Design and Implementation of Autonomous Identity System Based on OurChain

基於 OurChain 的自主身分系統設計與實作

Reporter: Chun-You Lin
Advisor: Chih-Wen Hsueh

委員好
我是林俊佑
指導教授是薛智文老師
現在要進行論文口試

我要報告的主題是: 基於 OurChain 的自主身份系統設計與實作

我的個人報告會包含 30 分鐘的內文與 5 分鐘的圖片 demo講解

Motivation

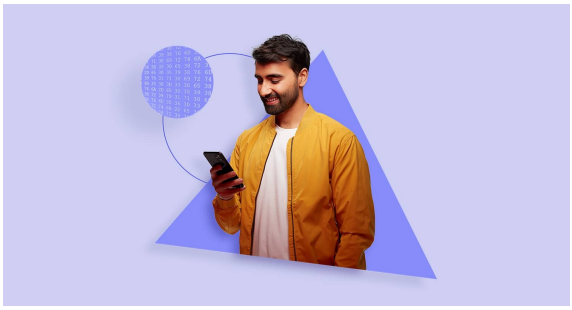
研究動機

2024/7/25 2

首先是我的研究動機

Digital Identity

- A collection of information about a person that exists online.
- Digital representation to access service



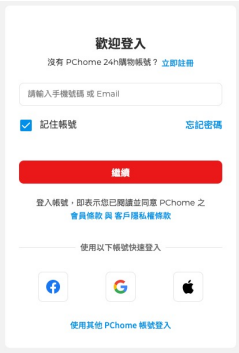
ref

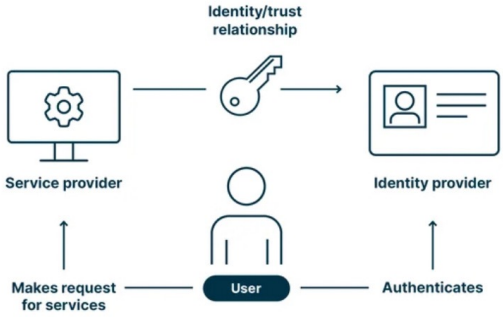
2024/7/25 3

數位身分能在數位世界中識別個人的資訊和資料，可以被定義為個人的數位表示方法。
更準確地說：數位身分是一組屬性，例如：姓名、出生日期和性別，以及ＩＤ。
換句話來說：數位身分即是個人的電子表示形式，可以讓人在網路上被認知到她是誰。
數位身分有許多紙本身份沒有的特性，例如可以透過數位管道遠端驗證個人身分或是追蹤個別活動並收集資訊等等

Google Login

- A collection of information about a person that exists online.
- Digital representation to access service





ref

2024/7/25

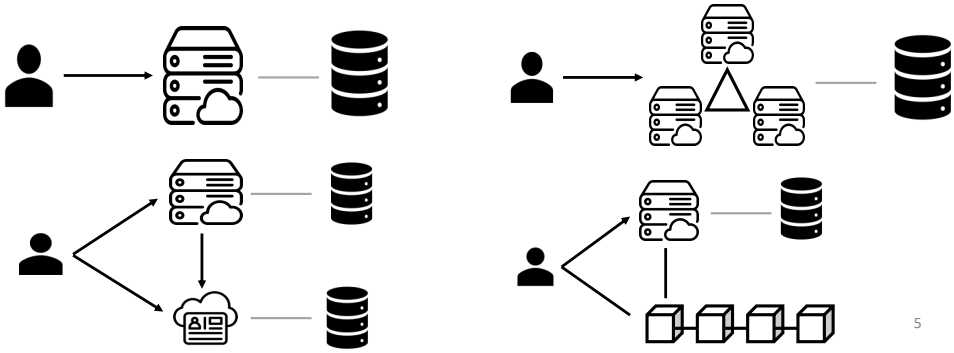
4

以使用 PC Home 網購為例：如果用戶想在 PC Home 上購物，他們可以透過現有的 Google 帳戶開設 PC Home 帳戶。
這是可能的，因為 Google 充當身分識別提供者 (IdP)，而 PC Home 信任 Google 作為身份提供者，這樣做的優點是顯而易見的：透過 Google 登錄，使用者可以節省時間並且只需管理一個帳戶。
這是以使用者為中心的身份管理，一種在數位世界中被廣泛接受的方法。
接著我們細看第三方登入的概念細節，
使用者對服務商做出請求，但服務商不知道使用者是誰，把使用者redirect到google的登入頁面，使用者在google登入後，google交給使用者一個JWT（json web token），使用者可以拿著JWT使用服務商的服務，因為Google發行的JWT內包含了google的簽章，而服務商信任google，因此服務商讓使用者使用服務。 至此，我們可以發現，第三方登入存在的支撐就是“服務商對身份提供者的信任”

當然，這裡還是補充一個基本假設：使用者必須要信任服務商與google才會使用服務與在google註冊身份

Trust Relationship Analysis

- People tend not to Trust anyone
- But Identity Management requires people to Trust it
- How users don’t need to Trust the service



2024/7/25 5

以下我展開來說明，歷史上的幾代身份系統如何面對信任問題，並且明確指出有什麼樣的信任問題從來沒有被解決。

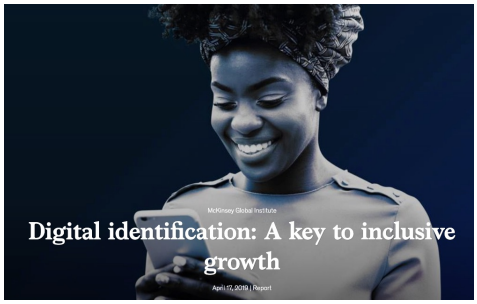
黑線的箭頭表示被迫產生的信任，黑色沒箭頭表示不是被迫產生的信任
左上角第一張圖: 描述的是最早的身份系統，中心化身份，用服務本身來控管使用者，使用者被迫要信任服務
右上角第二張圖: 描述的是聯盟身份，對等的服務聯合起來，彼此互相監控，互相信任，使用者轉為信任整個聯盟，一個人不能讓你信任，一群人你比較願意相信了。
左下角第三張圖: 描述的是以使用者為中心的身份，也是現今主流的第三方登入，讓大型企業擔任“公正的第三方”來協助用戶登入。注意，這邊不止加入了“公正第三方”，還加入了對數據的考量，因為他們知道，使用者之所以不信任服務，就是擔心服務隨便更改/外流/利用他們的數據，因此，讓數據分散到服務與公正第三方背後是一種面對信任，很好的做法。在這個模式下，使用者和服務都要信任身份供應商，另外使用者還是要稍微信任服務，因為他們知道即使服務商亂搞，也頂多影響到服該務商內部的數據。
右下角第四張圖: 描述了自治身份，他們使用區塊鏈技術下的智能合約來取代原先的身份提供者，最為新的公正第三方、注意，此時因為區塊鏈可以帶來信任的特性，至少相關開發者宣稱使用者和服務都能在無信任的情境下使用這個身

份提供者。(意思就是透過區塊鏈讓使用者自然信任, 不強迫使用者信任, 大家可以先對區塊鏈的這個性質有所記憶)

說到這裡，大家可以發現，有一個身份的信任問題從來沒有被解決，就是使用者對服務本身的信任。

Why Autonomous Identity

- Our users are not forced to trust anyone.
- The greatest value of the AID system is to keep users away from all the risks caused by trusting others.



ref 2030 : GDP 3% to 13%

2024/7/25 6

綜上所述, 我們發現從古至今的身份系統都存在著一個但書，那就是使用者對服務本身的信任。(甚至現在主流的使用者為中心身份還需要信任身份供應商)

那追根究底，到底我們為何需要AID（自主身份呢）? 為了讓我們的使用者不用被迫去信任任何人。

換而言之，AID系統最大的價值就在於讓使用者遠離所有信任帶來的危機。
我簡單向大家說明常見的危機:
包含：
•資料儲存：資料能否導出、資料是否會遺失、資料是否會被盜用
•GDPR: 被遺忘權、積極數據授權
•誰負責執行法規：服務提供者的？還是政府的？
當然還有一些對使用者更具傷害性的，例如因爲服務商的問題而導致:
•身份盜竊, 隱私保護, 假資訊, 網路霸凌

總而言之, 我沒辦法說完一個人的身份在網路上會遇到多少問題是來自於沒辦法自主掌握自己的身份, 但我可以給大家三個數字，讓大家了解數位身分的改革勢在必行。
根據美國投資機構麥肯錫，追蹤研究了七個重點國家的結果，他們認為擴大數

位身份的全面覆蓋，配合新的機制與應用，在2030年有望釋放整個國家3%到13%GDP的無價值成本。
我不認為這是空穴來風的數據，因為光台灣去年的詐騙總額就超過2000億台幣，佔GDP約0.9%，甚至還在高速上升，這都是自主身份的進步能解決的問題

Contribution

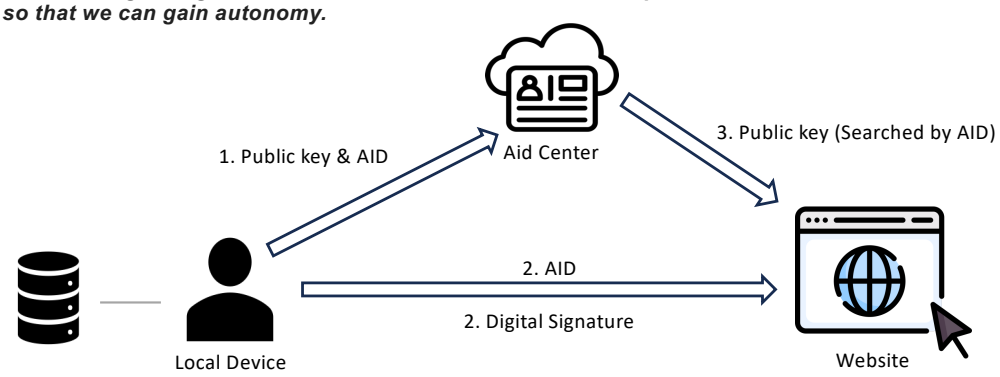
主要貢獻

2024/7/25 7

接著是我的主要貢獻

First Autonomous Identity

- Yuxuan, Lin: The Design and Implementation of Autonomous Identity for Social Network
- ***We use a digital signature scheme to do authentication, and put the data in local machine, so that we can gain autonomy.***



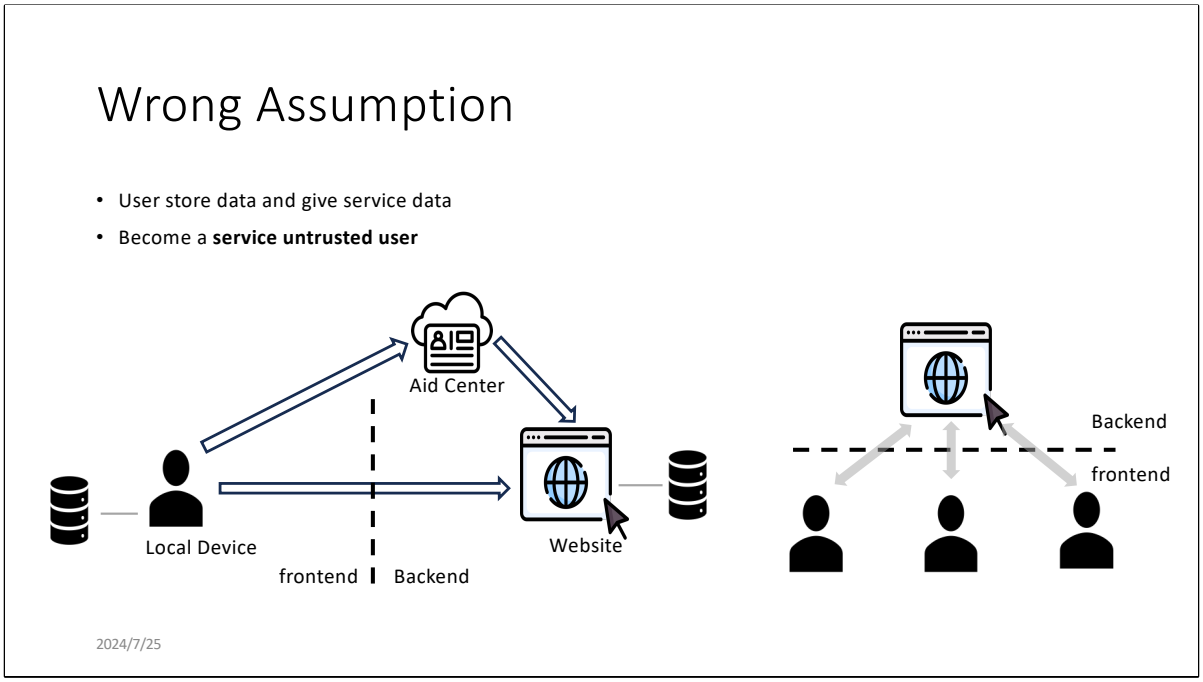
2024/7/25

AID最早的設計出現在本實驗室，由學長林玉環設計，完整的概念是:

1. 在個人設備產生 AID 與公鑰和私鑰
2. 把公鑰和 AID 傳入 Aid Center
3. 登入時網頁使用存在第三方伺服器內的公鑰解密使用者傳入的數位簽章，比對得知AID是否正確，其也作為一種驗證手段。因為私鑰由使用者自行掌握。

這步完成的是驗證的自主，下一步透過將數據保留在本地裝置完成數據的自主。

透過這樣的設計，學長聲稱他得到自主身份，但，真的是這樣嗎？他其實有一個重大問題與一個功能的限制



但是 AID 作為社群網路身份，從本質就是要被別人識別，但學長的假設卻要求不傳出任何數據到網路上，別人自然無法讀取我們裝置內的數據，那談何識別我們的AID，怎麼產生社群交流。
因此學長之後還是補充了一句內容：”當服務要求傳出數據時，把對應服務的AID數據都給傳出去”

但我想把數據存在 Local ，登入時別人想用就傳出去，甚至持續留在服務中，從本質上做了一個重大假設，即服務會信任用戶

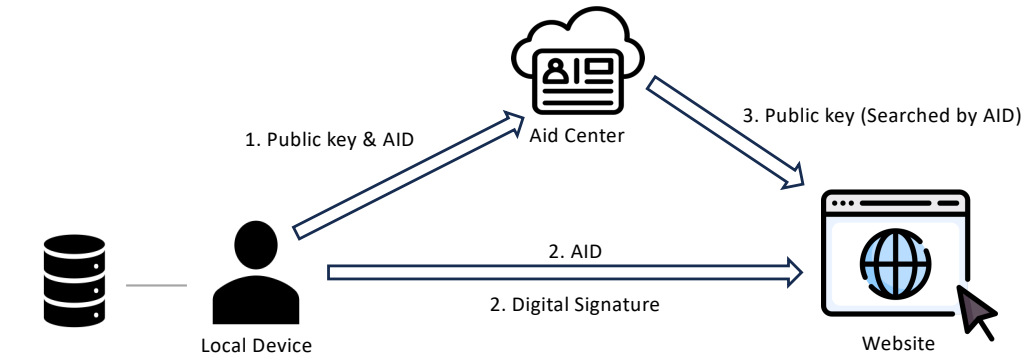
更進一步，這裡可以拿網路遊戲的設計史，來做簡略的說明: 最早的遊戲基本上所有數據都放在個人設備，但卻出現了作弊等外掛，這些外掛的原理就是直接修改本地的數據。

顯然，只是提出把數據放在使用者裝置是不夠的，真正的問題是，當使用者不得不對外溝通時要如何應對: 後端憑什麼信任使用者傳出去的數據，使用者憑什麼信任網頁傳入的數據

因此我必須要提出一個機制，即使不得不讀取或上傳數據，還是可以讓網頁伺服器與使用者彼此信任。

The website does not Trust the user

- **Let user Trust Aid Center**
- **Let website Trust Aid Center**



2024/7/25

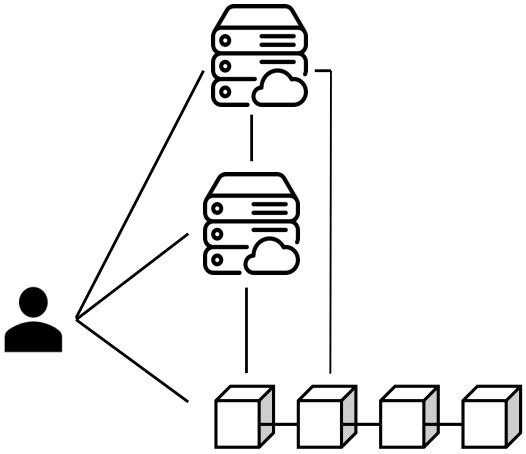
來到登入的驗證機制，學長的設計中，由使用者透過本身存儲的私鑰簽章AID後要求網站按照Aid Center 給予的公鑰解密後驗證用戶是否可以登入。透過這樣的做法，AID Center 最少只要存一個公鑰，確實讓使用者達到了自主性。
但我認為這不應該是所有的驗證方案，而應該只是驗證方案的子集。
為什麼這樣說呢? 我認為自主是方法而不是結果，我們真正希望的是透過自主自然的建構信任，信任是雙向的，單純的讓使用者自主，而缺乏讓服務願意信任的機制無法完整解決問題，只會讓使用AID的推廣受限。
甚至說的更嚴重一點，在這個機制中 Aid Center 造成前所未有的信任危機。

舉例來說，Aid Center 只要竄改內部存放的公鑰，就能輕鬆冒充任意使用者;
又或是，即便AID會實名認證，但使用者可以自行對網頁伺服器揭露自己的身份，可以輕易偽造，畢竟aid center不對使用者的聲明作任何保障。

我創建的機制，在保留使用者自主權的同時，會讓網頁伺服器不需要持續信任 Aid Center，甚至用戶也不需要持續信任 Aid Center, 分別對應前面兩個案例

My Contribution

- Propose a complete mechanism to construct an AID system based on blockchain
- Through the **receipt** and **evaluation system** supported by the blockchain, services and services, users and users, services and users can naturally trust each other.



2024/7/25

11

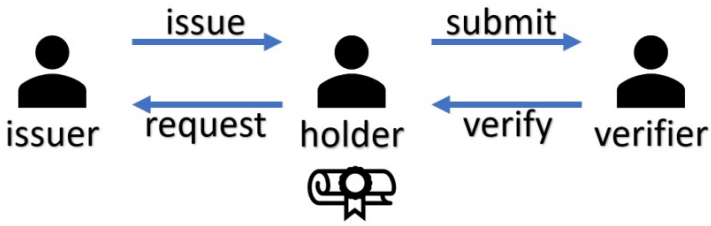
所以什麼是我最大的貢獻，我提出了一個完整的機制，基於區塊鏈解決了學長遇到的困境。

我想像學長一樣用一句話總結我的所作所為: 透過基於區塊鏈的收據與評價機制，讓服務與服務，用戶與服務，用戶與用戶能彼此信任。

關於評價機制和收據機制的設計，我在後面的章節會更深入的介紹。

Receipt: Autonomous Certificate

- Tze Nan, Wu: The Design and Implementation of General Autonomous Certification on Blockchain
- ***I design Autonomous Certificate (AC), a blockchain-based digital certificate with a credit rating mechanism to integrate various certificates with the same general certification mechanism to reach real autonomy, solving known problems in the digital certificate***



2024/7/25 12

在本節的最後，我要介紹哲南學長的論文，基於區塊鏈的一般化自主憑證設計與實作，他透過區塊鏈的機制設計出了一種自主的憑證簽發與評價機制，希望藉此解決數位憑證當前的問題。
我的貢獻中，收據機制的原型與評價機制的原型就是出自這位學長，因為收據的本質其實也是一種憑證，自然，自主的憑證正是我們所需要的。

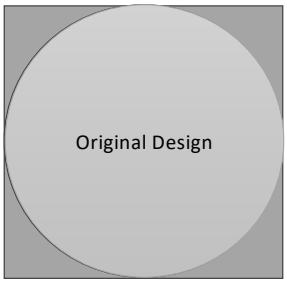
在後續的討論中，我不會再用收據稱呼，會用我論文中的用詞: 憑證。

Background

研究背景

design philosophy

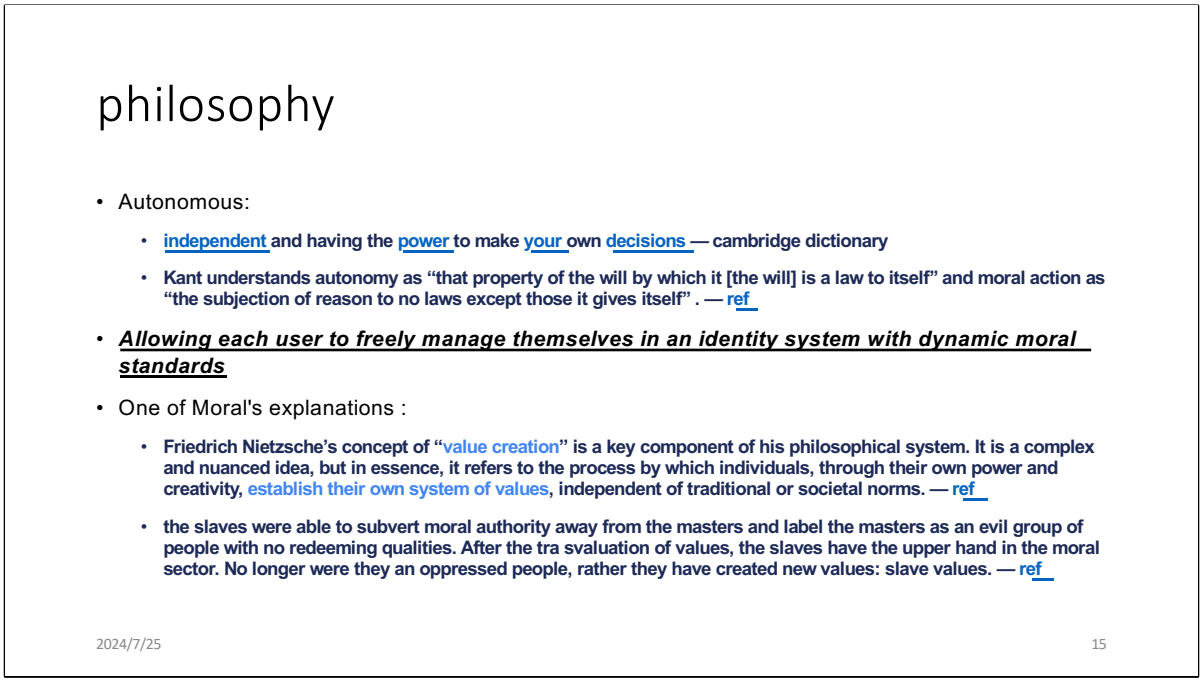
- In order to completely solve the problem
- I had to think through how to **implement the concept of autonomy into code**



2024/7/25 14

就像前面的所說，我並沒有推翻學長的貢獻，而是更徹底的分析與理解了前人的技術，藉由我對實務上的理解來更完整的設計AID系統，以此解決前人做不到的事，並且指出未來的方向。

在下一頁，我會介紹，我如何在哲學上定義出更完整的AID(自主身份系統)，再完成系統設計，



透過查詢自主的定義，我們可以很輕易的得道以下內容: 獨立，並且有力量做自己的決定
這顯然不甚直覺，獨立自然就會自由，自由當然可以做自己的選擇，為何要特別強調
因此，我更深入的調查了再西方文化中自主的內涵與根據，發現多數指向康德這位思想家，
在他的著作中有提到他對自主的見解，我提出沒那麼嚴謹的中文解析: 自主就是自由的做事，並且遵循自己願意遵守的道德準則
自此，我確定了第一件事，AID需要賦予使用者絕對的自由，同時還要賦予使用者遵循道德準則的能力。
轉換成技術用語就是: 自主身份就是允許所有使用者自由的管理自己，並且可以生活在具有動態道德標準的身份系統中，自由遵守想遵守的道德準則。
接著，更深入的探討道德是什麼，會發現極為龐大，但我們可以慢慢解析，慢慢實作，
在本研究中，我優先遵循文學家尼采的奴隸道德說完成設計，道德的設計。

下面提出了兩段話，第一段是分析尼采的底層道德觀“value creation”他認為每個生而為人的個體都有能力根據他們的價值觀創建他們的價值體系作為道德。
第二段敘述，分析了尼采聊到弱者如何建立道德，以下基於我的理解做換句話

說: 尼采認為世界上大多數是弱者，少數是強者，最早都由強者統治弱者，然而弱者漸漸找到了一種對抗強者的方案，就是建立自己的道德觀強制追加到強者身上，少數強者漸漸會被多數弱者的道德觀影響，從而改變原先的想法。

我認為，這正是評論機制的重點，我們要讓AID的用戶們可以通暢的對其他服務或人表達意見，而這些意見會被堆疊在目標身上，其他使用者可以遵循自己認為合理的演算法計算堆疊在一個AID身上的所有評論，藉此認知到自己是否願意信任該AID

最後，還是要強調道德的擴展，或許是AID未來進步的方向，例如老師提到，尼采還有一個強者的價值觀，那我該怎麼在區塊鏈中實作出這樣的機制呢?
還有，一定有人會疑問為什麼這類東西一定需要區塊鏈來實作，我給出一個答案: 因為我認為信任許多價值觀的底層，如果連信任都沒有，很難實作出這些東西，而區塊鏈洽巧就是這樣的工具。

Design

系統設計

Problems

Table 2.1: 身份系統需求比較表

需求	中心化身分	聯合身分	使用者中心的身分	自治身分
數據集中問題	✓	×	✓	✓
資料孤島化	×	△	△	✓
組織身分控管	✓	✓	△	×
便於系統管理	✓	✓	✓	×
系統管理一致性	✓	✓	✓	×
減少多重身分認知負擔	×	△	△	✓
實現單點登錄（SSO）	×	✓	✓	✓
促進組織間協作	×	△	△	×
降低運營成本	✓	×	✓	△
增強隱私保護	×	×	△	✓
使用者身分資料控制權	×	×	△	✓
身分提供者選擇靈活性	×	×	✓	✓
服務數據控制權	×	×	×	×
身分可攜性	×	×	△	✓
使用者與服務商平等性	×	×	×	✓
抗審查特性	×	×	×	✓
符合現有法律框架	△	△	△	×
高易用性	✓	✓	✓	×
系統互操作性	×	×	✓	✓

以下是我羅列出來自主身份需要解決的問題, 並且各個年代的身份系統處理的狀況, 有些AID可以完全解決, 有些 AID可以局部解決，我在論文中會一一介紹.

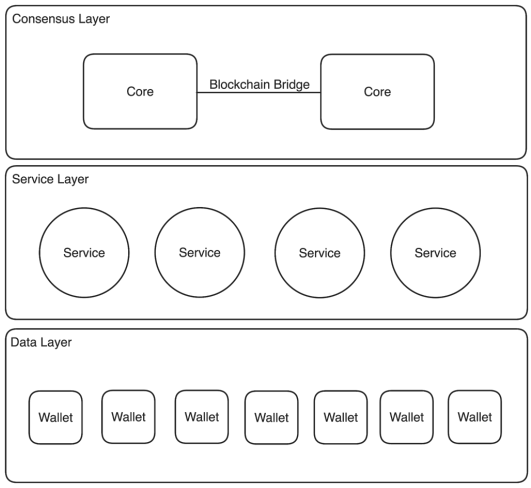
接下來我會介紹如何透過幾個核心機制解決，核心幾個問題。

Freedom and Morality

- Freedom
  - Code: action
  - Data: data
- Morality System
  - Trust

Consensus Layer	Service Layer	Data Layer
• Write Interface • Read Interface • Update Interface • Evaluation Interface	• Identity Management • Credential • Data Management	• Identity Management • Data Management • Credential • Data Storage

Table 3.2: AID System Interfaces by Layer



2024/7/25 18

這裡是我對 AID 系統的設計 , 包含三個層次，分別是共識層 服務層 數據層，其中共識層提供可信賴的數據讀寫，服務層可以用微服務的模式放置各種 Service，數據層放置用戶的數據和讓用戶和服務層溝通。

我會從前面背景提到的設計哲學出發，描述幾個核心問題的解法

分別是自由, 自由下面又分 Code 和 Data ，因為我覺得一個軟體是由程式碼和數據組成的，其中程式碼的部分我特別要解決用戶行為的自由，包含不該有管理者，還有驗證(也就是登入行為)不應該被破信任第三方。
而數據的自由則是強調當不得不分享數據或接受服務給予的數據，我們該如何讓人信任，又或是信任他人。

Autonomous Action

- Extreme Multi-factor authentication (EMFA)
- Avoid system admin

Over 50p can reset critical data

{ Factory 1: 10p Factory 1: 20p Factory 1: 18p Factory 1: 25p Factory 1: 3p }

2024/7/25 19

以Google的Cloud Identity為例，只要進入服務，服務就有權利重設使用者，甚至刪除使用者，這些都是管理員的權利，但這明顯不符合自主的精神。

因此 第一個要介紹的做法 極致多因素驗證，就是為了解決這個問題，這是我自己提出的嶄新機制，其概念簡單來說就是把多因素驗證中，每個因素都允許設置權重，而不是像過去那樣一條通過就通過了。
這樣的作法可以很簡單的解決包含密碼遺失、身份盜竊等在過去會需要系統管理者才能解決的功能。

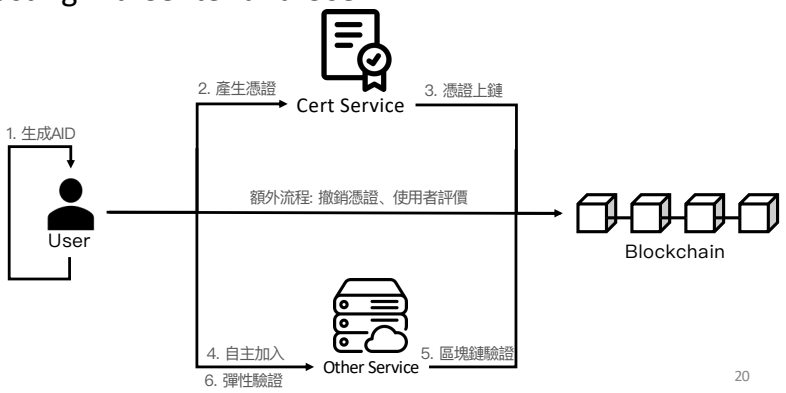
舉例來說: 我們可以給一個用戶設置 20 種認證的方案，規定必須要集齊10種認證方案才能做某種敏感行為，這樣即使最常用的密碼被拿走，他也無法做危險的事。
再舉個例子，為何這個方法重要，為什麼指紋辨識和臉部辨識明明已經很成熟了，許多系統依舊要求使用者設置密碼，因為指紋和臉部辨識等，雖然難以遺忘，但也有點不穩定，用戶不能接受因為手指骨折，被石膏包起來，導致一個月不能登入系統。

透過EMFA我們可以讓使用者同時加入手指與腳趾的指紋，只要超過 10 跟符合也算通過。

單談上面的方法可能，會覺得沒有徹底解決問題，因為除了權限問題，數據被服務掌握的問題會在後面解決

Autonomous Action (cont.)

- Autonomous AID Verify by Autonomous Certificate
- Services avoid trusting Aid Center and User



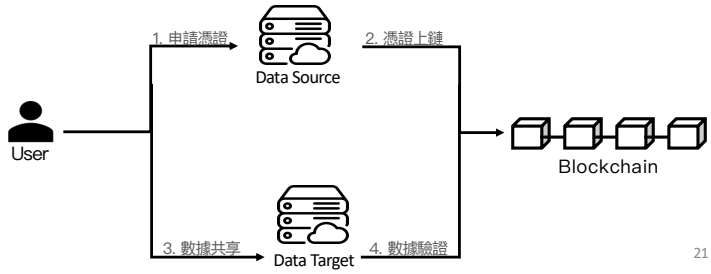
接著也是用戶行為的自主，我希望使用者驗證（即登入）是自主的。這需要強化前人的機制，因為前人雖然聲稱讓用戶自主了，卻沒顧慮到因此要求服務無條件信任用戶和簽章伺服器，簡單來說，我把服務也視為需要自主權的對象。我完善了自主簽章來解決這個問題，如今使用者在本地產生AID以後，除了可以把公鑰上傳到 Cert Service （也就是以前的 Aid Center）可以自定義的傳入其他驗證方案(只要用戶希望Cert Service)可以為這些數據背書，
接著 Cert Service 可以利用這些數據產生簽章，存入區塊鏈。

使用者之後登入時，一般服務不再需要向 Cert Service 詢問用戶的公鑰，而是向區塊鏈詢問 Cert Service 的公鑰後確認 AID 的完整性(intergrity)，服務確認使用者傳入的AID沒有竄改後按照使用者AID內的驗證方案，要求使用者驗證。
搭配使用者可以及時查看與設置區塊鏈與後面會提到的評價系統，在系統中沒有任何一方被破要去信任其他人，每一方都有制衡對方的手段。甚至即使 Cert Service 關閉了，AID 自主憑證還是可以被持續使用。

這邊我還是要改學長平反一下，加入區塊鏈學長的機制其實也是可行的,我修改後主要的價值是達成用戶的自主，讓用戶不需要被破使用公司鑰驗證 ，可以使用例如簡訊驗證等等

Autonomous Data

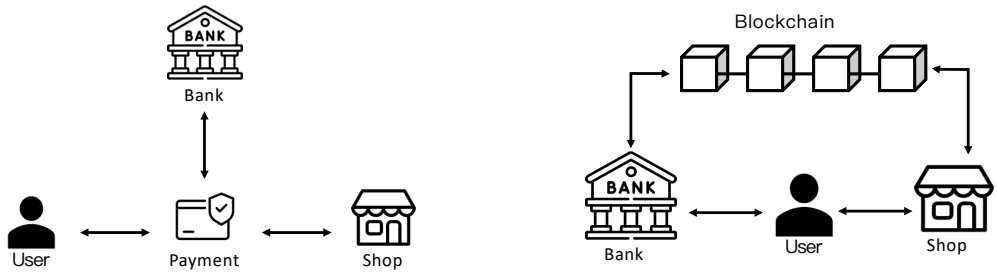
- Hybrid data management
  - Clear explanations for data requests
  - Gradual permission settings
  - Smooth transition from strict to relaxed security measures
  - Recording using Autonomous Certificates



接著說明數據如何得到自主，第一個問題是如何面對數據上傳或下載，我這裡一樣用了我發明的名詞: 混合數據管理。
裡面完整的說明了一個數據操作的流程，我認為按照這個流程可以在一定程度上解決數據自主的問題。
第一步是每一個應用都要從靜態應用的權限開始，接著每當需要對外數據交流，要明確的向使用者說明。
所有的設置都要是緩慢的從嚴謹到鬆懈。最後如果真的是重要的資訊傳入或傳出，需要透過數據簽章機制，給使用者和服務雙方提供收據，避免未來的爭議。
數據簽章機制類似把自主簽章的對象改成某筆數據，這裏不深入展開。

Autonomous Data (cont.)

- Autonomous Data Sharing



2024/7/25 22

再來是數據的分享也要自主，畢竟這是決定 AID 能否真正成為可以被使用的身份系統所必須的功能。

過去的後端服務，會讓數據在多個服務之間傳遞，這是個大問題。而AID透過前一頁中，數據頻證的機制，使自己成為橋樑，在服務之間搬運數據，再透過數據頻證證明自己並沒有竄改數據。

這樣的典範轉移，會徹底改變整個網頁生態。

Autonomous Morality System

- Concept
  - AID system viewed as a Decentralized Autonomous Organization (DAO)
  - Each participant sets own standards for judging and receiving evaluations
- Process
  - Certificate Generation
    - Create data or autonomous certificates
    - Deploy customized smart contracts on blockchain
  - Evaluation Production
    - Evaluate certificates based on smart contract rules
    - Evaluations must comply with contract specifications
  - Reputation Conversion
    - Read evaluation list from smart contracts
    - Convert evaluations to reputation scores using personal algorithms

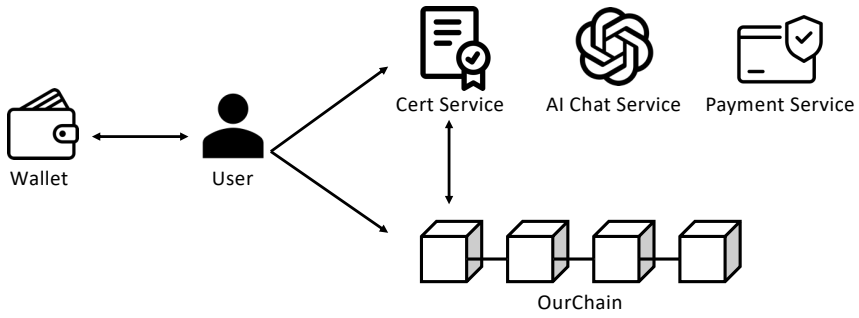
最後是自主的評價系統，簡單來說其概念就是所有在鏈上的憑證都可以被評價，並且每個系統參與者都可以按照自己設計或選擇的演算法，動態判斷一個AID的可信程度。

Implement

概念驗證

implementation details

- User generate an AID by Autonomous Certificate (Cert Service)
- The user pays in the payment service (Payment Service)
- User logs in to use AI chat software (AI Chat Service)



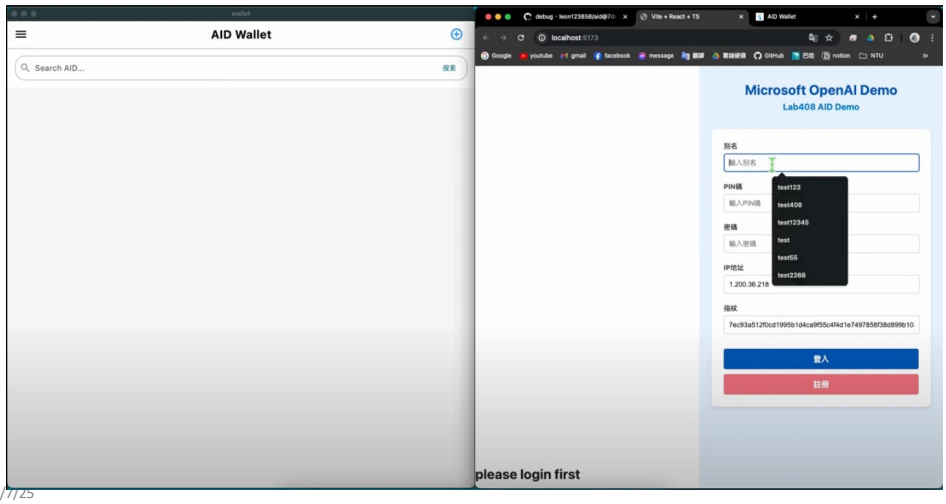
2024/7/25 25

在過去使用者用 AI 服務調用支付完成付款，甚至AI服務本身留存了使用者的所有聊天數據。

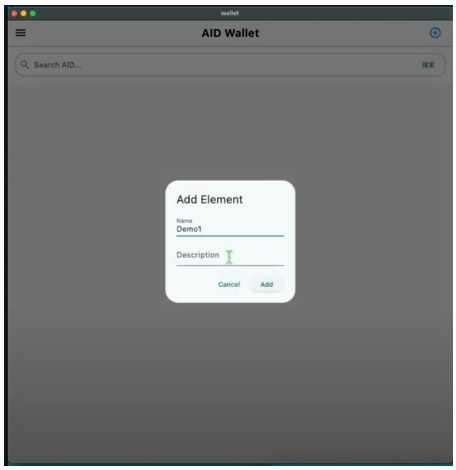
那我該怎麼利用AID達到自主呢? 有兩個東西需要自主，使用者要可以自主決定使用哪種支付服務，不像過去使用者被破使用系統商串接的服務。
還有聊天數據的自主：自己保留資料，保留數據憑證，如果抓到ＡＩ產生類似數據 有爭執的基礎。

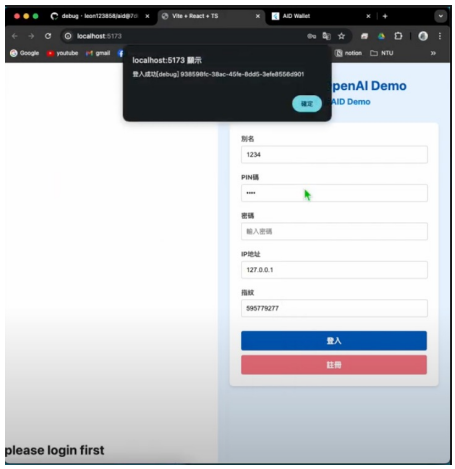
我實作了一個概念驗證，期望能證明AID足一取代當前主流的身份系統，成為身份系統的未來。因此我在PoC的過程遵循了外界應用普遍的協議。
我想像中的流程如下，分成三步
使用生成AID，需要和自主簽章服務互動
接著到支付服務，付錢後可以拿到數據頻證作為付過錢的證明。
最後到AI聊天服務，用 AID 登入後，使用數據頻證兌換點數，在使用AI點數和AI聊天
補充一下：當使用者離開AI服務時，我們還會清除所有AI服務內使用者相關的數據，為此AI 服務還要針對使用者剩的點數產生一個數據頻證給使用者

Demo


AID Wallet
Search AID...
localhost:5173
Microsoft OpenAI Demo
Lab408 AID Demo
別名
PIN碼
密碼
IP地址
指紋
登入
註冊
please login first

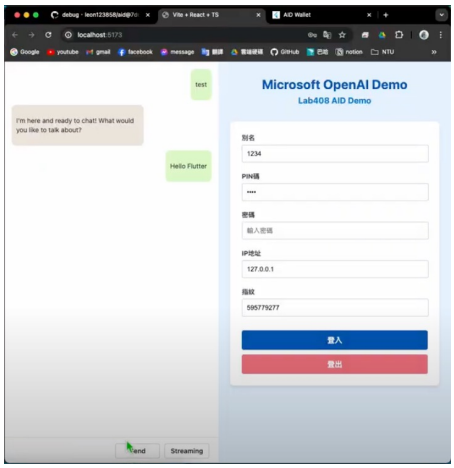
Demo (cont.)



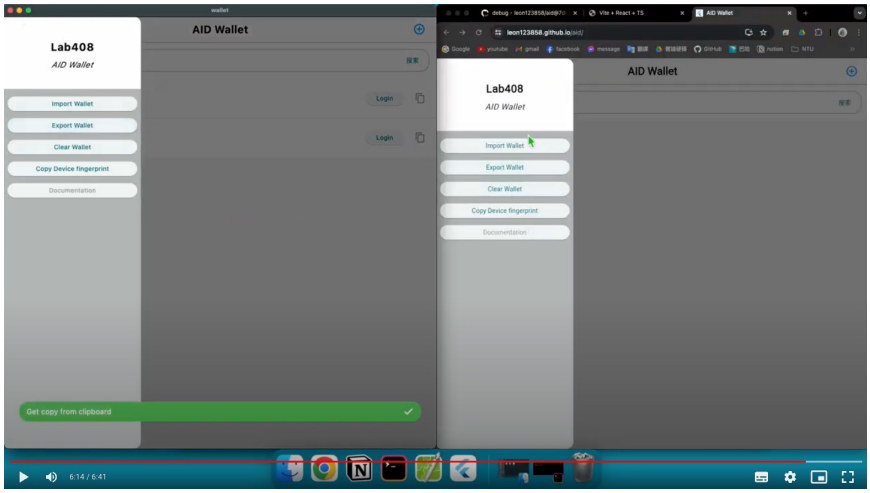


這裡補充一下，按照論文，錢包應該要內遷進前端應用，但是我這裡為了測試方便，使用了論文中的”時空分析機制”，會把近似時空的驗證關聯起來，所以只需要一個錢包

Demo (cont.)


test
I'm here and ready to chat! What would you like to talk about?
Hello Flutter
Microsoft OpenAI Demo
Lab408 AID Demo
別名
1234
PIN碼
••••
密碼
輸入密碼
IP地址
127.0.0.1
指紋
595779277
登入
登出
Send
Streaming

Demo (cont.)


AID Wallet
Lab408
AID Wallet
Import Wallet
Export Wallet
Clear Wallet
Copy Device fingerprint
Documentation
Login
Login
Get copy from clipboard
6:14 / 6:41
AID Wallet
Lab408
AID Wallet
Import Wallet
Export Wallet
Clear Wallet
Copy Device fingerprint
Documentation

Conclusion

結論

Achievement

- Autonomous Identity is method not result.
- The goal is to create an environment of trust (you can also say zero trust).
- Proposed the deep design philosophy of AID.
- A more complete AID is designed based on Blockchain.

2024/7/25 31

我們應該是為了解決許多問題，才讓身份自主。因此為了讓身份自主而喪失了信任是不合理的。因此，我的做法是把每個系統的參與者，包含服務與使用者都視作AID，他們都要自主。

如果捨棄掉我們自創的各種名詞，我認為別然看待AID可以簡單理解為零信任的身份環境

最後，我提出AID系統的完整哲學思考與基於區塊鏈該如何設計

QA

thanks

2024/7/25

32

我的報告到這邊結束，謝謝各位委員
歡迎委員們提問