地氣 (DiQi) 白皮書

2015/5/29

www.DiQi.us

摘要

地氣 (DiQi) 是新一代的分散式智能資產交易平台。它是基於一個可公開驗證之分散式網絡帳本，區塊鏈 (Blockchain)，使去中心化的電子商務與金融市場參與變為可能。地氣採用多角色架構和許可制區塊鏈，可以更準確地模擬現實世界的情況，並能滿足各種商業需求。透過地氣網絡的整合，傳統金融工具可以免除既有的集中式媒介風險，而仍然保持其高頻交易和合約的多樣性。藉由優化區塊鏈技術以更佳支持平台上的交易頻率和智能合約，地氣系統能夠在分散式架構下支持複雜的金融市場和電子商務應用。

前言

大部分的互聯網交易直到今天都需要仰賴金融機構作為可資信賴的第三方。在這種“基於信用的模式”(trust based model)下，所有的交易資訊的提供與存儲都被掌握在第三方的手上，交易者對於第三方必須完全信任，並且無法驗證。2008 年出現的比特幣區塊鏈技術是一個去中心化交易平台的概念性驗證，其採用密碼技術來控制貨幣的生產和轉移，屬於一種加密電子貨幣（Cryptocurrency）。比特幣經由一種稱為「挖礦」的過程產生，所有參與者透過驗證交易和記錄來獲取作為手續費的比特幣，或取得新產出的比特幣。比特幣首次將分散式交易架構的概念推向市場，在電子商務和金融業界尤其引發討論。

然而比特幣著重在分散式系統的密碼安全性時，卻犧牲了交易頻率作為代價。在金融市場的區塊鏈技術應用，交易頻率與監管議題一直是其最嚴重發展阻礙。相對於比特幣這種完全自由的區塊鏈，一些金融服務實體對於許可制區塊鏈技術更感興趣，因為他們有實際業務需求需要確認其消費者的身分，並且對所發生的交易有法律責任。針對採用比特幣作為交易媒介的電子商務系統，其交易頻率和貨幣價值波動性也阻礙了它的可用性。受限於原始設計，比特幣的最大交易頻率為平均 7 個每秒交易量（TPS）。另一方面，市場投機操作和監管機構態度也大幅度影響比特幣的價格波動性。

除了市場應用的問題以外，比特幣也有技術方面的議題。51%攻擊問題被認為是比特幣網絡的一大缺陷，即如果單一實體掌握大部分的計算能力，它將能夠操控區塊鏈帳本的內容，例如撤銷交易或者製造虛假交易等等。

地氣系統強調加密貨幣網絡的實用性。除針對區塊鏈技術做密碼學安全性的提升，地氣網絡提供了更符合商業應用需求的解決方案，以使其進一步擴大交易規模並將垂直結合既有電子商務系統與金融市場。

特色

地氣基於比特幣區塊鏈技術，且進一步擴展了比特幣的功能及性能，在原有比特幣之基礎上提供多貨幣功能，智能合約，並解決比特幣被詬病以久的性能問題。讓貨幣發行商可管制貨幣之發行及交易，自行決定數字貨幣之匯率並動態調整，另外可提供大數據以進行分析，將數字貨幣帶到一個新的高度。

地氣網絡使用多中心階層式架構，網絡頂端為一或多個聯盟成員 (Consortium) 負責生成區塊供網絡獲取交易歷史資訊，並擁有任命貨幣發行商之權力。每個聯盟成員可任命一或多個貨幣發行商 (Issuer)。貨幣發行商負責發行貨幣，並控制使用者之交易能力。網絡最下層為數量極大之使用者，每個使用者可持有一或多種貨幣，並可互相交易。

地氣多貨幣之功能乃比特幣缺乏之功能，地氣系統中可承載任意數量之貨幣種類，各貨幣有極大之貨幣總量上限，而非比特幣之兩千一百萬貨幣總量限制。各貨幣由發行商發行，每種貨幣可恰由唯一貨幣發行商發行，使用者需向該發行商註冊後方可使用該貨幣。使用者可自發行商取得貨幣，或與其他使用者交易以取得貨幣。地氣系統並內建有貨幣間互相兌換之功能。

地氣智能合約之功能為基於比特幣協定與原有之可供編程之交易腳本。比特幣雖提供可編程之交易腳本，但功能較為侷限無法涵蓋各式應用之需求且不支持較複雜之計算，且比特幣傾向支持較單純之交易腳本，較複雜之腳本並不保證被比特幣網絡接受。地氣系統透過協定方式定義基本交易種類，配上系統提供之進階編程交易腳本達到原比特幣無法完成之智能合約，例如提供自動執行之功能，此即為比特幣無法運行之計算。

比特幣無法承載較高頻之交易及等待確認時間過長已顯著造成交易之不便，目前比特幣只能負荷平均每秒七個交易，此負載能力對於熱門之應用顯然不足，且平均每十分鐘才生成一個區塊，小額交易需等待十分鐘以確認交易成功對許多應用明顯不足。地氣針對此問題將區塊改為彈性生成，最低可短至每十五秒鐘生成一區塊，如此可大幅提升可承載之交易頻率，且大幅縮短交易確認時間。在提升效能之同時地氣亦考慮資料量之問題，在無交易之狀況下並不生成無用之區塊，避免資源浪費。

數字貨幣管制鬆散、匯率波動過大亦是使數字貨幣無法被大範圍接納之原因之一，有鑑於此，地氣在多中心化點對點交易制度上提出了數項獨特之設計。多中心之聯盟成員設計不只節約區塊生成成本，地氣在區塊生成採取了獨有之區塊動態難度調整制度，此設計可避免單一聯盟成員擁有過多之話語權進而影響網絡之公正性，且大幅降低比特幣無法解決之 51% 攻擊之可能性。再多貨幣之基礎上，提供個貨幣發行商極為彈性的發行量，貨幣發行商可自行決定該貨幣的發行時程。也可透過地氣系統所提供之智能合約功能，由貨幣發行商提供相應之資產或信用擔保，自動按照時程發行貨幣，管制貨幣發行，藉此穩定貨幣之發行量，進而保障貨幣之價值。對於使用者地氣也提供了管制機制，發行商可選擇性要求已註冊之使用者方可進行交易，在提供點對點交易的便利性之外，發行商同時可追蹤使用者之交易紀錄，藉此獲取使用者之交易習慣與特性以進行大數據分析。

動態非線性工作量證明機制：基於比特幣中均勻工作量證明機制 (Uniform Proof of Work) 在區塊鏈技術中的應用，地氣採用動態非線性工作量證明機制 (Non-Uniform and Non-Linear Proof of Work)，調整每個聯盟成員獲選為驗證者的困難度，避免趨向獨佔驗證的可能性，解決了 51% 攻擊 (51% Attack) 的問題。在地氣的動態非線性工作量證明機制中，根據當時的時間點 (Timestamp) 往回推算 N 個區塊，每一個參與的聯盟成員依照此 N 個區

塊中獲選為驗證者的次數，動態的調整其在當時挖礦困難度，也就是調整工作量證明的期望大小。由於所有的交易資料都會在區塊鏈中顯示，於是所有聯盟成員皆可以輕易計算出其他聯盟成員在某個時間點的困難度為何，因此動態的調整是可實現的。透過馬可夫鏈 (Markov Chain) 的模擬，考慮所有獲勝可能性的分布及轉換關係，並且比較各種非線性模型後，地氣採用指數模型公開集體驗證演算法。若兩個聯盟成員的驗證次數差了 k 次，則驗證次數較多的聯盟成員其工作量證明困難度將會是另一個聯盟成員的 2^k 倍。結果顯示在由 10 個聯盟成員組成的地氣網路中，當計算能力一致時，動態非線性工作量證明機制將比均勻工作量證明機制安全 1444 倍。

地氣系統的參與者

作為一個許可制分散式帳本，地氣網絡有多種參與者存在，即聯盟成員，發行商，完整節點，和地氣行動錢包。每個角色在區塊鏈上皆有不同功能和權限。[表 1] 描述不同角色在地氣網絡中的功能比較。

聯盟成員 (Alliance)：維護地氣網絡安全與驗證交易

地氣採用聯盟架構驗證。聯盟成員支撐整個地氣系統網絡，與其他聯盟成員一同驗證交易之正確性，並將驗證過之交易收入區塊中，透過類似比特幣挖礦之技術，將新生成之區塊接上區塊鏈，是唯一在地氣系統中擁有挖礦憑證的

角色。這麼做的原因是為了避免運算資源在無意義的競爭下浪費。聯盟成員可發行鑄幣憑證給發行商。另一方面，聯盟成員之間通過一個投票系統，決定聯盟成員的加入或退出。這種競爭與合作並存的聯盟架構確保整個地氣網絡安全。聯盟成員擁有地氣系統上所有的功能，包括：挖礦，產生並發行鑄幣憑證，擁有完整的地氣區塊鏈。

投票 (*sendvotetoaddress*)：聯盟成員角色可發起投票。當一個新的節點欲申請成為聯盟成員一員時， 現有的聯盟成員可透過 “*sendvotetoaddress*” 進行記名制投票給新的節點，當該節點取得之票數超過現有聯盟成員數量的一半，該節點則取得聯盟成員權利。

發送鑄幣憑證 (*sendlicensetoaddress*)：聯盟成員角色可發送鑄幣憑證，當一個新的節點欲申請成為新的貨幣發行商時，聯盟成員可透過 "*sendlicensetoaddress*" 賦予該節點一個新鑄幣憑證，取得憑證即可發行該種貨幣。

發行商 (Issuer)：在地氣網絡成為多幣系統

哈耶克在他的晚年著作 “貨幣的非國家化” 闡述的理論有助於解釋為什麼數字貨幣的發明有重要價值。他的主要論點在於，通過允許私人企業發行貨幣，公開市場競爭將導致最有競爭力的貨幣出現。呼應哈耶克的理論，地氣網絡中也支持多種貨幣共存，每種貨幣皆對應一個擁有鑄幣憑證的發行商，而鑄幣憑

證需要透過聯盟成員的授權。在地氣網絡，新貨幣發行必須滿足兩個條件之一：（1）已驗證的購買力，亦即該貨幣發行商必須將該貨幣對應到其擁有或直接相關的電子商務系統使用，或（2）該貨幣有一個預先指定的鑄幣計劃和分配政策。在前者條件下，發行商僅僅是將現有存在中央數據庫的虛擬貨幣轉移到地氣網絡中發行。地氣網絡中的貨幣價值取決於發行商和聯盟成員的信用。透過聯盟成員的授權，發行商可以提供多種貨幣，並負責其鑄幣時程和分配政策。

鑄幣(*mint*)：發行商可以使用鑄幣功能。在地氣網絡中，可透過鑄幣功能產生新的貨幣。每個貨幣發行商皆可透過此鑄幣功能，發行極大上限的該種貨幣。

激活會員功能：地氣網絡允許發行商限制特定成員才能使用其貨幣。

完整節點 (Full Node)

一個完整節點在地氣網絡中同步所有區塊鏈資料，但沒有鑄幣或建造區塊鏈的功能。換句話說，發行商是一個擁有鑄幣憑證的完整節點，而聯盟成員是一個可以參與建造區塊鏈的完整節點。

地氣行動錢包 (DiQi Mobile Wallet)

錢包是一個區塊鏈地址的集合，存儲交易必要資訊。每個完整節點都有一個錢包。然而相對於發行商和聯盟成員的完整節點，“地氣行動錢包”是一個

輕量錢包，為使用行動裝置的終端用戶所設計。地氣移動錢包為一個簡化支付認證(Simplified Payment Verification, SPV)的錢包， 允許使用者不用下載整份的區塊鏈， 只下載跟自己相關的交易，只做簡易的支付認證， 降低對行動裝置的負擔。

地氣輔助套件

地氣的營運支援系統（OSS）是一個強大且有效率的用戶介面，為聯盟成員與發行商所設計。配合地氣區塊鏈探勘器（DiQi Blockchain Explorer, DBE），它可以讀取地氣區塊鏈並且用於監測，控制，分析和管理的地氣 blockchain 及其相關操作。

表 1. 不同角色在地氣網絡中的功能比較

	聯盟成員	發行商	完整節點	地氣行動錢包
挖礦	O	X	X	X
鑄幣	O	O	X	X
區塊鏈	完整區塊鏈	完整區塊鏈	完整區塊鏈	部分區塊鏈
錢包	O	O	O	輕量錢包
激活會員	O	O	X	X
OSS 介面	O	O	X	X
區塊鏈探勘器	選擇性	選擇性	選擇性	X

應用

電子商務市場的代幣系統

地氣網絡適合做為電子商務系統的代幣平台。電子商務運營商可以在地氣網絡發行自己的代幣，其相關交易皆不需要信用第三方的存在。在線商城和電子商務系統的運營商通常會採取會員制的結構，而運營商對其會員的權利義務皆有明確的服務條款。對應會員系統的需求，地氣網絡是一個許可制區塊鏈，它原生支持各種貨幣只允許會員交易。因此地氣貨幣的發行商可以在區塊鏈上標明使用者的會員身分，非會員將無法接收或使用該貨幣。

飛行常客獎勵計劃

地氣網絡支援只允許會員交易的特性，也可以應用在以點數為基礎的顧客忠誠計劃。採用地氣協議，發行商可以限制其忠誠點數只給其指定的成員使用。配合多重簽章的功能，地氣系統也支援多個單位聯名發行貨幣。商業實體之間的安全和信任問題可以通過分散式的區塊鏈系統解決。在地氣的網絡，一個新的貨幣可以由多個發行商聯合鑄幣，使用多重簽章，整個過程是由多位發行商共同簽署的鑄幣動作。各個航空公司之間可以在沒有實體化航空聯盟存在的情況下應用地氣系統進行飛行常客獎勵計劃。無論是聯合發行飛行里程點數或者各自發行，分散式區塊鏈解決方案和現有解決方案之間的主要區別是信用成本。

因為在地氣網絡的貨幣流通對各發行商是公開透明的，發行商可以很容易確認其他發行商沒有過度鑄幣。

分散式眾籌平台

眾籌（Crowdfunding）是一種透過團購與預售的方式，向投資者募集資金的模式。傳統眾籌平台作為可信任第三方，促成眾籌活動。傳統眾籌平台的模式為先將資金轉到眾籌平台賬戶，若資金達到目標數量時平台將資金轉到發起人賬戶，或者資金沒有達到目標數量時平台將資金返還給投資。投資者回報通常是預購產品或服務的權利。基於區塊鏈技術的眾籌則免除信任第三方的需求。地氣平台允許新創公司成為地氣貨幣發行商，透過將產品使用權綁定在區塊鏈的代幣上，新創公司發行商可向早期投資人發行代表產品使用權的代幣以籌集資金。

分散式私募股權平台

基於區塊鏈技術，地氣可以提供電子股權憑證的私募股權解決方案。有融資需求的新創公司成為地氣網路發行商，並發行其電子股權憑證作為募資媒介。作為新一代的智能資產交易平台，地氣能夠讓融資企業獲得更多的控制權，並且投資者也可以隨時買賣持有的份額。在地氣平台上進行融資的公司，將會讓出一部分股權並且轉讓給代持公司，這些轉讓的股權將可以在分散式的地氣平台上發行相應的電子股權憑證。與傳統私募股權平台不同的是，投資者獲得的

電子股權憑證建立在區塊鏈技術之上，所以能在任何時間與其他投資者進行交易而不需要任何中間商。並且投資者可以根據自己的需要任意拆分股權成很小的份額，以提高資產流動性。

去中心化的交易所

地氣網絡內建多貨幣系統，也支援分散式交易所。在這種去中心化的交易所裡不需要有信任第三方作為管理者，所有交易資料都寫在區塊鏈上，免除數據庫受到竄改或偽造的可能，因此所有買單、賣單都是公平公正且真實的。另一方面，地氣系統對於區塊鏈做了特定優化，內建分散式的電子搓合機制，並且支持交易所運營需要的高頻交易。

區塊鏈上的電子憑證與智慧財產

地氣網絡可以把智慧財產授權的唯一性、防偽造、不可分割性與區塊鏈對應起來，建立智慧財產權電子憑證。特定智慧財產可以拆成數個具有電子產權的代幣，並在地氣平台上發行，這些交易信息將會被寫入地氣區塊鏈，這些電子產權將可以在地氣平台即時交易，而持有人的權利將被挖礦機制算力所保護。當目標智慧財產增值後，該電子產權的持有人也可以在地氣平台中賣出手中的代幣獲利。

總結

從長遠來看，分散式帳本技術可能成為新一代數據存儲與交易平台的產業標準。現今的加密貨幣如比特幣等皆會激發更多相關區塊鏈技術創新，而目前主流加密貨幣未來也可能被擁有更高交易頻率與延展性的區塊鏈技術所取代。透過優化區塊鏈功能以更好地適應實際商業需求，我們相信地氣是新一代的分散式智能資產交易平台，將垂直結合既有電子商務與金融市場。