Censer Litepaper

Table of Contents

1 專案概要

Censer 是基於 Polkadot， 採用民主治理的機器學習機器學習模型託管服務， 相較於傳統由公司帶領產品走向的方式，Censer 將部署權利下放到由開發商、消費者與第三方稽核者組成的 DAO，使多方利害關係人可決定機器學習機器學習模型的治理方向以及消費者賠償機制。

Censer 讓每個機器學習機器學習模型都是一個 DAO，有專門的存款來承擔再保險的責任，負責管理風險不確定的機器學習機器學習模型的部署（和反部署）。所有的部署都要有可驗證聲明智能合約可供第三方稽核者檢驗，檢驗不通過，則執行可驗證聲明智能合約的的賠償機制。

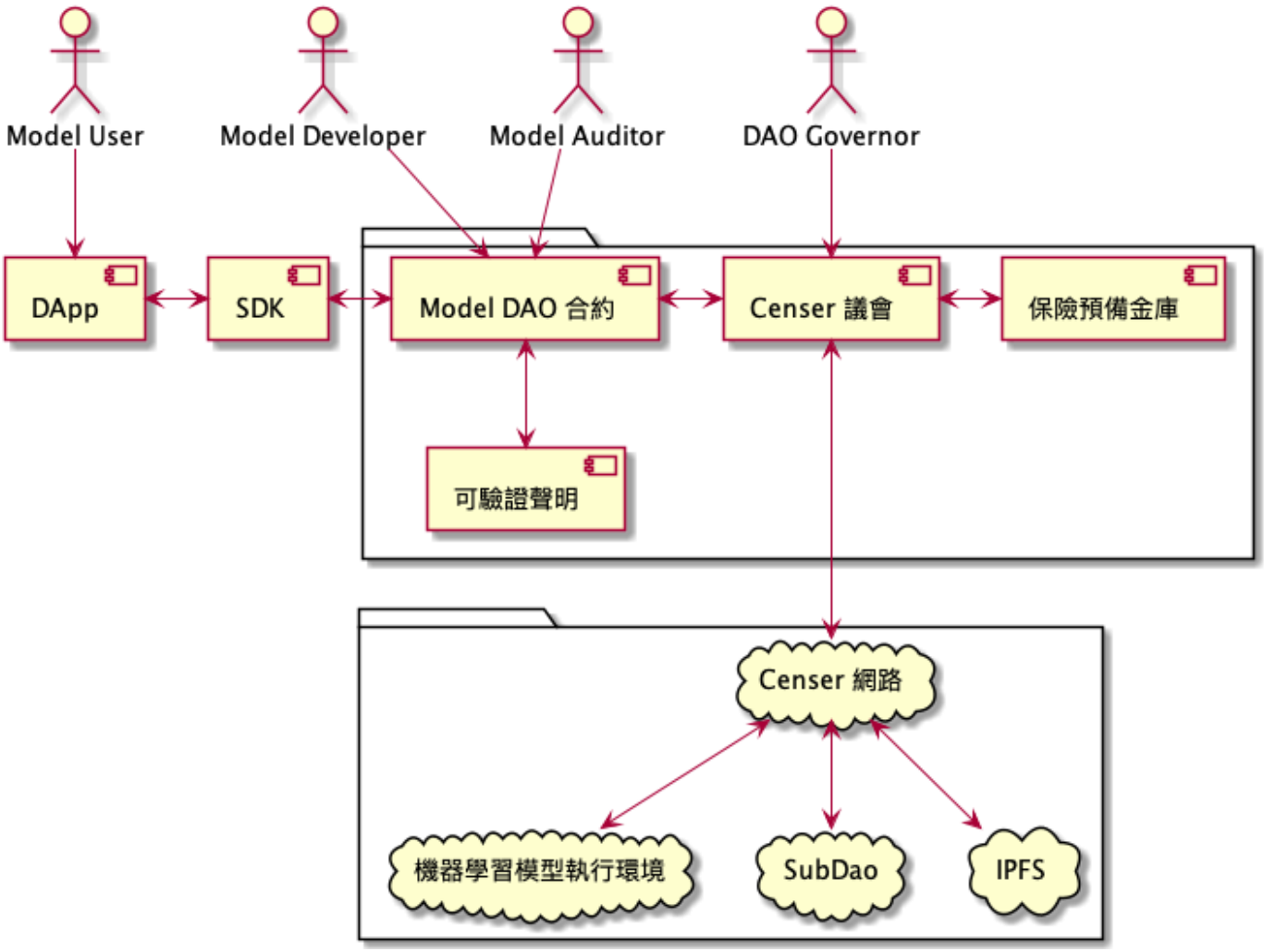
2 動機

由機器學習機器學習模型的投資者、開發者、使用者提撥一筆資金作為儲備金，在法律責任歸屬尚未明時，藉由智能合約的「無需信任」（trustless）特性，可以先動用儲備金支付損害賠償，使損害受到填補，也分散了機器學習開發者、使用者的責任風險，讓敏感的機器學習機器學習模型更容易被市場及監管者接受。

3 架構

Censer 專案將基於 Substrate 3.0、ink!，以及其它 Polkadot 平行鏈來達成目標。Censer 將包含 Censer 節點、Censer 議會、保險預備金庫，以及網頁前端。 DAO 相關的功能透過跨鏈通訊的方式或由 SubDAO 平行鏈實現。

3.1 基礎元件



3.1.1 Censer 節點（Censer Node）

由 Substrate 3.0 構建的客製化鏈節點，Censer 網路的基礎，包含一般節點的基本功能，同時提供連續部署跟執行機器學習機器學習模型的功能。

3.1.2 可驗證聲明（Verifiable Claims）

是支付機器學習模型保險金的智能合約，在該合約中會紀錄被保險的機器學習模型，被保險的機器學習模型的執行環境以及開發者聲明的特性，這個可驗證聲明可以不特定任何人嘗試證偽後取得獎勵，並使機器學習模型返回上一版本或是停止啟用，端看智能合約設定的條件。

3.1.3 保險預備金庫（Insurance Reserves Vault）

是存放機器學習模型保險預備金的智能合約，此合約管理任何有價代幣。

3.1.4 Web 前端（Web Frontend）

提供 Web 介面讓任何人可以跟 Censer 網路互動。前端介面提供基本的部署機器機器學習模型，質押保險金，轉帳等功能。基於 TypeScript 與 Node.js 開發。

3.1.5 SDK

此 SDK 讓 Model 開發者能將 DApp 與 Censer Network 互動。一開始將只支援 TypeScript。

3.2 使用情境

3.2.1 部署機器學習模型

機器學習模型開發者透過合約範本部署 DAO 機器學習模型，以及可驗證聲明合約。一開始 DAO 治理機器學習模型為 Moloch，這確保機器學習模型開發者、機器學習模型使用者、機器學習模型稽核者利益一致。

3.2.2 稽核機器學習模型

機器學習模型稽核者透過下載可驗證聲明合約，輸入可以證偽的「驗證資料集」（validation dataset)，取得稽核紀錄。

3.2.3 獎勵

機器學習模型稽核者提供稽核紀錄，比對可驗證聲明合約記載的條件取得稽核獎勵。

3.2.4 賠償

機器學習模型使用者提出賠償提案，賠償提案通過議會審議後支付賠償金。

4 Substrate / Polkadot 整合

Censer network 會以平行鏈的方式連接上 Polkadot。

4.1 Off-chain Worker

Censer Network 的節點會在 Off-chain Work 啟用的狀態下編譯。Off-chain Work 用於取得鏈外的資訊，例如機器學習模型與資料集；操作機器學習模型推論環境。

4.2 ink!

前面提到的智能合約將基於 ink! 開發，並運行在客製化的 pallet_contract。

5 開發路徑

Phase 1
: 完成上述提到的最小功能的 PoC 提供少數人測試。 功能包括：1. 機器學習模型推論, 2. 可驗證聲明 3. 保險預備金庫 4. 議會 5. 前端

Phase 2
: 支援更多機器學習機器學習模型框架跟可驗證聲明範本。

Phase 3
: 面向公眾提供服務。

Author: Hsin-Yi Chen

Created: 2021-05-03 Mon 17:13