



G G E

白皮書

WHITE PAPER

前 言

區塊鏈技術讓我們看到了數字經濟時代巨變的曙光。

在互聯網近 50 年的歷史中，曾發生過兩次巨變。第一次巨變是全球性的聯網，自 1969 年阿帕網誕生以來，全世界主流國家陸續開始接入互聯網，開啟全球聯網的征程。第二次巨變是全球性的應用，自 1989 年萬維網論文問世後，互聯網應用開始全面開花。

如今，互聯網的第三次巨變已見“雛形”。

2009 年比特幣的誕生是第三次巨變的標誌性事件。在區塊鏈技術的支持下，比特幣解決了傳統紙幣“無跡可循”的問題。實體紙幣的流通，是不可見的，沒有人可以準確的告訴我們這一張紙幣從哪里來的又到哪里去。而區塊鏈則可以讓數字貨幣的每一筆流動都“有跡可循”。

而區塊鏈的意義，不只在於讓數字貨幣“有跡可循”，而是可以構建一個更加可靠、安全、穩定的互聯網系統。從根本上杜絕數據交換、轉移等過程中可能存在的欺詐現象。區塊鏈技術的普及，將為我們打造一個更公正、透明的數據體系。2018 年，區塊鏈及相關行業、應用將會更加快速的發展，全球逐步進入“區塊鏈經濟時代”。在全國乃至全球範圍內，將會出現更多更成熟的區塊鏈應用。

目 錄

1 項目背景.....	1
1.1 區塊鏈是繼 IT、互聯網後的新技術	1
1.2 區塊鏈發展的瓶頸	2
1.3 區塊鏈發展的前景	3
1.4 公有鏈 AurumOx Protocol 的價值基礎.....	4
1.5 穩定幣的市場需求	5
2 黃金市場與痛點.....	6
2.1 區塊鏈方面問題.....	7
2.2 黃金行業的巨大痛點	8
3 黃金的價值與商業化	10
3.1 黃金的價值傳遞.....	10
3.2 黃金的原創性證明	10
3.3 黃金的產權交換憑證	10
3.4 黃金的防偽確定.....	11
3.5 黃金的投資.....	11
3.6 黃金的完整性證明	11
4 AurumOx Protocol 項目.....	12
4.1 AurumOx Protocol 項目簡介	12
4.2 AurumOx Protocol 項目願景	12
4.3 AurumOx Protocol 項目設計理念	14
4.4 AurumOx Protocol 項目技術架構	14
5 AurumOx Protocol 技術架構安全與網路的安全防護.....	24
5.1 區塊鏈本身具備的安全優勢	24
5.2 AurumOx Protocol 安全防護	25

目 錄

6 AurumOx Protocol 的優勢與應用	26
6.1 AurumOx Protocol 的優勢.....	26
6.2 AurumOx Protocol 的應用.....	30
6.3 AurumOx Protocol 的多元應用場景	34
7 GGE 代幣分配及戰略規劃	36
7.1 GGEC 代幣計劃.....	36
7.2 AurumOx Protocol 代幣分配	37
7.2 戰略規劃	39
8 GGE 核心團隊與資本方	39
8.1 GGE 核心團隊.....	39
8.2 GGE 資本方	41
免責申明	42
風險提示	43



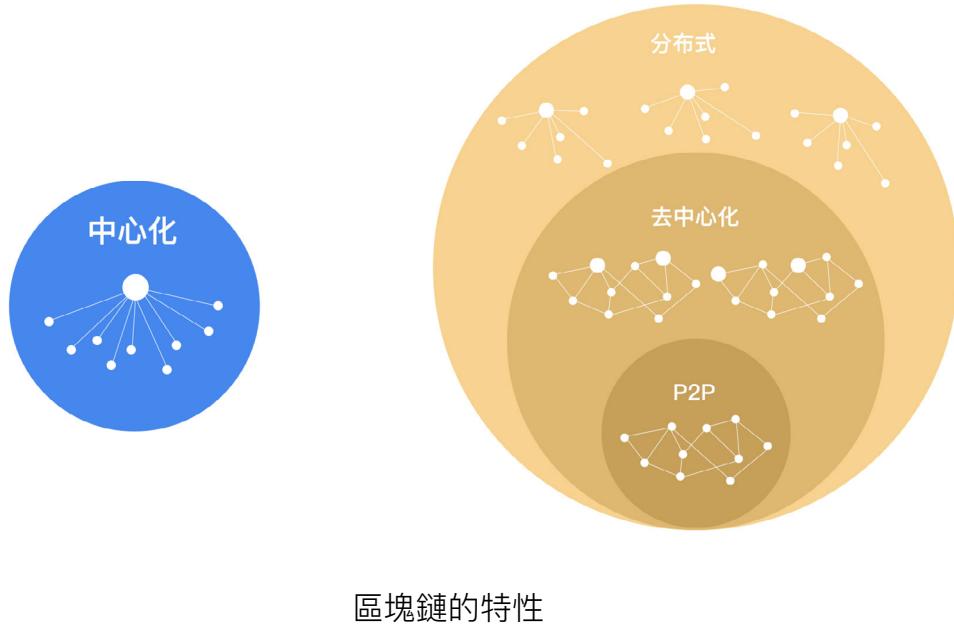
1 項目背景

1.1 區塊鏈是繼 IT、互聯網後的新技術

自互聯網誕生以來，人類社會的資訊傳播成本得到極大的降低，資訊傳播效率的飛躍帶來生產力的極大解放。然而現在的互聯網也存在固有的缺陷，它更關心的是資訊的送達，而不太關心資訊的所有權，出現了“數據裸奔”“資訊無主”等問題。而有些資訊具有很強的價值屬性，比如匯款轉賬資訊，這些有價值資訊的傳遞需要依賴第三方來“保駕護航”。因此，目前資訊的價值傳輸成本依然高企。

區塊鏈的誕生，帶來瞭解決這個問題的曙光。由於區塊鏈公開透明、難以篡改、不依賴仲介機構的特點，區塊鏈可以實現安全、高效、低成本的價值傳輸。人們有望基於區塊鏈建成價值傳輸的互聯網。在價值互聯網中，價值傳輸成本將極大降低，生產力將又一次獲得極大解放。區塊鏈獨特的優勢，如數據的確權使用、價值的高效傳輸，可以廣泛應用於很多行業，比如金融服務、合同契約、慈善公益、物聯網等，區塊鏈將在未來改變很多行業的面貌。因此，區塊鏈絕非無足輕重的領域，而是國際上的兵家必爭之地。就像 Android 系統的出現構架了基本的綱領準則。而古往今來可見一斑，區塊鏈就好比一個底層的技術構架得以被認知。而接下來則開始走入到應用的階段。“去中心化”是區塊鏈的核心構架。“公平、公開、公正”是區塊鏈的靈魂。

核心技術是國之重器。區塊鏈被認為是繼互聯網之後的下一個 IT 浪潮，眼下，區塊鏈應用在全球範圍內正呈現從星火燎原向火爆方向加速發展的勢頭。



區塊鏈的特性

1.2 區塊鏈發展的瓶頸

區塊鏈已經發展至 3.0 階段，具備支持大規模商業應用的可能，但數據處理能力有限，無法滿足高頻次、大規模應用需要。也就是說底層技術帶來的限制，阻礙了上層應用的正常發揮，雖然有美好暢想，實現起來還需要很長時間。具體來講，究其根本，區塊鏈現存的問題是吞吐量和交易確權速度的問題。

為了解決這一問題，區塊鏈行業在進行以下嘗試：其一是大區塊，即提升每一個區塊的儲存空間，此方法在比特幣中曾有過試用，比特幣一個區塊大小僅有 1MB 儲存空間，在 2017 年年底時 SegWit2x 將區塊大小從 1MB 提升至 2MB，但出於安全考慮，最終取消 SegWit2x 硬分叉；其二是鏈下交易，即在主鏈外加入閃電網路或者側鏈，此方法以太坊在嘗試，提前支付一些以太坊或比特幣作為押金，之後在鏈下通過其他方法來跟其他人進行交易；其三是代理人共識協議，即多人成為超級節點，形成小團體。EOS 在嘗試用這種“議會制”共識產生區塊，再將區塊廣播給整個網路，從而達成整個網路的共識。



然而這三種嘗試方式都不能完美解決區塊鏈的交易速度，去中心化和安全性的矛盾。AurumOx Protocol 公有鏈正是致力於打造一個可拓展、可相容的區塊鏈底層構架，真正突破行業瓶頸，實現區塊鏈技術商業價值。

1.3 區塊鏈發展的前景

區塊鏈技術被認為是繼蒸汽機、電力、互聯網之後的顛覆性創新。如果說蒸汽機和電力解放了生產力，互聯網改變了資訊傳遞的方式，那麼區塊鏈作為構造信任的機器，將可能改變價值傳遞方式。

例如在金融領域，金融機構特別是跨境金融機構間的對賬、清算、結算的成本一直很高，還有複雜的手工流程，而區塊鏈技術具有數據不可篡改和可追溯性，其應用有助於降低金融機構間的對賬成本及爭議解決的成本，能顯著提高支付業務的處理速度及效率，還使小額跨境支付成為可能。2017年12月，招商銀行完成從香港永隆銀行向永隆銀行深圳分行的人民幣頭寸調撥業務。這是全球首筆基於區塊鏈技術的同業間跨境人民幣清算業務。

區塊鏈技術解決了數字經濟時代的兩大問題：一是流向可見，二是零信任成本。在過去，實體紙幣的流通是看不見的，但所有數位化資產的流向都有“鏈”可查。中國社科院知識產權中心研究員楊延超也認為，區塊鏈的最大優勢是真正完成了一個匿名社會下的信用構建，給諸多領域帶來新的機遇，因此就使各種創新應用成為可能。目前，區塊鏈的應用已延伸到醫療健康、教育、慈善公益、社會管理等多個領域。拿文化產業來看，複製成本低、維權成本高、舉證困難等使得知識產權保護一直是行業痛點。有了區塊鏈，文化產品的生產、傳播、交易等記錄真實透明、可信可查，問題迎刃而解，總的來說，區塊鏈在發展的前景上面是非常有潛力的。



1.4 公有鏈 AurumOx Protocol 的價值基礎

經過上千年的演化，全世界對於貨幣的共識逐漸統一到黃金和白銀身上。因為金銀滿足這樣一些特徵：體積小，稀缺性高，價值大，容易分割，品質均勻，化學性質穩定，不會腐爛變質，便於攜帶，難以偽造等。因此，世界各地的人們，不論文化、種族、宗教、政體上有多大差異，都一直接受黃金和白銀為公認的硬通貨，正所謂“金銀天然是貨幣，貨幣天然不是金銀”（語出馬克思《資本論》）。從阿拉伯到印加帝國，從古羅馬到我國商周朝，幾乎所有文化的諺語和傳說中都離不開金銀的記載，黃金代表著財富、權利、幸運和永恆。

AurumOx Protocol 應用區塊鏈技術將實物黃金數位化，將區塊鏈技術的特性用在黃金生產、加工、交易整個產業鏈中，搭建黃金數字生態鏈，在特徵上更優於黃金，將黃金的流動性完美地釋放出來。

AurumOx Protocol 運用區塊鏈技術來實現現有黃金系統無法實現的以資產對標、黃金流通為導向的公鏈平臺。也就是通過建立一個公共的黃金流通的公鏈系統，滿足黃金的資訊可靠、透明性和安全性等所有的要求，實現可靠的資產安全交換，不限地域、國界、時間。平臺還提供的 API 和 SDK 便於各種應用程式和服務可以輕松訪問平臺上的數據資訊，並以此進行新服務的開發。

AurumOx Protocol 發行名為“GGEC”的黃金資產通證 (Token)，實現與實物黃金品質 100:1 的絕對錨定，遵循合規合法的原則為消費者、投資者提供有實物資產絕對錨定的數字通證 (Token)，並借助區塊鏈技術實現的實物黃金的數位化應用，形成全球流通聯盟機制，並通過數位化通證 (Token) 的流通來構建一個以實物黃金為交易基礎的創新應用生態系統。同時發行名為“AO”的公鏈燃料通證 (Token)，用於實現對 AurumOx Protocol 的公鏈系統網路使用時的資源控制，AurumOx Protocol 對通證 (Token) 轉賬、智能合約的運行和存儲進行收取 GAS 費，從而實現對記賬人的經濟激勵以及防止資源濫用。同時，AO 用於實現對 AurumOx Protocol 的公鏈系統網路的管理權。



1.5 穩定幣的市場需求

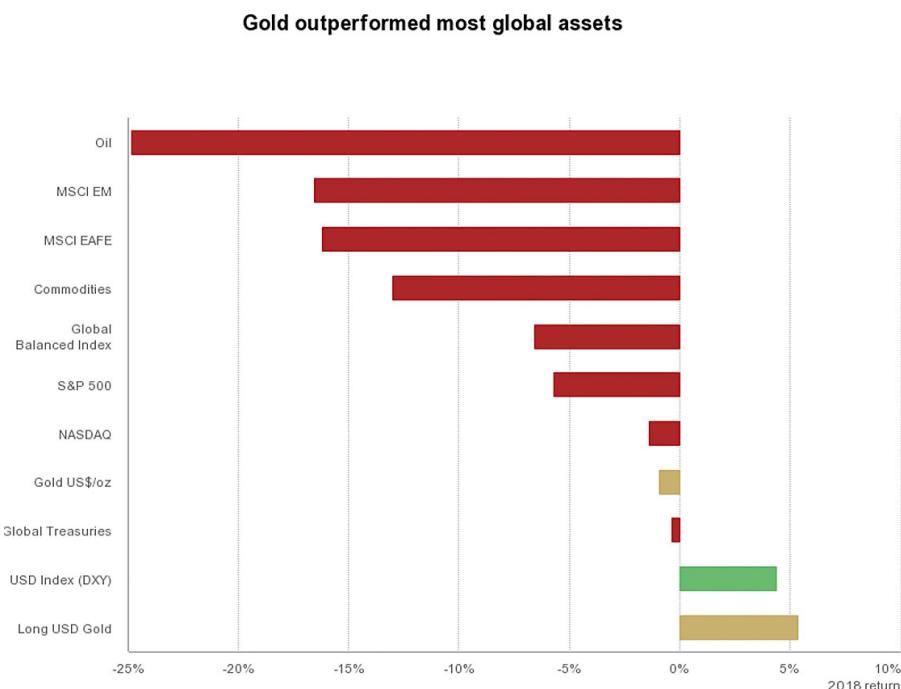
- 個人投資者進入虛擬貨幣市場需要首先將手中的法幣兌換成虛擬數字貨幣，而目前很多交易所都不支持法幣直接兌換數字貨幣，需要一個穩定的數字貨幣作為兌換的中間件。
- 機構投資者需要進行頭寸管理。隨著加密貨幣投資市場的發展，投資機構和資產管理機構也會越來越專業，他們會將加密貨幣作為他們資產頭寸中的一種，使用各種策略來進行套利和風險對沖，但非穩定幣價格波動過於劇烈，難以進行掛你，因此對穩定幣的需求也會越來越高。
- 用數字貨幣作為收入形式或融資方式的企業或組織，後續需要將數字貨幣兌換成穩定幣來控制風險或應付審計合規要求。目前很多區塊鏈公司的收入都是數字貨幣形式，未來要上市的話必須使用可審計資產。
- 要求價格波動平緩的區塊鏈應用，如消費者貸款，或是標的物為未來事項的預測 / 博彩應用等。這類應用也很難直接以比特幣或以太坊來對遠期的事項定價，因此需要穩定幣。
- 未來隨著加密數字貨幣的普及，普通民眾會更多持有加密數字貨幣，如果數字貨幣的價格波動過於劇烈，則會對普通民眾造成損失，財富縮水，不利於加密數字貨幣的普及。



2 黃金市場與痛點

作為獨立的貴金屬資源，同時也是稅務負擔最輕的投資項目，不少投資者選擇投資配置金幣、金條等實物黃金以對抗通脹，規避風險。

2018 年黃金價格隨著投資者興趣的增減而跌宕起伏。過去兩年埋下的風險種子以及在 2018 年後期出現的風險預計將會延續下去。再加上一系列的趨勢發展，將成為決定黃金需求的關鍵。展望未來，預計 2019 年市場風險與經濟增長之間的相互作用將推動黃金需求，黃金在投資組合中將扮演越來越重要的角色。



黃金表現優於大多數全球資產

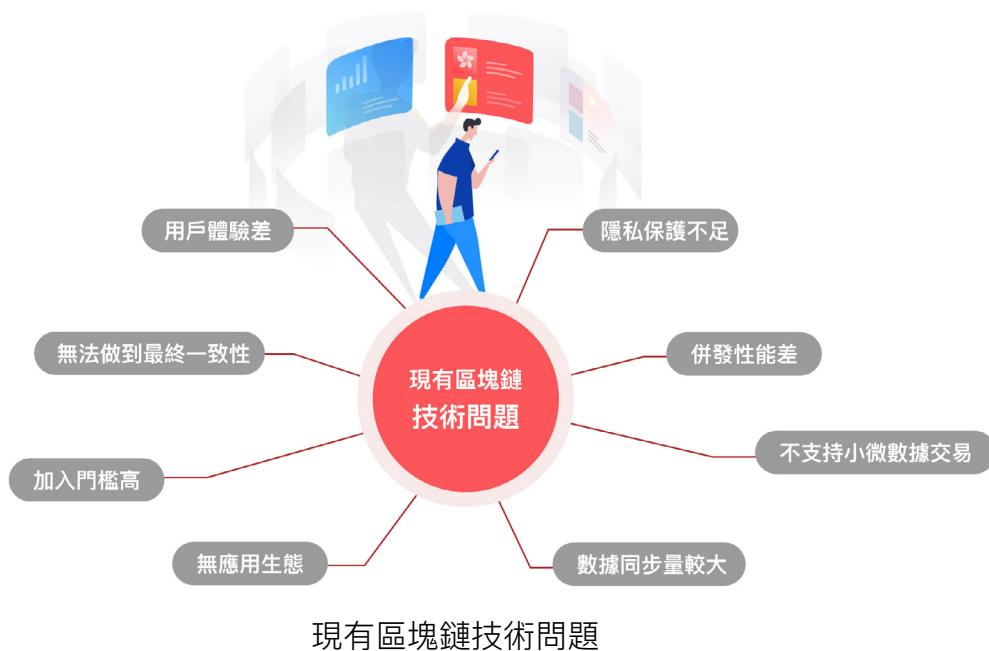
資料來源：世界黃金協會 (WGC)



2.1 區塊鏈方面問題

2.11 現有的區塊鏈技術

自互聯網誕生以來，人類社會的資訊傳播成本得到極大的降低，資訊傳播效率的飛躍帶來生產力的極大解放。然而現在的互聯網也存在固有的缺陷，它更關心的是資訊的送達，而不太關心資訊的所有權，出現了“數據裸奔”“資訊無主”等問題。而有些資訊具有很強的價值屬性，比如匯款轉賬資訊，這些有價值資訊的傳遞需要依賴第三方來“保駕護航”。因此，目前資訊的價值傳輸成本依然



2.12 以太坊、比特幣價格波動較大

以太坊 (ETH)、比特幣 (BTC) 作為獨立的、開源的區塊鏈技術，都具有極高的市場價值，但是因為去中心化的特性，不倚賴任何政府與機構發行，以太坊與比特幣的價格隨著市場需求的增加而加高，隨著市場需求的縮水而跌落，漲跌並沒有一定規律，存在極高的風險性。投資者除了自己持有的數字憑證，也需要有足夠良好的心態去承擔一切相關的損失，很難憑藉其他依據做投資上的判斷和把控。



2.1 3USDT 的存在有必然性，但同時面臨的風險

USDT 是與法幣相錨定的數字加密憑證，它的出現補充了 BTC 與 ETH 紋勢，因為與美元錨定價值，相對而言在價格浮動方面降低了這種不穩定性，但因為平臺的限制 (USDT 只能通過美國 Tether 公司兌換) 造成了兌換不便捷，在全球化 的流通性上存在明顯壁壘，而當前以美元為主導的國際金融環境下，在機制上存在“特裏芬 悖論”——美國 2008 年曾通過美元的主導地位向國際轉嫁其金融 危機，不但嚴重衝擊全球金融市場，部分地區、國家更因此爆發金融危機乃至經濟危機，它是定時炸彈。

GGEC	與黃金錨定，穩定易掌握
USDT	與美元錨定、由美國 TETHER 公司掌握
ETH	隨市場行情波動、難把握
BTC	隨市場行情波動、難把握
AO	實際資產價值的數字通證

GEEC 與黃金錨定，穩定易掌握

2.2 黃金行業的巨大痛點

自黃金行業傳統的銷售方式裏，門店市場集中度低，造成資產端獲客效率低、成本高。另一方面，傳統黃金因流動性較差、投資便利性不足及兌換管道不暢等條件制約，很難對普通國民進行覆蓋，還有傳統的黃金產品或多或少都存在著變現困難、投資門檻高、交易繁瑣、買賣存有價差、無法與金價即時掛鉤等種種局限性。



行情透明隨時查閱



黃金行業的痛點圖解

2.21 交易不透明

無論是市面上搶購實物黃金，還是投資者們依據銀行報價在交易平臺上購買“紙黃金”，大家更多將黃金作為一個資產儲備或者投資理財產品，而不是將它作為一種支付方式；主要原因在於實物黃金不好分割，攜帶不便，紙黃金實際上買賣的是虛擬黃金，定價不透明和對賬不清也一直是困擾黃金交易的難題。

2.22 流通效率低，保管費高

人民幣屬於流通紙幣，黃金和白銀屬於全球流通的金融產品，而黃金在全球又是公認的避險保值的產品，但黃金的貴重屬性單價高，貨品周轉慢，資金沉澱大行業短板在新時代的發展下顯得更加無力。黃金是貴金屬的一種，如何保存更安全，如何保養能讓其保值，對黃金投資者來說都是很頭疼的問題。銀行推出的黃金保管服務，如建行，每根金條每月收取 2 元保管費，保管成本較高。



同時，需要 提貨取 出時又增加了流通成本。還有地域性問題，造成交易流程繁瑣，成本較 高，流通效 率很低的局面。

3 黃金的價值與商業化

3.1 黃金的價值傳遞

黃金在出售的過程中，通過 GGEC 通證標定自己的價值 ($100\text{GGEC}=1\text{ 克黃金}$)。黃金的購買方可以通過購買 GGEC 的方式獲得黃金產品，獲取的同時即存在數字產權證明與黃金所有權證明，後續為黃金產品的價值轉移提供有效證據。

3.2 黃金的原創性證明

通過將黃金產品的公司資訊、產品資訊、內容資訊、生產時間資訊以及初始傳播資訊通過加密演算法換算和抽象，結合智能合約，形成數位化資訊，記錄在區塊鏈中，用於證明黃金的原創性。類似於著作權登記的方式，利用這些數字化資訊可以有效的證明黃金產品的原創性、獨特性及所有權。

3.3 黃金的產權交換憑證

作為針對非大眾市場的黃金產權轉移的應用領域，可以將黃金產品的公司信息、產品資訊、內容資訊、生產時間資訊、產權獲得者資訊依附於區塊鏈，進而完成黃金產權轉移。這種產權轉移具有唯一性，不可篡改或產生時間錯位，足以作為黃金產權轉移的憑證。



3.4 黃金的防偽確定

GGEC 具有不可篡改、透明可查詢的特點，一旦黃金產品的特徵標記和鏈標記以及生產時間標記進入區塊鏈，則不能進行更改。而特徵標記通過技術處理後是無法偽造的。當特徵標記與所謂偽創作者的證據無法對應或吻合時，則可以證明黃金產品的真偽。

3.5 黃金的投資

黃金作為投資標的物時，利用區塊鏈技術可以記錄黃金產品與投資分配的確定關係。黃金產品進行交易進而獲取的收益，投資人可以通過記錄在區塊鏈上產權投資證明來要求合理分配收益。

3.6 黃金的完整性證明

產品一旦最終確定後，可以將數字特徵記錄在區塊鏈上，進而提供完整性證明。一旦黃金產品的提供方並沒有將全部的數字產權轉移給資產購買方時，資產購買方可以通過區塊鏈上的數字特徵記錄來申訴自己的產權完整性權利。



4 AurumOx Protocol 項目

4.1 AurumOx Protocol 項目簡介

AurumOx Protocol 是一條基於 DDPOS 共識機制的公有鏈。我們致力於創建一個黃金買賣自由、價值支撐穩定、可追溯的流通環境。

AurumOx Protocol 的公有鏈系統，採用先進的區塊鏈技術，實現黃金的數位化、權證化。我們設定主網通證 (Token) 為 GGEC(GlobalGoldenExchangeCoin 黃金資產數位化加密權證)，與黃金進行永恆錨定 ($100\text{GGEC}=1\text{g 黃金}$)，GGEC 是將發佈在 AurumOx Protocol 的第一個重要資產通證 Token。

我們引入了智能合約機制，實現資產的可數位化編程。其中需要消耗的 gas 燃料為 AO。AurumOx Protocol 區塊鏈系統中將提供一個以錨定實物黃金為依託的穩定金融底層系統——GGEC，平行區別於現有以太坊 (ETH) 等公鏈系統；同時 AurumOx Protocol 系統中的 GGEC 區別於傳統的紙黃金等，具有真實資產所有權價值，並為實物黃金充分釋放了其流通屬性，實現了黃金價值可數位化編程和高速流通，讓黃金資產在區塊鏈數字世界中作為基礎的、有實際資產價值的數字通證 (Token) 廣泛流通。AurumOx Protocol 遵循成熟的六層技術架構，自下而上分別為：數據層、網路層、共識層、激勵層、合約層和應用層。

4.2 AurumOx Protocol 項目願景

針對當前區塊鏈行業的挑戰，AurumOx Protocol 在區塊鏈技術和理念上進行了一系列的創新：包括基於拜占庭共識機制和 DDPOS 共識機制相結合的共識機制，區塊鏈主控合約的理念和實現，去中心化錢包的應用，交易帳本和智能合約帳本的分離等，使得 AurumOx Protocol 成為區塊鏈世界與現實商業世界的橋樑。



AurumOx Protocol 的願景首先是構建未來全球商業區塊鏈基礎設置，無論是機構用戶還是個人用戶都能很方便的在 AurumOx Protocol 上搭建自己的智能合約、區塊鏈應用、甚至另一個區塊鏈。

- **AurumOx Protocol 支持百萬級用戶**

如 Ebay, Uber, AirBnB 和 Facebook 這樣的應用，需要能夠處理數千萬日活躍用戶的區塊鏈技術。在某些情況下，應用程式可能無法正常工作，除非達到了大量用戶，因此可以處理大量用戶數量的平臺至關重要。

- **AurumOx Protocol 免費使用**

有時候應用開發人員需要靈活的為用戶提供免費服務，用戶不必為了使用平臺而付出費用。可以免費使用的平臺自然可能會得到更多的關注，有了足夠的用戶規模，開發者和企業可以創建對應的盈利模式。

- **輕鬆升級和故障修復**

基於 AurumOx Protocol 的應用程式在進行功能迭代的時候自然需要能支持軟體升級。所有軟體都有可能受到 bug 的影響，一個區塊鏈底層平臺在遭遇 bug 的時候，需要能夠從 bug 中修復錯誤。

- **低延遲**

及時的回饋是良好用戶體驗的基礎。延遲時間如果超過了幾秒鐘，會大大影響用戶體驗，嚴重降低程式的競爭力。

- **串行性能**

有些應用程式由於命令執行必須是順序的，從而無法用並行演算法進行實現。諸如交易所之類的應用經常需要處理大量的串行操作，因此一個成功的區塊鏈架構需要具有強大的串行性能。



- **並行性能**

大規模應用程式需要在多個 CPU 和電腦之間劃分工作負載，AurumOx Protocol 可實現多端並行功能。

4.3 AurumOx Protocol 項目設計理念

AurumOx Protocol 是一種全新的區塊鏈體系架構，定位為易用的高性能區塊鏈平臺，旨在實現 分佈式應用的性能擴展，以滿足現實世界的真實商業需求。這是通過創建一個可以構建應用程式的類似操作系統的架構來實現的。該體系架構提供帳戶、身份與授權管理、策略管理、資料庫、非同步通信以及在數以千計的 CPU、FPGA 或群集上的程式調度。該區塊鏈為一個全新的體系架構，通過低延時高併發硬體加速技術，可實現每秒數百萬個交易，且達到秒級確認。

以太坊在一定程度上實現了基於電腦應用方面的基礎設置，但是層次還是很低，特別是其智能合約只能根據鏈上其他帳戶的狀態或其他智能合約的狀態來觸發，並且以太坊的智能合約會在所有的節點上都運行一次，極大的浪費了算力。

但 AurumOx Protocol 團隊設計的模型使得鏈上鏈下能夠打通，應用通過設置一系列的可信數據源，在現實中的特定事件發生後即可啟動鏈上的智能合約和智能應用。應用通過設置閾值，可以指定智能合約僅在少量節點上執行，極大的節省了全網算力，也可以指定少量節點進行主要數據的傳輸和存儲，這就使得大數據分析以及人工智慧運算在區塊鏈應用成為可能。

4.4 AurumOx Protocol 項目技術架構

- **協議層**

所謂的協議層，就是指區塊鏈最底層的技術。這個層次通常是一個完整的



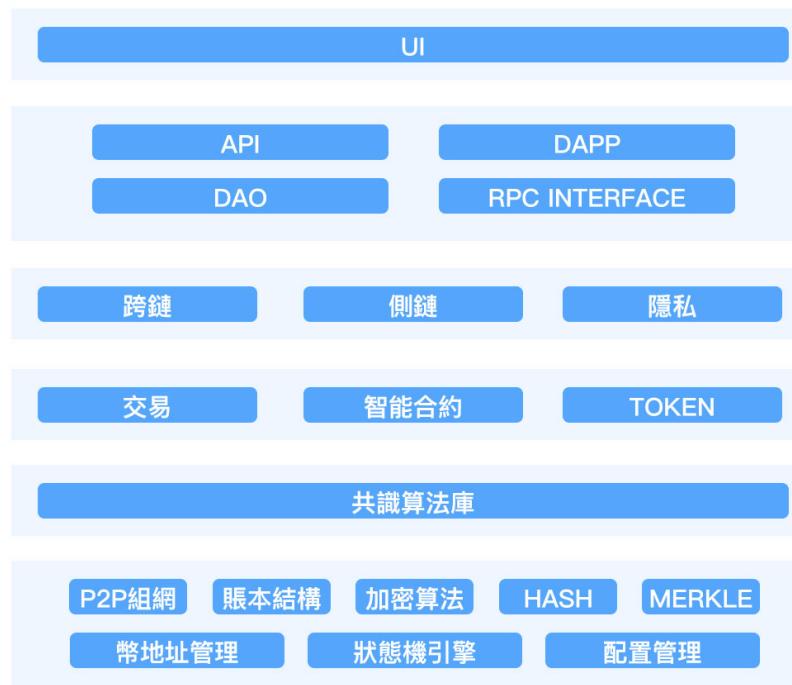
區塊鏈產品，它維護著網路節點，僅提供 API 供調用。通常官方會提供簡單的客戶端（通稱為錢包），這個客戶端錢包只能建立地址、驗證簽名、轉賬支付、查看餘額等。這個層次是一切的基礎，構建了網路環境、搭建了交易通道、制定了節點獎勵規則。從技術來說，協議層主要包括網路編程、分佈式演算法、加密簽名、數據存儲技術等 4 個方面，其中網路編程能力是選擇編程語言的主要考慮因素，因為分佈式演算法基本上屬於業務邏輯上的實現，什麼語言都可以做到，加密簽名技術是直接簡單的使用，資料庫技術也主要在使用層面，只有點對點網路的實現和併發處理才是開發的難點。分佈式演算法、加密簽名等都要在實現點對點網路的過程中加以使用。

• 擴展層

擴展層是為了讓區塊鏈產品更加實用。智能合約就是“可編程合約”，或者叫做“合約智能化”，其中的“智能”是執行上的智能，也就是說達到某個條件，合約自動執行，比如自動轉移證券、自動付款等。擴展層使用的技術基本沒有限制，分佈式存儲、機器學習、VR、物聯網、大數據等等，都可以使用。編程語言的選擇上，可以更加自由，因為可以與協議層完全分離，編程語言也可以與協議層使用的開發語言不相同。在開發上，除了在交易時與協議層進行交互之外，其他時候儘量不要與協議層的開發混在一起。這個層面與應用層更加接近，也可以理解為 B/S 架構的產品中的服務端（Server）。這樣不僅在架構設計上更加科學，讓區塊鏈數據更小，網路更獨立，同時也可以保證擴展層開發不受約束。

• 應用層

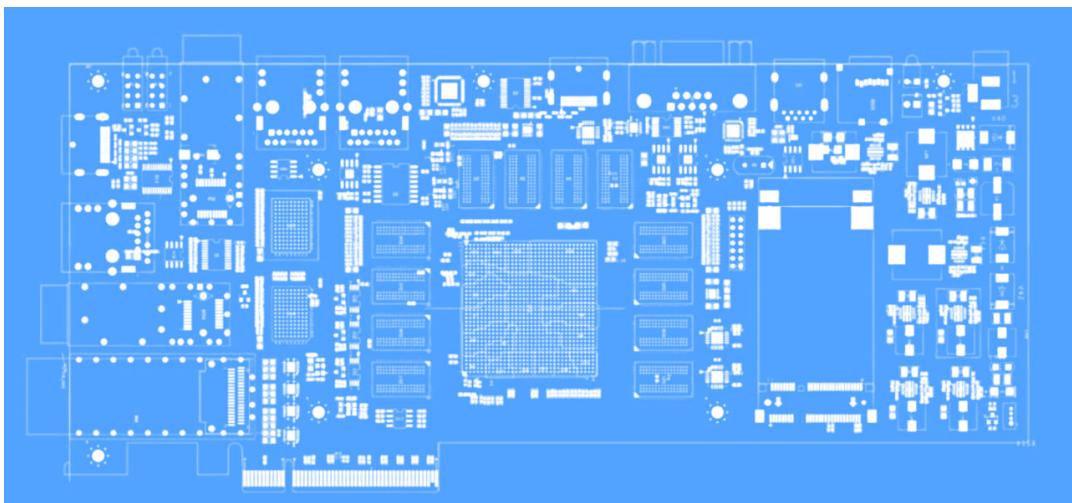
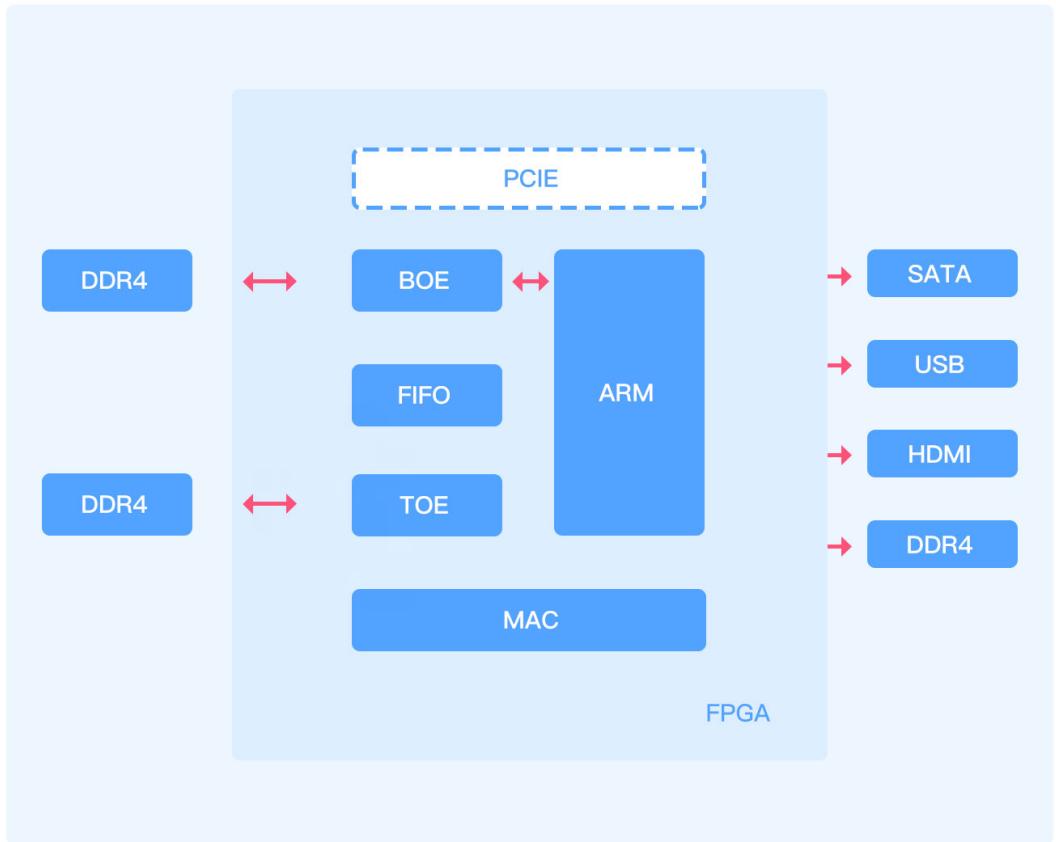
應用層是普通人可以真正直接使用的產品，也可以理解為 B/S 架構的產品中的流覽器端（Browser）。這個層面可以讓區塊鏈技術快速走進尋常百姓，服務於大眾。大家使用的各類輕錢包（客戶端），應該算作應用層最簡單、最典型的應用。編程實現：C++、Javascript、Python、Go 等



AurumOx Protocol 整體架構

4.4.1 創新的 BOE 技術

傳統區塊鏈的節點，交易廣播、交易驗證、區塊廣播、區塊生成等功能均基於軟體層面來實現，每個節點之間的數據連接均是串行處理，導致了網路拓撲結構複雜、延遲時間長、串行處理性能低等問題，用戶體驗較差。針對以上問題，AurumOx Protocol 創新性的設計了 BOE 技術，即 Blockchain Offload Engine，區塊鏈卸載引擎，該引擎是一個異構處理系統，包括 BOE 硬體、BOE 固件，以及與之匹配的體系軟體，該異構處理系統通過結合 CPU 串行能力和 FPGA/ASIC 晶片的並行處理能力，實現高性能和高併發計算加速。



BOE 版圖 & 邏輯框圖

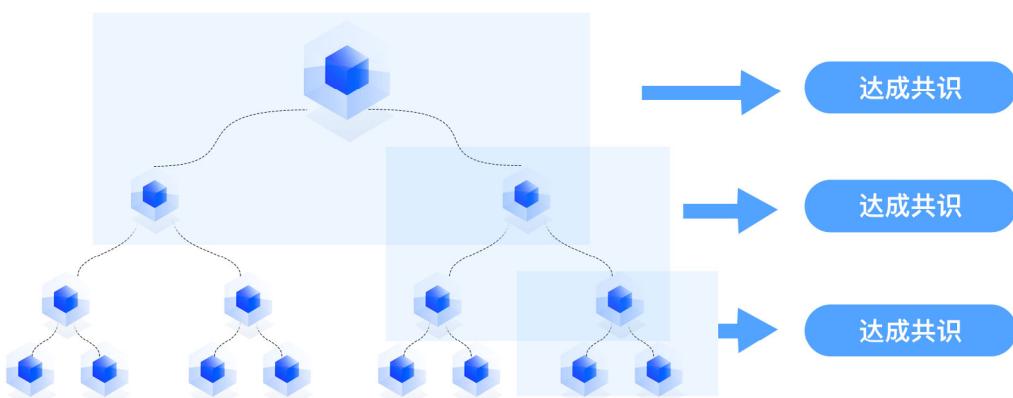
BOE 設備通過千兆 / 萬兆以太網介面連接 P2P 網路中其他設備，MAC 模組處理以太網數據報文，並與 TOE 模組進行數據交互。BOE 模組實現對 TCP 報文和 UDP 報文的解析，處理過程無需 CPU 參與以節約 CPU 資源佔用。BOE 模組負責通過 TOE 模組與其它節點建立加密通信通道，對收到的交易、區塊等



消息進行完整性檢查、簽名驗證、帳戶餘額校驗，對過大的待發送區塊數據進行分片處理並對各分片進行封裝以保證接收數據的完整性，並根據各條 TCP 連接的接收流量進行統計，以便能夠按照對系統的貢獻進行相應的激勵，從而吸引更多的用戶參與維護網路的運行。

4.4.2 共識機制

AurumOx Protocol 中的共識機制被設計成模組化的，可以類似插件一樣實現插拔，可以適用公鏈和私鏈的不同應用場景。在 AurumOx Protocol 的共識機制的選取中，根據技術的可靠性原則和去中心化原則，我們最終選取 ProofofStake 為基礎的共識機制作為公鏈的基礎共識機制。在基於 AurumOx Protocol 的公有鏈中，我們採用 ProofofTime 和 Raft 協議結合的共識機制，為行業客戶提供服務。從 POW 到 POS 到 DDPOS。共識機制的本質在於在一個分佈式系統中如何通過一些演算法，最後取得數據的一致性。關於共識機制的討論最後都會回歸到電腦領域的分佈式系統的一致性問題，之前這個領域已經有很多的研究和成果，例如分佈式系統中的 FLP 定理和 CAP 定理指導人們如何根據具體的需求來設計共識機制。



AurumOx Protocol 的共識機制



4.4.3 擴展 P2P 網路協議

可擴展性的提出，為了解決區塊鏈彼此不相容的資訊孤島問題。首先，我們認為升級、分叉是網絡進化的有效途徑之一，分叉後形成一個主鏈和若干子鏈。主鏈和子鏈從技術角度看完全對等，只是基於社區的共識給它們設置不同的標識。每一條子鏈可根據不同的商業應用做適度化定製，通過在子鏈之間構建 VEP，其工作方式類似於網關，子鏈之間通過 VEP 可交互資訊和交換價值。通過這樣的協作，可形成多應用的區塊鏈生態。不僅如此，非區塊鏈的線上數據也將納入 AurumOx Protocol 生態，輔以智能合約，可對現實世界中的事件做出回應。

4.4.4 多鏈並行機制

經典的區塊鏈網路，如比特幣網路、以太坊等都是採用單鏈結構，所有的事務和交易都是在一條鏈上進行。單鏈結構的優點是交易和共識流程比較簡單，在區塊鏈發展早期能夠很好地滿足用戶需求。但是隨著區塊鏈技術的發展和市場對區塊鏈的需求不斷增強，單鏈架構逐漸暴露出很多無法解決的痛點：整體吞吐量和性能存在瓶頸：比特幣只有 7TPS 以及需要 6 個區塊的確認機制，以太坊出塊間隔也需要 10–20 秒，這些都嚴重阻礙了日益增長的區塊鏈業務發展需求。

鏈內業務相互干擾：單鏈架構很容易由於個別業務的繁忙而造成整個系統擁堵，很多正常的交易都得不到及時處理和確認；封閉的網路結構：無法實現不同鏈之間的跨鏈交互，無法滿足多平臺之間的業務交互需求。為了克服單鏈結構的局限性，AurumOx Protocol 採取多鏈並行結構。

並行多主鏈機制：AurumOx Protocol 可以引出多條主鏈，每條主鏈負責專門的業務領域，相互獨立又相互關聯，主鏈之間耦合比較少，發揮並行處理的優勢，對過程性區塊，



引入封存策略，超期數據進行歷史歸檔，提升系統處理效率。多鏈並行解決不同業務、不同形態鏈的功能支持，同時提高性能；跨鏈共識實現數據審計和價值流通。由於現實世界的不同業務具有各種各樣的特殊性，如前所述單鏈結構是很難完美的支撐多種異構業務的。在 AurumOx Protocol 中，每一條鏈只服務於最小功能集合的業務，每個內聚型的業務運行在單獨的鏈，這樣既能做到有效的安全隔離，也能實現計算和資源的有效利用最大價值，不同鏈之間通過跨鏈協議進行交互，實現價值交換。

AurumOx Protocol 多鏈結構能滿足現實世界各種不同類型的複雜業務需求，不同類型不同特性的業務在不同的子鏈運行，比如計算密集型、IO 密集型、混合型分別在不同鏈上良好地運行；不同安全等級要求的業務也可以在不同層次運行，比領域，相互獨立又相互關聯，主鏈之間耦合比較少，發揮並行處理的優勢，對過程如針對銀行的業務需求，在數據的保密和安全以及事務的強一致性會有更高的要求，因此可以隔離在最安全的一層。

4.4.5 柔性跨鏈機制

AurumOx Protocol 通過一系列有針對性的協同智能合約，及非同步通訊、狀態機和哈希鎖定技術，實現一套通用的柔性跨鏈機制，打通各個區塊鏈系統的通信瓶頸，讓各種數字資產互聯互通，適當的跨鏈協同機制有效保證內部各條並行鏈之間，以及與其他公鏈之間的共識和價值的有效和可靠傳遞。

跨鏈技術包括兩個部分：一個是 AurumOx Protocol 與外部鏈的互聯互通，AurumOx Protocol 與其他鏈通過一個公共的智能合約來實現，適配其他鏈的特徵，基於狀態機的非同步操作，完成與其他鏈的交互。另外一個就是基於 AurumOx Protocol 平臺的其他鏈之間的互通。AurumOx Protocol 也提供一個



更複雜的智能合約來支持其他鏈之間的互聯互通，由於要支持兩種不同類型的其他鏈，智能合約結合中繼鏈完成不同類型鏈的互聯互通。

跨鏈交易是區塊鏈網路之間的去信任消息，這是一個關鍵的基礎設施組件，用於鏈路間通信。跨鏈交易最初是在源塊上創建的，然後在最終到達目標區塊鏈之前通過橋樑和連接網路進行處理和轉發。如前所述，跨鏈交易的創建者必須使用 AO 作為通信支付交易費用，從而激勵每個交叉點的參與者。AurumOx Protocol 跨鏈通信通過適配器來實現，適配器會創建一個相容的區塊頭。AurumOx Protocol 設計了層級側鏈機制來解決跨鏈交易匹配不同鏈區塊生成速度的問題，根據鏈的區塊生成速度把鏈劃分到不同的層，然後為每一層提供一個專有的適配鏈或者適配模組來帶動同層的跨鏈交易。

4.4.6 側鏈分層架構

在該側鏈體系中，側鏈同樣可以擁有自己的側鏈，但必須遵循從上到下的共識繼承關係，子鏈需要繼承全部上級鏈的共識，並同步全部上級鏈的消息，但同樣也可以通過向主鏈或其他父級鏈的共識和系統來保障共用服務的性能、安全性和消息數據服務。在此基礎上，次級鏈基於上級鏈的應用模型來開發自己獨立的應用場景，並與上級鏈隔離。AurumOx Protocol 側鏈在系統設計原理上並不限於一層，而是可以建立多層次鏈。所謂的多層輔鏈結構，就是從側鏈上再衍生出下一級側鏈，上一層鏈稱為父鏈，衍生出的鏈稱為子鏈。

4.4.7 靈活支持商業應用

AurumOx Protocol 通過兩方面來實現易用性。一是提供區塊鏈即服務系統 (Blockchain as a Service, 簡稱 BaaS) 來降低企業及個人的使用門檻。通過網路



分叉、數據定制、智能合約發佈和升級、資產交易監控等並輔以可視化功能，讓區塊鏈應用變得簡單易用。二是 G 鏈提供多種語言支持，從 Lua、C++ 到 Java，讓不同平臺的開發者都可以便捷地開發。

4.4.8 AurumOx Protocol 開源 Graphene 技術

2018 年被稱為公鏈元年，針對以太坊低效的傳輸速度及公鏈之間存在的資訊孤島。各公鏈都提出了自己的擴容和跨鏈方案，但實際落地卻不甚理想。很多公鏈都沒有如期上線，2018 年最火的公鏈 EOS 當時號稱 TPS 可達百萬，可實際運行中的 TPS 只有 3000 左右。但是 AurumOx Protocol 實際運行的 TPS 達到了 39523，是 EOS 的 10 倍，AurumOx Protocol 是怎麼做到的？

AurumOx Protocol 基於優秀的開源 Graphene 技術，能直接從 Graphene 繼承成熟的架構、性能等技術優勢。Graphene 主要的技術優勢包括：能支持 100,000TPS 的交易吞吐能力，每筆交易確認時延平均可達秒級。

針對數據資產價值交換網絡特徵，AurumOx Protocol 創造性地設計了 DDPoS 共識演算法。DPoS 起源於 Bitshares，它的原理是讓每一個持有權益的節點進行投票，由此產生代表節點（在 AurumOx Protocol 中被稱為三體節點），由這些代表組成超級節點池或者礦池來進行交易確認，而這些超級節點彼此的權利是完全相等的；但是僅僅通過以 Token 投入為中心的選舉機制容易導致一系列激勵偏差問題，如賄選、刷票等。在 AurumOx Protocol 網路中，通過加入對代表節點支持數據資產價值交換能力的評比與比較，來平衡單純的 DPoS 帶來的激勵不相容問題。

4.4.9 分片技術

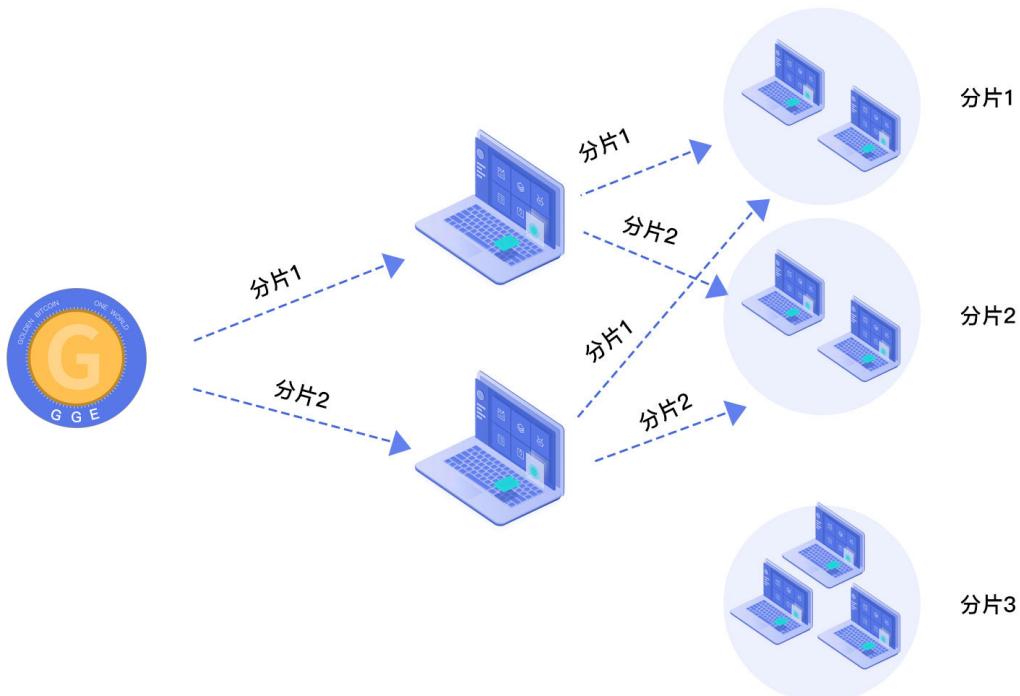


AurumOx Protocol 引入了 (Sharding) 分片技術，支持水準擴展，採用網路分片和交易分片相結合的分片技術；同時提供 BaaS(Blockchain as a Service) 服務，為開發者提供豐富的 BaaS API、數據交易 API、原生 API 開發區塊鏈應用。

AurumOx Protocol 通過採用 DDPOS 共識協議，結合市場上先進的開源 Graphene 方案和分片技術，實現了擴容和跨鏈目標，在實際運行環境中 TPS 達到了 39523，是目前 EOS 的 10 倍。

AurumOx Protocol 提供了一個先進穩定的底層公鏈，黃金穩定幣 GGEC 是 AurumOx Protocol 上的第一個應用。GGEC 與南非、剛果、阿聯酋等主要黃金產地達成合作，依託豐富的黃金儲備發行黃金穩定幣。

GGEC 之后，AurumOx Protocol 上會上线一个去中心化交易所，促进 AurumOx Protocol 上的资产流动，完善生态。同时去中心化交易所上的商城模块，也为黄金稳定币 GGEC 提供了一个线上兑换渠道。



AurumOx Protocol 的分片技術



5 AurumOx Protocol 技術架構安全與網路 安全防護

5.1 區塊鏈本身具備的安全優勢

5.1.1 區塊鏈安全優勢

如今駭客可以破壞整個網路、篡改數據或誘導粗心的用戶落入安全陷阱。他們竊取盜用身份資訊，並通過對中心化資料庫的攻擊及單點故障引發其他安全威脅。但區塊鏈技術中的數據存儲和共用數據的模式，與目前資訊安全是截然不同的做法。比特幣和以太坊都使用相同的密碼學技術來保障安全交易，但現在也能夠作為一種防範安全攻擊和安全威脅的工具。區塊鏈在資訊安全上的優勢主要在於以下幾個方面：

- 利用高冗餘的資料庫保障資訊的數據完整性
- 利用密碼學原理進行數據驗證，保證不可篡改
- 許可權管理方面，運用了多私鑰規則進行訪問許可權控制
- 區塊鏈上的交易數據全部都附有交易者的數字簽名，不可偽造。
- 利用區塊鏈的安全優勢可以進行多重安全應用的開發。

由 MIT 開發的 CertCoin 可能是第一個應用基於區塊鏈的 PKI。PKI 是一種常見形式的公鑰密碼可以用來保護郵件，消息應用，網站和其他形式的通訊。然而由於多數 PKI 介面需要依賴中心化的，受信任的第三方認證機構 (CA) 來發行、吊銷、和為每個參與者保存鑰匙對，駭客能夠通過冒用用戶的身份進入加密通訊中獲取資訊。而 CertCoin 移除了中心化的權利機構，使用區塊鏈作為分佈式帳本分發公鑰，能夠有效降低駭客單點侵入的風險。



而在認證領域，同樣也有很多例子，如公政通 Factom 系統。它基於區塊鏈建立鏈式結構的存儲，將認證分解成存在性證明、過程性證明和可審計證明三部分。對於任何數字資產的認證處理，都可以按照這三個步驟實現數據記錄的安全性和監督合規。

5.2 AurumOx Protocol 安全防護

5.2.1 以身份驗證保護邊界設備安全

正如 IT 關注數據和連接向“智慧”邊界設備的遷移，安全同樣關心這種轉變。畢竟，網路的擴展可能會提升 IT 效率、生產力並降低耗電量，但也給 CISO、CIO 和整個公司帶來了安全挑戰。很多公司因而尋求應用區塊鏈來保護 IoT 及工業 IoT(IIoT) 設備安全的方法——因為區塊鏈技術可增強身份驗證，改善數據溯源和流動性，並輔助記錄管理。

5.2.2 提升機密性和數據完整性

儘管區塊鏈最初創建時是沒有特定的訪問控制機制的（源於其公開分發的屬性），有些區塊鏈實現如今卻在解決數據機密性和訪問控制問題。在當今數據極易被篡改或偽造的時代，確保數據機密性和完整性問題無疑是巨大的挑戰。但區塊鏈數據的完全加密特質確保了這些數據不會被非授權方染指，但又仍具有流動性（中間人攻擊幾乎沒有成功的可能）。



這種數據完整性也擴展到了 IoT 和 IIoT。比如說，IBM 就在其 WatsonIoT 平臺上提供了以私有區塊鏈帳本管理 IoT 數據的選項，該功能已集成到了 IBM 的雲服務中。愛立信的區塊鏈數據完整性服務，可為在通用電氣司 PredixPaaS 平臺上工作的 App 開發人員提供完全可審計、符合規定且可信的數據。

5.2.3 保護隱私消息

AurumOx Protocol 正用區塊鏈保護即時聊天工具和社交媒體上流轉的隱私資訊。WhatsApp 和 iMessage 之類 App 所用端到端加密不同，AurumOx Protocol 使用區塊鏈來保護用戶的元數據。因為元數據是帳本中隨機分發，不存在單一的收集點，所以不會被黑。

6 AurumOx Protocol 的優勢與應用

6.1 AurumOx Protocol 的優勢

6.1.1 AurumOx Protocol 技術優勢

AurumOx Protocol 是一個面向大數據時代的區塊鏈數據價值生態體系，其核心目標是建立一個可以高效、安全、激勵正向強化的數據交換與數據價值挖掘的區塊鏈網路。當前數據交易中最為顯著的四大痛點分別是：數據資源浪費、數據孤島、數據沉澱與數據供需不匹配。而 AurumOx Protocol 通過構建一個需求導向、獎勵數據貢獻、分包實現數據結構化的社群網路，打造一個安全、高效、可溯源、無數據沉澱、可再深度開發的數據交易平臺，通過數據競賽和數據去中心化交易來系統化地解決上述痛點。結合區塊鏈網路與數據價值發掘、交換的需求，AurumOx Protocol 的構架設計遵循如下基本原則：



- **交易可信**

交易記錄進入區塊鏈並永久存證，交易雙方低成本信任交易網路，這要求網路兼具可靠性與私密性，同時規避數據沉澱等仲介問題。

- **激勵相容**

經濟體系設計促進網路節點發佈數據，基於數據開發衍生價值發掘功能，同時參與整個生態開發促進數據價值發掘、交換成本不斷下降。

- **精細化交易模式**

通過網路機制設計促進數據資產交易更趨性細化。

- **市場化數據定價**

通過網路機制設計保證市場化數據定價更細緻化。

- **支持高併發交易**

支持高併發量數據交換，實驗室網路環境可達百萬級，實際網路環境可達39523TPS，成為未來海量人工智慧、物聯網、機器人進行大規模數據採集、交換、邊緣計算結果交換等能力的基礎設施。

- **支持數據品質驗證**

支持對數據進行採樣、交叉比對、格式比對、類型識別、範圍識別等自動化驗證手段，在保障交易安全的同時，預設提供多種數據品質驗證的能力設置。

- **支持衍生數據服務**



支持對數據進行可編程模型計算的功能，支持開發者採用通用語言編制更複雜的數據分析工具並接入 AurumOx Protocol，支持接入預言機(Oracle)網路提升智能合約功能範圍。

- **支持跨鏈區塊鏈服務**

支持在數據存儲、計算能力方面具有成熟解決方案的區塊鏈服務接入 AurumOx Protocol。

6.1.2 AurumOx Protocol 提升甚至替代 PKI

公鑰基礎設施(PKI)是保護電子郵件、消息應用、網站和其他通信形式的公鑰加密體制。然而，大多數PKI實現依賴中心化的第三方證書頒發機構(CA)來頒發、撤銷和存儲密鑰對，這就給網路罪犯留下了窺探加密通信和假冒身份的機會。而在區塊鏈上發佈密鑰則在理論上可杜絕虛假密鑰傳播，並可令應用具備驗證通信對象身份的功能。

AurumOx Protocol是首個基於區塊鏈的PKI實現。該項目整體摒棄了中心證書頒發機構，使用區塊鏈作為功能變數名稱及其公鑰的分發帳本。另外，AurumOx Protocol還提供不帶單點故障的，可審計的公開PKI。AurumOx Protocol區塊鏈技術，我們就可以用公民生成的身份來簽名交易了。

6.1.3 網路層訪問控制

AurumOx Protocol公有鏈允許節點自由進出網路，且區塊鏈的網路層沒有登記用戶身份。金融行業的風險和安全性相對更高，未登記身份的節點自由進出網路為系統安全帶來很多不可控性。AurumOx Protocol區塊鏈技術在金融行業應用時，應結合業務需求，分析必要使用公有鏈，並登記網路中節點的身份。此外，還應採用VPN專網、



防火牆、物理隔離等技術對節點，特別是礦工節點的物理網路和主機進行保護。

6.1.4 AurumOx Protocol 網路傳輸安全

在 AurumOx Protocol 的網路傳輸的安全性更多的體現在是否有良好的對抗中間人攻擊的能力上。中間人攻擊（英語：Man-in-the-middle attack，縮寫：MITM）是指攻擊者與通訊的兩端分別創建獨立的聯繫，並交換其所收到的數據，使通訊的兩端認為他們正在通過一個私密的連接與對方直接對話，但事實上整個會話都被攻擊者完全控制。

安全的數字錢包需要能夠對終端裏面全部的數字證書的合法性進行掃描、對網路傳輸過程中的代理設置進行檢查並能夠保障基礎的網路通訊環境的安全性。

6.1.5 高吞吐量

區塊鏈的本質是一種分佈式共用記賬的技術，其分佈式特徵主要體現在分佈式一致性而非分佈式併發處理。例如比特幣網絡每秒只能處理 7 個交易，以太坊每秒處理 15 個交易。當前所有的公有鏈網路都面臨系統的擴展性問題，為保證數據的一致性，防止拜占庭將軍問題，某些特定環節只能串行執行，而無法並行。通過長期的測試與優化實踐，AurumOx Protocol 的 BOE 技術能讓 AurumOx Protocol 可以在鏈外直接多次、高頻、雙向地通過軌差方式實現瞬間確認，AurumOx Protocol 擁有全球頂尖併發速度，每秒可處理 39000 筆交易，比 EOS 快 10 倍以上，與現有的區塊鏈系統相比，AurumOx Protocol 有更快更穩定的交易確認，並且提供夠足夠的靈活性設計。AurumOx Protocol 的 BOE 技術讓處理性能已經能滿足萬級 TPS 的需求。如果再引入 Off-Chain 等機制，還能進一步大幅提高交易吞吐量。



6.2 AurumOx Protocol 的應用

AurumOx Protocol 的 BOE 技術，可實現黃金的確權、加密、存證、交換、分發、發行、交易、打賞、眾籌、眾包等。典型應用場景如下：

6.2.1 GGE 黃金交易中心

GGE 項目其核心是打造 GGE 黃金交易中心，傳統的黃金交易都需要通過銀行卡組織或者添加銀行的信任網關，這是依賴和中心化的黃金交易方案，而 GGEC 是應用區塊鏈技術將實物黃金數位化，投資者可以隨時交易同時區塊鏈技術保證了交易的安全性和便捷性。其次，GGE 的架構中不存在任何中心化的節點，無論是數字貨幣的傳遞還是法幣的結算都是由網路上的用戶節點自主協調完成的，再將區塊鏈的特性用在黃金生產、加工、交易整個產業鏈中，搭建成黃金數字生態鏈，在特徵上更優於黃金，將黃金的流動性完美地釋放出來。區塊鏈的去中心化和開放性，使得交易不受第三方限制且系統資訊高度透明和公開，即在 GGE 公有鏈平臺上任何人在任何時候的任何地域都可以進行黃金的交易，且方便快捷。GGE 與多家持牌黃金企業深度合作，因此區別於傳統的



紙黃金，具有真實資產所有權價值。同時 GGEC 與黃金 100:1 真實錨定，不像比特幣隨市場行情波動大、難把握，GGEC 與實物黃金直接掛鉤，而黃金價值又永久恒定，所以 GGE 是個極其穩定的系統。不但低成本、高效率地解決了數字貨幣在黃金交易場景中遇到的問題，還能最大限度地保障用戶和商戶的資金安全。

在 GGE 黃金交易中心中，如果交易環節中有節點出現問題，交易都可以自動切換到其他路徑繼續進行；即使大部分節點癱瘓導致交易無法進行，用戶的資金也會按照 RSMC 和 HTLC 協議自動提現到主鏈帳戶或退回法幣帳戶，不會被竊取或丟失。另外，APC 網路中交易通道內的節點只能接觸到相鄰節點資訊，由於沒有中央節點的存在，以及協議中的多層次加密保障，用戶在 APC 中的轉賬和交易都是完全匿名的，這是中心化或半中心化解決方案無法做到的隱私保障。

6.2.2 GGEC 穩定幣的投資邏輯

- **流通量大**

僅以市值來看，穩定幣市值僅占數字貨幣總市值的 0.8%，不過以數字貨幣市場的 24 小時交易量來看，目前還處在起步階段的穩定幣卻已占到整個數字貨幣市場的 13.5%。因此，成功的穩定幣專案絕對不是以市值取勝，而是要在流通量上尋找突破口。雖然現在市場中大部分交易仍發生在非穩定幣中，但這樣的趨勢很可能被逆轉。隨著其他數字貨幣較大的價格波動、投資風險凸顯以及市場逐漸成熟與理性，投資人將更加注重長期性盈利而不是短期暴利，資金不再偏愛具有更高投機性的幣種，這就使得具有巨大流通總量的穩定幣專案得以脫穎而出。



• 長期匯率穩定

保持相對於法幣比較穩定的匯率是衡量穩定幣未來成功與否的重要標準。只有在保證匯率穩定的基礎上，穩定幣實現價值尺度、交易媒介、記賬單位等，貨幣基本職能才有可能性。

• 革新性 – 落地的应用场景

投資者需要關注哪些穩定幣項目是革新性地解決了現階段無法解決的問題，亦或者是為用戶或服務商提供了謀取利益的新方式。以史為鑒，第一代穩定幣 USDT 看到了比特幣的不穩定性給用戶所帶來的問題，所以將 USDT 打造成可以作為交易憑證的，價格穩定的數字貨幣。就目前市場的發展來看，新一代的革新項目應該是將穩定幣與支付平台所掛鈎的項目。最近已陸續有同時發行穩定幣並建立 DApp 系統的項目，或將穩定幣應用于物聯網和金融交易平台的項目白皮書橫空出世。未來，穩定幣項目可以合作的平台還有很多，比如穩定幣與醫療，供應鏈，或者是娛樂門戶等方面。

6.2.3 確權

確權是依照法律、政策的規定，經過資產申報、權屬調查、審核批准、登記註冊、發放證書等登記規定程式，確認某資產的所有權、使用權的隸屬關係和他項權利。

6.2.4 交易

交易是在 GGE 網路中，各種黃金的消費，所有權轉移，租賃等行為，消費存在消費主體和權益主體。



6.2.5 打賞

打賞是互聯網新興的一種非強制性的付費模式。如今現實中也出現打賞，比如餐廳，酒吧，KTV，景區等等消費地帶都出現給服務員打賞付費管道。

6.2.6 署籌

由發起人、跟投人、平臺構成。具有低門檻、多樣性、依靠大眾力量、注重創意的特徵，是指一種向群眾募資，以支持發起的個人或組織的行為。在過去的兩年多的時間中，AO 團隊與多個行業企業、機構合作並落地數個區塊鏈項目，如為某地方機構建設了基於區塊鏈的小貸征信服務平臺，基於區塊鏈的去中心化智能投顧平臺 RobotABS，以及為某金融機構打造了通用積分平臺可以看出，團隊在區塊鏈技術研發的實戰中積累了大量的實踐經驗，這也為其白皮書中描述的多元化場景奠定了技術基礎。

AO 團隊在未來將深耕行業拓展，為更多的應用場景提供堅實的區塊鏈基礎設施，提升行業效率，降低業務運營成本。



6.3 AurumOx Protocol 的多元應用場景

6.3.1 供應鏈管理

- **供應鏈金融**

傳統供應鏈金融領域，核心企業的信任背書只支持一級供應商或一級經銷商，無法擴展到二級、三級供應商，因為核心企業的絕對優勢地位，常常導致二級、三級供應商存在較大的融資需求。基於 AurumOx Protocol 的供應鏈金融，可以將核心企業的信任背書傳遞到二級、三級甚至更遠層級的供應商，使圍繞核心企業的生態鏈系統可以健康發展。同時，對於金融機構，也可以通過作為節點方式，回放相關供應商的歷史數據，降低金融風險，提升金融信任。

- **供應鏈清結算**

對於傳統的複式記賬而言，最大的問題莫過於供應鏈的清算過程。基於 AurumOx Protocol 的解決方案，可以圍繞著核心企業的多個供應商，當交易完成後，通過供應商和核心企業確認的交易簽名資訊，同步在區塊鏈上，使相關的交易記錄無法進行任何篡改。實現交易即清算，令牌即結算等高效的供應鏈清結算服務。

6.3.2 健康醫療

在健康醫療方面，AurumOx Protocol 將與行業進行結合與商業推廣，有效提升醫療體系運作、管理效率，構建誠信、可追溯、透明、安全的醫療保障體系。



6.3.3 分佈式能源

在分佈式能源方面，基於 AurumOx Protocol 開發的去中心化電能交易平臺 SPX(SmartEnergyExchange) 將致力於通過資訊平臺的搭建和商業模式的重構，建立一定範圍內的、虛擬化的社區能源互聯網。

6.3.4 物聯網

在物聯網場景中，AurumOx Protocol 致力於最終實現設備自治(ThingsAutonomy)，價值互通(VALUETRANSFER)，人工智慧(AI)與機器人(Robotics)技術融合的物鏈網時代拓展。AurumOx Protocol 將會為該場景中的分佈式充電樁(DCP)以及互聯汽車(InteractiveAutomousDriving)提供技術解決方案。

此外，在個性化需求強烈的時尚產業中，AurumOx Protocol 將會為該行業的設計、出樣、生產等環節提供技術支持，以保證產品的知識產權、記錄樣品變更等。





6.3.5 溯源領域

AurumOx Protocol 可應用於各類物品的溯源領域，主要採用了區塊鏈的“鏈”特性。溯源領域包括食品溯源、產品溯源、奢侈品溯源、珠寶玉石溯源等。將代表實物資產的資產代碼在區塊鏈的各個環節流通，保證溯源的資訊不可篡改，且可完整追溯。AurumOx Protocol 在溯源領域，可通過其自身具有的備註字段，為每個溯源環節加多自定義的溯源資訊（如資產故事等），以實現資產價值的提升。

7 GGE 代幣分配及戰略規劃

7.1 GGEC 代幣計劃

通證全稱：Global Golden Exchange Coin

英文簡稱：GGEC

發行數量：初始發行 50 億

AurumOx Protocol 實現黃金的數位化、權證化。我們設定主網通證 (Token) 為 GGEC 黃金資產數位化加密權證)，與黃金進行永恆錨定 ($100\text{GGEC}=1\text{g 黃金}$)，GGEC 是將發佈在 AurumOx Protocol 的第一個重要資產通證 Token。GGEC 初始發行量 50 億枚，後續根據市場黃金交易進行合理增發。



- GGEC 穩定幣的市場規模會持續擴大

穩定幣的需求主要為個人投資者進入虛擬貨幣市場的過渡器、機構投資者的風險管理工具、企業融資後合規及避險的手段、Dapp 應用中定價四類。個人和機構投資者進入加密數字貨幣的數量正在快速增加；而僅 2018 年 Q1 區塊鏈專案融資額就達到了 58.3 億美金，超過了去年全年的數量。由此可見，市場對於穩定幣的需求還會持續擴大。

- 能獲取更多應用場景的 GGEC 穩定幣才能在長期取勝

目前市場規模最大的 USDT 其實就是看到了比特幣的不穩定性給用戶所帶來的問題，用戶需要將自己的法幣兌換成某種幣值相對穩定的數字貨幣，然後才能開始投資數字貨幣市場。所以將 USDT 打造成可以作為交易憑證的，價格穩定的數字貨幣。在未來隨著穩定幣種類增加，幣與幣之間的競爭會愈發激烈。只有擁有明確的使用場景，能得到用戶和開發者共同認可的穩定幣才有機會獲取更大的發展。而最好的使用場景，目前看來可能會出現在支付領域。

7.2 AurumOx Protocol 代幣分配

通證全稱：AurumOx

英文簡稱：AO

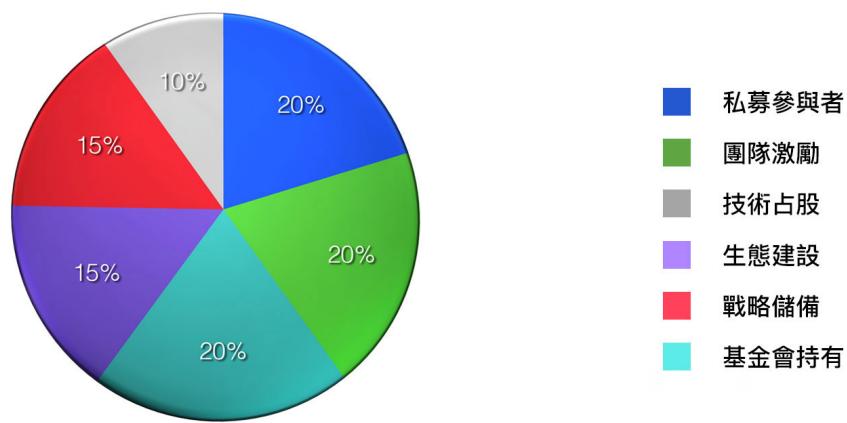
發行數量：恒定發行 70 億

AO 是由 AurumOx Protocol 基金會發行的應用於公鏈的燃料消耗 Token，在轉移數字黃金資產的時候需要消耗它。AO 初始發行量 70 億枚，且永不增發，其分配比例如下：



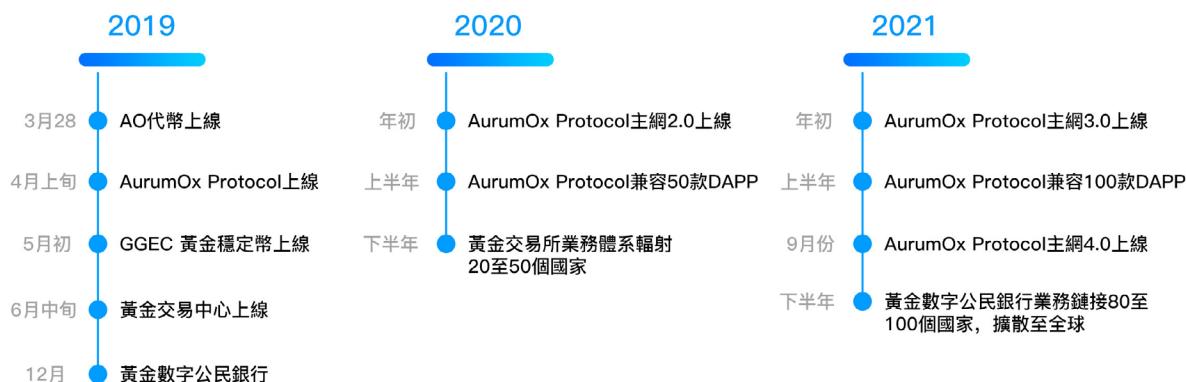
- 20% 為私募參與者，第 3 個月釋放 30%，第 6 個月釋放 30%，第 9 個月釋放 40%
- 20% 為團隊激勵，第 13 個月開始釋放，每個月釋放 0.2%
- 10% 為技術占股，第 13 個月開始釋放，每個月釋放 0.5%
- 15% 為生態建設，用於空投、市場活動
- 15% 為戰略儲備，用於技術投資、戰略投資
- 20% 為基金會持有，維護專案日常運營和開銷

AO市場計畫





7.2 戰略規劃



8 GGE 核心團隊與資本方

8.1 GGE 核心團隊



文木源(任 GGE CTO)

北京數字引擎科技有限公司 CEO, DBX 鏈創始人。中國人民大學學士(高考保送)。技術極客, 15 歲 開發 DIY-PAGE 軟體成為“讓百度改變演算法的軟 體作者”, 第 22 屆 CASTIC 電腦類金牌, 第四屆中國青少年科技創新獎、第八屆高士其科學獎獲得者。



蔡志川

畢業於 WESTCLIFF UNIVERSITY, USA 工商管理博士 亞洲區塊鏈學會創會會長、中國投資發展促進會數 字經濟委員會副主任、香港東區協進社榮譽主席; 香港國際區塊鏈金融總會榮譽顧問;亞洲數字科技有限公司首席執行官 ;香港區塊鏈資產管理有限公司總裁;中國社會科學院研究生院經濟研究所經濟學博士研究生



李大偉

李大偉先生曾擔任中國比特幣的 CEO, 也是 ZB 的聯合創始人之一, 他是數字貨幣和區塊鏈行業的早 期投資人和堅定擁護者, 多年的實踐閱歷使他擁有 豐富的行業經驗。



G E

新一代黃金流通體系



黃連金

中國電子學會區塊鏈專家委員 曾任職加拿大 CGI 集團公司(主營 IT 諮詢)，擔任技術總監、雲安全技術負責人。黃連金先生創建了 CGI 聯邦身份管理和網路安全能力中心，並為美國聯邦政府、金融機構和公用事業公司提供金融、區塊鏈、安全等方面專業諮詢，被行業內列為“區塊鏈撲克牌大佬”之一。



張建國

曾任大象礦機創始人，量子比特幣創始人，幣塊科技 CEO、中國區塊鏈俱樂部 CBCC 發起人。在 2013 年創立了大象礦機，並與阿瓦隆、南瓜張合作生產 比特幣挖礦機，當時的全球銷售量逾 10 萬臺。



本先生

本先生曾就职于新西兰前十的国际贸易公司。随后，他在澳大利亚创办了自己的旅游和投资公司。本先生是区块链早期投资者，最初投资在2015年，并且成为以太零的联合创始人。本先生拥有丰富的顾问经验，以其商业敏锐和洞察力而闻名。本先生与BDDFINEX交易所、GFX、GELOS、美国CARLIFE汽车项目等建立了密切合作关系。2017年，他投资了区块链咨询公司TODO BLOCK，并同时获得蛮子资金，保利资本和中以科技创新中心等顶级风险投资公司的投资。



張宏彬

燈火區塊鏈董事長
漢晨資本合夥人 PK.TOP 交易所聯合創始人 赤途資本合夥人
李銀河學院特別顧問，RAPIDASH 大中華區戰略顧問



沈大海

WBO 世界區塊鏈組織教育署署長、中國區塊鏈創業學院院長、BDFUND 發起人
JAVA 高級講師。國內最早推廣 JAVA 技術和利用 J2ME 進行移動遊戲開發的專家之一，在移動增值領域有多年的實際開發和研究經驗。



张议云

19岁创立了口袋兼职APP，创业半年先后获得比亚迪董事、分众传媒VP、广东中科招商2500多万元融资。专注区块链全产业投资孵化，包括玛雅矿机、矿世云算、AILINK、职业链、ZAG区块链钱包等项目。



王翔宇

资本运作专家，中国式管理专家，基金管理模式创始人，先后为数百家企业提供发展战略、股权融资、境外上市、资产并购等高级顾问服务；指导数家企业实现“无为而治”的管理境界



8.2 GGE 資本方



大中華國際集團



加密資本



優優金融



黃家控股



京城傳媒



大中華傳媒



大中華文化廣場



漢晨資本



免责申明

除本白皮書所明確載明的之外，GGE 平臺不會作任何陳述或保證（尤其是對其適銷性和特定功能）。任何人參與 GGE 的公開售賣計畫及購買 GGE 的行為均基於自己本身對 GGE 的瞭解以本白皮書的資訊。在無損於前述內容的普遍性前提下，所有參與者將在 GGE 項目啟動之後按現狀接受 GGE，無論其技術規格、參數、性能或者功能等。GGE 平臺在此明確不予承認和拒絕承擔下述責任：任何人在購買 GGE 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；任何人在購買 GGE 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，以及由此導致的無法付款或無法提取的問題。GGE 由於任何原因的公開售賣計畫被放棄；GGE 的開發失敗、推遲或延期，以及因此導致的無法交付 GGE 或延遲交付；以太坊或相關區塊鏈源代碼的漏洞、錯誤、瑕疵、崩潰、回滾或硬分叉等技術問題引起的平臺故障；對公開售賣所募集資金的使用；任何參與者洩露、丟失或損毀了數字加密貨幣或代幣的錢包私鑰；GGE 公開售賣的第三方平臺的違約、違規、侵權、崩潰、癱瘓、服務終止或暫停、欺詐、誤操作、不當行為、失誤、疏忽、破產、清算、解散或歇業；任何人對 GGE 的交易或投機行為；GGE 在任何交易所的上市交易或退市；GGE 被任何政府、主管當局或公共機構歸類或視為是一種貨幣、證券、商業票據、流通票據、投資品或其他事物，以至於收到禁止、監管或法律限制；本白皮書披露的任何風險因素，以及與該等風險因素有關因此導致或伴隨發生的損害、損失、索賠、責任、懲罰、成本或其他負面影響。



風險提示

GGE 開發和運營團隊相信，在 GGE 的開發、維護和運營過程中存在著無數風險這其中很多都超出了 GGE 開發和運營團隊的控制。除本白皮書所述的其他內容外，每個 GGE 購買者還均應細讀、理解並仔細考慮下述風險之後才決定是否參與本次公開售賣計畫。

每個 GGE 的購買者應特別注意這一事實：儘管 GGE 開發和運營主體是在新加坡設立的，但 GGE 只存在於網路虛空間內，不具有任何有形存在，因此不屬於或涉及任何特定國家。參加本次公開售賣計畫應當是一個深思熟慮後決策的行動，將視為購買者已充分知曉並同意接受了下述風險：

- **公開售賣計畫的終止**

本次 GGE 公開售賣計畫可能會被提前終止，此時購買者可能由於比特幣 / 以太幣 的價格波動以及 GGE 開發和運營團隊的支出而僅被部分退還其支付的金額。

- **不充分的資訊提供**

截止到本白皮書發佈日，GGE 仍在開發階段，其哲學理念、共識機制、演算法、代碼和其他技術細節和參數可能經常且頻繁地更新和變化。儘管本白皮書包含了 GGE 最新的關鍵資訊，其並不絕對完整，且仍會被 GGE 開發和運營團隊為了特定目的而不時進行調整和更新。

GGE 開發和運營團隊無能力。且無義務隨時告知參與者 GGE 開發中的每個細節（包括其進度和預期里程碑，無論是否推遲，因此並不必然會讓購買者及時且充分地接觸到 GGE 開發中不時產生的資訊。資訊披露的不充分是不可避免且合乎情理的。



• 監管

加密代幣正在被或可能被各個不同國家的主管機關所監管。GGE 開發和運營團隊可能會不時收到來自於一個或多個主管機關的詢問、通知、警告、命令或裁定，甚至可能被勒令暫停或終止任何關於本次公開售賣計畫、GGE 開發或 GGE 的行動。GGE 的開發、行銷、宣傳或其他方面以及本次公開售賣計畫均因此可能受到嚴重影響、阻礙或被終結。由於監管政策隨時可能變化，任何國家之中現有的對於 GGE 或本次公開售賣計畫的監管許可或容忍可能只是暫時的。在各個不同國家，GGE 可能隨時被定義為虛擬商品、數字資產甚至是證券或貨幣，因此在某些國家之中按當地監管要求，GGE 可能被禁止交易或持有。

• 密碼學

密碼學正在不斷演化，其無法保證任何時候絕對的安全性。密碼學的進步（例如密碼破解）或者技術進步（例如量子電腦的發明）可能給基於密碼學的系統（包括 GGE）帶來危險。這可能導致任何持有的 GGE 被盜、失竊、消失、毀滅或貶值。在合理範圍內，GGE 開發和運營團隊將自我準備採取預防或補救措施，升級 GGE 的底層協議以應對密碼學的任何進步，以及在適當的情況下納入新的合理安全措施。密碼學和安全創新的未來是無法預見的，GGE 開發和運營團隊將盡力迎合密碼學和安全領域的不斷變化。

• 開發失敗或放棄

GGE 仍在開發階段，而非已準備就緒隨時發佈的成品。由於 GGE 系統的技術複雜性，GGE 開發和運營團隊可能不時會面臨無法預測和 / 或無法克服的困難。因此 GGE 的開發可能會由於任何原因而在任何時候失敗或放棄（例如由於缺乏資金）、開發失敗或放棄將導致 GGE 無法交付給本次售賣計畫的任何購買者。



- **眾籌資金的失竊**

可能會有人企圖盜竊 GGE 平臺所收到的公開售賣所獲資金。該等盜竊或盜竊企圖可能會影響 GGE 開發和運營團隊為 GGE 開發提供資金的能力。儘管 GGE 開發和運營團隊將會採取最尖端的技術方案保護眾籌資金的安全，某些網路盜竊仍很難被徹底阻止。

- **源代碼瑕疵**

無人能保證 GGE 的源代碼完全無瑕疵。代碼可能有某些瑕疵、錯誤、缺陷和漏洞，這可能使得用戶無法使用特定功能，暴露用戶的資訊或產生其他問題。如果確有此類瑕疵，將損害 GGE 的可用性、穩定性或安全性，並因此對 GGE 的價值成負面影響。

- **安全弱點**

GGE 區塊鏈基於開源軟體並且是無准入許可的分佈式帳本。儘管 GGE 開發和運營團隊努力維護 GGE 系統安全，任何人均有可能故意或無意地將弱點或缺陷帶入 GGE 的核心基礎設施要素之中，對這些弱點或缺陷，GGE 開發和運營團隊無法通過其採用的安全措施預防或彌補。這可能最終導致參與者的 GGE 或其他數字代幣丟失。

- **“分佈式拒絕服務”攻擊**

區塊鏈設計為公開且無准入許可的帳本。因此，可能會不時遭受“分佈式拒絕服務”的網路 攻擊。這種攻擊將使 GGE 系統遭受負面影響、停滯或癱瘓，並因此導致在此之上的交易被 延遲寫入或記入區塊鏈的區塊之中，或甚至暫時無法執行。



- **處理能力不足**

GGE 的快速發展將伴隨著交易量的陡增及對處理能力的需求。若處理能力的需求超過區塊鏈網路內屆時節點所能提供的負載，則 GGE 網路可能會癱瘓或停滯，且可能會產生諸如“雙重花費”的欺詐或錯誤交易。在最壞情況下，任何人持有的 GGE 可能會丟失，回滾或甚至硬分叉可能會被觸發。這些事件的餘波將損害 GGE 的可使用性、穩定性和安全性以及 GGE 的價值。

- **GGE 錢包私鑰**

GGE 所必需的私鑰丟失或毀損是不可逆轉的。只有通過本地或線上 GGE 錢包擁有唯一的公鑰和私鑰才可以操控 GGE。每位購買者應當妥善保管其 GGE 錢包私鑰。若 GGE 購買者的該等私鑰丟失、遺失、洩露、毀損或被盜，GGE 開發和運營團隊或任何其他人士均無法幫助購買者獲取或收回相關 GGE。價格不穩定普及度 GGE 的價值很大程度上取決於 GGE 平臺的普及度。GGE 並不預期在發行後的很短時間內就廣受歡迎、盛行或被普遍使用。在最壞情況下，GGE 甚至可能被長期邊緣化，僅吸引很小一批使用者。相比之下，很大部分需求可能具有投機性質。缺乏用戶可能導致 GGE 市場價格波動增大從而影響 GGE 的長期發展。出現這種價格波動時，GGE 團隊不會（也沒有責任）穩定或影響 GGE 的市場價格。

- **價格波動**

公開市場上交易，加密代幣通常價格波動劇烈。短期內價格震盪經常發生。該價格可能以比特幣、以太幣、美元或其他法幣計價。這種價格波動可能由於市場力量（包括投機買賣）、監管政策變化、技術革新、交易所的可獲得性以及其他客觀因素成，這種波動也反映了供需平衡的變化。無論是否存在 GGE 交易的二級市場，GGE 開發和運營團隊對任何二級市場的 GGE 交易不承擔責任。因此，GGE 開發和運營團隊沒有義務穩定 GGE 的價格波動。GGE 交易價格所涉風險需由 GGE 交易者自行承擔。