ATN技術白皮書

用區塊鍊網絡組織AI計算和服務

版本0.3.4
ATN.IO

摘要

區塊鏈技術前景廣闊的原因是目前非常多的行業存在壟斷。人工智能就是這樣一個領域，各大廠商相互割裂，基於目前人工智能的深度學習算法，每一個人工智能都是由大數據餵出來的一頭怪獸，只有那些擁有大量數據的軟件公司才能訓練出更加強大的人工智能怪獸，因此，本來應該屬於用戶的數據卻成為了互聯網公司們爭搶的最有價值的資源，但是因為每個公司的業務類型不同，擁有的數據也多種多樣，所以每家公司即使再強大，也最多只能壟斷一個領域的數據，而不能壟斷所有的數據，因此每家公司陷入了尷尬的自給自足境地，因為無法也不願意交換和共享自己最有價值的資源（也就是數據），導致各自陷入了孤島和困境。

數據壟斷帶來的這些風險和問題，讓區塊鏈的去中心化有了用武之地，區塊鏈最有價值的應用方法，就是協調各方面的問題：不同公司之間的協調，不同實體以及機構之間跨越疆界的協調，並以互信的方式進行充分互動，構建價值網絡並相互交換價值，打破原先的壟斷，在未來的人工智能網絡中讓不同的人工智能服務可以共建一個生態。

我們提出ATN的解決方案：一種去中心化的，無需授權的，用戶自定義人工智能服務和使用接口的開放區塊鏈平台。整體設計結合了Oracle，跨鏈代幣，以太坊等區塊鏈項目的想法，側重解決人工智能服務(AIaaS)與EVM兼容的智能合約之間互操作性的問題，未來計劃利用下一代區塊鏈技術為AIaaS搭建一個開放的經濟系統，使得AI服務可以更多的交易和互操作，形成更強更豐富的人工智能。平台設計了AI服務接入方式，中間通過ATN智能合約進行連接並將接入的AI服務無需授權的提供給任何人，使得AI服務提供者和使用者都更加容易使用AI網絡。

目錄

一、介紹

1.1連接區塊鏈世界和AI世界

共享AI的第一步，是我們如何通過區塊鏈建立一個將不同AI服務連接到一起的服務，以及如何搭建區塊鏈智能合約世界和AI世界之間的橋樑，讓用戶獲益。我們將介紹如何用DBot技術鏈下共識技術來讓區塊鏈的智能合約和AI服務互相操作，我們將首先在以太坊上實現一個Dapp來向以太坊網絡上的合約開放這種能力。在這個階段，還將提供一個ERC20的Token合約，提供代幣作為使用這些AI服務的燃料(手續費)。

ATN的第二步，就是搭建一條獨立的基礎鏈，並將代幣互換服務、DBot平台等融合進一條獨立的鏈中，利用側鍊和分片技術與其他的網絡進行交互並實現價值交換。代幣合約將遷移至獨立鏈中變成本地代幣。

1.2 ATN網絡

ATN可以解決智能合約中調用AI服務的問題。目前類似以太坊網絡中的智能合約中的“智能”並不真正智能，“智能”的說法來自於“智能手機”，更傾向於自動化的意思，而ATN通過引入AI，可以讓智能合約及區塊鏈系統成為真正的”智能”。另外，由於目前類似以太坊網絡中的這些Dapp生態，很多都是用智能合約實現並治理，當智能合約可以使用AI服務後，AI將會給智能合約賦能，並幫助類似Aragon這樣的智能合約實現Dapp的人工智能治理。

ATN可以解決目前互相割裂的諸多AI服務之間相互調用的問題，因為ATN通過Dapp(或第二階段的區塊鏈系統)提供了一個去中心化的，無需授權，人人皆可訪問的AI經濟網絡，解決AI參與方之間合作問題，ATN成為了AI生態的一個支付網絡和具備智能合約能力的經濟基礎設施。

1.2.1 無需互信的AI互操作

與傳統AI服務相比，系統更加易於實施。
加入ATN網絡非常簡單：

1.基於ATN提供的API和Schema包裝現有的人工智能服務

2.開發dbot的Oracle預言機程序，接入AI服務，並部署到ATN的多個預言機Relay服務器中.

3.開發調用AI服務的代理智能合約，定義價格和其他參數，並部署和註冊到ATN的AI服務管理智能合約中。

ATN將對常規用戶開放提供AI服務調用接口，對常規用戶隱藏所有復雜的區塊鏈技術，但對社區開源這些複雜的技術規範和實現。

1.2.2開放平台

ATN是一個可通過智能合約擴展的開放平台，從而實現與其它基於以太坊的Dapps的交互和協作。 ATN的開源特性使得第三方開發人員能更好的在平台之上構建可交易應用程序。該平台可以支持多種應用程序。

二、解決方案

2.1跨鏈代幣ATN

2.1.1 ATN代幣

ATN代幣為ATN網絡的主要代幣。 ATN代幣可以作為用戶使用ATN區塊鍊網絡和AI服務的費用和燃料，也可以作為DBot賬戶提供約定服務的激勵報酬和AI服務提供商的收入。 ATN代幣是ATN網絡的通用代幣。

ATN代幣的經濟激勵系統將會作為ATN去中心化自治系統的重要部分參與網絡的升級和管理。同時，代幣經濟系統也會給AI和機器人帶來更充分的經濟獨立[1]。

ATN代幣最終將基於不同的網絡標準實現對應的標準代幣，以EVM兼容的智能合約平台為例，將會遵循以太坊上提出的ERC-20和ERC223兩個標準。

ERC20[2]代幣標準描述了以太坊代幣合約必須實現和遵循的方法和事件，標準化有利於幫助不同的功能和組件共享基礎設施。

與大部分代幣合約只支持ERC20標準不同，ATN代幣合約還會支持ERC223標準[3]，這是因為ERC223將會解決ERC20的諸多問題並帶來一些好處：

1. 當代幣轉賬的接收方是合約賬戶時， ERC-20是無法實現對這個轉賬交易的回調處理的，因此無法實現類似本地代幣ETH那樣的fallback功能。 ERC223使得代幣可以像本地代幣那樣，除了用於代幣轉賬，還可以用於與各種合約交互，包括用於代幣分發合約。
2. 代幣有可能會被用於發送至那些對ERC20代幣並不友好的合約，因為這些合約缺乏對代幣良好的接收處理，大量的代幣可能會因為這個缺陷而丟失。
3. 當賬戶需要某個合約來花費他的ERC20代幣餘額時，這個賬戶必須先對這個合約進行額度授信操作(approve)，然後合約才可以調用轉賬操作(transferFrom)來進行花費，並且，這樣需要產生兩筆網絡交易，消耗更多的手續費和時間。而ERC223可以將這兩個交易和操作合二為一，大大簡化了這種場景的流程。

[1] 在傳統的銀行系統中，需要法律支持才能獲得獨立的身份支撐，因為大部分地區存在滯後和限制，AI或機器人無法獲得獨立的法律身份，所以也無法在傳統銀行系統中獲得經濟獨立，區塊鍊和智能合約可以讓AI或機器人更充分的享有自主的經濟獨立。 AI或機器人在ATN中的經濟價值，將很大程度上通過ATN代幣激勵系統得到體現。

[2] ERC20詳細標準接口參考https://github.com/ethereum/EIPs/issues/20

[3] ERC223詳細標準接口參考https://github.com/ethereum/EIPs/issues/223

雖然ERC223是一個還在修訂中的標準，且目前大部分錢包和基礎設置還沒有完全支持ERC223，但是因為其給代幣模型帶來的諸多優點，隨著時間的推進，會有越來越多的錢包和基礎設施支持這個標準，目前雷電網絡項目已經支持ERC223。

2.1.2代幣跨鏈支持

不同於其他以太坊上面的代幣，ATN被設計成一種跨鏈代幣，也就是說，ATN代幣可以再多個區塊鍊網絡上面運行和流通，例如以太坊，量子鏈，RSK等等。

為了讓ATN可以再不同的網絡中流通和互換，在ATN的初級階段，將會引入代幣Swap網關的概念，這是一種幫助代幣在不同的網絡中Swap流通的一種中心化服務。

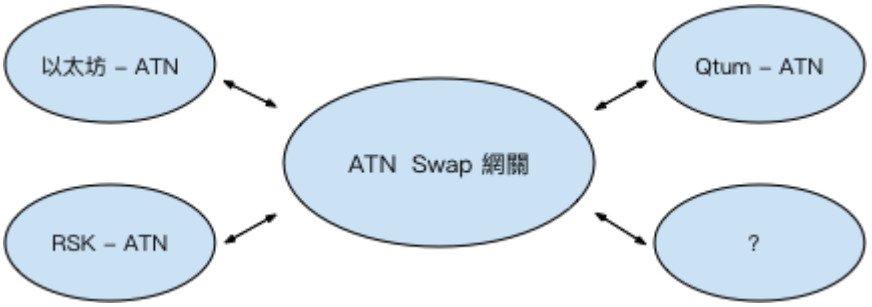


圖3-1 ATN Swap網關

隨著後期側鏈的引入或者其他跨鏈協議的發展，Swap網關將會成為未來ATN基礎鏈的一部分，這樣借助於側鍊或Cosmos[4]等技術將其去中心化並實現代幣的原子跨鏈。同時ATN基礎鏈自身也可以流通ATN 。

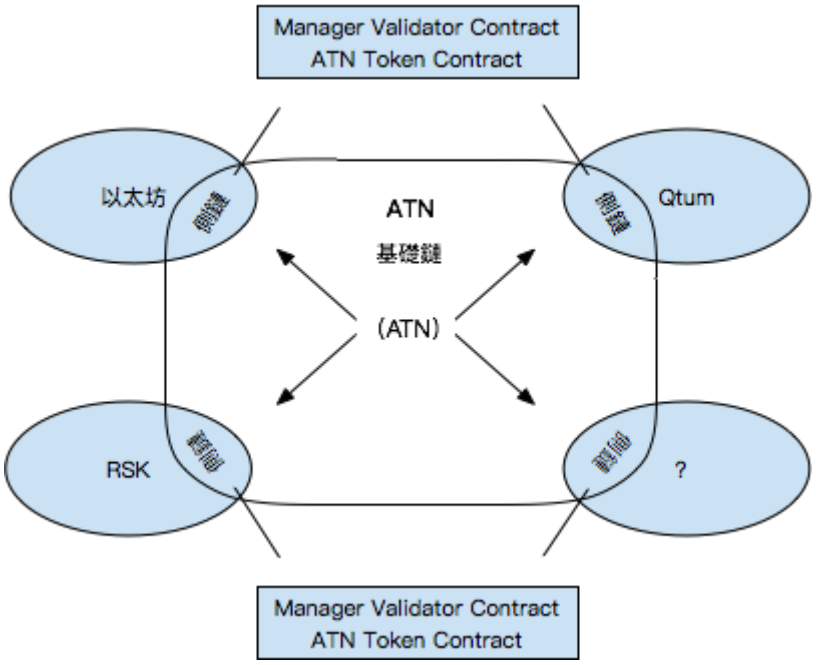


圖3-2 ATN基礎鏈跨鏈概念圖

[4] https://cosmos.network/

雖然在不同的區塊鍊網絡上面都可以具備ATN代幣，但是所有網絡上的ATN代幣模型仍然遵循固定總量的模式，假設有A、B兩個區塊鍊網絡，當ATN從A網絡流動到B網絡時，A網絡的ATN數量會相應減少，B網絡的ATN數量會相應增加。

2.2跨鏈跨平台的Dapp

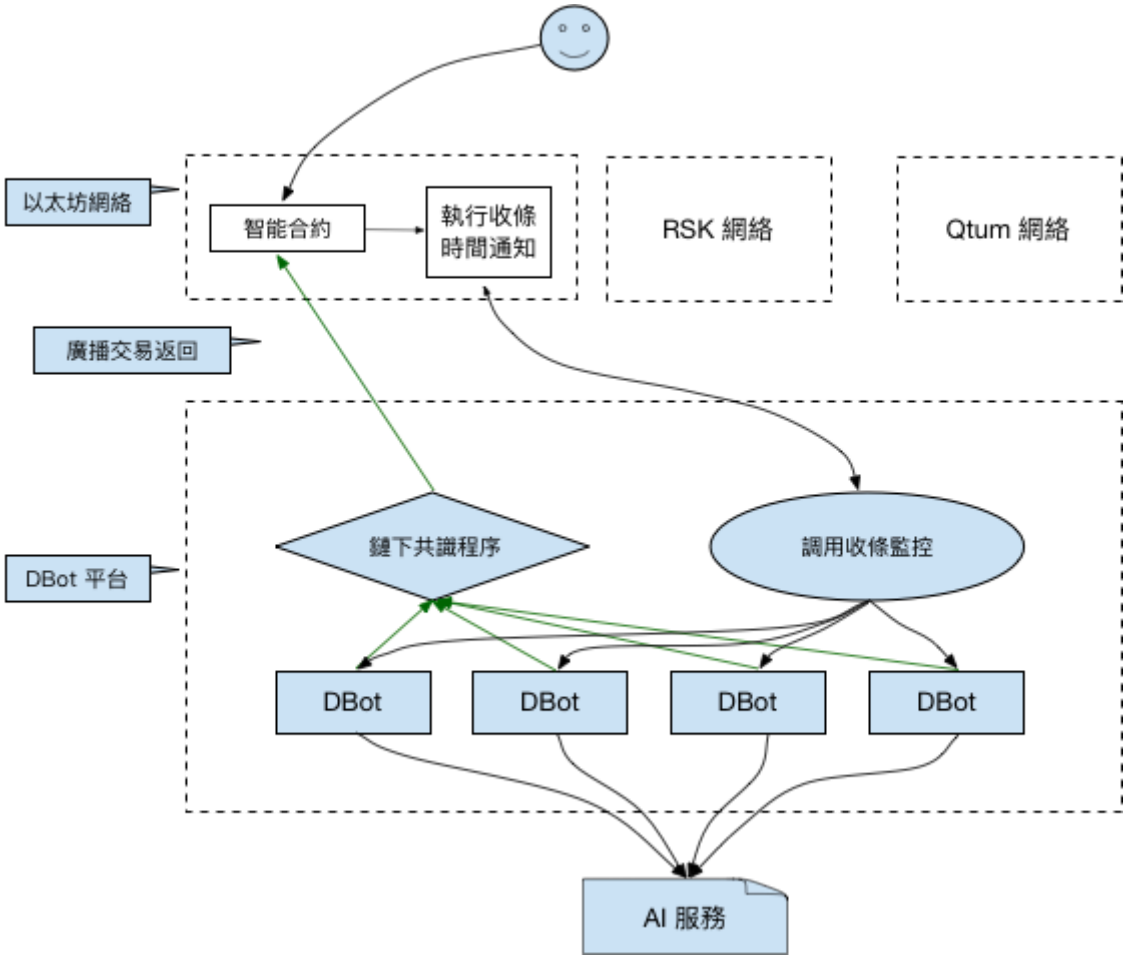
為了讓不同的區塊鍊網絡都可以調用AI計算和服務，ATN將不僅僅在以太坊上面實現Dapp，還將包括其他的智能合約平台，包括Qtum，RSK等等。不同區塊鍊和平台的Dapp將會需要藉助ATN的基礎鏈實現合約跨鏈的互操作性。

Dapp的合約主要包括以下一些類型:

- 代幣合約
- 賬戶權限管理
  包括AI服務方的賬戶，DBot賬戶，消費者賬戶，以及接入第三方合約（例如uport）的用戶身份認證模塊。
- AI服務註冊管理
  包括AI服務的註冊，查詢，以及AI服務的定價策略，計費扣除等相關合約。另外，還包括與諸如雷電網絡等狀態通道的建立和交互等功能。
- DBot代理合約
  負責與外界服務的交互以及作為回調用於獲取AI服務返回值等等。包括Oracle實現、DBot賬戶治理、鏈下共識程序定義、AI服務結果的回調合約。
- Dapp自治和更新管理合約
  包括升級更新相關合約，Dapp自治管理，合約的邏輯和數據分離設計等。

2.3 DBot平台

- 鏈下共識程序的運行支持
- 提供DBot服務器開源程序，供DBot賬戶運行維護。
- 提供DBot賬戶註冊和AI服務開發工具
- AI服務開放市場和瀏覽器
- AI深度學習算法，算力開放市場



2.3.1 智能合約和DBot的通信方式

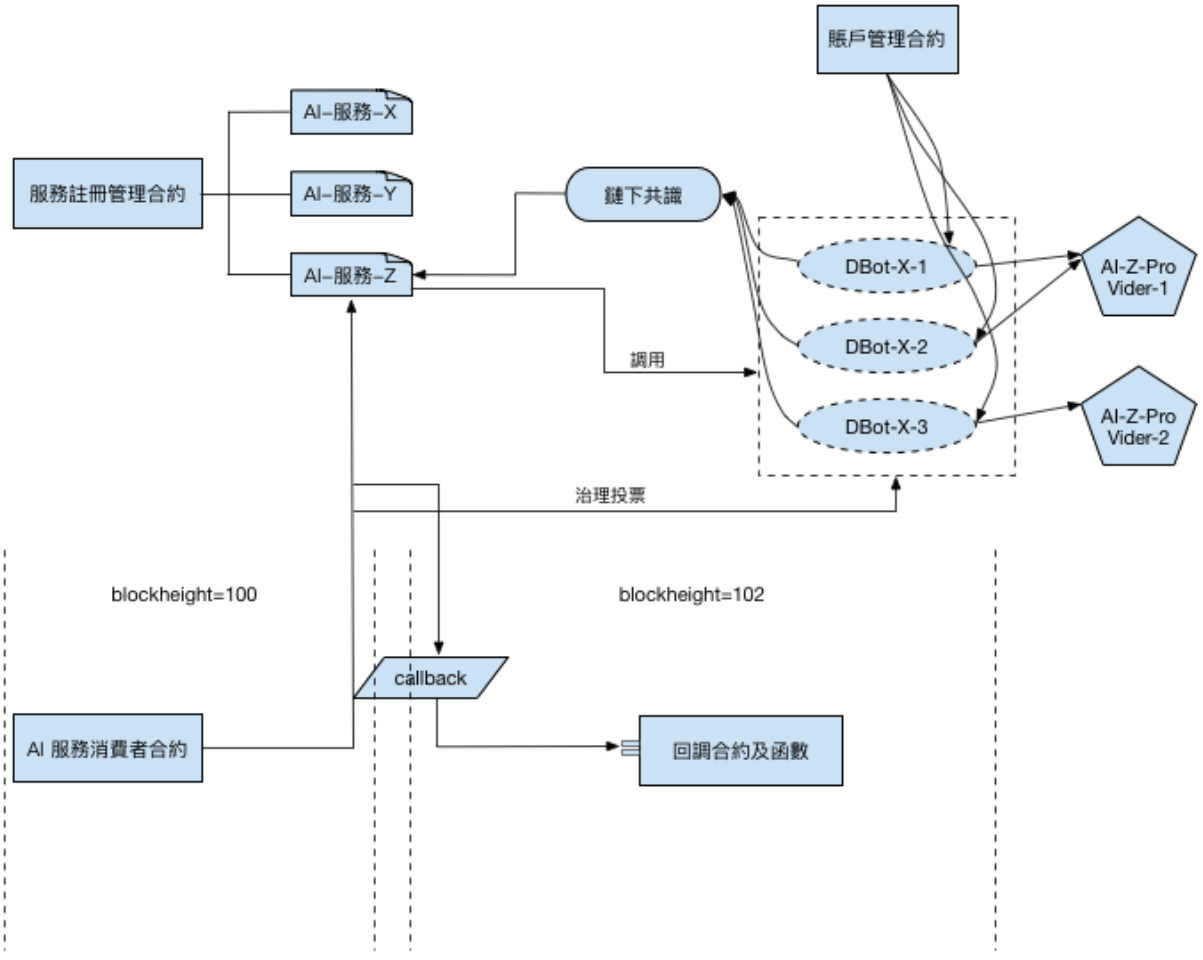
智能合約是在區塊鍊網絡上每個節點中確定性的執行的程序，並對區塊鏈賬本做出修改，因此智能合約執行過程中無法直接訪問外部數據或調用外部的服務接口，比如訪問互聯網上的資源等，因為這樣做會引入非確定性，使得各個節點對合約執行的結果出現不一致。在ATN中實現智能合約和DBot之間的通信是異步的，首先，智能合約對外部AI服務的調用將會觸發事件，DBot節點在收到這個事件通知後，將會根據事件的參數信息請求外部AI服務，並將得到的外部AI數據通過交易的形式發送到區塊鏈對應的智能合約上，使得這些信息成為賬本數據的一部分，從而消除非確定性。

這裡的DBot可以是一個可信的第三方，也可以是一個ATN通過治理機制選出的DBot服務節點群。 ATN通過DApp來實現一套用經濟激勵來保證數據可靠DBot的機制，提供給其他智能來調用。這套機制包含如下幾個部分：

1. 需要一個AI服務註冊管理的智能合約，以及對應的DBot賬戶管理策略。這些DBot賬戶負責按照AI服務的接口定義和AI提供商，來運行對應的DBot節點。
2. 一個AI服務的查詢服務，通過智能合約來查詢，不需要消耗Gas。
3. 當其他智能合約通過AI服務註冊表智能合約調用某個AI服務時，實際上相當於發送了一個異步的請求並附帶一個回調函數，調用者的智能合約將會繼續執行，DBot節點群

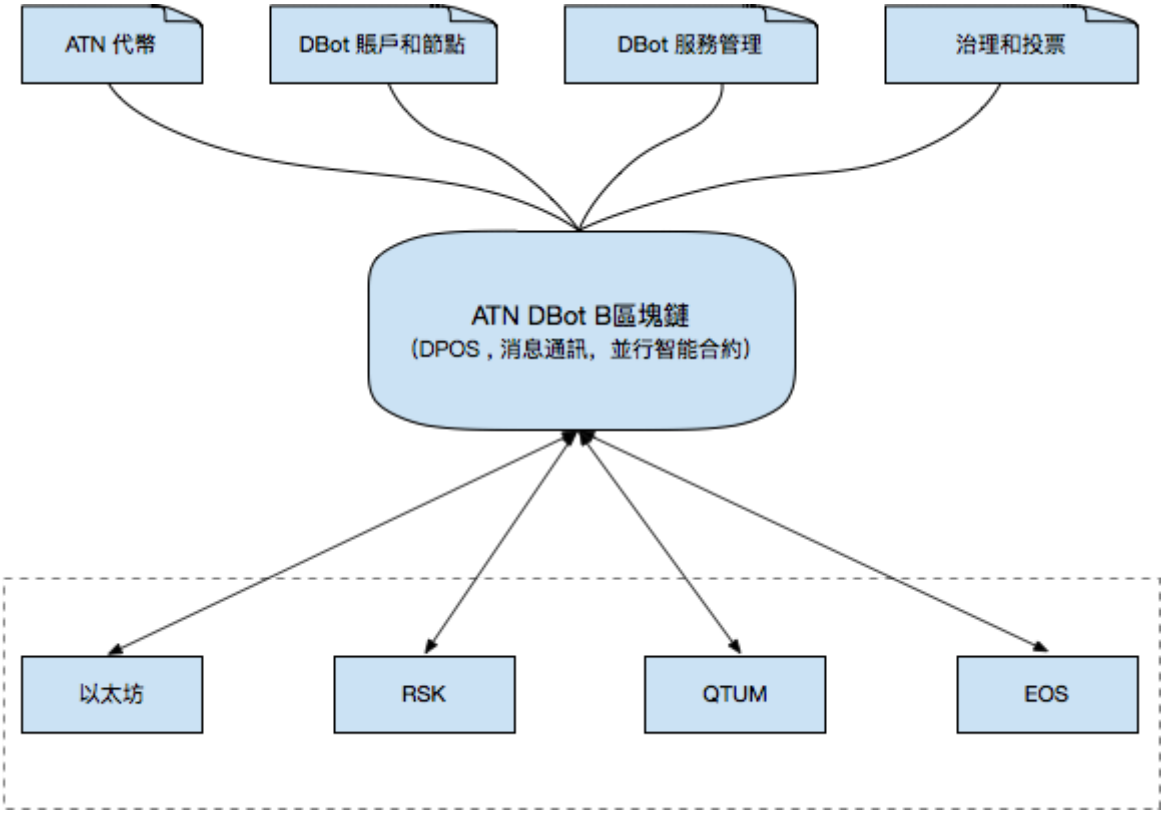
通過註冊表智能合約，在收到AI服務請求時間之後，將會在鏈下執行AI服務請求，並得到結果，這些DBot節點在各自得到數據後，在通過提交交易返回給區塊鏈之前，需要經過ATN的DBot平台提供的鏈下共識過程達成最終共識，形成統一的最終數據。

4. AI服務註冊表智能合約在收到AI結果之後，將AI結果中轉給調用者設定的智能合約回調函數。
5. 區塊鏈智能合約的回調函數，在交易調用並拿到AI結果之後，繼續執行。
6. AI服務註冊表智能合約，在這個過程中負責調用者的燃料扣費，和DBot賬戶的經濟激勵和分賬。至於AI服務提供商所需的費用則與智能合約無關，AI服務提供商收取的費用將由Robot賬戶承擔，DBot賬戶可以在收到Token激勵後，通過在交易所交易對應貨幣後支付給AI服務提供商。在有些情況下，支持某種AI服務的DBot賬戶可能就是AI服務提供商的賬戶，AI服務提供商收取Token作為其經濟收入。
7. 同一AI服務可能有多家AI服務商提供的不同服務組合而成，DBot賬戶的治理策略、鏈下共識策略、分賬策略等也可以參數化，可以自定義。
8. ATN將會為DBot節點和AI服務提供商提供開源程序，方便接入整個網絡。



2.4 ATN基礎鏈

2.4.1基礎鏈設計



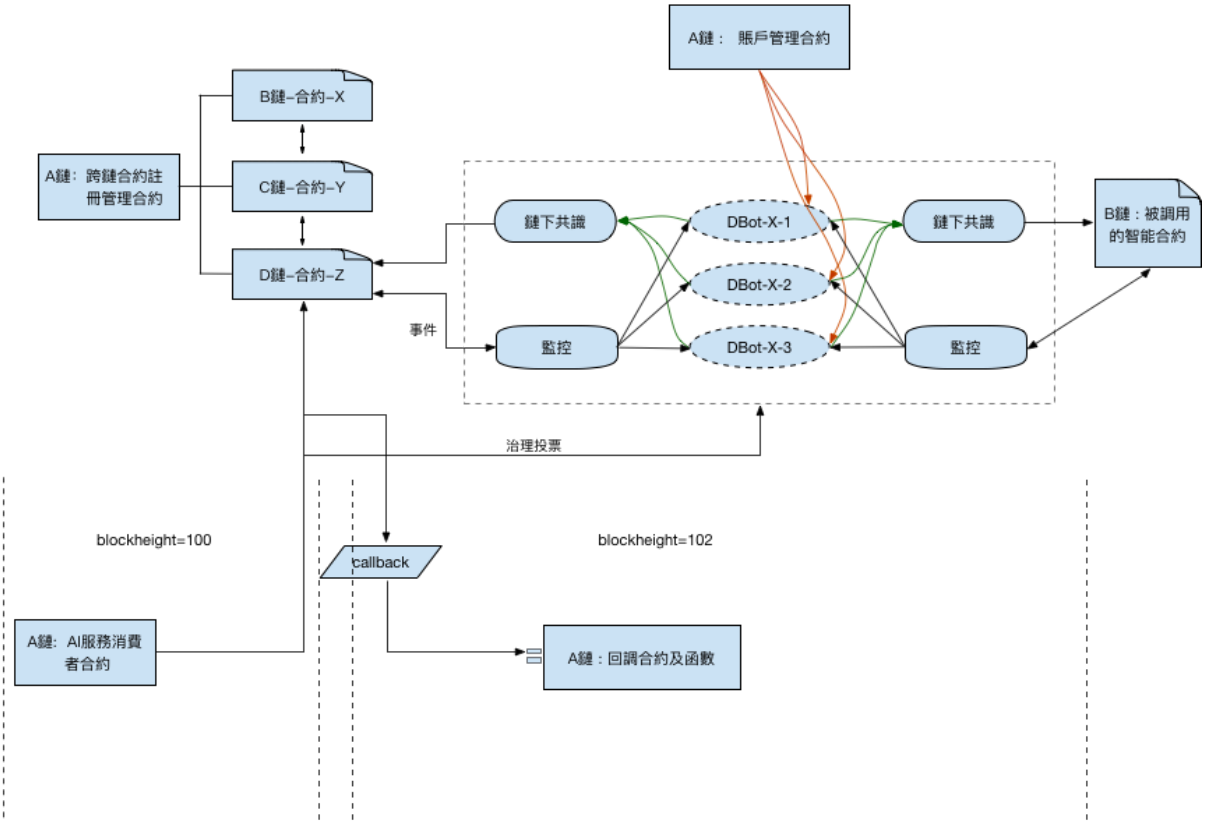
- DBot區塊鏈支持EVM兼容的智能合約
- 改進的DPOS共識算法
- 改進的EOS手續費寬帶流量控制方式
- 實現：Graphene(或EOS) + EVM
- 借鑒Ethereum 2.0和EOS的分片、並行智能合約、消息通訊設計，每一組AI服務(可能是按照提供商分組)設置對應的分片區，將每一個DBot服務群鏈下共識的部分轉至鏈上。
- ATN代幣遷移至ATN基礎鏈作為主代幣
- DBot賬戶遷移至DBot區塊鏈
- DBot服務管理合約遷移至DBot區塊鏈合約
- 為不同的EVM兼容的智能合約平台開發對應的互操作智能合約，提供不同區塊鏈平台智能合約間的互操作性
    - RSK互操作合約
    - Qtum互操作合約
    - EOS互操作合約
- 治理:系統內置結合AI的代理投票治理合約

2.4.2不同區塊鏈平台智能合約間的互操作性

DBot平台可以與支持的智能合約平台上的合約進行通信互操作，但是存在不同的區塊鍊網絡，僅就EVM兼容的智能合約來說，目前就存在很多，除了以太坊之外，目前還有RSK，Qtum,正在開發中的EOS和Ethereum Classic，那麼這些DBot平台尚未未支持的區塊鍊網絡上的智能合約如何與DBot通信。

DBot平台(或之後的Dbot區塊鏈)將提供不同區塊鏈智能合約間互操作的能力。當某個智能合約想要操作另外一個區塊鍊網絡中的合約時，將經過下面的步驟：

1. DBot平台存在一個服務註冊合約，以及對應的DBot賬戶管理策略。這些Dbot賬戶負責管理互操作的合約，並運行對應的DBot節點。
2. 智能合約通過註冊表合約調用另一個合約時，實際上相當於發送了一個異步的請求並附帶一個回調函數，調用者的智能合約將會繼續執行，DBot節點群通過註冊表智能合約，在收到合約調用請求時間之後，將會在鏈下執行合約請求，在交易確認之後，將合約執行結束後的收條返回給之前區塊鏈的調用者合約
3. 因為在被調用合約的區塊鍊網絡中存在收條證據和Merkle記錄，因此無需鏈下共識過程即可證明調用過程可靠和確定性，所以在這裡，不需要鏈下過程。但我們仍然可能需要設定多個DBot賬戶用來競爭執行該調用，以保證可靠性，競爭執行的過程可以設定經濟激勵。
4. 調用者合約在收到收條，並拿到結果數據之後繼續執行。



2.5 AI服務授權管理(AI authorisation service management)

目前主要的AI服務提供商接入都需要授權，例如通過安全簽名的方式，對<app_key, app_secret>進行簽名，而這裡的<app_key, app_secret>通常由AI服務提供者分配給AI服務調用者用戶。對於ATN來說，直接調用AI服務的就是DBot賬戶，但是由誰來最終調用AI服務通常是由系統選擇或者投票競選出來的，也就是說調用AI服務的DBot賬戶會動態變化，因此，在AI服務那裡給哪些DBot賬戶分配訪問令牌(Token)，以及如何正確的分配訪問令牌(Token)變得困難。因此，在ATN中，提出一種統一的AI服務授權管理辦法，需要AI服務提供者對該授權訪問方式提供支持。

因為在ATN中，每一個DBot賬戶都會有一個對應的活躍<公鑰，私鑰>對，每一次調用AI服務時，DBot賬戶需要用私鑰對調用請求內容或其hash做簽名，而AI服務通過DBot對應的賬戶公鑰驗證該簽名，同時還需要通過DBot平台提供的狀態查詢服務，查詢改DBot賬戶是否是有效的被選舉出來具有操作該AI服務權限的賬戶。為了避免重放攻擊(Replay Attack)，請求裡面應該包含一個nonce隨機數值，並且相應請求的AI服務應該對請求做避免重複性的校驗。

2.6 AI資源協同開放網絡(AI data computation open platform)

2.6.1 AI資源協同計算的必要性

2016年是機器智能歷史上非常具有紀念意義的年份，這一年距離達特茅斯學院提出這個概念正好過去60年，這一年圍棋計算機AlphaGo以4:1戰勝了世界著名棋手李世石。這不僅是人工智能領域的一個里程碑式的勝利，更是標誌著智能時代的來臨。 AlphaGo之所以能戰勝人類，並不是依靠圍棋的邏輯推理，而是依靠海量訓練數據、優化的並行算法和強大的計算力。在數據方面，Google使用了幾十萬盤圍棋高手之間對弈的數據來訓練AlphaGo，並讓不同版本的AlphaGo相互對弈了上千萬盤棋，這才保證了它能做到“算無遺策”；在算法方面，AlphaGo使用了Value Network to evaluate board positions and Policy Network to select moves，在Monte Carlo搜索樹和並行lbfgs優化算法方面都有創新；在算力方面，AlphaGo配備了1900個CPU和200個GPU協同運作，具有強大的算力。
從AlphaGo的例子可以看出，人工智能的資源三要素是數據、模型、硬件計算力。很不幸的是，AI資源三要素需要很大的資金投入，對於眾多的AI創新實體和個人來說，是難以承受的。
AI模型需要較強的科研能力，這是高校科研機構和AI科技創新企業的強項，而數據和算力往往掌握在政府、計算中心和大公司手中。通過AT network，將AI資源的提供方和需求方協同起來，將創造巨大的AI創新效應。在為AI資源提供方帶來經濟收益的同時，為AI需求方提供了一個一點接入的創新平台，是一個“win-win”的方案。

2.6.2、AI數據共享的方案

個人隱私的洩露和數據版權的侵犯是影響數據共享意願的最大因素，利用區塊鍊及安全加密技術可以有效保障數據擁有者的權利，減除數據共享的顧慮。

2.6.2.1個人隱私的保護

法律層面及數據擁有者都有保護個人隱私的訴求。單個用戶的一些屬性可以被看做是隱私，個人隱私保護主要是防止單個用戶信息被洩露。而AI技術可以從宏觀上對數據進行建模、並不需要精確知道每條數據的單個用戶是誰。因此，個人隱私保護和AI建模並不矛盾。對數據中的個人隱私信息進行刪除或安全加密後，在保證數據宏觀上及匿名個體的唯一性的基礎上，保障數據中涉及到的個人隱私不被洩露。

2.6.2.1.1 Hash技術

採用SHA256等散列算法對涉及用戶ID、手機號、年齡等用戶信息的字段進行加密，可以在一定程度上保障個人信息的匿名。

2.6.2.1.2差分隱私保護

差分隱私保護為了允許研究者在不洩露個體信息（用戶隱私）的前提下對一個數據集的整體（用戶行為）進行分析而研究出的加密手段。利用差分隱私保護，研究者可以計算出用戶群體的行為模式，但是對每個用戶個體的數據卻無法解析。
研究表明，通過record linkage技術仍能發現Hash後數據中的用戶id。例如，將VISA交易數據的卡號等信息hash後，花旗銀行等發卡行仍能將自己的交易與VISA交易根據交易時間、交易金額、交易機構等明文字段進行匹配，一旦匹配成功就推測出真實卡號並間接獲取該卡號在VISA中的所有交易。
差分隱私保護Differential Privacy，是C. Dwork於2006年提出來的一種隱私保護技術，其核心思想是在數據集中加入隨機性，在保證數據集的每個個體都不被洩露的情況下，數據的整體的統計學信息仍可以被外界了解。

2.6.2.2安全多方計算Secure Multi-Party Computation

著名計算機科學家、圖靈獎獲得者姚期智先生在1982年提出一個百萬富翁問題(Yao's Millionaires' Problem)，兩個百萬富翁想比較誰更多有錢，但又不能讓對方知道自己有多少錢。百萬富翁問題是一個典型的安全多方計算場景，在保證參與方的隱私不被洩露的情況下，能夠在多方數據融合計算中獲取信息。
另一個常見的例子是，Alice認為她得了某種遺傳疾病，想驗證自己的想法。正好她知道Bob有一個關於疾病的DNA模型的數據庫。如果她把自己的DNA樣品寄給Bob，那麼Bob可以給出她的DNA的診斷結果。但是Alice又不想別人知道，這是她的隱私。所以，她請求Bob幫忙診斷自己DNA的方式是不可行的。因為這樣Bob就知道了她的DNA及相關私人信息。

2.6.2.2.1不經意傳輸協議簡介

不經意傳輸是一種重要的安全多方計算，也是安全多方計算的基礎。傳統信息查詢過程中，Alice將請求發送給Bob，Bob在收到請求後將相應的信息發送給Alice。在這個過程中，Bob是知道Alice的數據請求的。但是在不經意傳輸（Oblivious Transfer，OT）中，Bob並不知道Alice的數據請求，同時Alice只拿到了自己請求的數據。

2.6.2.2.2同態加密

同態加密是基於數學難題的計算複雜性理論的密碼學技術。對經過同態加密的數據進行處理得到一個輸出，將這一輸出進行解密，其結果與用同一方法處理未加密的原始數據得到的輸出結果是一樣的。

經過同態加密的數據經傳輸後，使用方不用解密就可以正常處理。同態加密技術側重於數據處理安全，而不是數據存儲安全。同態加密提供了一種對加密數據進行處理的功能。也就是說，其他人可以對加密數據進行處理，但是處理過程不會洩露任何原始內容。同時，擁有密鑰的用戶對處理過的數據進行解密後，得到的正好是處理後的結果。同

同態加密在隱私數據保護和AI模型訓練方面發揮著重要作用，數據擁有者可以將數據經過同態加密後提供給訓練模型的開發者，保護數據不被洩露的同時得到訓練模型。

2.6.3、AI算力共享的方案

2.6.3.1集中算力共享

超算中心、雲企業擁有較強的獨立算力，將這些算力開放給AI創新企業，一方面可以利用閒置的算力獲取收穫，另一方面可以在提供服務過程中提升自己的計算平台的技術水平。算力共享主要用於模型訓練階段，對於模型預測階段可以直接使用雲平台方案。
對於算力提供者來說，需要搭建模型訓練平台，並說明支持的AI模型：
單機類AI模型，例如：python的scikit-learn、java的weka等；
分佈式類AI模型，例如：spark的ML -lib；
深度學習類AI模型，例如：tensorflow、Caffle等；
ATN為AI算力集中共享提供SDK包，該SDK包分provide和require兩個版本，算力提供者利用該SDK暴露接收服務，算力訪問者利用該SDK發起AI模型訓練服務。主要包含如下接口：
數據上傳接口：上傳訓練數據，並做好數據隱私保護；
模型訓練接口：發起模型訓練；
模型評估及導出接口：通過該接口進行模型評估並導出模型。

2.6.3.2眾包算力共享

在AI模型中，有許多模型具有分塊學習並結合的結構。例如，GBDT、RF等集成模型（Ensemble Model）由一棵棵的樹聯合起來形成一個模型，神經網絡模型以一種搭積木的方式建模。
在算力眾包的情況下，在ATN中預建算力較強的節點作為模型聚合結點。參與算力眾包計算的節點，將收到一小批加密後的訓練數據和標準的測試數據，節點利用訓練數據構建一個獨立的模型，例如，樹或神經網絡，節點將構建的模型對測試數據進行分類，並將生成的模型和分類結果發送到模型聚合節點。聚合節點重放小模型的分類結果，並與眾包節點發送的分類結果進行比較，以此判斷節點是否真正模型訓練。

2.6.4、模型共享的方案

2.6.4.1預訓練的模型共享

深度學習模型的層數越來越深，在ImageNet的比賽中，從8層的AlexNet、16層的VGG、22層的GoogLeNet，到152層的ResNet。由於神經網絡模型具有極強的泛化能力，隨著層數的加升能更好地表達訓練數據中的特徵，其分類效果也會更好。
神經網絡模型的層數加深，訓練時間也更長，動輒達數週。另外，具有較小的訓練語料不能很好地使用深層次的神經網絡。通過採用遷移學習使用較深的神經網絡模型。將在大規模的數據

集上預訓練的深層次神經網絡模型共享出來，使用者可以利用自己的數據重新訓練神經網絡模型的後面幾層，就能達到很好的分類效果。
ATN提供SDK包，用於pre-trained模型的發布和版本保護以及模型的搜索和下載使用。

2.6.4.2參數化的模型服務

此類場景屬於AIaaS的一種，用戶在使用此類模型前，需要先上傳一批語料數據，然後再使用模型服務。以人臉識別為例，用戶先上傳自己的人臉庫，再使用人臉識別服務。

相關工作：零知識證明

“零知識證明” - zero-knowledge proof，是由S.Goldwasser、S.Micali及C.Rackoff在20世紀80年代初提出的。它指的是證明者能夠在不向驗證者提供任何有用的信息的情況下，使驗證者相信某個論斷是正確的。零知識證明實質上是一種涉及兩方或更多方的協議，即兩方或更多方完成一項任務所需採取的一系列步驟。證明者向驗證者證明並使其相信自己知道或擁有某一消息，但證明過程不能向驗證者洩漏任何關於被證明消息的信息。大量事實證明，零知識證明在密碼學中非常有用。如果能夠將零知識證明用於驗證，將可以有效解決許多問題。

相關工作：安全多方計算(MPC)

安全多方計算（SMC）是解決一組互不信任的參與方之間保護隱私的協同計算問題，SMC要確保輸入的獨立性，計算的正確性，同時不洩露各輸入值給參與計算的其他成員。

為了說明什麼是安全多方計算，首先我們先介紹幾個實際生活中的例子。

1． Alice認為她的了某種遺傳疾病，想驗證自己的想法。正好她知道Bob有一個關於疾病的DNA模型的數據庫。如果她把自己的DNA樣品寄給Bob，那麼Bob可以給出她的DNA的診斷結果。但是Alice又不想別人知道，這是她的隱私。所以，她請求Bob幫忙診斷自己DNA的方式是不可行的。因為這樣Bob就知道了她的DNA及相關私人信息。

2．經過一次花費昂貴的市場調查後，A公司決定擴展在某些地區的市場份額來獲取豐厚的回報。同時，A公司也注意到B公司也在擴展一些地區的市場份額。在策略上，兩個公司都不想在相同地區互相競爭，所以他們都想在不洩露市場地區位置信息的情況下知道他們的市場地區是否有重疊。 (信息的洩露可能會導致公司很大的損失。比如另一家對手公司知道A和B公司的擴展地區，提前行動佔領市場；又比如房地產公司知道A和B公司的擴展計劃，提前提高當地的房租等等)所以他們需要一種方法在保證私密的前提下解決這個問題。

3．兩個金融組織計劃為了共同的利益決定互相合作一個項目。每個組織都想自己的需求獲得滿足。然而，他們的需求都是他們自己專有的數據，沒人願意透露給其他方，甚至是“信任”的第三方。那麼他們如何在保護數據私密性的前提下合作項目呢？

以上三個例子的共有特點是：

a.兩或更多方參與基於他們各自私密輸入的計算。
b.而且他們都不想其他方知道自己的輸入信息。

三、架構設計

3.1業務架構

ATN由ATN區塊鏈系統，AI計算和服務開放平台，DBot網絡平台和AT用戶開放平台組成。整個業務生態還包括底層的智能合約平台(以太坊，量子鍊和RSK等)、DBot節點礦工、算力模型礦工、AI集成解決方案供應商、AI消費者服務和智能合約，手機系統應用等設施，將基於這些基礎設施和服務，搭建面向不同行業的AI開放平台，例如醫療行業AI開放平台，智慧城市AI開放平台，海洋行業AI開放平台。業務架構如圖4-1所示。

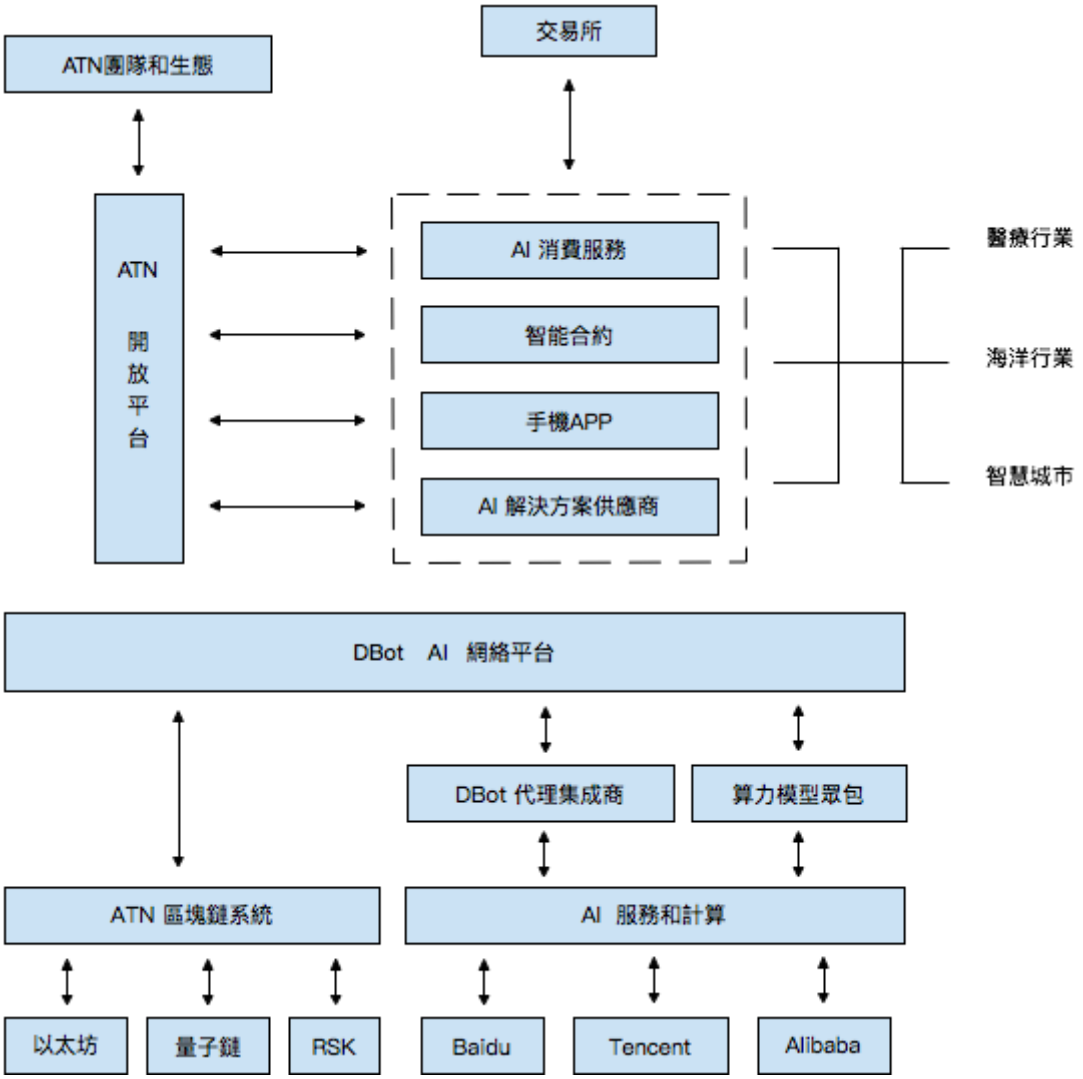


圖 3-1 ATN 業務架構圖

3.1.1角色構成

1)AI服務提供者
指AI服務的開發和提供者，通過分析學習大數據，對外提供AI計算和服務。在ATN中，將可以通過ATN的AI計算和服務開放平台接入ATN生態，提供服務並獲取代幣收益。

2)AI消費者
通過恰當的解析ATN中註冊的AI服務接口和數據，任何開發者都可以開發ATN的AI服務瀏覽器，便於AI服務使用者查詢和使用AI服務。 AI服務使用者有可能是某個智能合約，也有可能是另外一個服務或程序，需要支付ATN代幣才能使用AI服務，ATN系統受到代幣費用後，將會根據服務表現進行自動分賬。

3)DBot開發者 DBot developer
是指在ATN平台上開發並發布DBot合約並接入經過授權的AI服務的第三方開發者，DBot合約更像是AI服務和ATN間的一個適配器。 DBot合約提供者為開發並部署這些合約收取恰當的手續費。 DBot合約提供者有可能和AI服務提供商重合，但不是必須，也有可能是經過AI服務提供商授權，或者是AI服務提供商的客戶。

4)DBot礦工[5]
提供並負責運行DBot服務節點的賬戶，參與AI服務鏈下共識過程，任何人可以申請和註冊DBot賬戶，但是成為某一組AI服務的DBot賬戶，需要經過系統投票選擇過程。

5)ATN區塊鏈系統
基於區塊鏈技術的賬本和合約管理系統，用於解決跨鏈合約互操作和代幣SWAP等功能，將會對接以太坊、量子鍊和RSK等智能合約平台[6]，同時將會引進內生的代幣和智能合約系統[7]。

6)AI計算和服務開放平台
用於對接各大AI服務供應商的AI服務市場，提供AI服務的註冊、報價及檢索功能，最終形成一個AI服務開放市場，提供給DBot開發者用於集成和開發。

7) AT用戶開放平台
提供各種主要的面向AI消費者的API服務，包括支付，交易，合約，開放數據等API。

8) AI解決方案供應商
利用自有技術和ATN提供的各種AI服務搭建面向C端用戶的整套解決方案的供應商。更廣泛一點說，面向各個行業的AI開放平台將由這個行業的各種解決方案構成。

3.2技術架構

ATN的技術架構分為應用層、中間件層和底層基礎設施，底層基礎設施部分又分為通用區塊鍊網絡和AI計算和服務開放平台。

[5]跟傳統的礦工只提供算力服務不同，這裡的“礦工”是廣義的礦工，意思是給系統提供某種服務並換取代幣報酬。
[6] 可能會基於側鍊或ManagerValidatorContract等技術。
[7] 可能是基於Dfinity，EOS或Ethereum2.0等下一代區塊鏈的其中一種。

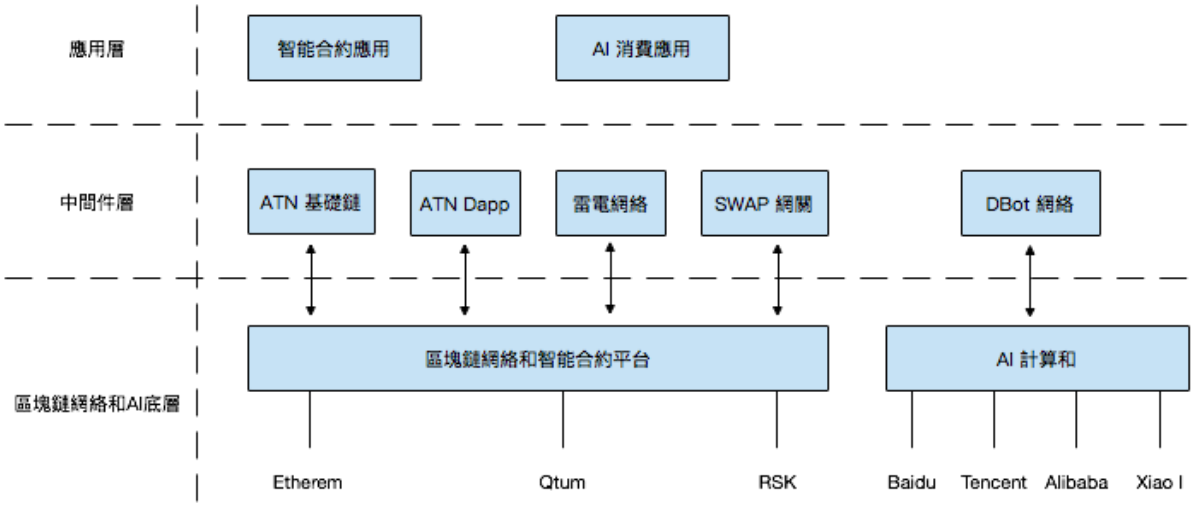


圖4-2 ATN技術架構示意圖

3.2.1 Dapp應用

拿以太坊智能合約平台舉例，ATN將在以太坊上開發一個DApp，這個DApp實際由一系列智能合約組成，包括主調用合約，代理合約，治理合約，Token合約，用戶信息管理合約等等。

服務管理合約
賬戶管理合約
代幣合約
治理合約
支付合約
分賬合約

3.2.2狀態通道網絡

對於AI服務應用來說，存在高頻次調用和低頻次調用的區別。對於簡單的事實預測類的AI服務來說，比如“2012年的足球世界杯冠軍是哪個球隊”，可能被用於智能合約中作為判定條件，有可能並不會調用很頻繁。但是在人工智能領域中，還存在一些其他類型的AI服務，比如聊天機器人或者客服機器人，他們的調用交互頻次會非常高，由於目前區塊鍊網絡的性能限制，一方面是單筆交易的手續費成本還是比較高，另一方面網絡負載性能(也就是TPS:每秒交易數)也不能滿足高頻詞調用的需求。因此，利用類似雷電網絡這樣的高頻微支付技術來擴展和改善性能就變得非常重要。

狀態通道技術將網絡分成了兩層：一層是支付網絡，也就是狀態通道這一層，利用信息傳輸協議交換包含轉賬信息、金額和數字簽名的加密票據，另一層就是由區塊鍊網絡所構成的清算網絡。頻繁的交易會在支付網絡上發生，當支付交易結束之後，會回到區塊鏈清算網絡上進行結算。

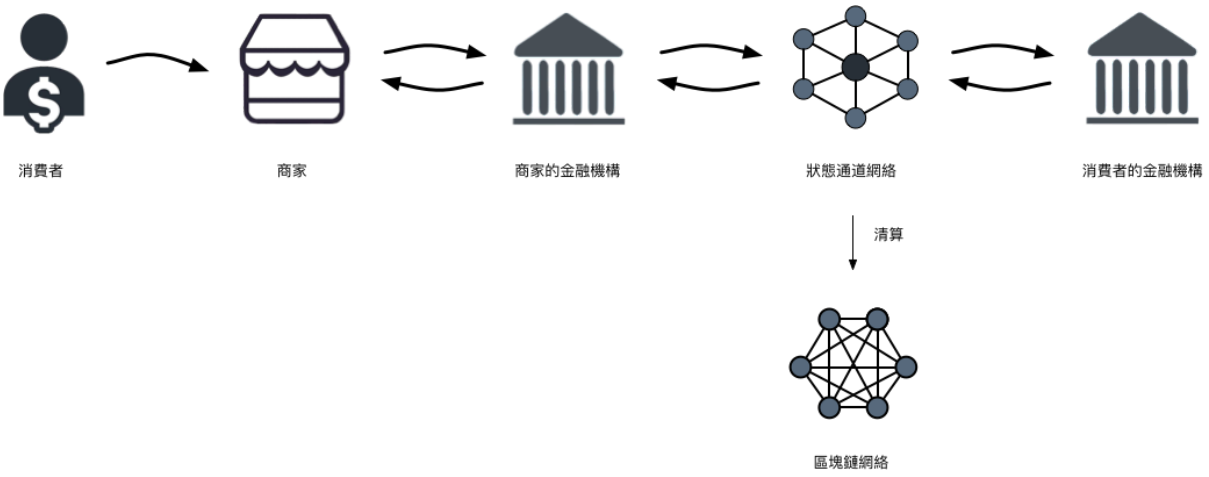


圖4-3區塊鍊網絡支付過程圖(支持狀態通道技術)

相關工作：閃電網絡

閃電網絡（ Lightning Network），簡單來說，它的目的是將比特幣的絕大多數交易帶離區塊鏈，而且不會犧牲可證性以及安全性。

閃電網絡可允許創建“微支付渠道”，除了發起通道的初始交易之外，多筆比特幣交易在無需與區塊鏈進行互動的情況下，還能安全地進行。它也不存在交易對手的風險：如果任何一方終止合作，或者說在約定的時間內沒有響應，該通道可以被關閉。

這些在通道中的支付交易會瞬間完成，這與當前的比特幣支付不同（往往需要1個小時的時間來完成交易驗證）。更重要的是，支付是可路由的，它是跨越多跳路徑的，這就像是互聯網上的數據包。相對於為每一個新的合約方創建一個渠道，你可以維持一些渠道，連接少數良好的安全中介機構，並通過他們來完成交易。

從理論上來講，這種分佈式小額支付網絡（閃電網絡）可以將比特幣的日交易量擴充到數十億筆每天，並且極少地使用到區塊鏈，以及僅需少量的交易費。

然而，閃電網絡需要再次對現有的比特幣協議進行改動（雖然這是一個軟分叉，即現有的區塊鏈將繼續完全有效），這項技術目前還處於早期階段。

以比特幣上的閃電網絡為例，閃電網絡是基於微支付通道演進而來，創造性的設計出了兩種類型的交易合約：序列到期可撤銷合約RSMC（Revocable Sequence Maturity Contract，哈希時間鎖定合約HTLC（Hashed Timelock Contract）。RSMC解決了通道中幣單向流動問題，HTLC解決了幣跨節點傳遞的問題。這兩個類型的交易組合構成了閃電網絡。

如果Alice和Bob希望在他們之間建立支付渠道，他們中的一人或兩人要把比特幣整合到一筆特殊的多重簽名交易，發送者直接向接受者發送這筆簽名交易，而不是對它進行廣播，這就和（傳統）支付本身一樣便捷。只要交易不是發生在區塊鏈上，你就可以選擇把這些比特幣發送給別人。兩個人可以決定各自把一些比特幣整合到一筆單獨交易，只有他們同時進行加密簽名，這筆交易才能對外發送。這是所謂的多重簽名或pay-to-script-hash，也是支付渠道建立的依據。

然後，他們創建和簽名一筆新交易，但原始的資金會在支付通道關閉並清算後回到他們手上，而且直至之後的某天才能使用（例如未來的30天）。當他們彼此需要發送資金時，各自的資金餘額隨之更新，同時會縮短交易可花費的時間（29天，28天，等…），後，新的交易變化會被廣播到網絡。

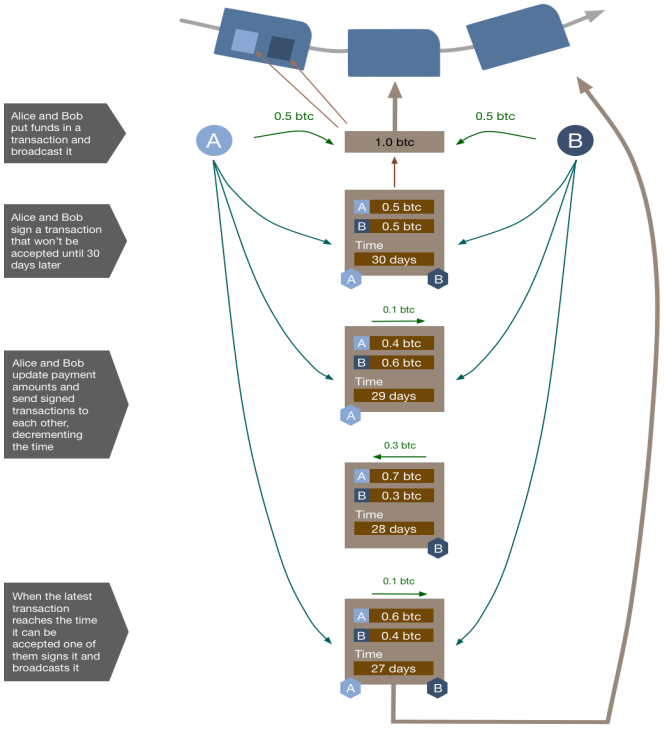


圖4-6閃電網絡支付渠道的創建和形成過程

因為這些信息只會在Alice和Bob之間傳送，它們有助減少發生在區塊鏈上的交易數，從而讓區塊鏈能大規模處理交易。它們也可視為即時支付，同時解決零確認問題，因為沒有任何手續費，他們可進行任意麵額的小額支付。唯一要考慮的是交易被廣播到網絡的時間，這取決於Alice和Bob 什麼時候關閉渠道，或者如果他們中的一個要停止交易（此時其他人會等待新的可被花費的交易被廣播到網絡，再向他們發送合適的比特幣數額）。

上面的描述的場景發生在兩個支付參與者之間。真正讓支付渠道有用武之地的是狀態通道網絡還能將它們鏈接在一起，形成一個網絡。 如果Alice和Bob有渠道，Bob和Carol有渠道，然後Alice可通過Bob支付給Carol。Bob或許收取小的手續費，但是比區塊鏈的手續費要少得多。

相關工作：以太坊雷電網絡 Ethereum Raiden Network

以太坊提高交易處理能力的方式主要有兩個，一個是分片技術（shard），另一個就是狀態通道技術（state channels）。雷電網絡（Raiden Network）是狀態通道技術在以太坊上的實現。

以太坊的雷電網絡類似於比特幣的閃電網絡。雷電網絡的基本理念是，用戶可以私下交換轉賬簽名消息，而不是所有的交易都放到的區塊鏈上處理。雷電網絡通過以太坊網絡中的點對點支

付與保證金存款保留了區塊鏈系統所具備的保障機制。參與方之間不斷發生的交易在鏈下進行，但最終可以在鏈上進行清算。

四、用戶案例

本節列舉了ATN可以應用的一些典型場景和案例，僅僅是未來眾多應用的冰山一角，更多的應用案例等待用戶去發掘和想像。

智能合約調用AI-aa-Service

智能合約的最大優勢之一就是不可中斷的執行一段程序或者契約，但是某些契約的執行需要依賴依賴於一些外部的數據事實或者證據，通常來說這些數據事實會有一些可信的第三方通過提交數據提供，未來AI帶了的趨勢之一就是，可信的第三方將會變成多個可信的第三方分別提供的AI，以達到更高的參與率與可靠性。

例如某個保險相關的合約需要通過調用AI來獲取下個月上海的天氣狀況(溫度，災害概率)，以幫助該保險合約完成在該地區中與天氣相關的賠率精算，後續的保險賠付執行將根據這個賠率自動執行。因為智能合約是在諸如以太坊這樣的網絡中的每一個節點中確定性執行的，任何的確定性差錯都會帶來網絡共識的失敗，因此節點各自執行的確定性智能合約中無法直接調用外部服務，他們將通過由鏈上智能合約選舉出來的賬戶執行收集信息並執行鏈下共識過程後，獲取外部AI信息和數據。智能合約將因為有了ATN提供的通向AI服務的橋樑，獲得了外部信息的高度及時性和可靠性。

基於AI的智能合約去中心化治理

Aragon Network[6]提出了一種基於智能合約的去中心化司法仲裁機制，本案例將在此基礎之上做進一步的改進，為去中心化的司法仲裁中的法官提供更加自動化高效和公正透明的支持，主要從兩個方面，利用AI更加高效的事實數據和證據獲取，利用鏈下共識在AI事實數據的基礎上更加透明的得出仲裁結論。 AI能否完全取代人類可能還有爭議，但是因為人類做出決策的過程存在於大腦黑盒之中，有非常多的不確定性和不可信性，AI有理由在他們擅長的深度學習和區塊鏈確定性領域比人類做的更好，未來去中心化自治組織(DAO)的治理將很有可能被AI取代，但在此之前，ATN提供的DBot賬戶仍然可以保留"法官"角色的功能，與類Aragon的系統保持兼容，但法官將可以被AI替換。

區塊鍊網絡強調確定性，確定性帶來信任和低風險，AI替換仲裁法官將帶來確定性的提升，從而提高網絡的信任，降低系統風險。

鏈上的智能合約可以利用AI服務對區塊鏈的鏈上和鏈接的鏈外數據做大數據分析，通過ATN提供經過AI服務和DBot平台後的確定性結果給智能合約，並做進一步的執行。通過這種方式，ATN可以很好的滿足鏈上類似智能合約這樣的AI服務消費者的需求，幫助解決區塊鏈合約學習分析能力不足的問題。

AI服務的互操作性

目前的AI服務是割裂的，因為數據的不同，對應AI擅長的地方各不相同，比如Alpha Go只懂下圍棋，微信的AI更懂社交，支付寶的AI更懂支付，谷歌的AI可能更懂搜索行為和熱點，其他一些AI更懂語音或語義分析，類比於人類，現在的AI看起來更像是智能的一部分功能，比如只會游泳，只會走路，或者只會說話。未來的超級智能必定功能更加全面和豐富，比如當遇到一個對手需要下圍棋時就調用Alpha Go的AI服務，當需要檢索搜索時，就調用谷歌的AI服務，當需要分析對方的社交關係時，就調用微信的AI服務。

ATN希望為這種未來的超級智能提供AI服務間的互操作性。當需要完成某件複雜的AI任務的時候，通過操作其他的AI服務來共同協作完成是最經濟和可行的方式。在ATN中，AI服務的互操作性是通過智能合約和DBot平台來實現的，註冊在ATN註冊表智能合約中的AI服務已經被標準化，其他AI服務所調用只需支付一定的費用，均可以調用。因為ATN的開放、無需互信和無需授權的特點，ATN網絡也可以理解為AI服務提供商和使用者之間的網絡基礎設施和價值交換網絡。

五、總結

傳統的信息中介平台是互聯網信息交換的重要應用，他提供了經濟領域基於信息聚集和信任中介的合作基礎。但是，在AI領域，因為數據在AI服務中的重要價值，使得利用信息中介平台很難達成價值交換和協作機制，共有鍊和基於共有鏈的DApp為各自分裂的AI服務參與者提供了這樣一個價值交換和通信協作的網絡。我們已經展示瞭如何通過ATN來實現區塊鏈世界和AI世界的橋樑，讓智能合約和AI服務間都可以互相操作。我們也列舉了該系統如何為未來的AI應用提供支撐。特別的，它具有傳統信息中介平台所不具備的與生俱來的優越性。

六、術語

本節解釋下面的文檔中涉及的一些核心概念。

AI服務

AI服務是由具備大數據和人工智能服務能力的公司或個人提供的一種雲服務，通常表現為雲服務接口API。

用戶賬戶

很多AI服務會根據不同的用戶特徵數據來進行相應的分析和回應，以提供更好的AI服務和用戶體驗。因此ATN有必要在區塊鏈的地址賬戶之外，為用戶創建一個帶有用戶數據狀態的賬戶，除了包含例如轉賬地址這樣的值之外，還會包含其他更多的用戶自定義信息，這些信息可以根據成本和隱私保護的不同考慮，存放在鏈上或類似IPFS這樣的鏈下。另外，AI合約應該可以接入類似uport這樣的用戶身份合約，來獲取用戶身份的認證信息。

AI消費者

AI消費者按照鏈上和鏈下兩個層面，又可以分為兩大類：

1. 鏈上消費者
    - 為智能合約提供Oracle服務（事實型）

      像競猜對賭，以及法律文件等智能合約發布後，需要oracle激發後進行合約處理。例如，賭一場球賽的智能合約需要等待球賽的結果。這一類的結果都是事實型服務調用，但仍然會有作弊的服務商的可能。 ATN可以調用多個DBot，使用共識機制來甄別可靠的服務商。

- 為智能合約提供AI服務

數字資產文件以hash的方式存儲在鏈上，有AI解讀的需求。

數字資產校驗：從URL取得數字資產內容，與hash的結果進行比對；

自然語言處理：從數字資產內容中進行實體識別，能回答一些基本問題。

鏈下消費者

a.調用前無需訓練模型、且無session的概念

例如，語音識別、車牌識別等AI服務。此類需求對AI服務提供商不要求是固定的，可以隨機發往這類AI服務商中的某一個。

b.調用前無需訓練模型、但有session和用戶的概念

例如，閒聊問答。需要將請求發往固定的某個AI服務提供商，在問答的過程中AI逐漸了解調用方，達到越來越智能的目標。

c.調用前需上傳語料訓練模型

例如，智能客服。需先提供領域知識進行模型訓練，再提供服務。

DBot，DBot服務器和DBot平台

DBot是一個ATN引入的新的概念術語，用來表達銜接以太坊智能合約和AI服務之間所有事物和通信的用戶定義程序，ATN將提供DBOT程序的開發規範，用戶將可以依據這些規範開發DBot程序，並發佈到DBot平台上面。 DBot平台由一系列DBot服務器組成並共同運行，Relay服務器將由很多註冊在ATMaxtrix DApp上的DBot賬戶來託管，這些賬戶會由治理合約通過合約定義的治理機制選擇出來，只有經過這些賬戶的授權，DBot服務器可以和ATN進行通信。

DBot的註冊信息，包括接口定義的指紋是存放在區塊鏈上的，供DBot平台來查詢和驗證。每一類AI服務對應一個Dbot群組，這個群組中的Dbot共享同一種權限管理和治理機制，還有可能會共享一些智能合約來協助做鏈下共識。

DBot平台負責接收來自用戶(包括普通用戶，AI或智能合約)的請求，並將請求發送給ATN DApp負責解析請求和分發給負責相應AI服務的DBot服務群，每個DBot服務節點實際上運行的都應該是一樣的DBot程序，用來請求AI服務提供商獲取AI服務，經過鏈下共識(預言機)之後再返回給DApp和用戶。Dbot的概念部分來自於預言機(Oracle)，通過多中心的服務節點結合鏈下共識解決現實數據源可信性的問題，但是Dbot的涵義更廣，不但包括預言機的可信數據，而且包括智能合約與AI服務間的通信和互操作性，強化的鏈下共識的部分.

鏈下共識

最早由ATN引入，通用意義上是指在區塊鍊網絡和智能合約的外部，利用預言機、 DBot等多中心化的機制獲取數據源，並經過特定共識程序，在鏈下達成達成最終的共識結果數據源，並將該結果數據源返回鏈上的過程。在ATN中，鏈下共識的過程經過改進，參與鏈下共識的多中心賬戶和共識程序，是可以參數化後經由鏈上智能合約選擇和設定的，最終提交給鏈上合約的數據源將包括由提供者簽名的原始數據源，以及最終的數據源。因為鏈下的多中心和共識程序由鏈上程序或合約提供，因此鏈上程序或合約將可以對數據源的提供者以及鏈下共識過程做校驗。

案例一：Schelling Coin

Schelling Coin來源於一種古老的隔離調查方法，跟囚徒困境也有關係。分別將兩個人帶到兩個隔離的屋子裡，給他們看一串數字，如果他們回答相同，則都能得到獎勵，如果不同，則受到懲罰。例如如下這個串數據：

14237 59049 76241 81259 90215 100000 132156 157604

通常情況下，這兩個人都會選擇大家都認為特別或者對的那個選項，也就是常識。一般人都會覺得100000這個數字比較特別，並且都會認為另外一個人覺得這個特別，並且可以一直這樣遞歸思考下去。

案例二：中位數餵價

在比特股的系統中，為了構建跟實際資產錨定的穩定貨幣，以在BTS抵押物不充足時平倉買多做空產生出來的比特美元，需要受託人在塊產生時餵入外部交易所的USD/BTS的價格，每個受託人餵入的價格都不相同，最終以哪個價格為準呢？比特股採取了一個簡單的算法，試圖獲得最公允的外部價格，也就是去掉一個最高值，去掉一個最低值，在剩下來的數值中取中位數作為最終的價格。

七、參考

1. 小I機器人：http://www.xiaoi.com
2. 以太坊為什麼選擇POW+POS混合機制？ http://www.8btc.com/powpos-vitalik-burterin
3. Oraclize: http://oraclize.it/
4. NEO白皮書： http://docs.neo.org/zh-cn/
5. EOS技術白皮書：https://github.com/EOSIO/Documentation/blob/master/TechnicalWhitePaper.md
6. Aragon白皮書: https://raw.githubusercontent.com/aragon/whitepaper/master/Aragon%20Whitepaper.pdf
7. Algorithm人工智能算法平台 https://algorithmia. com/
8. 以太坊分片： https://github.com/ethereum/wiki/wiki/Sharding-FAQ
9. Comit網絡： http://www.comit.network/doc/COMIT%20white%20paper%20v1.0.2.pdf
10. 雷電網絡：http://raiden.network/
11. 雷電網絡POC：https://github.com/raiden-network/raiden/wiki/Raiden-PoC%E2%80%900
12. 理解Oracle：https://blog.oraclize .it/understanding-oracles-99055c9c9f7b
13. Schelling Coin : https://blog.ethereum.org/2014/03/28/schellingcoin-a-minimal-trust-universal-data-feed/
14. Sharding: https://github.com /ethereum/sharding