LONGITUDE-LATITUDE

INTELLIGENT INVESTMENT

一、金融時代的發展

1.1 世界金融發展主要趨勢

現代市場經濟是一種開放型經濟 ,經濟關系的國際化意味着國際分工合作的加強與深化。超越國界和社會制度差异的世界市場的形成 ,擴大了金融活動的空間 ,使得金融全球一體化日益加強。這主要表現為金融流通工具空前國際化 ,國際金融流量規模不斷擴大 ,參與國際金融活動的國家和地區越來越多 ,全球性的高速化、系統化、電子化、網絡化的資金融通系統逐步建立。目前 ,隨着資本流動和貿易的全球化、自由化 ,國際金融業呈現出以下幾個基本發展趨勢和特點。

一、金融國際化

經濟國際化的發展是導致金融國際化的內在原因。 30 年代的大蕭條和第二次世界大戰 ,導致整個世界經濟陷入嚴重混亂狀態。戰后初期 ,各國經濟相互分離 ,金融市場也彼此分割 ,幾乎所有國家都在戰后初期實行了外匯和資本管制措施。這種狀況在 60 年代由于世界經濟國際化 (包括生產國際化、市場國際化和資本國際化)的迅速發展而改變。經濟國際化的發展 ,必然導致金融國際化。特別是跨國公司的發展 ,直接推動了金融國際化的形成。歐洲貨幣市場作為金融國際化的最主要內容 ,正是在跨國公司及其推動產生的生產國際化、市場國際化和資本國際化的基礎上形成和發展起來的。

1957 年發生的英鎊危機 ,促成歐洲美元首先正式在倫敦出現。到了 60 年代中后期 ,歐洲美元市場的借貸活動已經超過美元範圍 ,陸續出現了歐洲英鎊、歐洲德國馬克、歐洲法國法郎等系列歐洲貨幣 ,從而使該市場從一個在美國境外經營美元存放款業務的貨幣市場發展成為一個在貨幣發行國以外進行該貨幣儲存與貸放的市場。歐洲貨幣市場與傳統的國際金融市場不同 ,它是一種離岸市場 ,主要是在非居民之間進行的國際借貸 ,其業務一般不受東道國的法律限制 ,因此它通常被認為是真正的國際金融市場。

金融管制的松動加快了金融國際化的進程。自 70 年代中期以來 ,在發達國家出現了放松管制的浪潮 ,主要表現在:

①放松或取消資本流動的限制和外匯管制。 1979 年英國取消了妨礙國際資本自由流入或流出的一切限制。到 1984 年 ,日本給予美國銀行進入東京金融市場的許多權利 (包括承銷政府債券)。1986 年日本的三家最大的證券公司獲準在美國承銷美國國庫券。到 80 年代末 ,“ 十國集團 ”中的大部分國家都放松或取消了資本流動的限制和外匯管制 ;

②削減稅收法規。1984 年美國率先取消了對外國投資的利息預扣稅 ,此后其他發達國家也相繼降低或取消了這種利息預扣稅。

③放松對服務貿易的管制。 1986 年開始的“ 關稅與貿易總協定 ”烏拉圭回合談判中正式提出放松對服務貿易的管制。 1994 年生效的《北美自由貿易協定》中明確規定了美國、加拿大和墨西哥三國之間開放金融市場。放松管制就其實質而言 ,如同拆除了阻擋國際資本流動的“ 圍牆 ”,消除了各國金融市場之間的界限 ,推動了金融國際化的進程。

二、國際金融一體化

金融國際化是國際金融一體化的條件 ,國際金融一體化則是金融國際化的高度發展。一般認為國際金融一體化的標志是 ,世界儲蓄對風險進行調整之后將流向回報最高的地方 ,不同金融資產在對風險調整之后將提供相同的收益率。一體化意味着同一金融產品在不同的國家和地域的市場上由于套利而只有一個價格。實現了一體化的金融市場的最好範例是外匯市場。外匯市場是一個世界範圍的市場。世界上的國際商業銀行的外匯部門通過一個復雜的通訊系統保持着 24 小時的聯系。倫敦、阿姆斯特丹、法蘭克福、米蘭、巴黎、紐約、巴林、東京、香港和新加坡是主要的外匯交易中心 ,這些作為通訊樞紐點的中心的存在使 24 小時的連續交易成為可能。一體化不僅意味着一種金融市場在世界範圍內或某個地區內的連通 ,而且意味着不同金融市場在世界範圍內或某個地區內的貫通。不同金融商品回報率的趨同可通過資金在兩個市場之間的流動或通過第三個市場間接實現。歐洲貨幣體系是金融區域一體化的最好例證。西歐國家正在向單一貨幣的目標邁進 ,屆時在歐洲貨幣體系內 ,金融體系和金融市場的民族國家特征和由此而導致的分隔將被高度一體化的貨幣體系和金融市場所代替。

國際金融一體化的內在原因是全球經濟一體化的發展。 70 年代以來特別是 80 年代中期以來 ,世界經濟、政治格局的變化 ,使國際金融市場已不再局限于倫敦、紐約等著名的國際金融中心 ,從而出現了許多新型的國際金融中心 ,如香港、新加坡等。同時 ,全球國際資本流動也日趨活躍 ,而規模巨大的跨國金融機構 (包括商業銀行、投資銀行和各類保險公司)在全球大量設立分支機構 ,形成了全球性的業務網絡 ,也促進了資本的國際間流動 ,加速了國際金融市場一體化、全球化的進程。

科學技術 ,特別是電子通訊技術的迅速發展 ,對國際金融一體化、全球

化的影響極為深遠:

①改變了傳統的金融業務操作手段 ,實現了金融業務操作手段的現代化;

②微電子技術的通訊技術的進步對全球 24 小時金融市場的形成發揮了重要的作用。

③計算機和信息處理技術的進步推動了金融工具的創新 ,使金融機構能夠對層出不窮的新工具進行設計和定價 ,并能有效地管理新工具的風險。

三、金融自由化

金融自由化是指政府當局將過去對金融的各種管制予以放寬或解除 ,特別是將不合時宜的金融管制加以解除 ,以創造公平合理的競爭環境 ,使價格機能得到充分發揮。因此 ,這里的“自由化”指的是管理體制的松動或放松管制 ,而并非一般意義上的自由發展或自由交易。

西方國家大規模的金融管制始于本世紀 30 年代 ,直接原因是 30 年代的經濟大危機 ,因此金融管制成為反經濟危機的措施之一 ,其管制內容主要是對各類金融機構的業務範圍、利率、信貸規模和地理分布等進行限制。其中利率管制和業務範圍的限制是最有代表性和最嚴厲的。美國、日本、英國、意大利等西方國家都實行過嚴厲的金融管制。金融管制雖然在當時起着穩定金融秩序的作用 ,但也限制了金融運行的效率和靈活性。到 60 年代特別是 70 年代中期以后 ,隨着世界經濟金融形勢的變化 ,金融創新得到了蓬勃發展 ,西方各國紛紛開始放松對金融業的嚴格管制 ,從而掀起了金融自由化的浪潮 ,其主要內容為:

①價格市場化 ,也就是取消利率限制 ,放開匯率 ,取消證券交易中的固定傭金制度 ,由市場來調節金融價格;

②擴大各類金融機構的業務範圍和經營權力 ,放寬金融從業登記 ,使各類金融機構公開競爭;

③改革金融市場 ,放松各類金融機構進入金融市場的限制 ,豐富金融工具和融資技術 ,放寬和改善金融市場的管理;

④放寬流動自由化 ,允許外國資本和金融機構進入本國市場 ,同時也放寬了本國資本和金融機構進入國外市場的限制。

澳大利亞是金融自由化較為迅速的國家。從 1980 年取消商業銀行和儲蓄銀行的存款利率上限開始 ,到 1985 年短短的六年間 ,澳大利亞取消或放松了幾年所有的金融管制措施。美國從 60 年代起開始醞釀金融自由化的改革 , 1980 年的《放松存款機構管理法和貨幣管制法》和 1982 年的《加恩—聖杰曼存款機構法》的實施 ,加速了這一變革過程。這兩個法案打破了美國幾十年來形成的不同金融機構之間嚴格的業務限制 ,使儲蓄機構與商業銀行的區別趨于消亡。 1994 年的《跨州銀行法》的頒布第一次在聯邦層次上為銀行跨州經營奠定了法律基礎 ,宣告了美國長達半個多世紀單一銀行制的徹底結束。1997 年美國取消了禁止銀行通過子公司從事保險、證券業務的禁令 ,使銀行的兼營進一步合法化。 1986 年英國首相撒切爾夫人為挽救日益衰退的英國金融業 ,重振倫敦交易所昔日雄輝 ,斷然宣布實行金融體制改革 ,并為此制定了金融服務法 ,此次改革帶來了更大的自由化 ,如率先實行證券交易代理手續費自由化 ,經紀人與出場代理人互相兼營并實行自由的市場作價人制 ,開放交易所會員資格限制 ,廢除各項金融投資管制 ,銀行開始提供包括證券業務在內的綜合性金融服務等 ,這次改革被稱為金融“創世紀大裂變”。 1980 年日本通過新銀行法并于 1982 年正式實施 ,其主要內容就是放松金融管制 ,促進金融自由化 ,允許銀行涉足證券業務。 1984 年日本公布了《金融自由化與日元國際化的狀況和

展望》,提出了加快金融自由化與國際化的步驟。 1992 年日本國會正式通過金融制度改革法案 ,使日本金融自由 化的步伐 進一步 加快。而 1997 年 6 月日本大藏省公布的金融體制改革規劃方案 ,其改革力度之大 ,期限之短都是歷史上罕見的。按照這一改革方案 ,日本政府將在 5 年期間對金融界的企業限制、銀行資金業務的期限限制、外匯交易限制、金融衍生商品交易限制、場外交易限制以及證券交易手續費的限制等數十種限制規則進行撤銷 ,實行金融自由化 ,同時將對現行的外匯法、銀行法、證券法、保險法等有關法律進行修改 ,并將制定一系列新的相關法律。從目前日本、美國、英國等公布的金融改革方案來看 ,金融自由化是大勢所趨、大多數發展中國家也正步入金融自由化的進程。

四、金融證券化

在任何金融體系中 ,資金的流動可以是直接的也可以是間接的。直接金融所涉及的是債權債務在借方和貸方之間的直接交換 ,這種交換往往涉及股票、債券和其他金融工具的交易 ,間接金融則涉及金融中介機構為借方和貸方所提供的服務 ,證券化是 80 年代以來國際資本市場的最主要特征之一。所謂證券化是指借款人和貸款人日益通過直接融資 (發售股票債務、商業票據等)實現資本的轉移 ,而不是主要通過銀行的中介來確立債權債務關系的趨勢。80 年代中期 ,國際金融市場上的證券融資金比例首次超過國際信貸。國際融資者的資金來源由原來的依靠銀行信貸為主轉向發行各種類型的股票債券和商業票據等直接在資本市場上籌資。 1981 年 ,債券融資只占資本市場融資總額的 30% , 1983 年證券融資超過信貸融資 ,而 1986 年債券融資已占資本市場融資總額的 70 % 。世界經合組織在 1996 年初指出 ,盡管發生了墨西哥金融危機及世界經濟增速放慢 ,但

1995 年世界資本市場總借貸額 增加 30% ,達 到創 紀 錄的 12580 億美元。1995 年增長的借貸額中主要是中期銀團貸款和中期歐洲債券 , 1995 年世界債券市場債券總額為 4610 億美元 ,高于 1993 年的 4290 億美元 , 接近 1994 年創紀錄的 4810 億美元。

此外 ,在國際金融業不斷變革和發展的過程中 ,還出現了許多引人注目的新情况、新特點:

①金融創新不斷發展 ,金融工具日趨多樣化 ,金融衍生商品層出不窮。目前國際金融市場中的金融創新不斷推出 ,經過組合再組合、衍生再衍生的“ 金融魔方 ”的變化而產生的金融衍生商品多達 1200 多種。1995 年初 ,據總部設在瑞士巴塞爾的國際清算銀行對全球 26 個主要國家從事國際金融活動的銀行機構的調查表明 ,在國際金融市場上每天成交的金融衍生業務的票面協議額度達到了 8390 億美元左右 ,以全年的金融衍生交易運轉日來計算 ,全球金融市場上的金融衍生業務票面協議成交總額已達到了 407000 億美元。

②全球銀行業重組與兼并浪潮十分迅猛。美國 1995 年共發生了 200 起銀行兼并案 ,使用資金超出 240 億美元。日本及其他發達國家近年來也掀起了銀行兼并浪潮。繼美國大通銀行和化學銀行的合并之后 ,今年美國又有第一銀行和第一芝加哥銀行、國民銀行與美洲銀行合并;此外去年日本三菱銀行和東京銀行也進行了合并 ,這都很令人注目。銀行兼并的結果表現為銀行規模越來越大 ,銀行數目普遍減少。到 1995 年底 ,美 國的銀 行數 只有 12067 家 , 與 1980 年最高峰時期相比下降了 36% ;德國的銀行數只有 3487 家 ,比最高峰時期下降了 31% 。

③國際金融市場日趨動蕩 ,金融風險加大。近年國際金融市場的風波迭起。如 1994 年墨西哥金融危機、1995 年英國巴林銀行破產倒閉、1995

年日本大和銀行事件、1997～ 1998 年的東南亞和韓國金融危機等等。金融市場的動蕩、金融風險的加劇 ,使世界經濟的發展產生了巨大的影響 ，也給全球銀行業和投資者提出了挑戰。

1.2 新金融模式

新型金融模式是整體性而非碎片化的互聯網應用，并非簡單地將互聯網技術應用在傳統金融行業的單一環節上，例如實現投資者找到優質合法正規的金融機構和資管機構，解決投資者投資金融產品的各種門檻（資金門檻，區域門檻，身份門檻等）。金融機構和資管機構找到有效的投資者，解決金融機構和資管機構耗費成本過高問題，解決金融機構和資管機構融資難等問題。解決全球金融跨區域融投局限！化解雙向選擇盲區！以區塊鏈技術為傳統金融服務升級！以傳統優質金融承載區塊鏈應用落地！讓所有投資者直接對接正規、專業、優質的資管機構團隊！從雙方問題構建起在互聯網技術支持下的金融組織的新模式。所以，這是實現金融全產業鏈的應用。

新型金融模式以金融產品為紐帶，以互聯網、區塊鏈等信息技為手段，融合金融產品交易、流通等要素實施“ 便捷式 ”融投資，實現“ 為金融導航 ”。這可以說是對傳統金融產業鏈的整體性、系統性、顛覆式升級。

還有，新型金融模式是系統性而非叠加式的互聯網應用。它并非簡單地應用互聯網技術于自身，而是通過互聯網技術改造金融模式實現金融產業流程的升級。換言之，新型金融模式實現了金融各環節之間相互促進的 1+1>2 的系統性成效，所以是“ 以信息技術支撐起的金融生態體系 ”。它借助移動互聯網技術讓投資者與優質正規的金融機構直接挂鈎，這就從根本上消除了由于信息不對稱所造成的市場調節失靈的弊端，為構建起投資

“便捷式”融投資奠定了基礎。

二、新型金融模式勢在必行

2.1 國際金融行業的現狀及啟示

一、國際金融市場現狀

（一）國際金融市場的含義

一般廣義上的國際金融市場是指在國際領域里操作和實施國際金融業務的場所。除了廣義上的金融市場，還存在狹義上的國際金融市場，狹義上說國際金融市場是為各國際經濟交流主體提供進行長期或短期借款和貸款的場所。國際金融市場在國際社會上有着相對較高的地位，主要是因為金融活動為幾乎所有的傳統經濟活動提供支持，是世界經濟發展的重要推動力。

（二）國際金融市場的劃分

根據劃分標準和依據的不同，國際金融市場的分類也各不相同。首先，依據資金的融通周期可以將國際金融市場劃分為資本市場以及貨幣市場兩大類。資本市場具有較長的資金融通周期，一般為一年以上、中期或者長期的資金市場。國際貨幣市場相對借貸資金周期較短，為一年以內，因此又被稱作短期資金市場。

除了按周期長短劃分外，還可以根據交易分割的形式將國際金融市場劃分為期貨市場、現貨市場以及期權市場三大類。期貨市場是指以利率、貨幣以及貴金屬期貨為主要交易方式的期貨市場；現貨市場顧名思義指現貨交易的場所；期權交易市場則指供投資者進行期權交易的場所。

國際金融市場還可以根據經營業務的種類劃分為國際資金市場、國際外匯市場、證券市場以及國際黃金市場。國際資金市場即狹義上的國際間的資金借貸市場。國際外匯市場則是由各類外匯提供者和需求者進行外匯買賣、資金調撥以及清算的場所。證券市場則是公司債券、股票以及政府債券等有價證券進行發行和交易的場所，是金融市場的一個重要組成部分。

（三）國際金融市場的基本特征

國際金融市場的基本特征有以下三個方面

1、總體市場形勢相對平穩

近年來，一些歐元區重債國的債務問題暫時得到了一定程度的緩解，同時以美國為代表的高風險的資本價格正在逐步回升。由此可預見，當前階段國際金融市場整體的大環境相對平穩，市場環境得到了一定改善。但是由于世界經濟存在復雜性和多樣性，再加上一些國家的國際政策存在很大的不確定性，很大程度上影響了國際金融市場的穩定性。

2、國際金融市場業務和利率的自由化

近年來，隨着各國逐漸放松了對金融機構的業務限制以及鼓勵金融市場的合理競爭。除了銀行業，很多行業開始逐漸參與到了金融業的發展中，一些非銀行的金融機構也開始開展支票的存款等傳統的銀行業務。與此同時，各國都逐漸打破了金融壁壘、逐漸開放金融市場，再加上各國金融政策改革的驅動，利率在市場機制的調節下一定程度上實現了自由化，整個國際金融市場呈現出寬松自由的發展景象。

3、國際資本流動方向發生改變

當下全球的經濟格局處于變化的格局中，市場格局呈現出南降北升的局面。造成這一局面的原因主要是發達經濟體以及新興起的經濟體股市較為疲軟。相應地由于新興經濟體的發展速度變緩和發達國家經濟自主增長

力增強使得國際金融市場格局也發生了較大的變化。這一經濟格局導致的直接后果就是流通中的資金將會向發達經濟體傾斜，新興經濟體將會向發達經濟體的方向進行轉移。

二、國際金融市場啟示

自從金融業網絡化發展興起以來，金融網絡化模式的發展態勢就勢不可擋，并迅速成為當前世界各國金融業改革的主要手段與目的。金融業網絡化，極大地推進了世界整個金融業向現代化，科技化發展的進程，但在某種程度上來講，其也為傳統金融業帶來一定的冲擊。如何充分利用全球金融業網絡化所帶來的發展和機遇，而避開其所來的影響與冲擊，就成為一個很值得思考的問題！總結了一些全球金融業網絡化啟示，具體如下所述。

1、各國加快傳統經濟向互聯網經濟的進程，只有經濟走向了信息化，傳統經濟轉向那互聯網經濟，金融業的網絡化發展才有基礎。

2、各國加大金融業信息系統基礎建設的投資，促進金融業網絡化的發展。銀行，證券，保險業的全面網絡化。政府大量的資金投入，使人們體驗數字經濟的優越性，轉變觀念，為接受電子貨幣打下基礎 。

3、 金融業的網絡化發展，使資本流動突破了規模上地域上和有形無形的限制，使得金融活動國際化。目前國際金融交易額是國際貿易交易額的 50 倍，新的信息傳輸技術和交易的電子化是全球金融市場中的“ 傳染性效應 ”，更加明顯，對全球金融業的網絡化提出了更高的要求。

2.2 金融市場的痛點

金融具有交易數據碎片化、交易節點多樣化、交易網絡復雜化的特點。

人們通過在綫上綫下購買金融產品及服務。但我們很難判斷這些信息的真實性。由于造假的利潤空間很大，金融造假不僅損害投資者利益，損害金融市場的信譽和品牌形象，社會也不得不消耗資金、人力來行使法律監督和法律制裁。

對于金融市場，目前存在幾個痛點：一是全球金融跨區域融投局限。二是雙向選擇盲區，存在信息孤島問題；三是投資者找不到優質的金融項目、金融機構；四是金融機構融資難，融資成本高；五是中心化系統都存在個體作惡的風。

2.3 新型金融模式的重要性及好處

以區塊鏈技術構建的金融門戶平臺！解決全球金融跨區域融投局限！化解雙向選擇盲區！以區塊鏈技術為傳統金融服務升級！以傳統優質金融承載區塊鏈應用落地！讓所有投資者直接對接正規、專業、優質的資管機構團隊！解決投資者投資難；解決投資者找不到優質正規的金融項目、資管機構；解決投資者的投資門檻（資金門檻、區域門檻、身份門檻）等問題。解決金融項目、資管機構融資難，融資成本高等問題。

三、區塊鏈介紹

區塊鏈介紹

區塊鏈是比特幣的底層技術，像一個數據庫賬本，記載所有的交易記錄。這項技術也因其安全、便捷的特性逐漸得到了銀行與金融業的關注。區塊鏈是比特幣的一個重要概念，本質上是一個去中心化的數據庫，同時

作為比特幣的底層技術。區塊鏈是一串使用密碼學方法相關聯產生的數據塊，每一個數據塊中包含了一次比特幣網絡交易的信息，用于驗證其信息的有效性（防偽）和生成下一個區塊。 區塊鏈在網絡上是公開的，可以在每一個離綫比特幣錢包數據中查詢。比特幣錢包的功能依賴于與區塊鏈的確認，一次有效檢驗稱為一次確認。通常一次交易要獲得數個確認才能進行。輕量級比特幣錢包使用在綫確認，即不會下載區塊鏈數據到設備存儲中。

一般說來，區塊鏈系統由數據層、網絡層、共識層、激勵層、合約層和應用層組成。其中，數據層封裝了底層數據區塊以及相關的數據加密和時間戳等基礎數據和基本算法；網絡層則包括分布式組網機制、數據傳播機制和數據驗證機制等；共識層主要封裝網絡節點的各類共識算法；激勵層將經濟因素集成到區塊鏈技術體系中來，主要包括經濟激勵的發行機制和分配機制等；合約層主要封裝各類腳本、算法和智能合約，是區塊鏈可編程特性的基礎；應用層則封裝了區塊鏈的各種應用場景和案例。該模型中，基于時間戳的鏈式區塊結構、分布式節點的共識機制、基于共識算力的經濟激勵和靈活可編程的智能合約是區塊鏈技術最具代表性的創新點。而區塊鏈有着以下特點:

1.去中心化：由于使用分布式核算和存儲，不存在中心化的硬件或管理機構，任意節點的權利和義務都是均等的，系統中的數據塊由整個系統中具有維護功能的節點來共同維護。得益于區塊鏈的去中心化特征，比特幣也擁有去中心化的特征。

2.開放性：系統是開放的，除了交易各方的私有信息被加密外，區塊鏈的數據對所有人公開，任何人都可以通過公開的接口查詢區塊鏈數據和開發相關應用，因此整個系統信息高度透明。

3 自治性：區塊鏈采用基于協商一致的規範和協議（比如一套公開透明的算法）使得整個系統中的所有節點能夠在去信任的環境自由安全的交換數據，使得對“ 人 ”的信任改成了對機器的信任，任何人為的干預不起作用。

4 信息不可篡改：一旦信息經過驗證并添加至區塊鏈，就會永久的存儲起來，除非能夠同時控制住系統中超過 51%的節點，否則單個節點上對數據庫的修改是無效的，因此區塊鏈的數據穩定性和可靠性極高。

5. 匿名性：由于節點之間的交換遵循固定的算法，其數據交互是無需信任的（區塊鏈中的程序規則會自行判斷活動是否有效），因此交易對手無須通過公開身份的方式讓對方自己產生信任，對信用的累積非常有幫助。

四、經緯智投結構和機制

經緯智投通過在參與的區塊跨鏈傳遞邏輯和價值來創建一個連續的價值鏈，其中每個交易都發生在鏈上，邏輯和價值像流動資產一樣在跨鏈自由流動，這些基礎設施，協議和概念將一起工作，以確保跨鏈通信從始發到目的地的傳輸。這些技術的價值在于它們使一個區塊鏈與另一個區塊鏈交互以及一個區塊鏈與多個連接的區塊鏈進行交互。

4.1 連接網絡—經緯智投

連接網絡即經緯智投由指定的角色要求來定義連接網絡和跨鏈事務提供了通用接口，使區塊鏈開發者、投資者、資管機構、金融機構能將消息從一個網絡路由到另一個網絡。是連接網絡促進多個

私有或公共區塊鏈網絡之間的跨鏈通信和跨鏈事務的網絡，具體來說，連接網絡應提供以下核心功能:

•通過通用橋接協議在不同的區塊鏈網絡之間路由消息，該最終協議涉及消息的轉換和傳播。

•提供去中心化的問責制。

•提供橋接協議。

經緯智投通過引入第三方將消息從 A 點路由傳遞到 B 點,代替使用網橋和去信任的區塊鏈網絡來驗證并確保流動交易的正確性,網絡本身不存在管理困難或不清楚的情況。規定了外部組件的標準。

經緯智投協議諸如跨鏈交易中繼或 BTC 交易中繼的點對點連接作為中心集綫器存在。這樣的協議雖然簡單而有效，但往往導致復雜的狀態可能引起爭議，并且經常會依賴于運維中繼網絡的員。
雖然每個連接網絡的實際功能和內部組件可能因農產商和預期目的而异，但是這些核心功能應該被實現。

4.2 智能合約

智能合約由自己獨特的驗證者網絡組成，或者由交易雙方共同確認，提供交易的問責和確保協議被正確執行。

4.3 參與網絡

經緯智投設計的核心概念之一是它專用于兼容區塊鏈或區塊鏈相關網絡的聯合。這些可以是特定的區塊鏈，私有網絡或聯盟區塊鏈。無論上下文如何，以更有效、更安全和更透明的方式相互聯系和相互操作以至逐漸

增加了每個網絡的價值，并為區塊鏈生態系統提供穩定性。

參與網絡是成功實現與連接網絡集成的任何網絡。參與網絡應該是區塊鏈，但不一定局限于此。唯一的限制是參與網絡與連接網絡集成的靈活性。一旦與經緯智投集成，參與網絡可以訪問先前指定的通信協議，從而實現許多可能的用例。

參與網絡具有完全靈活性，可以自定義其區塊基礎設施的不同模塊，包括共識算法，散列算法，虛擬機（VM）和腳本語言。

4.4 共識

用共識來實現連接兩個或多個區塊鏈的架構。將設計 BFT 協議的兩個變體，以便在橋梁和連接網絡上達成共識:

橋梁共識只是一個輕量級的變化，可以在橋梁上快速達成共識。經緯智投共識是一個共識協議，重點是提供規模穩定性。我們首先探討網絡中的共識算法，旨在解決連接網絡的要求。該共識算法需同時支持鏈上交易和跨鏈交易的共識。為了以有效和不變的方式滿足這些要求，將使用基于拜占庭容錯算法的共識算法，并結合混合協議。其目的在于公平支持兩方代表：部分通過令牌系統，部分通過基于現代神經網絡中使用的新穎驗證算法的智能證明。為了滿足運營規模并能夠廣泛參與網絡驗證過程，經緯智投將采用類似于 BitShares 團隊和 Lisk 的委托模式的代表性驗證模型。這種驗證模型將使經緯智投參與者能夠支持積極參與共識的驗證者，從而大大增加參與度，超出傳統的 BFT 算法技術上允許的範圍。基 BFT 的協議的具體細節尚未確定，但保證活動性和安全性的標準屬性。因為網絡應該激勵選擇最優和正確的驗證者，所以這些假設由代表性選擇方法補充。我們正在研究當前的一些 BFT 提議，如 HoneyBadger, Tangaroa 和

Stellar，尤其關注 HoneyBadger 中的提案行為和 Stellar/Tangaroa 協議中的選舉協議。

代表性網絡驗證背后的概念設計源于代表民主制，候選人通過從選民獲得的投票來讓自己獲選。不同的是，在這個系統中，驗證者必須得到支持者的支持，同時每個支持者都會收到網絡獎勵的一部分。這種設計背后的理由是相信網絡的自治，網絡的集體行動直接通過適當的投票影響網絡的安全。

總而言之，所提出的共識協議是網絡中的每一個節點都可以自己作為候選人并向候選人提供支持。在每個時期開始時，獲得最高支持
的候選人被選定為這個時期的驗證者。這些驗證者通過基于 BFT 的協議為區塊鏈生成過程做出貢獻，并通過這種方式獲得區塊鏈分配的獎勵。這將持續到期限結束，下一個時期開始，重新啟動此過程。

4.5 聲譽

用戶可以通過互聯網自由地訪問這些統計信息。擁有掌握經緯智投一切信息的用戶群對于形成民主網絡的基礎是必要的。

代表性共識決定了選擇最佳驗證者節點的義務在于網絡。如果網絡沒有具備觀察候選人和主動驗證者過去行為的機制，這個過程是很難實現的。一種替用方法是依靠外部統計來選擇最佳候選人。但是，會造成操縱這些數據的動機。因此，需要在網絡內建立信譽系統，其中節點的過去動作和統計是網絡協議的一部分，提供去信任數據以允許用戶選擇其適當的候選人。可以包含在節點信譽中的功能包括:

•正常運行時間是節點在網絡上活動的時間量，并且在確定節點的年齡（可靠性）時很重要。

•總支持是在該時間點之前收到的支持的總計或總支付總額，并且在每個時期結束時（在該持續時間內被鎖定）匯總，可以用來評估節點的過去績效。

•向心性在與社交網絡中相同的上下文中使用，可以用來評估哪些節點即哪些消費者或者哪些農產供應者是網絡中最佳連接的節點，并且是評估可靠性和性能的有效指標。

•網絡信任是特定對等體的全局網絡值，指示對等體從網絡的每個角度的令人滿意的行為。這是最初設計用于 P2P 文件共享系統，并且具有可以適應于考慮與我們的用例相關的參數的算法。

最后，聲譽系統作為一個機制，說明了節點對網絡的投資。這種投資受到節點的良性或惡意行為的影響，并且在評估支持風險方面是有效的。

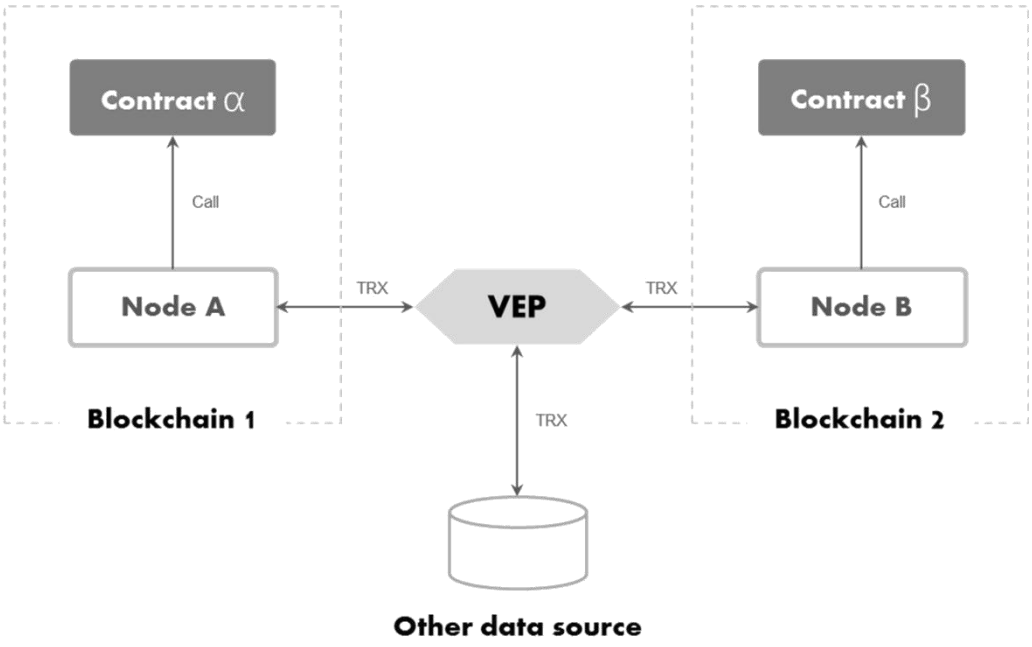
4.6 價值互換協議

該協議是不同區塊鏈或參與網絡之間連接的標準協議。如前所屬，一個網絡能夠承載的應用有限，彼此連接起來形成更大的網絡，可產生的價值叠加就越大。我們先了解單個網絡節點是如何相互信任的。區塊鏈網絡最大的優點在于能夠提供可靠的信息查詢，這種可靠性體現在分布式賬本和分布式共識。

依賴于這種分布式賬本和分布式共識，我們能夠了解到在當前網絡上登錄在記得每一個節點（農產商或客戶）的產品及其信譽情況，區塊鏈網絡是眾多參與者按照某些共識組建起來的一個社區，節點在共識和激勵的作用下形成了相互信任關系。推而廣之，把一個參與網絡當作節點，多個參與網絡之間形成連接，也需要這樣一個共識機制。因為不同網絡的平等性、可信度、利益訴求讓網絡協作變得困難，再加上網絡中總有壞節點。

因此，協作前預先設定的規則尤為重要。這就如同人類社會中跨組織協作需要有法律，契約和道德的約束。

該協議為如何協作制定了準則。它登記每個鏈每個節點的注冊信息，并提供服務給受信列表中的鏈進行查詢和連接請求。支持跨鏈節點交互和跨鏈合約調用兩大應用場景。前者利用存儲在節點的數據或外部數據的狀態變化，間接地讓合約之間產生交互，并可能產生新的信息。例如：按照合同約定到期未支付尾款，將會影響到個人信用。貸款記錄可以存儲在區塊鏈 A，而信用數據則可以存儲在區塊鏈 B，個人身份信息可能來自外部的公用數據庫。在溯源網絡中進行信息互換，并讓總價值保持不變。



跨鏈節點交互

跨鏈合約調用

五、經緯智投元件

5.1 測量儲備

經緯智投測量儲備元件為特定產品測量管理，一個分布式數據庫，用于存儲一條供應鏈特定位置上的批處理的特征記錄。測量儲備的關鍵特性包括驗真、透明度和檢測。該元件作用于于測量智能合約環境之下，管理一個基于可編譯區塊鏈(Ethereum)和 BFT 協議的、測量特定產品的分布式數據集。這個智能合約被用于存儲一條供應鏈特定位置上的批處理的特征記錄。這個數據庫的一些特性包括:

1. 真實性：數據源經過驗真且可通過加密方式驗證。

2. 容量：這個系統能儲存大量的小數據包。

3. 透明度：所采集數據對任何有興趣的一方都為公開。

4. 監測：用戶能驗證一個特定數據集的質量滿足先前定義的要求。

我們將在接下來的部分討論前兩個特性。最后兩個特性則是整體設計的自然結果。

5.1.1.驗真

經緯智投中的每個設備都用其特有的私人密鑰為數據傳輸簽名，用公用-私人密鑰加密來認證設備以認證其作為授權設備的身份。設備上的簽名能被一系列授權設備認證，即在一個智能合約中公開的密鑰配置。

測量智能合約包括一個被定義的授權設備系列，由經緯智投認證的設備能通過經緯智投被加入該系列。在未來的經緯智投實現中，我們計劃包括一個對整個金融開放的市場并采用關聯的評價系統。當一個被授權的設備向經緯智投發送信息時，它的公用密鑰將與驗真列表比對以進行驗證。

驗證通過后，該信息被接收并錄入區塊鏈。如果一個未經授權的設備向經緯智投發送測量數據，簽名認證將不能通過，測量數據將直接被忽視。

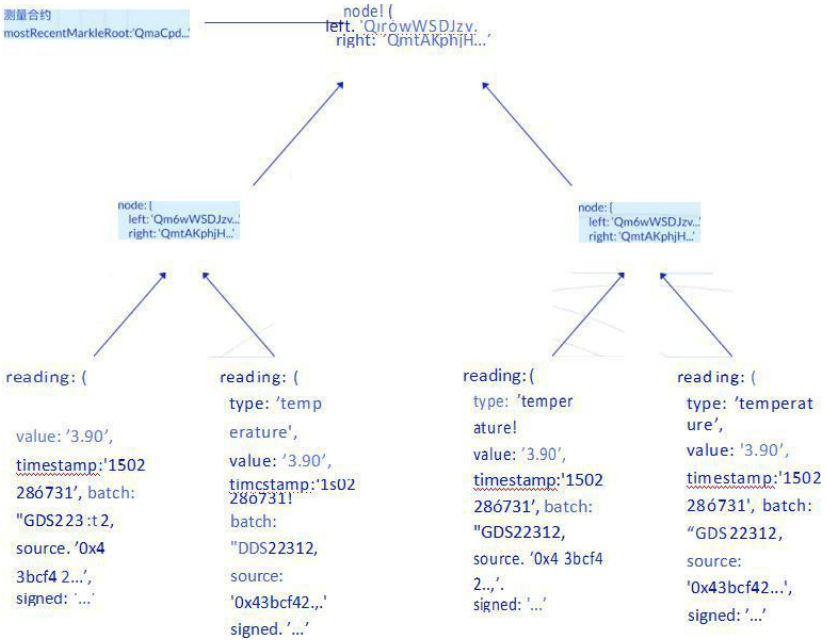
5.1.2.容量

盡管一個測量數據的大小一般小于 100 字節，但這個系統被設計用來收集潛在的數千個測量數據構成的數據集，而每個批處理可能包含來自多個設備的數據。所以從長遠來看，經緯智投每天要處理好幾 TB 的數據。

為了達到這樣的網絡容量，經緯智投創造了一個和以太坊整合的自定義區塊鏈以及一個分布式儲存系統。新的測量數據被作為梅克爾樹(MerkleTree)的葉子存儲，然后測量樹節點被映射至 IPFS 節點。梅克爾樹是能讓任何人快速通過根散列(roothash)來驗證一根數值或葉子上數據的有效性的結,這使得所有參與網絡能快速驗證一個特定的測量數據是一個已知測量儲備的一部分。梅克爾樹的根被永久儲存于 經緯智投的測量智能合約中。合約每增加一個測量數據就創造一個具有新根的新梅克爾樹版本，之后可被儲存于測量智能合約中。經緯智投選擇不在樹每次發生改變時都保存一個新根(亦即當有新測量數據加入時)以保持一個可被廣泛應用

的結構。與之相對，樹根在智能合約中進行周期性更新(比如每 100 次讀取)。

在區塊鏈上存儲梅克爾樹根保證數據一旦寫入合約即不可被修改。經緯智投也保留所有梅克爾樹根的完整歷史以確保在梅克爾樹更新時沒有數據消失或被更改。



5.2 要求智能合約

經緯智投的第二個元件是要求智能合約，用于定義能與測量智能合約中的項目進行比對的質量標準。重要的是用戶創造一系列在區塊鏈上公開的、定義優秀設計精良且經過測試的測量合約。用戶定義的要求將對用于監控生態系統中物件的應用至關重要。

簡而言之，要求智能合約判定一個產品是否持續滿足經緯智投中參與者定義的標準。例如，一方可能如此定義分布要求以確保能被安全消費。然而，消費的概念是相對的，且取決于產品的目的。比如，一個產品可能

需要滿足不同的要求：真實的金融項目、真實的盈利
(不同類型的)進一步處理對于金融產品來說，經緯智投能更加深入地定義一個特定金融產品的不同層次(比如低/中/高/極高)。

5.3 CPEX 幣

經緯智投由一個被稱為 CPEX 幣的代幣支持。當產品在供應鏈上移動或在生產過程中演變時，一個批處理分得的代幣額度可被分割并合并至許多其他的測量智能合約，它們共同組成一個物件的歷史圖表。CPEX 代幣和讀數一起被發送至網絡，直到一個批處理在供應鏈上完成移動時一直被鎖定在測量智能合約中。

在被定義的到期日來臨或可由購買、運輸或供應鏈上任何其他事件定義的“ 終止事件 ”發生之前，CPEX 代幣保持與金融產品的捆綁。

終端消費者能在循環末尾獲取代幣。這樣代幣就能被循環，并回到生態系統中。回收獲得的價值能激勵消費者購買由經緯智投追踪的金融產品。這個循環也有利于金融機構，他們能獲得免費的宣傳。

對于其他信息供應者，包括金融類服務、金融類知識等也能通過該代幣在我們網絡中出售，獲取相關價值，并能與市場流通貨幣相流通。

六、CPEX 技術基礎6.1 優化網絡成本

為了支撐 CPEX 的運作，優化使用網絡的成本非常重要。每個單獨的供應鏈在以太坊上使用各自的交易和合約配置以在物件于供應鏈上移動時處理數據。在以太坊上進行交易已變得相當昂貴，而我們的自

定義區塊鏈解決了這個問題。

CPEX 使用的主要交易網絡是 CPEX 區塊鏈，這是以太坊的一個私人版本，而不是以以太坊為主。注意“私人”在這里可能具有潛在的誤導性，因為這個網絡是公開的，且可以被任何人接入。這個術語僅用于區分 CPEX 區塊鏈和以太坊主網絡。所有與 CPEX 協議有關的智能合約將在 CPEX區塊鏈上運行，為了進一步認證會周期性地復制到以太坊主網絡上。 CPEX 幣一開始的眾籌會在以太坊區塊鏈上進行，建成之后代幣會被轉移至經緯智投。

同時 CPEX 用一個額外的三層架構來存儲數據。

1.第一層是用于儲存大量小數據的庫，以及區塊鏈和分布式文件系統。這層能以透明、連貫和不變的方式儲存每個數據。這里的核心概念是簽名數據和梅克爾樹。

2.第二層完全用于供應鏈。它應用諸如測量和要求智能合約這樣的概念。

3.最上層是 CPEX.js，一個專用于金融行業的協議，并有與這些行業相關的特殊測量和要求。

6.2 零知識證明

“零知識證明”的定義是：證明者能夠在不向驗證者提供任何有 的信息的情况下，使驗證者相信某個論斷是正確的。零知識證明（被稱為“zk-SNARK”）是實現 Zcash 的匿名特性的核 技術。因為 CPEX 的海量數據交互量，我們采種安全性是基于計算離散對數的困難性的鑒別文案，可以做預計算來降低實時計算量，所需傳送的數據量亦減少許多。為了 產 密鑰對， 先選定系統的參數：素數 p 及素數 q，q 是 p 1 的

素數因　。p≈21024，q>2160，元素 g 為 q 階元素，l≤g≤p　1。令 a 為 GF(p)的　成元，則得到 g=a(p　1)/qmodq。由可信賴的第三　T 向各戶分發系統參數(p,q,g)和驗證函數（即 T 的公鑰），　此驗證 T 對消息的簽字。對每個　戶給定惟　　份 I，　戶 A 選定秘密密鑰 s，0≤s≤q　1，并計算 v=g　smodp；A 將 IA 和 v 可靠地送給 T，并從 T 獲得證書，CA=(IA,v,ST(IA,v))。

協議如下:

（1）選定隨機數 r，1≤r≤q　1，計算 x=grmodp，這是預處理步驟，可在 B 出現之前完成；

（2）A 將(CA,x)送給 B；

（3）B 以 T 的公鑰解 ST(IA,v)，實現對 A 的　份 IA 和公鑰 v 認證，并傳送　個介于 0 到 2t　1 之間的隨機數 e 給 A；

（4）A 驗證 1≤e≤2t，計算 y=(se+r)modq，并將 y 送給 B；

（5）B 驗證 x=gyvemodp，若該等式成　，則認可 A 的　份合法。

安全性基于參數 t, t 要選得　夠　以使正確猜對 e 的概率 2t 夠。建議 t 為 72 位，p 約為 512 位，q 為 140 位。

此協議是　種對 s 的零知識證明，在認證過程中沒有暴露有關 s 的任何有　信息。

CPEX 將會借鑒 Zcash 的零知識證明技術，不單單在資產轉移的過程中可以實現雙向加密，還可以應　到很多其他對交易隱私要求極的領域。CPEX 在客戶端集成了即時通信功能，它不但能夠利　暗地址實現代幣的跨平臺轉移，也可以在　常的點對點（P2P）通信中利　零知識證明的機制實現　度的隱私通信，更能夠跨越平臺實現諸如從 CPEX 客戶端到 Byteball 客戶端的加密通訊。

6.3 底鏈發幣技術—CPEX

使用這種 CPEX 規則來發出代幣，表現出一種通用的和可預測的方式。這樣 CPEX 幣能立即兼容以太坊錢包（幾乎所有支持以太幣的錢包，包括 Jaxx、MEW、imToken 等，也支持 erc-20 的代幣），也有利于立即進行交易。

CPEX 讓以太坊區塊鏈上的其他智能合約和去中心化應用之間無縫交互。以下是網絡的發幣代碼:

```
pragma solidity ^0.4.16;
interface tokenRecipient { function receiveApproval(address _from, uint256 _value, address _token, bytes _extraData) external; }
contract TokenERC20 {
    // Public variables of the token string
    public name;
    string public symbuint8 public decimals = 18;
    // 18 decimals is the strongly suggested default, avoid changing it
    uint256 public totalSupply;
    This creates an array with all balancesmapping (address => uint256) public balanceOf;
    mapping (address => mapping (address => uint256)) public allowance;
    // This generates a public event on the blockchain that will notify clients
    event Transfer(address indexed from, address indexed to, uint256 value);
    // This notifies clients about the amount burnt
    event Burn(address indexed from, uint256 value);

    /**
     * Constructor function
*
     * Initializes contract with initial supply tokens to the creator of the contract
     */
```

```
    function TokenERC20( uint256
        initialSupply, string tokenName,
        string tokenSymbol
    ) public {
        totalSupply = initialSupply * 10 ** uint256(decimals);
//  Update total supply with the decimal amount
        balanceOf[msg.sender] = totalSupply;
// Give the creator all initial tokens
        name = tokenName;                                   //
Set the name for display purposes
        symbol = tokenSymbol;                               //
Set the symbol for display purposes
    }
    /**
     * Internal transfer, only can be called by this contract */
    function _transfer(address _from, address _to, uint _value) internal {
        // Prevent transfer to 0x0 address. Use burn() instead
        require(_to != 0x0);
        //  Check if the sender has enough
        require(balanceOf[_from] >= _value);
        // Check for overflows
        require(balanceOf[_to] + _value >= balanceOf[_to]); // Save this
        for an assertion in the future
        uint previousBalances = balanceOf[_from] + balanceOf[_to];

        // Subtract from the sender
        balanceOf[_from] -= _value;
        // Add the same to the recipient
        balanceOf[_to] += _value;
        emit Transfer(_from, _to, _value);
        //  Asserts are used to use static analysis to find bugs in your
code. They should never fail
        assert(balanceOf[_from] + balanceOf[_to] ==
previousBalances);
    }
    /**
     * Transfer tokens
     *
     * Send `_value` tokens to `_to` from your account
```

```
*
                * @param _to The address of the recipient
                * @param _value the amount to send
                */
               function transfer(address _to, uint256 _value) public
                   { _transfer(msg.sender, _to, _value);
               }
               /**
                * Transfer tokens from other address
*
                * Send `_value` tokens to `_to` on behalf of `_from`
*
                * @param _from The address of the sender
                * @param _to The address of the recipient
                * @param _value the amount to send
                */
               function transferFrom(address _from, address _to, uint256 _value)
    public returns (bool success) {
                   require(_value <= allowance[_from][msg.sender]); // Check
    allowance
                   allowance[_from][msg.sender] -= _value;
                   _transfer(_from, _to, _value); return true;
               }
               /**
               function approve(address _spender, uint256 _value) public
                   returns (bool success) {
                   allowance[msg.sender][_spender] = _value;
                   return true;
               }

               /**
                * Set allowance for other address and notify
*
Allows `_spender` to spend no more than `_value` tokens

                * on your behalf, and then ping the contract about it
*
                * @param _spender The address authorized to spend
                * @param _value the max amount they can spend
```

```
        * @param _extraData some extra information to send to the
    approved contract
        */
        function approveAndCall(address _spender, uint256 _value, bytes
    _extraData)
            public
            returns (bool success) {
            tokenRecipient spender = tokenRecipient(_spender); if
            (approve(_spender, _value)) {
                spender.receiveApproval(msg.sender, _value, this,
    _extraData);
                return true;
            }
        }
        /**
         * Destroy tokens
         *
         * Remove `_value` tokens from the system irreversibly
*
         * @param _value the amount of money to burn
         */
        function burn(uint256 _value) public returns (bool success) {

            require(balanceOf[msg.sender] >= _value); // Check if the
    sender has enough
            balanceOf[msg.sender] -= _value; //
    Subtract from the sender
            totalSupply -= _value; // Updates
    totalSupply
            emit Burn(msg.sender, _value);
            return true;
        }
        /**
         * Destroy tokens from other account
         *
         * @param _value the amount of money to burn
         */
function burnFrom(address _from, uint256 _value)
```

```
        public returns (bool success) {
            require(balanceOf[_from]                    >=
                                                        _value);
// Check if the targeted balance is enough
            require(_value        <=    allowance[_from][msg.sender]);
// Check allowance
            balanceOf[_from] -= _value;                                    //
Subtract from the targeted balance
            allowance[_from][msg.sender]                -=
                                                        _value;
// Subtract from the sender's allowance
            totalSupply -= _value;                                         //
Update totalSupply
            emit Burn(_from, _value);
            return true;
        }}
```

七、項目計劃

發行總量：10 億

發行價格：0.015美金

流通總量：1 億

發行價格：0.015美金

全仓销毁制：每日总量的千分之5

八、創始團隊

8.1 金融團隊核心成員

Rachel：有豐富的國際金融機構、國際金融組織與貨幣政策部門任職經歷。歐洲央行工作的資深經濟學家，在歐洲央行工作期間，主要負責亞太經濟預測和分析曾擔任國際貨幣基金組織和芬蘭央行經濟學家、經合組織顧問、麻省理工學院訪問學者。

Frederica:金融行業最佳領袖人物、著名投資人、高級金融風險管控顧問、斯坦福大學工程學院系統優化實驗室與美中硅谷發展促進會美國企業系統優化研發中心研究員

Candice:賓夕法尼亞大學沃頓商學院金融學博士執教于多家知名的商學院，其中包括沃頓商學院、密歇根州立大學、俄亥俄州立大學、金融學講座教授世界銀行擔任公司治理顧問

8.2 技術團隊核心成員

Angel Versetti：項目聯合創始人，擁有計算機工程學士學位和管理碩士學位，19 年工作經驗，4 年的比特幣和區塊鏈從業經驗。

Malcolm Povey:是一名專長于數據科學領域的技術負責人，有着十多年開發經驗的資深軟件工程師。曾在歐洲聯盟委員會擔任過信息技術官，是一名微軟認證的專業開發人

Michael terpin:資深全棧工程師，曾為多種加密數字貨幣開發 SPV 代碼庫，并且為 50 家以上數字貨幣交易所提供過 API 開發及市場數據分析服務