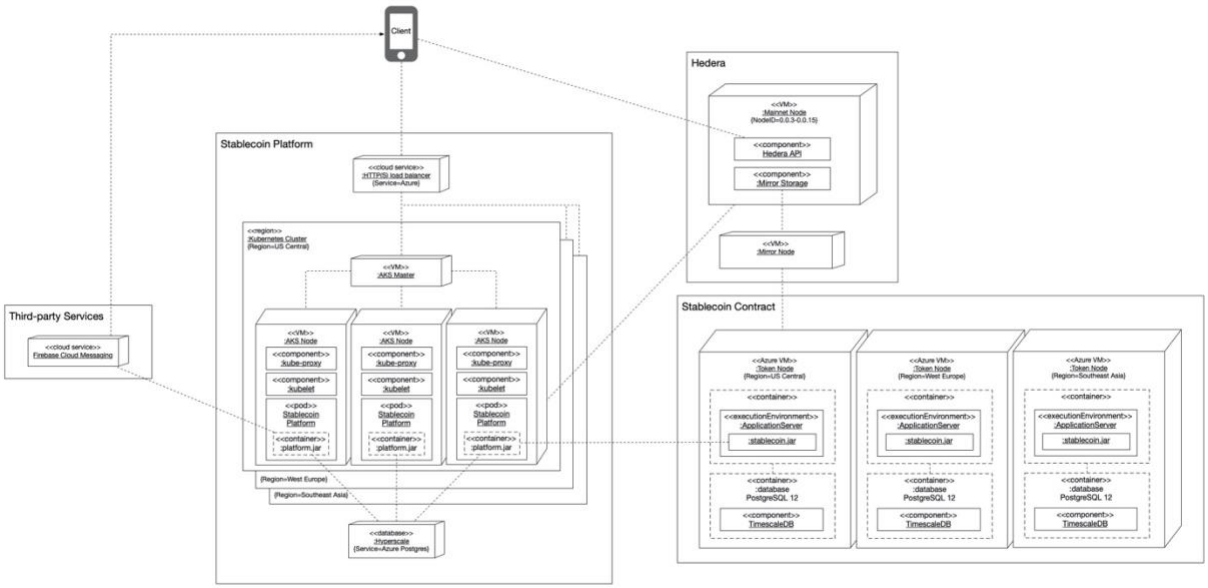
4.3.1 Design Concerns

Composition and modular assembly of the system in terms of subsystems and components. The component diagram illustrates the logical components of the network and a general flow of activity and communication across those components. The deployment diagram is a reference infrastructure architecture for implementation of the components of the token network.

4.3.2 Component Diagram



4.3.3 Deployment Diagram



4.4 Information

4.4.1 Design Concerns

Persistent information. The state of the token network represents the object of consensus that enables the stablecoin. Each token node on the network receives token ledger updates from the Hedera Consensus Service, validates the updates, and applies the changes to the state. If every node runs the same deterministic logic and receives the same series of updates from HCS then they are guaranteed to result in generating the same state. In this, in essence, is how token nodes can maintain consensus without ever communicating with each other.

4.4.2 Class Diagram / Token State

4.5 Interaction

4.5.1 Design Concerns

Object communication and messaging. The sequence diagram illustrates how the user application, platform, and token contract all interact to provide a complete system that delivers the desired functionality to stakeholders. In this diagram, the user is any actor who submits a transaction to the network to change state. This actor may be an administrator, token holder, compliance, or third-party service providers.

4.5.2 Sequence Diagram