# 針對海關的AEO解決方案

我之前為某地海關設計過改進AEO認證的區塊鏈方案， 它與供應鏈金融有相通之處，簡單介紹如下。

## 需求：

### 海關需求：

* 企業提供的通關數據如果能實現三流合一（單證流、數據流、資金流），就可以進行AEO認證，減輕海關工作難度。
* 在企業通關數據中，如果有一筆交易的數據有問題，海關需要企業提供與該交易的所有相關數據進行稽核。但因爲是被要求后才提供，所以企業有機會和動力針對這些數據造假，如何保證數據真實性？

### 企業需求：

* 業務經營三流數據是企業的核心數據，如果對外暴露，會讓外界對企業資金流狀況、訂單狀況等有清晰認識，相當於在激烈的市場競爭中把底牌暴露出來，因此是不可接受的。但是AEO認證帶來的好處，對企業來説是有吸引力的。如何平衡這兩者？
* 供應鏈金融能給企業帶來資金流，如何能獲得金融機構提供的供應鏈金融服務？

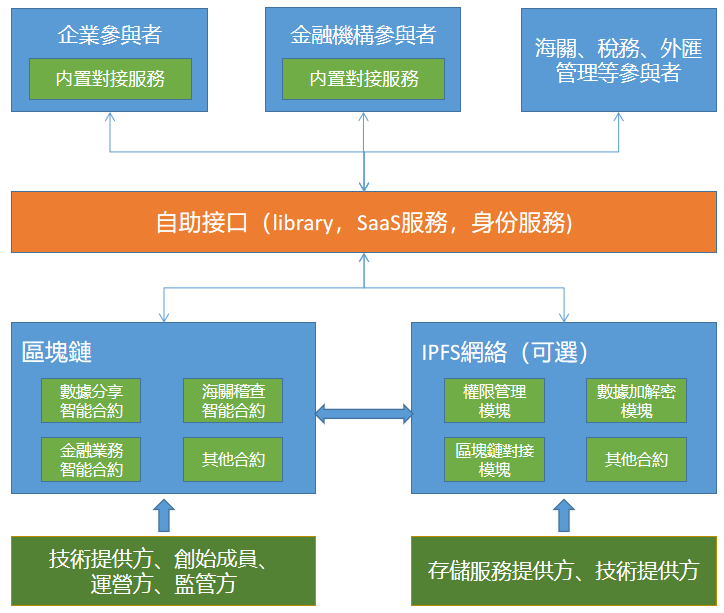
### 金融機構需求：

供應鏈金融業務的發展空間很大。但是供應鏈金融面臨諸多問題：

* 供應鏈金融是一單一單的，每單的營業利潤一般不是很大。但其風控工作的難度并不比其他業務小，因此如何降低風控成本、提高風控水平成爲關鍵。而風控的重點在於獲取企業的相關訂單、物流、資金流等數據，且企業各種數據必須保證真實。
* 有能力獲取貨物抵押品處置權。

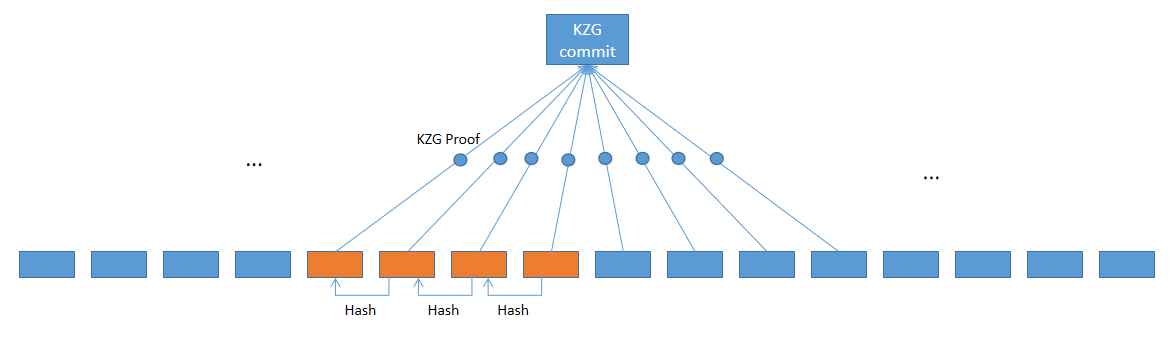
## 方案設計

針對如上各方需求，提出架構設計如下：



技術提供方、創始成員、監管方等創建區塊鏈和可選的IPFS網絡，通過接口層向企業、金融機構參與者、海關部門等提供區塊鏈服務。

下面介紹核心數據結構。該數據結構運行於企業内，定時從企業ERP等系統獲取數據，並上傳至區塊鏈。（使用溯源系統可能更加容易，但之前設計時出於非技術原因，考慮使用如下結構）。



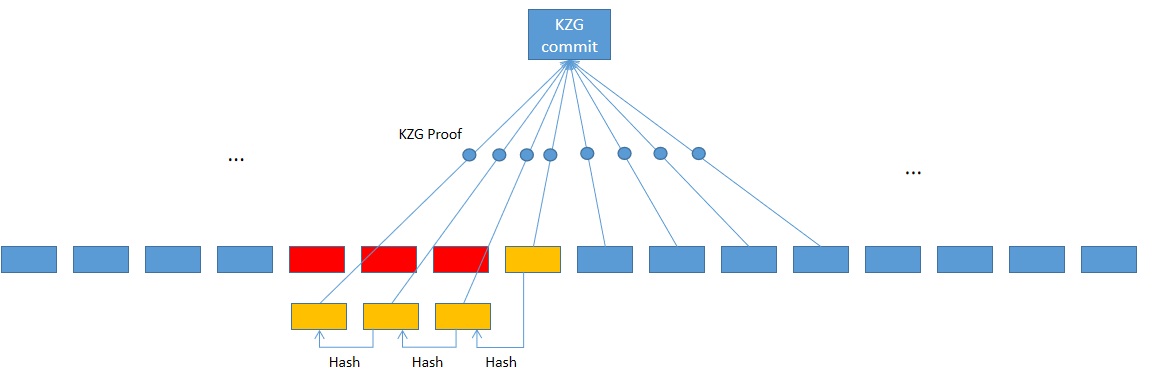
該數據結構用於讀取企業内訂單、物流、資金流等各類數據；定期生成承諾，將承諾上傳至區塊鏈，後續可針對承諾的數據生成證明，以證明企業數據未被篡改。

這是一個基於KZG承諾的數據。關於KZG承諾的介紹請見[這裏](https://dankradfeist.de/ethereum/2021/10/13/kate-polynomial-commitments-mandarin.html)。圖中每個葉子節點是一項數據的Hash值，樹根是所有數據的KZG承諾，是個固定大小的數據。針對每個葉子，都可以生成一個很小的證明，來證明該葉子屬於該樹根承諾。其功效類似於Merkle樹根及SPV證明。但是SPV證明的大小正比於Merkle樹的高度，所以對於擁有極多訂單的大企業來説，SPV證明是比較大的，驗證耗時也長。而KZG證明使用多項式特性，可針對大量數據（如上百萬個）提供極小的承諾和證明，以及極快的驗證速度（相應地，對大數據量來説，承諾生成計算量較大。但本場景中對該時間不敏感，因此適用）。

如上橙色四個數據來源於同一個訂單。對該訂單的每次變更（如資金流、物流更新）都是順序的，這些數據使用Hash值串聯在一起，因此通過該Hash順序即可確定該訂單的生命周期。針對一個訂單，其數據在其生命周期内應該是只能新增，不能刪除和修改的，就像區塊鏈的區塊一樣。

企業定期（如每天）讀取來自ERP等内部系統的訂單等數據，生成如上KZG commit，將其提交至區塊鏈上。後續儅需要針對某筆訂單申請供應鏈金融服務時，即可提供相應數據及證明，由金融機構輕易驗證相關數據的真實性。

安全性方面，如果企業想對某個訂單數據造假，它需要修改歷史上的多個數據，甚至要生成一條全新的數據鏈，這會造成從歷史KZG commit中移除該訂單的葉子節點，並新增一些節點，即如下情形，紅色葉子節點是被移除的正確數據，黃色葉子節點是新增的假數據：



因爲各個葉子節點之間使用Hash相連，因此必定從第一個虛假數據，至最新的數據，其均被從最新的KZG commit中移除。金融機構僅需對訂單的第一個歷史數據、最新數據、以及中間抽查極少數據，要求企業在歷史上對應的KZG commit上提供對應的存在證明即可。如果企業提供的數據是虛假的，它在歷史commit上就必然無法提供存在性證明。

使用該方案，可以獲得如下優點：

* + - 企業數據不外泄情況下，即可錨定海量訂單數據，僅需提供慾獲得供應鏈金融服務的訂單數據給金融機構即可。
    - 金融機構可以輕易證明企業數據是否有篡改，提升對數據的信任程度。
    - commit和proof的體積很小，讓企業、金融機構的區塊鏈gas消耗很低。
    - 儅一個訂單完全完成時，可以將其從後續的KZG commit中移除，避免浪費算力。
    - 對監管機構來説，該方案也足夠可信。

本設計中的IPFS網絡雖然是可選的，但如果部署該網絡，會讓整個系統更流暢，運行成本更低。因爲訂單證據比較大，不可能加密后上傳至區塊鏈，因此通過文件方式分享是最好的，否則有業務往來的兩個實體閒還需要建立可信的數據傳輸渠道。同時爲了保持文件私密性，文件需要考慮使用加密和權限管理能力，這要求對原生IPFS客戶端進行改造。

在區塊鏈選型方面，爲了同時保證安全性、業務開放性，使用單純的聯盟鏈和公鏈都是不合適的。因爲聯盟鏈裏每個參與方需要擁有自己的節點和CA系統，每個用戶也需要歸屬於某個參與方；而公鏈架構的安全性對資金資源要求較高，gas成本等也較高。因此需考慮將聯盟鏈和公鏈的特點結合起來，綜合選型。