AutoMobile Chain汽車數據服務平臺

白皮書

目錄

AutoMobile Chain作為智能網聯汽車的關鍵技術，正逐漸成為汽車產業數位化轉型和關聯領域協同創新的重要抓手。隨著汽車產業數位化程度不斷提高，產業鏈間逐漸暴露出數據安全難、數據共用難、數據監管難等問題。而區塊鏈是解決多方協作問題的利器，可在提升車聯網安全防護能力的同時，應用於汽車產業各參與方之間的數位化協作環節，促進優質數據在汽車產業鏈中有序流通，加快汽車數據的價值釋放。同時，區塊鏈與邊緣計算、隱私計算等技術的結合，可為AutoMobile Chain的數據共用和智能協作提供有效的技術路徑和解決思路。

為促進車聯網與區塊鏈技術的跨領域交叉融合，可信區塊鏈推進計畫（TBI）與 IMT-2020 推進組 C-V2X 工作組聯合，組織成員單位深入研討區塊鏈技術在車聯網場景中的技術細節和應用方向，共同編制白皮書。本白皮書綜合分析AutoMobile Chain產業發展現狀，梳理目前AutoMobile Chain在數據共用、數據安全和數據監管等方面面臨的痛點問題，提出了區塊鏈運用於汽車產業的應用價值，並詳細介紹了區塊鏈運用於協作式智能交通、車電互聯、汽車供應鏈和汽車金融等領域的具體解決方案，為整個汽車產業的數位化協同發展提供參考建議。

目錄

一. 背景介紹

1.1 智能網聯汽車數據安全合規行業背景

隨著車聯網及人工智慧技術的日益成熟及商業化 ， 智能網聯汽車 （Intelligent Connected Vehicle，簡稱“ ICV”）應運而生。智能網聯汽車兼具智能與聯網的特性 ，通過V2X（Vehicle to Everything）通信技術實現了車輛與車輛、人、道路交通設施、雲之間的成熟交互。智能網聯汽車不僅能進行數據交互和資訊共用 ，優化駕駛路徑並降低交通事故發生的風險 ，還能實現通過傳感設備進行自動駕駛等功能，提供個性化的用戶體驗 ，引發對未來駕駛方式的展望。

近年來，汽車企業和互聯網企業蓬勃發展，加速了車聯網、自動駕駛、互聯網地圖、智能交通技術的升級與革新，世界各國家地區政府對智能網聯汽車的大力支持和消費者對出行方式的需求轉變，推動了智能網聯汽車的研發、生產與普及 ，商用場景正在不斷增加。

為提供更好的用戶體驗，智能網聯汽車及其後臺支持系統每時每刻都在處理海量數據 ，包括車輛運行數據、路況資訊、位置資訊、車載應用操作資訊等。對於這些數據資訊，如果沒有嚴格的數據安全合規管控措施，處理這些數據極易造 成安全合規隱患，對國家、公共安全、企業經營、個人隱私等產生影響。因此，智能網聯汽車的數據安全合規在數據生命週期中至關重要 ，數據安全合規也 成為智能網聯汽車產業健康發展的重要基礎。隨著監管與消費者對數據安全和隱私保護關注程度的提升 ，全球各國家與地區對於 數據安全的法律法規相繼出臺 ，針對智能網聯汽車的行業規範也在逐步完善。

1.2 各國數據安全進展

● 歐洲數據安全进展

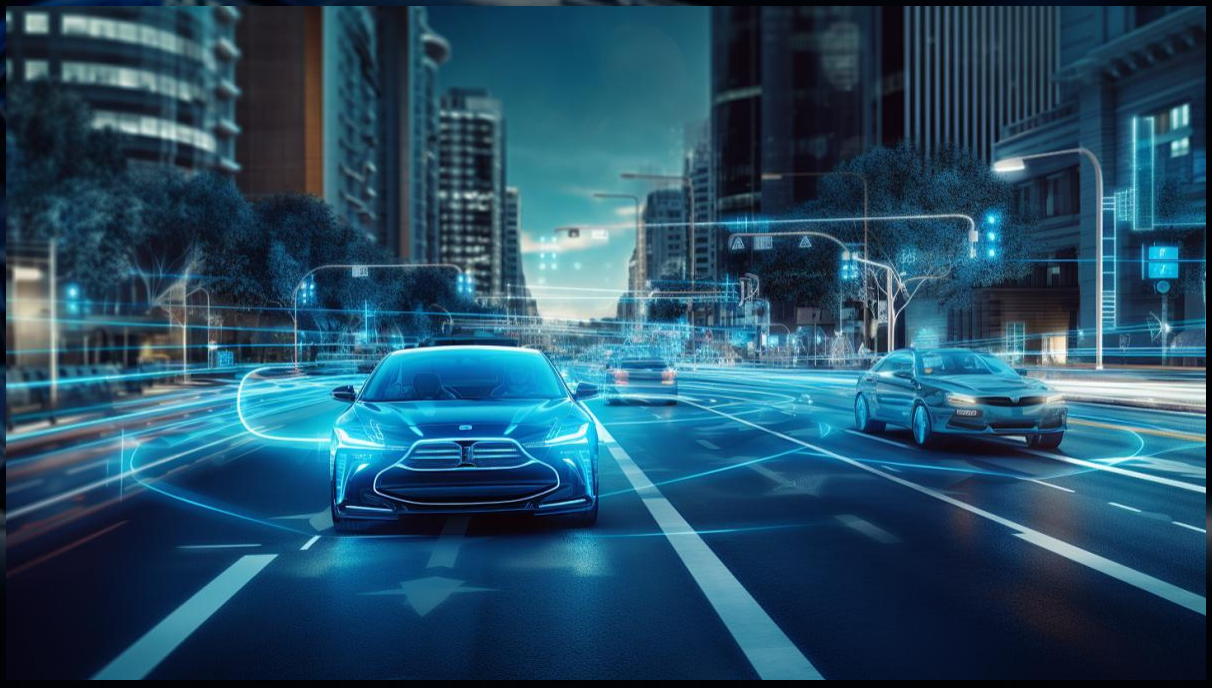
歐洲在智能交通領域全方位佈局，率先開展數據安全專項政策。 自 2003 年起，歐盟先後發佈《歐洲自動駕駛智能系統路線》《歐盟未來出行戰略》《協作式智能交通體系戰略》等多 項戰略措施，其核心目的是推動協作式智能交通技術及產業應用，促進整個歐洲範圍內投資、 政策、監管框架的相容性和一致性。為強化智能網聯汽車的數據監管要求，歐盟在政策法律方面作出多項修訂和革新。2018 年 5 月，歐盟出臺了《通用數據保護條例（GDPR）》，成為 全球個人數據安全立法中極具標誌性的一部法案， 其對於智能網聯汽車產品的數據安全具有直 接約束力。2021 年 3 月，歐洲數據保護委員會（EDPB）通過了《AutoMobile Chain個人數據保護指南》， 該指南提出智能網聯汽車需默認提供數據保護措施，並明確智能網聯汽車產生的數據應被視為 個人數據，必須按照數據保護原則進行處理。2021 年 5 月，德國通過的《自動駕駛法》要求智能網聯汽車需安裝記錄駕駛過程的“黑匣子”，並開創了監督機構遠程監控智能網聯汽車的監管制度。

● 美國数据安全进展

美國在平衡創新與安全的基礎上，更強調數據開放與技術創新。 自 2013 年起，美國先後發 布《聯邦自動駕駛汽車政策》《自動駕駛系統 X.0》《自動駕駛汽車立法大綱》等戰略規劃，為 美國順利開展智能網聯汽車的創新、研發、測試以及安全部署提供了重要支持。在數據安全方面， 美國聯邦層面尚未正式出臺智能網聯汽車的數據安全法案，現階段美國智能網聯汽車的測試及布 局是由各州法律進行分別監管。加利福尼亞州在 2018 年頒佈的《加州消費者隱私法（CCPA）》 規定了企業應如何對收集的個人資訊進行訪問、刪除和共用。儘管 CCPA 並非針對自動駕駛的專門立法，但卻是現階段相對有效規制智能網聯汽車個人資訊保護的重要法律。2021 年 1 月，美國 交通部發佈《自動駕駛汽車綜合計畫》報告，在安全優先、確保隱私和數據安全等十大原則的基礎上， 強調優化交通監管環境，希望通過簡化行政豁免程式和修改現有法規，掃清不必要的監管障礙， 來加大數據開放和數據協作力度，加快智能網聯汽車的測試驗證和商業化落地的進程。

● 中國数据安全進展

我中國加快謀劃“交通強國”頂層設計，並逐步開展AutoMobile Chain安全體系建設。我中国先後發佈了《車聯網（智能網聯汽車）產業發展行動計畫》、《交通強國建設綱要》、《智能汽車創新發展戰略》 等多項政策，政策導向已逐步由提出目標、制定規範、發展核心技術開始逐步向加快部署、落地應用、安全監管等方向遷移。在數據安全方面，《數據安全法》和《個人資訊保護法》的出臺， 分別從數據安全和個人資訊的角度， 規範了數據處理活動的合規要求， 對智能網聯汽車的數據安全要求起到綱領性作用。2021 年下半年，智能網聯汽車的數據安全管理規範進入密集出臺期。2021年 6 月，工信部發佈了《AutoMobile Chain （ 智能網聯汽車 ） 網路安全標準體系建設指南》，在智能網聯汽車的網路安全防護、平臺安全防護、數據安全防護、安全漏洞管理等方面提出了明確要求。2021 年 8 月，工信部印發了《關於加強智能網聯汽車生產企業及產品准入管理的意見》，強調了對智能網聯汽車生產企業的網路安全和數據安全要求， 明確企業應當建立健全汽車數據安全管理制度，依法履行數據安全保護義務， 實施數據分類分級管理， 加強個人資訊與重要數據保護。 2021 年 9 月，中央網信辦聯合發改委、工信部、公安部和交通運輸部共同發佈了《汽車數據安全管理若干規定 （ 試行 ）》， 主要聚焦對汽車數據處理活動中的重要安全風險予以事前預防、事 中監管和事後處罰，規範和促進汽車數據的合理開發利用。2021 年 10 月，我國首個汽車數據安全技術檔《汽車採集數據處理安全指南》正式發佈， 該指南細化了重要數據和個人敏感資訊範圍，明確了需向用戶披露汽車採集數據並向車外傳輸的完整情況的要求，為汽車製造商面對的數據安全問題提供了細化可執行的解決方案。



二. 專案介紹

2.1 AutoMobile Chain汽車數據服務平臺

- AutoMobile Chain

AutoMobile Chain是一个基于区块链+万物互联、物联网+大数据+AI为核心的汽车数据服务平台，是 新一代网络通信技术与汽车、电子、交通运输等领域深度融合的新兴产业形态。而狭义的物联网+区块链概念技术， 是指车辆利用无线通信技术实现“人 - 车 - 路 - 云”之间交换信息的通信方式。其中，蜂窝车联网通信方案 是目前车联网 通信的主流技术方案，具有 4G/LTE 版本和 5G 版本，该技术在中国、欧盟等国家得到广泛应用。

- 區塊鏈應用

區塊鏈集分佈式存儲、點對點傳輸、共識機制、智能合約、密碼學等技術為一體，具備數據防篡改、數據可追溯、主體協同、價值共用和柔性監管等特點，是一種在多方協作場景下建立互信機制的分佈式帳本技術。在AutoMobile Chain場景中，環境感知、資訊交互和決策協同都必定是建立在數據可信的前提下。而區塊鏈可作為車聯網的 “可信數字底座”，對車聯網場景下的數據進行可信驗證、冗餘存儲和共識計算，保障車聯網的安全性、可用性和一致性，賦 能各個環節都增加“可信”屬性，實現“人 - 車 - 路 - 雲”之間協同互信。

- 物聯網（IoT）的應用：

物聯網技術使得汽車和周邊環境能夠即時交換數據，為AutoMobile Chain汽車數據服務平臺提供了豐富的數據源。通過在汽車上安裝感測器和通信模組，可以即時收集車輛狀態、行駛軌跡、環境感知等各類數據。這些數據不僅有助於提升駕駛安全性，還能為汽車數據服務平臺提供關於車輛性能、用戶行為等方面的深入分析。

- 大數據技術的應用：

大數據技術能夠對從物聯網收集的海量數據進行存儲、處理和分析。通過數據清洗、整合和挖掘，AutoMobile Chain汽車數據服務平臺能夠為用戶提供個性化的服務。例如，根據用戶的駕駛習慣和偏好，為用戶提供智能推薦、路況預測、維修保養建議等。此外，大數據技術還可以幫助汽車廠商發現產品缺陷，優化產品設計，提升產品品質。

● AI技術的應用：

AI技術在AutoMobile Chain汽車數據服務平臺中發揮著至關重要的作用。它能夠對大數據進行深度學習和分析，發現數據中的規律和趨勢，為決策提供支持。例如，通過AI演算法對車輛行駛數據進行預測分析，可以預測車輛可能出現的故障，提前進行預警和維修。此外，AI技術還可以應用於自動駕駛、智能導航等領域，提升駕駛的便捷性和安全性。

綜上所述，物聯網、大數據和AI在AutoMobile Chain汽車數據服務平臺中形成了一個緊密的生態系統，它們相互協作，共同為用戶提供更加智能、高效的汽車服務。隨著技術的不斷發展，這一生態系統將在未來發揮更加重要的作用，推動汽車行業向更加智能化、綠色化的方向發展。

2.2 數據安全與隱私保護戰略願景

AutoMobile Chain汽車數據服務平臺為了实现数据安全，保护用户隐私，为产品、服务的持续运行提供所需的信息安全保障 ，路特斯科技制定了”分级保护、风险管控、持续改进、安全高效、行业领先、用户信赖”的总体信息安全和数据安全策略。并在此基础上，为更好地保护用户数据，提出以下隐私保护的愿景与方针：

1.隱私保護願景“塑造信任，做智能汽車時代最讓公眾放心的隱私保護踐行者。

a.注重主動預防

b.嵌入隱私設計

c.培養隱私文化

b.落實運行機制

● 2.2.1面向用戶的隱私保護承諾

AutoMobile Chain汽車數據服務平臺重視並致力於保護用戶隱私 ，面向用戶承諾：

1.AutoMobile Chain汽車數據服務平臺僅在合法、正當、必要的原則下收集用戶的資訊，並僅在實現數據處理目的必要的期限記憶體儲.

2.AutoMobile Chain汽車數據服務平臺只會將用戶的個人資訊用於用戶預先同意或者法律法規規定的合法目的.

3. AutoMobile Chain汽車數據服務平臺通過嚴格的數據保護措施保護用戶的個人資訊.

4. AutoMobile Chain汽車數據服務平臺僅在用戶明確同意或法律規定的前提下向第三方提供用戶的資訊，並持續向用戶披露共用資訊清單.

5. 如果發生數據洩露或其他安全事件，路特斯科技會及時通知用 戶，並採取適當措施來減輕損害

6. AutoMobile Chain汽車數據服務平臺尊重用戶依法享有的對自身資訊處理的權利.

2.3 已獲得的第三方認證及說明

ISO/IEC 27001

ISO/IEC 27001是目前為國際上最為認可的資訊安全管理體系標準之一。AutoMobile Chain汽車數據服務平臺通過建立ISO/IEC 27001體系和ISO/IEC 27701體系能夠從企業內部的管理程式（尤其是資訊安全管理和個人資訊隱私保護）獲得巨大的改善， 提升企業在資訊安全和隱私保護領域的可靠性 ，降低企業資訊洩露的風險，從而更好地保護企業數據。

CSMS

網路安全管理體系（CSMS）認證是聯合國世界車輛法律協調論壇（WP.29）通過的R155法規的合規認證。通過CSMS認證說明了汽車製造商在車輛完整生命週期的各個階段均制定了網路安全管理流程，能識別潛在風險，持續監控和檢測網路攻擊及漏洞，及時回應網路安全事件。

SUMS

軟體更新管理體系（SUMS）認證是聯合國世界車輛法律協調論壇（WP.29）通過的R156法規的合規認證。SUMS認證標誌著企業構建的軟體開發和運營管理體系符合國際車輛軟體升級法規要求，表明了汽車製造商在車輛全生命週期內具備確保軟體升級過程安全、可靠、合規的工程能力。

MLPS 2.0

中國實行網路安全等級保護制度（MLPS 2.0） ，對網路運營者針對不同安全保護等級網路的安全保護義務提出了明確、細化的要求。等級越高，說明資訊系統重要性越高。獲得網路安全等級保護測評標誌著企業在技術服務能力、資訊安全管理能力和資訊應急保障能力等方面達到了國家資訊安全標準，用戶的資訊安全需求能夠得到充分保障。

三. 關鍵技術

3.1 AutoMobile Chain區塊鏈網路架構

AutoMobile Chain區塊鏈是由雙層多鏈組成的混合區塊鏈網路。 從網路組成上來看，主要分為雲計算層和邊緣計算層，層與層、鏈與鏈之間跨鏈協同。同時，單獨依賴區塊鏈技術無 法完全滿足AutoMobile Chain中的數據共用和智能協作需求，區塊鏈需要與邊緣計算、隱私計算等鏈下異構網路協同，來實現AutoMobile Chain場景下數據挖掘、數據安全和可信協作的有效聚合。

- 雲計算層

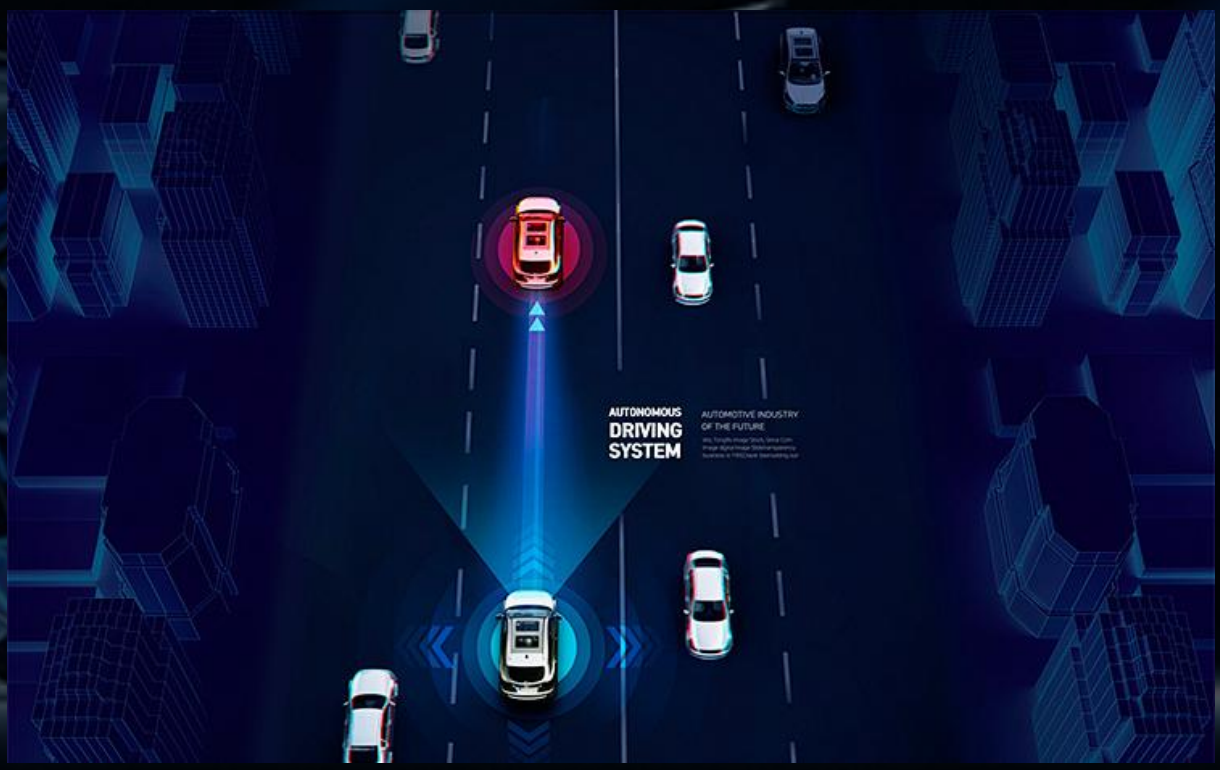
雲計算層是由AutoMobile Chain參與方在雲端共建的聯盟鏈網路。其中AutoMobile Chain數字身份管理作為主鏈，參與方可包含執法部門、交通部門、零部件製造商、汽車製造商等，負責以AutoMobile Chain設備 DID 為索引記錄設備從生產、使用、交易到報廢的全生命週期資訊。而交通司法、汽車供應鏈、汽 車保險、汽車金融等特定場景作為側鏈，通過跨鏈技術與主鏈保持一定程度的互操作性，從而形成雲計算層“ 一主鏈多側鏈”架構。

- 邊緣計算層

邊緣計算層是由AutoMobile Chain基礎設施組成的公有鏈網路，包括宏基站、微基站、路側單元、網聯車等終端和通信設備。邊緣計算層區塊鏈網路可複用現有蜂窩移動通信網，劃分為多個蜂窩區域，在每個蜂窩區域或交通區域內都有一個分佈式帳本。在特定蜂窩區域內的基站 、路側單元 和車輛車載單元 、邊緣計算單元可以共同維護帳本，以實現特定交通區域內數據的聚合和驗證。設備之間、設備與邊緣計算伺服器之間或邊緣計算伺服器之間的通信被記錄為交易並存儲在邊緣伺服器分佈式帳本上。其中 ，OBU 是安裝在車 輛上的移動節點，只參與數據交換，不過問分佈式帳本的共識環節，其主要功能是對車輛和交通關鍵資訊進行存證記錄並確保AutoMobile Chain通信的安全性。RSU 是被大規模部署在道路兩旁的固定節點。RSU同時具有兩個身份，帳本共識節點和邊緣計算伺服器，既對特定區域的環境和交通數據進行聚合驗證，又可根據帳本上彙聚到的多方數據實施邊緣計算任務。當車輛進入蜂窩區域時， 車載 OBU 與 RSU 交互完成身份驗證後，車輛便會加入該區域的分佈式帳本網路， 車載感測器從感知環境中提取資訊，OBU 對感知資訊本地預處理後，將有效資訊加密簽名併發送給 RSU，隨後 RSU 對資訊達成共識並廣播給其他 OBU。

● 駕駛行為分析

以駕駛行為分析為例，交管部門通過部署在車路兩側的攝像頭來識別過往車輛的“異常駕駛行為”，包括超速、違章違規、疲勞駕駛、未禮讓行人等行為，並利用聯邦學習結合秘密共用、同態加密等密碼學技術來實現針對駕駛行為數據的隱私保護計算。每輛車在進入服務所覆蓋的區域內，都變成該區域的交通監控節點，並參與到該區域的聯合建模和聯合決策的任務當中。如圖　所示，AutoMobile Chain邊緣計算服務可通過分佈式帳本來管理聯邦學習的訓練過程。在車輛行駛過程中，行車記錄儀記錄周圍行駛車輛行駛狀況，車內攝像頭採集駕駛員的體態特徵，車載聯邦學習客戶端基於收集到的資訊在本地對“異常駕駛行為”進行檢測或模型訓練，然後通過同態加密公鑰對梯度更新參數進行加密併發布到分佈式帳本中，之後邊緣計算服務再將局部模型參數更新到雲端進行聚合。在模型訓練過程中，可通過分佈式帳本對全局模型發佈、關鍵參數更新、預測值變化等環節進行記錄，對車載聯邦學習客戶端上傳的局部梯度進行異常識別並拋棄那些可疑的數據，核驗各方在聯合訓練過程中是否有作惡行為，以此來保證聯合訓練流程的安全性。在模型決策過程中，車載聯邦學習客戶端通過分析帳本上的附近車輛資訊（比如，　駕駛員駕齡、駕駛習慣、駕駛歷史、駕駛員疲勞、駕駛員注意力分散）和交通感知資訊（比如，　行人數量、人群密度、老人兒童是否存在）來決定決策任務的結果



3.2 區塊鏈在AutoMobile Chain中的應用價值

● 為AutoMobile Chain提供身份認證和訪問

AutoMobile Chain設備的數字身份管理是AutoMobile Chain安全的基礎。通過結合分佈式帳本、分佈式身份協議（Decentralized Identity，DID）和數字證書等技術，可為AutoMobile Chain設備提供數字身份管理和認證服務， 滿足AutoMobile Chain場景下的交互安全認證、資訊完整性保護和隱私保護等安全需求。車載單元、路側單元、 邊緣計算單元等AutoMobile Chain設備都可在鏈上賦予 DID，將設備的全生命週期資訊以 DID 格式進行標準化改造並存儲在分佈式帳本上， 同時，允許AutoMobile Chain各參與方在無需依賴第三方的情況下，對車聯網設備進行聯合資訊管理，並在鏈上完成證書申請、證書頒發、簽名驗簽和證書吊銷等流程，實現AutoMobile Chain設備註冊登記、產權管理、車主認證、設備認證、資訊發佈等環節可控可追溯。

以車輛訪問控制為例，車輛在生產時，車載錢包生成主密鑰並將其車輛識別號碼（Vehicle Identification Number，VIN）注 冊 為 DID 標 識 符，OEM 可 將 車 輛 具 體 信 息 以 可 驗 證 憑 證 （Verifiable Credentials 或 Verifiable Claims，VC）的形式頒發給車輛 DID，該可驗證憑證包 含車輛的一組屬性資訊，車輛可向其他主體提供該憑證來證明自身資訊。此外，車主 DID 可向其 他主體DID授予訪問該車輛資源的 VC，其他主體通過向車輛提供該 VC 來獲得車輛某組資源的訪問許可權。

● 提升AutoMobile Chain協同控制的安全性

AutoMobile Chain能夠為車路之間提供即時的感知融合、資訊交互與決策協同，不僅拓展了單車智能的形勢覺察能力，也使得更多協作式的交通出行應用得以實現。一方面，智能網聯汽車需要收集大量的資訊來進行感知定位、路徑規劃和決策控制。AutoMobile Chain作為一種另類感知手段，可幫助車輛獲得更多維度的資訊，比如道路狀況、交通環境、附近車輛行駛狀態等資訊。另一方面，隨著汽車智能化程度越來越高，車輛行駛過程中會產生大量的資訊，比如車輛使用情況、行駛狀態、環境感知等資訊。市政當局、其他車輛和自動駕駛提供商等企業希望獲得這些資訊，來進一步提升駕駛體驗、出行安全和交通效率。同時，AutoMobile Chain的連接性和開放性也增加更多的潛在風險，分佈式的感測器和多智能體如何在開放環境中高效的、安全地、自組織地協同控制成為AutoMobile Chain的難點問題。 每個感測器不僅需要獨立地對環境變化進行資訊收集和處理，還需要通過協同其他感測器對重複採集的數據進行交叉核驗，對多維度數據進行關聯融合，來避免電子對抗對單個感測器系統所造成的單點故障問題。為了避免AutoMobile Chain安全引起的交通事故和財產損失，就要求整個AutoMobile Chain具備高　度的可靠性和協作性，而區塊鏈為此提供了合適的解決方案。

● 增強AutoMobile Chain資訊交互的隱私性

通過將分佈式帳本與隱私增強技術相結合， 可為AutoMobile Chain提供全程閉環的數據安全和隱私保護服務，在數據共用的同時，有效保護企業和個人資訊免受洩露。隱私增強技術在AutoMobile Chain中主要應用在以下兩個方面。

對AutoMobile Chain資訊匿名化處理。利用分佈式帳本結合 K- 匿名、差分隱私、環簽名、隱私資訊檢索、基於屬性的匿名證書方案等技術可在數據共用的同時，對車輛身份資訊進行匿名保護。 例如，動態的、不可鏈接的匿名證書方案可實現數據發送方的匿名性和不可追蹤性，通過集成環 簽名和基於屬性的匿名證書方案，個人設備的公鑰對其他用戶保密，只有AutoMobile Chain監管方能夠獲得各設備的公鑰。AutoMobile Chain設備對數據進行群簽名後併發布到分佈式帳本中，由於其公鑰對於其他參與方來說是隱藏的，在一定程度上保障了AutoMobile Chain設備的匿名性。在AutoMobile Chain監管方需要查詢數據時，可通過陷門機制從群簽名中獲得設備的公鑰，查詢到區塊鏈上的AutoMobile Chain設備的具體資訊，從而實現數據對於監管機構的可追蹤性。

對AutoMobile Chain資訊加密處理。 利用分佈式帳本結合同態加密、秘密共用、零知識證明、可搜 索加密、代理重加密等技術可實現車輛感知數據的可控機密共用。在車輛眾包感知的應用中，由第三方可信機構為客戶和車輛的提供密鑰管理服務，車輛使用TA的公鑰加密採集到的感知數據，並將其發佈到分佈式帳本上。客戶使用 TA公鑰對眾包感知任務進行可搜索加密併發布到帳本上， 邊緣計算服務執行眾包任務並在分佈式賬 本上匹配相應的加密感知數據，當檢索到數據之後，向TA請求代理重加密密鑰，通過代理重加密將已經用TA公鑰加密的感知數據密文轉換為對應客戶可解密的密文，最後生成結果並返回給客戶。

- 培育移動出行領域數位化協作生態

區塊鏈的核心價值是數位化的合作共贏。汽車產業是個龐大複雜的產業鏈，涉及到交通運輸、資訊通信、工業製造和電力能源等眾多領域，任何單一企業都無法獨自應對“智能網聯”時代的挑戰，需要各方攜手共建數位化協作的新產業形態。

基於區塊鏈的自動駕駛數據共用平臺，可加快自動駕駛的測試驗證速度。 在整個自動駕駛訓練過程中，規劃、感知、控制回饋等工作都需要大量的數據採集和驗證。利用區塊鏈平臺，不同車主、汽車製造商、自動駕駛平臺廠商和技術方案提供商之間可以安全地共用自動駕駛數據，使得自動駕駛系統獲得更多維度的測試數據，消除自動駕駛訓練中極端情況引發的長尾現象，從而提高共建模型的魯棒性，避免了因為“閉門造車”所造成的資源浪費和安全隱患。同時，利用分佈式帳本有助於各參與方高效地進行可信協作並產生網路效應，從而吸引更多的研 究機構、科技企業、公益團體等社會機構參與到平臺中來，共建、共用、共治整個自動駕駛的數據合作生態

基於區塊鏈的出行數據共用平臺，可加強多元化交通方式間有機銜接。通過將汽車整車廠、公共交通、拼車、網約車、共用汽車、汽車租賃等不同出行方式的終端用戶數據相互關聯，利用多方的優勢數據，在精准客戶行銷、客戶購車機率等模型進行數據合作，幫助企業識別潛在用戶並提供更加高效的出行服務。此外，通過整合多供應商、多模式的公共和私人出行服務，可提供統一的出行即服務聯運模式。客戶可從任意平臺入口購買一次 旅途的所有交通服務，其中可以包括公共交通、地鐵、計程車和各種形式的共用出行服務。各出行服務提供商利用區塊鏈對聯運方案、載運工具、拼車需求和運載範圍等資訊進行共用，從而實 現跨平臺的客戶出行供需匹配。

基於區塊鏈的交通執法數據共用平臺，可提升交通執法各方的統籌協調。各地交通運輸主管部門、交通安全監管部門、執法部門、車廠、物流平臺、出行服務提供商通過將車輛資訊、執法記錄、 行政處罰、交通信用評價等資訊上鏈，實現車輛許可、審批、運營、處罰等的全流程監管，促進跨部門、跨地區一體化交通執法資訊共用，增強執法的規範性和透明度，以及交通運輸全過程監管數據的時效性和安全性。

四. 應用場景

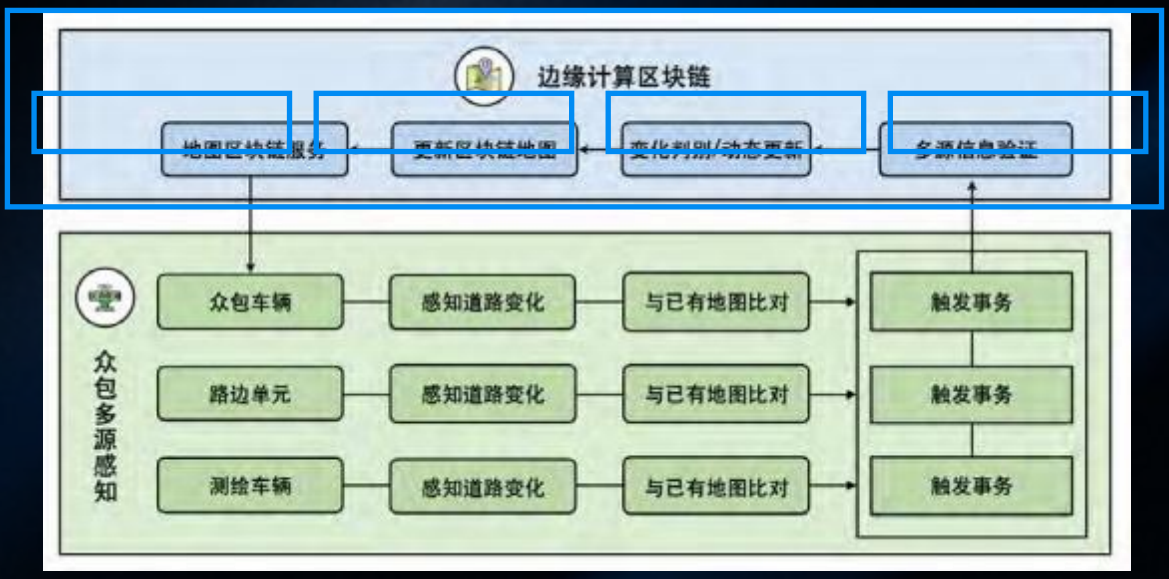
AutoMobile Chain區塊鏈發展可分為三個階段，第一階段是數位化轉型，主要聚焦在汽 車供應鏈、車電互聯、汽車後市場等領域。以核心企業為主導，在雲端建設聯盟鏈網路，利用區 塊鏈賦能上下游關聯企業數位化轉型， 同時為核心企業降本提效。第二階段是數位化協作， 隨著 AutoMobile Chain各產業鏈數位化程度逐漸提升，跨企業跨產業的數位化協作成為場景創新、業務增長的核 心勢能，各企業開始全面探索區塊鏈應用場景，以求打通企業間、產業間的資訊壁壘，更好地發 揮數據內在價值。第三階段是智能化協作， 隨著網聯化及智能化終端在車路端持續滲透，傳統集 中式的雲端數據聚合和管理中心逐漸向分佈式、多層次的泛在計算方向發展，AutoMobile Chain由網聯化和雲端化逐漸向邊緣智能化和協作化轉變，區塊鏈的可信協作能力下沉到邊緣計算端，為智慧交通、 智慧製造和智慧城市等場景下的多智能體協作提供安全保障。

4.1 協作式智能交通

● 高精地圖眾包

高精地圖的即時更新對於自動駕駛的路徑規劃至關重要，某些複雜場景甚至要求地圖數據以 秒級來更新。地圖數據一般由專業地圖公司集中採集， 由於專業的測繪車有限、測繪效率較低且 更新不及時等劣勢，難以滿足自動駕駛對於高精地圖的高時效性需求。近年來，部分車企和自動 駕駛公司開始探索高精地圖的分佈式眾包採集方式。通過將地圖數據採集任務交給道路上的任意 車輛，結合邊緣計算服務，將車輛採集到的路況資訊發送至邊緣雲進行處理，然後將即時更新的 地圖內容廣播給區域內的自動駕駛車輛。然而，高精地圖採集屬於測繪活動， 由於涉密地理資訊 數據不可記錄和公開、眾包個體無法滿足測繪資質要求、眾包採集缺乏審計和追責能力，分佈式 地採集地理要素資訊面臨著法律及數據安全問題，導致目前沒有一種眾包方式能在嚴格的數據監 管要求下，為自動駕駛提供高時效、大規模和跨區域的高精地圖服務。

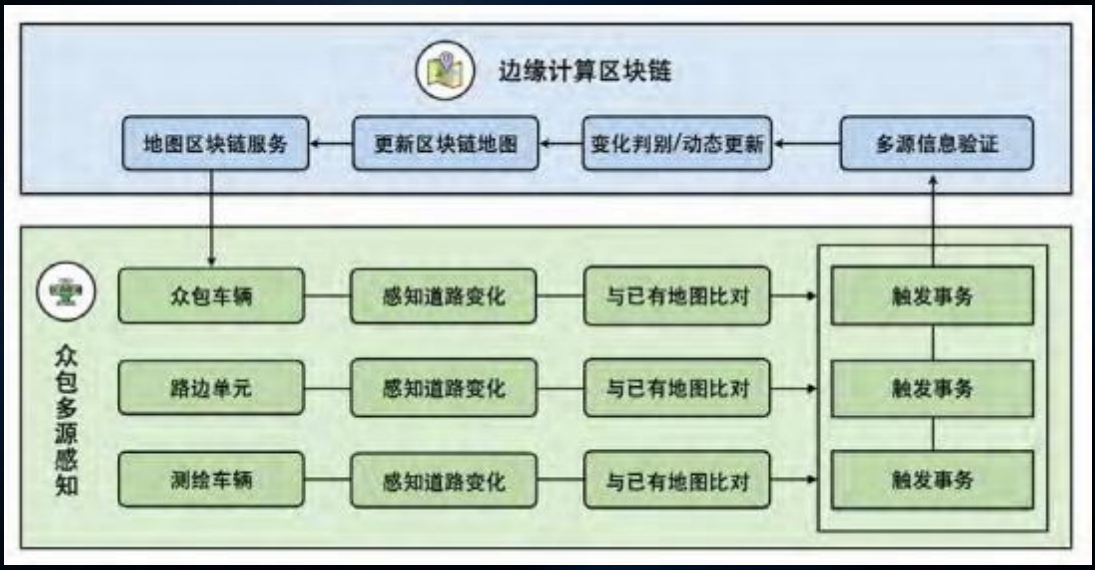
邊緣計算區塊鏈是指由不同交通區域的邊緣計算伺服器一起協同工作組成的區塊鏈網路。在 AutoMobile Chain中，邊緣計算處在“端 - 邊 - 網 - 雲 - 智”縱深架構的關節位置，在邊緣計算環節上引入 區塊鏈能夠為AutoMobile Chain應用的“前線指揮”提供可靠的服務保障，同時可以打通不同運營商之間的“邊 緣計算孤島”現象，解決移動終端在多個邊緣計算服務之間遷移的信任問題。



基於邊緣計算區塊鏈的高精地圖眾包採集平臺，可將同一區域內車輛採集到的差分地圖數據加密並上傳到此區域的邊緣計算區塊鏈進行數據融合、建圖與定位計算，再將新生成的地圖數據下發給區域內的自動駕駛車輛，從而提升高精地圖的時效性、完整性和準確性。邊緣計算區塊鏈可通過預言機和智能合約維護覆蓋區域的地圖資訊，並儲存區域內交通單元的詳細數據，每個車輛感測器都將成為該區域地圖模型的眼睛和耳朵，當車輛感測器檢測到道路變化時（比如車道變化、交通標誌、限速變化等），會將感知到的變化資訊傳達給邊緣計算服務，邊緣計算服務根據多車多感測器上傳的觸發回應，並將對不同時刻、不同角度所獲取的數據進行感知融合以確定某個交通單元是否變更。當置信度超過預先設定的閾值，則認為該地圖要素確定發生了變 化。隨後邊緣計算服務會將該資訊與地圖智能合約進行交互，並與已註冊地圖數據之間進行比對。 一旦收集到足夠多的變更資訊時，地圖將被視為有效更改，鏈上的地圖模型將自動更新並推送給 車輛以反映地圖變化情況。

- 雲控節能巡航

雲控預見性節能巡航駕駛是通過雲控平臺實現對車輛節能巡航速度的即時調節，在不降低車輛巡航平均車速的情況下，根據車輛當前所在位置前方的道路資訊和交通狀況規劃經濟車速，實現車輛的節能巡航駕駛。雲控預見性節能巡航駕駛應用採用車雲分層協同控制方法：雲端的節能巡航演算法即時根據車輛的 GPS 位置資訊和道路交通資訊對經濟車速進行預測，車端通過接收雲端下發的推薦速度對車輛行駛速度進行控制。使用雲控平臺線上計算車輛能耗最優的行駛策略，對整車動力系統進行動態調控，實現大範圍多車群體的協同節能行駛。與單車自主式巡航控制系統 相比，該方法可顯著提高道路交通資訊利用的廣度和深度，提升了車輛節能策略與行駛環境匹配的合理性。通過累計超過 5000 公里的實車測試結果表明：相較於傳統定速巡航，雲控預見性節 能巡航的平均節油率在 1.31%-5.39%之間；相較於人工駕駛，雲控預見性節能巡航的平均節油率在 3.72%-6.35% 之間。



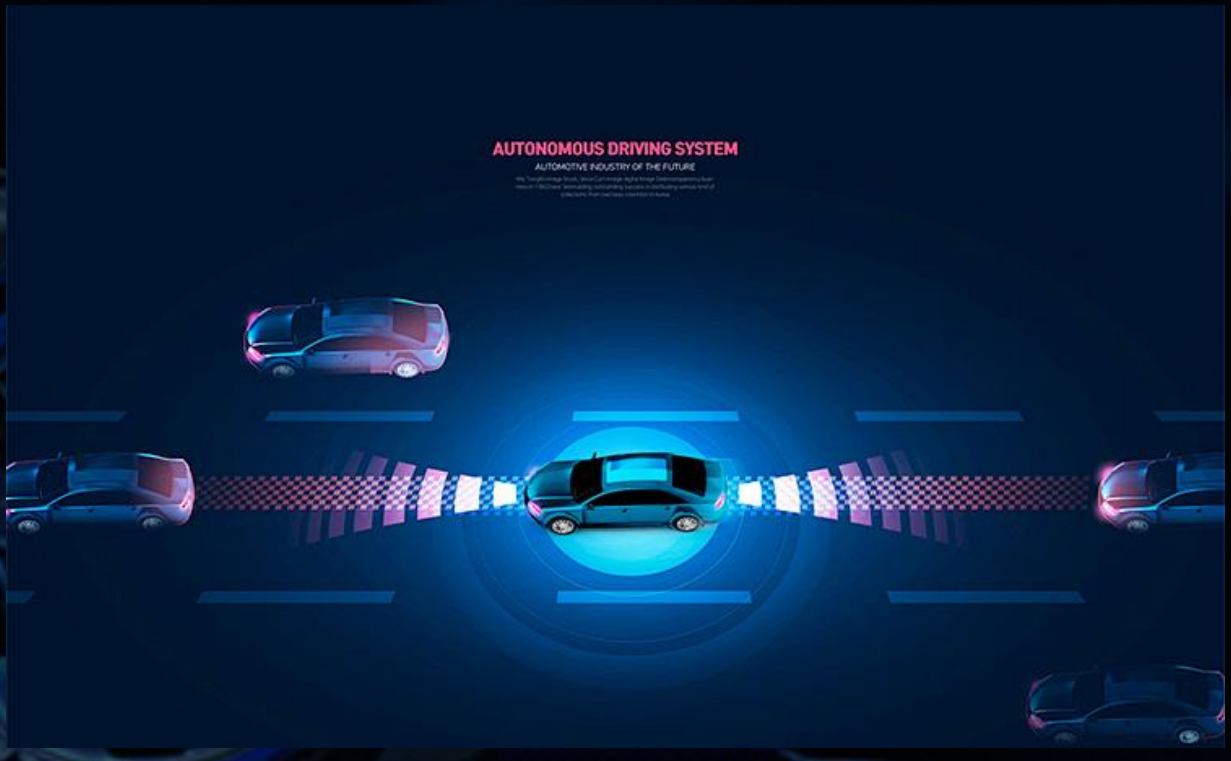
基於邊緣計算區塊鏈的高精地圖眾包採集平臺，可將同一區域內車輛採集到的差分地圖數據加密並上傳到此區域的邊緣計算區塊鏈進行數據融合、建圖與定位計算，再將新生成的地圖數據下發給區域內的自動駕駛車輛，從而提升高精地圖的時效性、完整性和準確性。邊緣計算區塊鏈可通過預言機和智能合約維護覆蓋區域的地圖資訊，並儲存區域內交通單元的詳細數據，每個車輛感測器都將成為該區域地圖模型的眼睛和耳朵，當車輛感測器檢測到道路變化時（比如車道變化、交通標誌、限速變化等），會將感知到的變化資訊傳達給邊緣計算服務，邊緣計算服務根據多車多感測器上傳的觸發回應，並將對不同時刻、不同角度所獲取的數據進行感知融合以確定某個交通單元是否變更。當置信度超過預先設定的閾值，則認為該地圖要素確定發生了變 化。隨後邊緣計算服務會將該資訊與地圖智能合約進行交互，並與已註冊地圖數據之間進行比對。 一旦收集到足夠多的變更資訊時，地圖將被視為有效更改，鏈上的地圖模型將自動更新並推送給 車輛以反映地圖變化情況。

- 雲控節能巡航

雲控預見性節能巡航駕駛是通過雲控平臺實現對車輛節能巡航速度的即時調節，在不降低車輛巡航平均車速的情況下，根據車輛當前所在位置前方的道路資訊和交通狀況規劃經濟車速，實現車輛的節能巡航駕駛。雲控預見性節能巡航駕駛應用採用車雲分層協同控制方法：雲端的節能巡航演算法即時根據車輛的 GPS 位置資訊和道路交通資訊對經濟車速進行預測，車端通過接收雲端下發的推薦速度對車輛行駛速度進行控制。使用雲控平臺線上計算車輛能耗最優的行駛策略，對整車動力系統進行動態調控，實現大範圍多車群體的協同節能行駛。與單車自主式巡航控制系統 相比，該方法可顯著提高道路交通資訊利用的廣度和深度，提升了車輛節能策略與行駛環境匹配的合理性。通過累計超過 5000 公里的實車測試結果表明：相較於傳統定速巡航，雲控預見性節 能巡航的平均節油率在 1.31%-5.39%之間；相較於人工駕駛，雲控預見性節能巡航的平均節油率在 3.72%-6.35% 之間。

在雲控智能網聯汽車研發和行駛控制過程中，經濟車速規劃的最優性依賴於車輛真實的發動 機的萬有特效數據（發動機在不同轉速和扭矩的情況下的燃油消耗率等特性參數曲線） 。由於發動機關鍵特性參數曲線在汽車行業內屬於整車和發動機生產企業廠商的核心數據，直接釋放給產業鏈上的其他企業存在核心機密洩露等資訊安全隱患。

將區塊鏈技術與同態加密演算法相結合，對發動機關鍵動力參數加密，併發布到區塊鏈上進行機密共用，是一個行之有效的解決途徑。在系統研發階段，整車企業對上下游企業不熟悉的情況下， 無需將真實的發動機等關鍵數據交給其他平臺，亦可進行相關系統的研發對接和測試驗證，對整車廠的關鍵商業機密實現了最大化的隱私保護。當雲平臺在需要使用發動機關鍵數據時，通過區塊鏈向整車廠請求數據，請求許可權驗證通過後，雲平臺即可獲得並使用加密的發動機關鍵數據。根據同態加密的特性，雲平臺可以對加密後的數據進行隱私保護計算，並獲得預測的最優節能車速結果。



● 泊車邊緣計算

泊車邊緣計算是以停泊車輛為邊緣計算算力的一種新型計算範式。通過利用數量眾多、資源 空閒的停泊車輛，力求通過資源虛擬化技術，將停泊車輛融入AutoMobile Chain基礎設施，進一步緩解傳統 AutoMobile Chain邊緣計算資源不足的問題 15 。根據現有的城市停車報告 16，大約 70% 的私家車輛每天停放 的平均時間超過 20 小時，車輛即使在停車狀態下，仍可以正常地接受資源調度，對外共用計算、 存儲和通信資源。通過區塊鏈的協作和撮合機制，對AutoMobile Chain泊車算力資源進行管理，將分散在邊 緣的計算資源整合起來，並與車載終端協同，充分調動停泊車輛資源用於計算和存儲任務，將“雲 - 邊 - 端”多級異構的計算資源連接適配，解決AutoMobile Chain算力多級異構、算網分散無序、難以統一協 同等痛點問題，實現AutoMobile Chain算力的統一編排和全局優化，並且可以在鏈上對AutoMobile Chain算力進行記錄、 調配、確權和交易，從而實現算力從產生、調度、交易到消費的信任閉環。

1）服務請求方（SR）： 包括智能交通系統中心、雲計算中心、行駛車輛等，它們需要獲得 環境感知結果，如城市道路行駛時，車載攝像機捕獲和緩存的圖像數據；

2）服務提供方（SP）： 包括本地停車場、邊緣伺服器、路側設備等服務供應商，負責資源 協調和分配停泊車輛來完成服務請求者的環境感知任務，通過網路邊緣的計算伺服器，可以直接 處理服務請求者請求的計算任務；

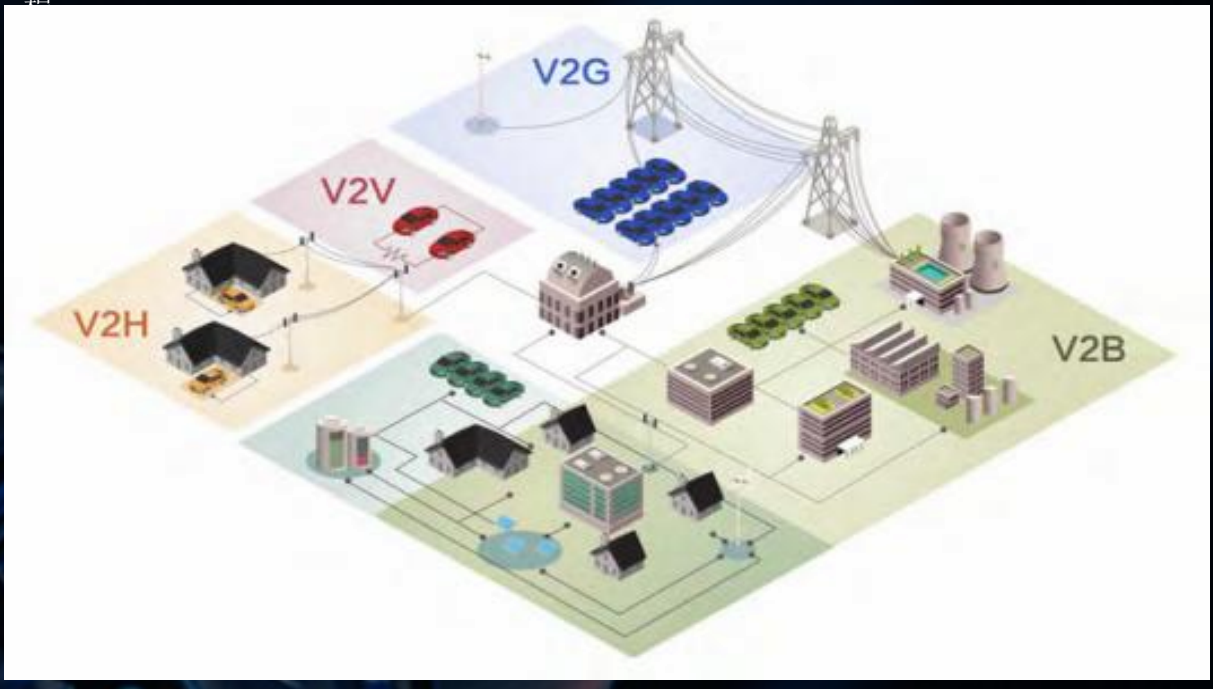
3）停泊車輛（PVs）： 提供計算、存儲和通信資源的停泊車輛，是任務的執行者，每輛車停留的時間不同，完成的環境感知和模型推斷任務也不同。

在實際應用中，交通管理部門可擔任權威認證中心角色，負責系統初始設置，並為車輛和路 側單元生成私鑰。當道路上的某些移動車輛想要使用泊車計算資源時，它需要與附近的路側單元 建立安全通道， 同時路側單元也需要與停泊車輛建立安全通道。此外，該系統需要設計一種公平 有效的資源管理模型，以激勵停泊車輛參與計算任務。通過在服務請求方、服務提供方、停泊車 輛之間構建區塊鏈網路，可在保障網路安全與數據安全的同時，使AutoMobile Chain設備相互信任，激勵車 輛參與路側單元的邊緣計算任務。通過鏈上記錄車輛資訊、車輛行為、算力貢獻大小等資訊，基 於信譽管理機制評判出該車輛的信任值，從而鼓勵停泊車輛共用邊緣計算能力，擴大AutoMobile Chain資源 容量，實現資源動態調度。

4.2 汽車電力能源

● 車電互聯

電動汽車與電網交互（Vehicle-to-Grid，V2G）作為智能電網的重要方向，既解決電動汽車大規模發展帶來的充電壓力問題，又可將電動汽車作為移動的、分佈式的儲能單元接入電網，用於削峰填穀、應急安保、旋轉備用等，在提高電網供電靈活性、可靠性和能源利用率的同時，延緩電網壓力。V2G 技術包括車輛與家間交互（V2H）、車輛與車間交互（V2V）、車輛與建築 間交互（V2B）等。例如，房主可將家中多餘的太陽能轉移到電動汽車中，同時使 用電動汽車的電池作為電能的臨時存儲載體。在公共建築設施發生電力故障期間，電動汽車可用 作應急備用電源裝置為停電建築充電。以上基於 V2G 的點對點電力交換案例，需要一個安全的基 礎設施來支撐故障識別需求回應、訂單匹配、執行交易等流程。



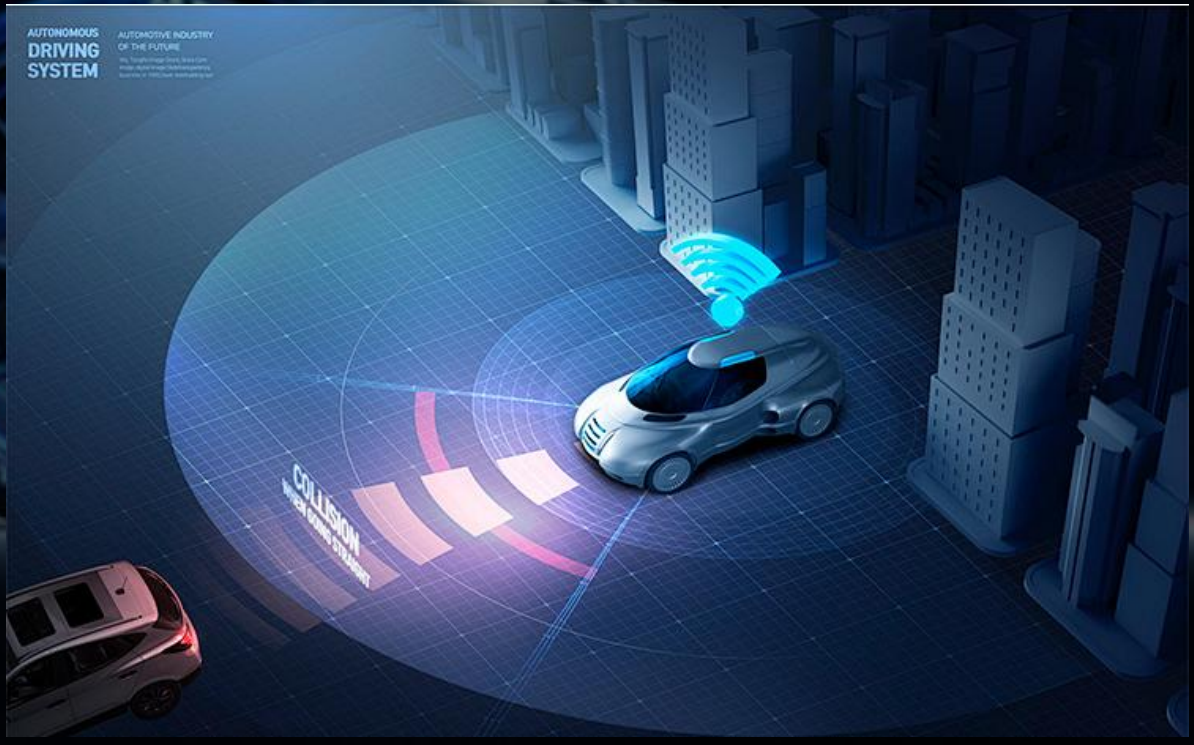
4.3 汽車供應鏈管理

● 供應鏈協同管理

由特斯拉掀起的“超級工廠”風暴正在席捲全球汽車產業，置身其中的核心零部件企業也迎 來了前所未有的挑戰和機遇。汽車工業製造是多方參與的複雜生態系統，從產業鏈的角度來講，參與方不僅包括零部件生產商、汽車生產廠商、汽車貿易商、銷售維修商和報廢回收商，還涉及 到政府和第三方物流組織等眾多機構；從製造的角度來講，汽車是一個裝配產品，它由大量的零 部件組裝起來，不同整車技術、內部構造雖然不盡相同，但所需要的零部件大概在 1-2 萬件；從 銷售的角度來講，汽車年銷售量超過千萬輛，在年銷售達到千萬件以上的商品中，只有汽車是由 上萬件零部件組成。

汽車產業供應鏈結構不斷延伸，出現了零碎化、複雜化、地理分散化等問題，給供應鏈管理帶來了極大的挑戰。 大部分零部件由外包供應商提供，提供商數量巨大又分佈在全球各地， 存在資訊透明度低、摩擦成本高昂、汽車供應鏈協調難等問題。供應鏈上下游的資訊共用障礙 正嚴重制約著國內汽車產業的發展，整車供應鏈中的眾多廠商資訊化基礎良莠不齊，造成資訊 共用出現斷層，大量的零部件數據被擱置、被堆積、無法得到運用。以汽車發動機為例，發動 機的電子控制單元 ECU 採集到的數據有 300-400 個相關參數，按照國六排放相關規定，其 中 27 個參數經由車載終端 T-box 採集， 傳輸給汽車遠程服務提供商（Telematics Service Provider，TSP）並最終匯總至國家監管平臺，剩下的數據處於漠然置之的狀態。由於當前 汽車數據匯流排、T-box 及 TSP 都由整車廠管理，因此零部件廠商並不能拿到超出監管要求的 數據，而零部件廠商與整車廠之間的博弈關係，也使得零部件廠商不願意將所有數據直接對接 給整車廠。

對於車主而言，關鍵零部件的運行狀態直接決定車輛是否能安全行駛， 因此圍繞關鍵零部件的狀態監控、預防性維護、故障精准分析都具有較大的市場價值； 對於零部件廠商而言，希望通過供應鏈的數據共用獲得構成任何零部件的“成分”證明，從而增強零部件製造過程的可追溯性，把控零部件品質，實現從原材料到生產、使用、報廢的零件跟蹤和召回。同時，可針對零部件數據進行分析和建模，對於上下游供應計畫制定、產品設計優化、生產環境參 數配置等具有重要的指導意義； 對於汽車製造商而言， 通過區塊鏈進行數據共用，能夠完全掌握上游供應和下游經商的真實資訊，即時獲取上游庫存水準和下游銷售情況，解決汽車庫存積壓、生產柔性不足等問題，從而降低供應鏈管理風險和管理成本，提升整個供應鏈運營效率。



● 汽車碳足跡管理

為應對全球氣候的合規要求，車企需要定期報告碳排放數據、披露產品碳足跡，還需要為這 些數據提供真實性證明。區塊鏈技術是證明數據的完美工具，它可以在保證供應鏈數據真實可信 的同時，為企業碳排放數據、產品碳足跡數據打上“可信任”的標籤。基於區塊鏈技術的碳排放 數據核算平臺有助於企業提高資源利用率和整體運營效率、構築綠色供應鏈體系、促進企業工藝 與技術轉型升級，形成“雙碳”目標下的低碳競爭力。

基於區塊鏈技術的碳足跡管理平臺可記錄汽車供應鏈從礦石原料開採、零部件製造、整車制 造、倉儲物流、汽車貿易商、售後服務商和回收企業等整條供應鏈的溯源數據與產品全生命週期碳足跡數據。通過建立覆蓋整條汽車供應鏈的溯源應用，以聯盟鏈的形式打造一個多中心、高效率的汽車供應鏈追溯平臺，充分評估供應商的碳排放情況，幫助車企判斷是否能夠將其納入自己的供應鏈體系中。供應鏈上的各家企業還可以根據鏈上可信溯源數據，分析企業與產品的碳排放量， 提高能源利用率，助力企業實現“碳中和”。

在可信數據採集方面，將企業在生產製造過程所產生的原材料供應、加工製造、能源消耗、產品物流運輸等數據經企業密鑰加密簽名後，通過智能合約上鏈存證。結合安全硬體、物聯網和 邊緣計算技術，讓碳排放數據在產生的同時就被加密上鏈，保障數據的即時性、真實性和不可篡改性，為整個汽車供應鏈中碳排放核算、碳足跡溯源提供可信數據來源。

在碳排放數據核算方面，將可信供應鏈溯源數據與汽車生命週期碳排放核算方法有效結合，通過將碳核算邏輯寫入智能合約，保證業務規則的可信執行， 同時對執行結果自動存證，為碳足 跡生態的整體運行提供可信環境。通過秘密共用計算能力，不同企業的關聯排放數據共用計算出 最終的產品碳足跡結果。

在數據授權訪問方面，只有通過數據所有者的簽名授權，其數據訪問權方可臨時開放給特定 的合作夥伴、上下游企業以及監管機構，保障企業數據在傳輸、儲存、處理過程中安全可控，解 決各企業商業資訊機密與環境資訊公開的矛盾，有效消除企業對自身數據安全和被濫用的風險，靈活適應碳議題的數據披露策略，以及在政府部門、第三方審核和金融機構所構成的碳排放監管 體系下規避風險。

● 供應鏈智慧監管

基於區塊鏈的供應鏈監管平臺可記錄汽車生產過程中商流、物流、資金流、資訊流“四流合一 ” 的全生命週期資訊。在汽車生產過程中，通過將 IoT感測器設備與區塊鏈的系統連接，向工廠許可的入站鏈提供多維和準確的端到端視圖，其中包括零件位置、數量、狀態和其他有用資訊，生產廠商能夠更準確地制定其生產計畫，提高零件生產的可追溯性。在汽車運輸途中，每輛汽車都會安裝GPS 設備並即時獲取汽車物流數據，監控汽車運輸軌跡。當汽車運到目的地後，整車物流公司提車， 將車輛運送至相應倉庫，全程物流數據即時上鏈，監控車輛位置與路線。基於鏈上全量全要素的資訊，政府相關監管機構能夠依據相關法律法規條例，設定法律智能監管合約，對資訊系統上的數據流進行即時監控，自動驗證交易和用戶的合規性，實現汽車供應鏈的智能監管。智能監管幫助監管部門即時監管汽車生產、汽車運輸安全、供應鏈金融洗錢和欺詐、供應鏈企業偷稅漏稅等問題。監管的重心也從傳統的事後追溯，逐漸轉向事前預警和事中控制，將各方損失降到最低。

● 供應鏈金融

供應鏈金融以其提高融資效率、緩解中小企業資金緊張、促進產融結合、賦能實體經濟等優勢，受到各個主機廠、金融機構的高度關注。然而，目前供應鏈金融業務發展仍面臨多方痛點。上游企業由於其規模較小、業務經營範圍較窄、企業信用不足，難以獲得金融機構的認可。上下游企業融資管道主要是銀行，融資管道單一。大銀行因為審批成本高、交易成本高和“資訊不對稱” 等原因，不願涉足中小企業貸款，導致中小企業生產運營面臨嚴峻的資金約束。對於整體產業鏈，每家企業關注的只是自己的利益，掌握的資訊數據也不跟整個產業共用，形成資訊孤島，很難做到圍繞客戶統一佈局。供應鏈運行過程中，各類資訊分散保存在各個環節中，關鍵資訊流則由核心企業掌握，整個供應鏈資訊不透明、不流暢，各個參與主體難以瞭解交易事項的進展情況，影響整個鏈條效率，最終導致信用體系難以建立。

汽車供應鏈金融以主機廠的應付賬款為基礎，由核心企業通過系統方式線上確權，然後向供　應商開立可轉讓、可融資的電子憑證，在上游供應鏈體系內流轉，解決上游供應商融資難、融資貴等問題。電子憑證相較於商票具易拆分、易流通、易變現的優勢， 相較於銀票具有開立靈活、零保證金的優勢。區塊鏈技術具有價值傳輸和高效協同的特性，可在整個供應鏈參與方之間構建聯盟鏈，使得消費者、汽貿商、經銷商、主機廠和金融機構之間達成互信共識。通過區塊鏈技術將各參與方的數據互通互聯，以鏈上電子憑證流轉實現供應鏈上下游的信用穿透，各級供應商都可享受到核心企業的優質信用，更容易獲得較低成本的融資。利用區塊鏈去中心化、防篡改的特性，供應鏈中生產、倉儲、物流、貿易等多維度數據經過鏈上核驗，可作為金融機構風控的有力抓手。同時利用多方安全計算技術打通多維度數據價值，建立鏈上可信數據風控與第三方風控無縫銜接，提高反欺詐能力。

五. 代幣經濟學

5.1 通證發行

致力於建立一個公平，穩定，可信任和可持續的金融發展機制，AutoMobile Chain汽车数据服务平台網通過發行AMCT通政代幣充分調動生態參與者的積極性，增加生態的吸引力。讓各位參與者能夠在參與AMCT生態發展的同時，享受新一代金融帶來的紅利。

代幣經濟學

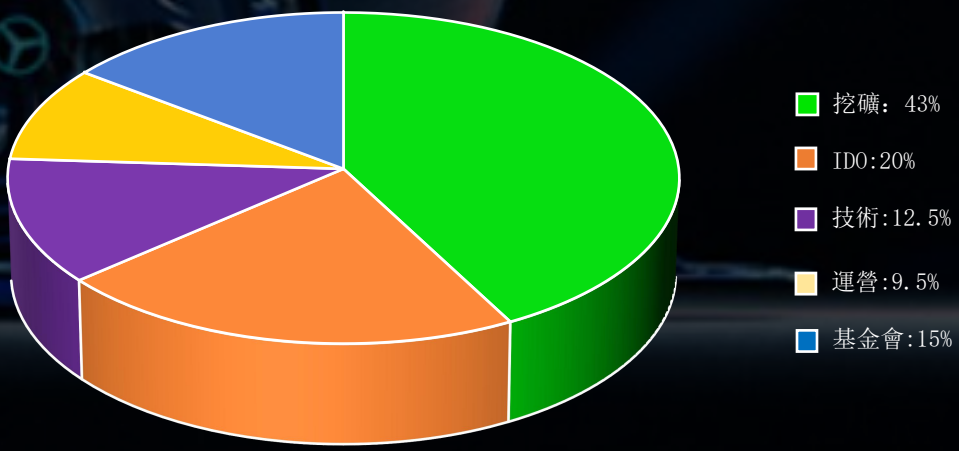
專案名稱：AutoMobile Chain

代幣名稱：AMCT

代幣發行總量：3億枚

AMCT具體分配如下:

- 挖礦:43%，由用戶數據挖礦產出。
- IDO:20%，全部由市場IDO產出，不鎖倉，上線前全部釋放;
- 技術:12.5%，鎖倉3年，之後每年釋放2%，直至全部釋放完畢;
- 運營:9.5%，由基金會審核，不定期發放，具體釋放比例將在社區公示。
- 基金會:15%，鎖倉5年，之後每季度釋放1%，主要用於公共關係的處理和獎勵對平臺有貢獻的用戶和機構;



六. 未來展望

AutoMobile Chain經過長期的技術發展，已處於規模化部署階段，數據爆炸性增長正在顛覆傳統汽車的 商業模式，以“軟體定義”、“數據驅動”、“智能網聯”為特徵的新汽車產業形態正在加速形 成。隨著區塊鏈技術逐步滲透到汽車行業的各個領域， 可信執行能力會生長在AutoMobile Chain的每個角落， 鏈上的優質數據也會流向關聯產業，整個汽車產業的協同力度將大幅提升，更豐富的應用場景也 會如雨後春筍般成長起來。對於進一步推動區塊鏈在汽車產業的創新發展，主要有以下三點建議。

一是堅持標準規範先行，優化AutoMobile Chain數據監管機制。 為滿足區塊鏈產品在汽車產業下的兼 容性、可擴展性和可持續性的需求，亟需戰略性開發並部署一批的汽車行業區塊鏈標準，推動智 能網聯汽車數據格式和服務介面標準化統一，並與國際標準接軌；為滿足AutoMobile Chain數據安全、數據 監管的需求，在健全完善相關法律法規和政策要求的同時，應完善AutoMobile Chain數據安全標準和分級， 鼓勵和支持基於標準的測評認證，汽車行業的區塊鏈產品也需依照相關法律法規建設數據安全體 系和流程，通過等級保護及汽車產品安全相關的強制性認證； 為滿足AutoMobile Chain數據開放、數據共用 的需求，應充分借鑒區塊鏈在其他行業已有的數據共用經驗，在兼顧數據安全的同時，積極探索 基於區塊鏈的AutoMobile Chain數據共用機制，建立多方共治、產業聯動、政企協同的汽車行業數據共用平臺， 有效引導和規範汽車產業數據流通體系健康發展。

二是推進關鍵技術攻關， 探索AutoMobile Chain安全能力創新。 基於區塊鏈的交通基礎設施一旦建成， 將對整體社會產生長期且深遠影響。為應對國外密碼學技術封鎖的挑戰，應加快國產化演算法的研 究和使用，實現區塊鏈自主可控軟硬體全國產化替換； 為應對後量子時代面臨的挑戰，應提前引 入並推動量子安全演算法，構建量子安全的區塊鏈體系標準和演進機制；為擺脫晶片短缺造成的“卡 脖子”難題，應加強對車規級晶片行業的扶持力度，提升車規級晶片國產化體系能力，保障汽車 區塊鏈產品有芯可用；為滿足AutoMobile Chain場景下的特殊技術要求，區塊鏈廠商應積極探索區塊鏈結合 物聯網、AutoMobile Chain、邊緣計算等概念的應用示範，在考慮規模效益、算力效益、安全效益的前提下探索新的共識計算範式，實現區塊鏈技術在AutoMobile Chain場景下的相容適配；為滿足企業和個人的數據 安全需求， 區塊鏈產業需從合規角度和技術上充分考慮，加強分佈式系統、安全硬體和密碼學等 關鍵技術研發，厘清技術安全水位和使用場景，提升區塊鏈產品的系統安全和數據保護能力，打 造一套自主可控的數字基礎設施。

三是強化示範引領作用，加快汽車區塊鏈應用落地。 汽車行業位於工業製造、交通出行、電力能源與互聯網行業的交叉口，應充分發揮區塊鏈的凝聚力和穿透力，以AutoMobile Chain為載體，聚合 多方優勢資源，打通產業間資訊壁壘，積極探索產業協同應用創新，推動整個汽車產業鏈轉型升級。 我國在AutoMobile Chain和區塊鏈領域均是技術高地，應抓住難得的歷史發展機遇，在堅持產業協同發展的 同時，應進一步強化AutoMobile Chain與其他高新技術的深度融合，組織AutoMobile Chain企業與區塊鏈企業協同攻關，積極開展“AutoMobile Chain + 區塊鏈”試點示範，遴選一批行業應用標杆案例，以保障AutoMobile Chain安全為前提， 以培育互聯互通的產業生態為目標，率先開展基於區塊鏈的車輛資訊管理和AutoMobile Chain身份認證體系 構建，並逐步向智能交通、車電互聯、汽車供應鏈等領域延伸，由點及面推進整個AutoMobile Chain生態協 同體系成熟。

七. 風險與合規

7.1 風險與合規

本文檔只用於傳達資訊之用途，不構成任何的投資建議，投資意向或教唆投資。本文檔不組成也不理解為提供任何買賣行為，或任何邀請買賣任何形式證券的行為，也不是任何形式上的合約或者承諾。

AutoMobile Chain明確表示：相關意向用戶已明確瞭解AutoMobile Chain專案的風險，投資者一旦參與投資即表示瞭解並接受該專案風險，並願意個人為此承擔一切相應結果或後果。

AutoMobile Chain明確表示不承擔任何參與AutoMobile Chain專案造成的直接或間接的損失（包括但不限於）：

(1) 因為用戶交易操作帶來的經濟損失；

(2) 由個人理解產生的任何錯誤、疏忽或者不准確信息；

(3) 個人交易各類區塊鏈數字資產帶來的損失及由此導致的任何行為；

(4) 在參與AutoMobile Chain專案時違反了任何國家的反洗錢、反恐怖主義融資或其他監管要求；

(5) 在參與AutoMobile Chain專案時違反了本白皮書規定的任何陳述、保證、義務、承諾或其他要求。

- 關於 AMCT

AMCT是AutoMobile Chain專案及其所有產品使用的官方數字通證。AMCT不是一種投資，我們無法保證AMCT一定會增值，在某種情況下也有價值下降的可能。沒有正確使用其AMCT的人有可能失去使用AMCT的權利，甚至可能會失去他們的AMCT。AMCT不是一種所有權或控制權，持有AMCT並不代表對AutoMobile Chain專案或AutoMobile Chain應用的所有權，除非AutoMobile Chain明確指定授權外，AMCT並不授予任何個人任何參與、控制，或任何關於決策的AutoMobile Chain專案或AutoMobile Chain應用權利。

風險提示

1. 安全：

許多金融征信平臺因為安全性問題而停止運營。我們非常重視安全，已與業內頂尖安防團隊和公司達成了戰略合作關係，但世界上不存在絕對意義上的 100%安全，例如： 由於不可抗力導致的各種損失。我們承諾盡一切可能確保您的交易安全。

2. 競爭：

我們知道區塊鏈征信領域是一個具有廣闊空間但競爭異常激烈的領域，有數千個團隊正在計畫並著手開發支付通證，競爭將是殘酷的，但在這個時代，任何好的概念、創業公司甚至是成熟的公司都會面臨這種競爭的風險。但對我們來講，這些競爭都是發展過程中的動力。