ivyKoin

白皮書2018

目錄

重要提示

本文檔是一份技術白皮書，介紹了ivyKoin技術當前和未來的發展。本檔不是披露檔。本文件專供接收方（**接收人**）用於通過按照 Ivy Koin LLC (**ivyKoin** 或公司)發行的預售承諾函授予的代幣權利（**權利**），考量購買代幣（代幣）的機會（如後文所述）。

本文檔中包含的任何資訊，或隨後代表公司或其各自雇員，代理人或顧問口頭或書面提供給接收人的資訊均按照本檔所述條款和條件提供給接受方。

本檔為保密檔，未經本公司事先書面同意，不得以任何形式複製或傳播給其他任何人。

通過保留此檔，接收人承認並向公司表示已閱讀，理解並接受本檔條款。如果接收人不接受這些條款，則必須立即將此檔退回給公司。

本檔僅為傳達資訊目的及協助接收人決定是否進一步調查可能獲得權利和代幣的機會，並且僅可用於此目的。本檔日期為2018年1月16日，由公司根據當時可用資訊發佈和製作。

本檔並非意圖提供任何投資或信用決策或任何其他風險評估的唯一或主要依據。任何接收人都應根據其認為必要或可取的獨立調查來確定其獲取權利和代幣的權益。

儘管公司在編制本檔時已經採取了應有的注意和盡職調查，但本公司或其任何顧問並不就本檔資料的準確性或完整性作出任何聲明或保證。本檔中包含的任何資訊或向接收人傳輸或提供的任何其他書面或口頭通訊均不得作為可供接收人依賴的承諾或聲明，且公司對此文件中任何估計，預測或預期的準確性或可實現性均不作出任何陳述或保證。對於任何此類資訊，估計，預測或預期，本公司或其顧問概不負責。

本檔尚未並將不會提交給澳大利亞證券和投資委員會（ASIC）。本檔的目的僅為接收人提供資訊，並不構成2001公司法（Cth）（**公司法**）或其他司法管轄區的任何同等立法中所定義或提及的招股說明書，簡易招股說明書或其他披露檔。

潛在的權利和代幣購買者應閱讀本檔的全部內容。如果您在閱讀本檔後有任何疑問，請聯繫向您提供此檔的人員。本公司保留全權決定是否向任何人士出售權利或代幣的權利。

責任免除

對於由於與此檔任何方式相關原因，包括但不限於本檔中包含的資訊，任何錯誤或遺漏，或其準確性或可靠性，而導致（包括疏忽）使接收人或任何其他人員或實體遭受或產生的任何損失或損害，公司均不承擔任何責任。

免責聲明

本文件僅供參考。本檔中的資訊可能並不完整，可能會在任何時候被公司更改，修改或修訂，並不意圖也不構成公司的聲明和保證。此外，公司可不限以任何其認為合適的方式使用權利及代幣出售所籌集的資金。

公司或公司的任何其他顧問均不意圖更新本檔或接受任何義務向接收人提供資訊的存取權限或增加任何其他資訊，或更正檔中或可獲得的關於公司、權利或代幣的其他任何其他資訊中出現的不準確之處。

公司業務最近剛剛形成，是一家“創業企業”，沒有任何顯著的經營歷史可作為依據來對其業務和前景以及代幣的發展前景進行評估。因此，這裡所包含的資訊本身就屬於推測性質。

無推薦意見

本檔不代表購買權利或代幣的建議。任何購買權利或代幣的決定必須基於擬購買者自身情況，調查，分析和對公司運營和前景以及權利和代幣的評估。潛在購買者必須自行獨立評估購買權利和代幣的好處，並諮詢自己的專業顧問，在認為必要時進行進一步調查。潛在購買者會注意，任何權利或代幣的購買都可能涉及高度的風險。

根據《公司法》第766B條的規定，本檔中的任何內容都不應解釋為個人或一般的金融產品建議。本檔不涉及或暗示對是否購買，出售或持有金融產品的建議或意見陳述。

稅收

購買權利或代幣將產生稅收後果，情況因每個權利或代幣購買者的個人財務狀況而異。我們要求所有潛在的權利或代幣購買者從稅收角度和一般情況獲得有關購買權利和代幣的後果的獨立財務建議。在法律允許的最大範圍內，公司，公司高級管理人員及其各自的顧問不承擔購買權利或代幣稅收後果的責任和義務。

美元

除非另有說明，否則所有貨幣金額均以美元為單位。

合格聲明

本檔包括“預測”，“計畫”，“針對”，“認為”，“潛在”，“估計”，“意圖”和“目標”等術語。這些陳述是基於當前對公司業務的理解以及業務所抱有的期望目標。但是，應該指出，實現這些陳述存在固有風險，潛在的購買者在購買權利或代幣時應以這些目標可能不會實現為基礎。

代幣使用

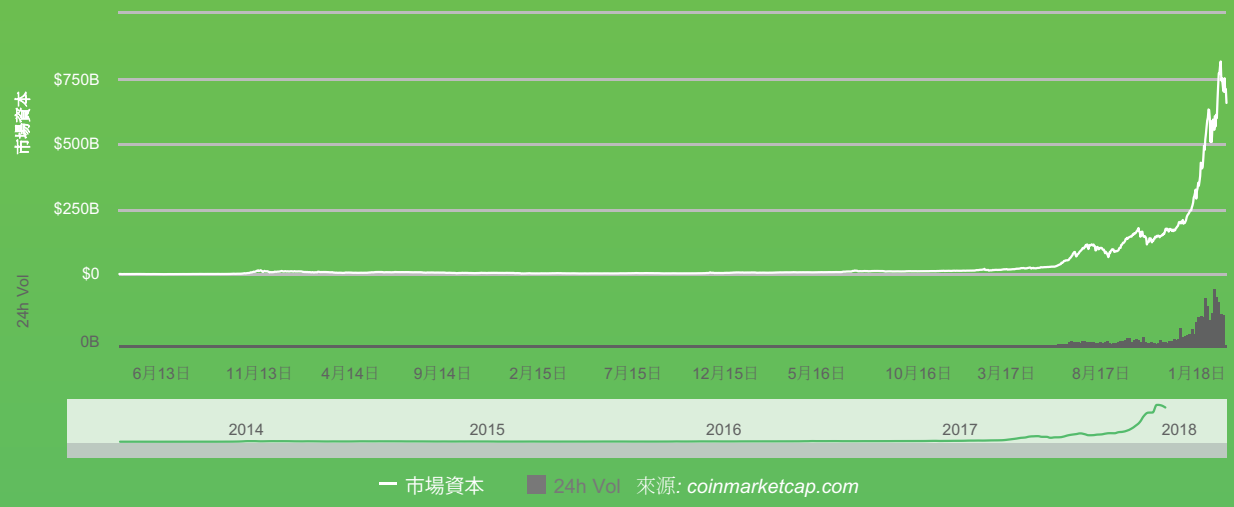
公司建議建立數位平臺來使用代幣，該數位平臺還將用於支付（**ivyKoin 網路**）。

如果實施，代幣持有者可以自願地將交易資料取消匿名直到金融機構滿意，以便在利用加密貨幣促進交易的同時具備區塊鏈的安全性和可靠性。

1

介紹

加密貨幣市場正在迅速擴大和深化，目前加密貨幣市場資本總額為720億美元。[1]



雖然這些貨幣的優勢和潛力得到了廣泛認可，但匿名卻導致缺少支援涉及加密貨幣交易的金融機構，進而阻止了其更主流的接受度。

全球銀行業和金融業缺乏支持的主要原因是由於適用法規要求的某些交易資訊與匿名性產生了衝突。

代幣將是一個基於區塊鏈的加密貨幣，意圖與金融機構進行交易，與現行支付網路（包括目前的基準支付系統，如SWIFT協定，CHIPS和Fedwire）相比，嵌入了更多的瞭解交易（**KYT**）和瞭解客戶（**KYC**）資訊。

代幣持有者將有能力自願地對交易資料進行去匿名化處理，直到金融機構滿意，從而利用區塊鏈的安全性和可靠性促進使用加密貨幣的交易。

我們我們相信代幣的機會是巨大的，因為有：

- 藍天市場
  - 潛在的加密貨幣市場持續增長
  - 全球金融機構交易的潛在滲透
- 我們的高度顛覆性技術
  - 與我們最相近的同行Ripple和全球領先的Altcoin的相比，ivyKoin網路預計會有架構上的改進。目前，Ripple的市值約為1240億美元。[2]
- 我們的世界級一流團隊，有交付歷史記錄

我們在下面詳細列出我們的建議，並期待您能成為一個代幣持有者。

Ivy Management Group LLC
2018年1月16日

1. *https://coinmarketcap.com/* 2018年1月9日
2. *https://coinmarketcap.com/* 2018年1月7日

2

行業概況

1) 全球金融機構支付系統 - 藍天市場

全球金融機構支付意義重大。我們的SWIFT平臺每天指導全球轉移轉帳近5萬億美元，即每年1250萬億美元[3]。

下面的圖表也顯示了該行業的同比增長。表格揭示了新興市場支付的增長速度，但是在北美和歐洲等更為成熟的地區，基於加密貨幣的支付解決方案存在著更大的可立即打開的市場。

Figure 2 – 2017年世界支付報告[4]

球	CAGR ('15 - '20E) 10.9%	增長 ('15 - '16E) 9.1%	
拉丁美洲	7.1%	7.2%	
中東歐，中東和非洲	10.2%	8.9%	
新興亞洲	30.9%	28.6%	發展中 19.6%
成熟亞太	7.6%	8.8%	
歐洲（包括歐元區）	6.5%	6.5%	
北美（美國和加拿大）	4.3%	4.4%	成熟 5.6%

3. *https://www.fincen.gov/sites/default/files/shared/Appendix_D.pdf*
4. *Capgeminin & Royal Bank of Scotland 2017*

2) 現行資金轉帳過程如何運作

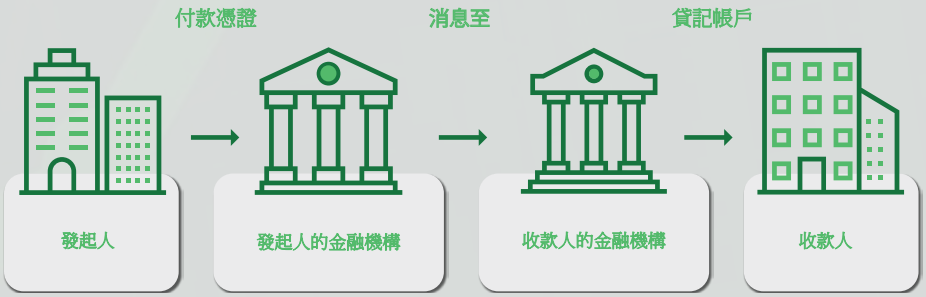
電子資金轉帳是在金融機構客戶的指示下，將金錢從一個金融機構轉移到另一個金融機構（或從一個帳戶轉移到另一個帳戶）的交易。金融機構通過電子資訊的交流實現了這一點，這些資訊構成了進行必要的記帳條目和提供資金的基礎。電子資金轉帳是企業用來在雙方間轉移資金的主要形式。

金融機構按照通用和有有良好基礎的標準通過收發電子消息來實現電子資金轉帳，標準包括SWIFT和ISO 20022。金融機構之間發送的資訊指示發送銀行借記發送方帳戶，收款銀行貸記收款方帳戶。.

參與轉帳的實體包括：

- 發起者（如企業或個人）——轉帳發起人；
- 收款人——轉帳的最終接收方；
- 發起人的金融機構——接收發起人轉帳指令的金融機構，並將資金轉移到收款人的金融機構；
- 收款人的金融機構——接收資金並持有貸記帳戶的金融機構；和

其他/中間金融機構——可能需要執行交易的其他機構。



常用的支付形式包括：

SWIFT	全球銀行間金融電信協會（簡稱"SWIFT"）是成員所有制的資訊網路，用於使用標準化代碼的資金轉帳指令。 SWIFT是一個通信網路，一個國家的金融機構可以用它與其他國家的分支機搆或其他金融機構進行通信。SWIFT是一種用於資金轉帳指令的通訊系統，而不是一個財務結算系統。 大多數國際銀行間資訊都使用SWIFT網路。SWIFT將其消息分成一系列格式，稱為消息類型。每種消息類型表示一種交易或消息。消息類型分為十類：（MT0xx - 系統消息；MT1xx - 客戶支付和支票；MT2xx - 金融機構轉帳; MT3xx – 國債市場；MT4xx - 收款和現金運送單；MT5xx - 證券市場；MT6xx – 國債市場 - 金屬和聯合企業；MT7xx - 跟單信用證和擔保；MT8xx - 旅行支票；以及MT9xx - 現金管理和客戶狀態）。 SWIFT平均每天記錄2,840萬條FIN消息[5]。SWIFT每天在全球轉帳近5萬億美元，即每年1250萬億美元[6]。
CHIPS	結算所銀行間支付系統（"**CHIPS**"）是一種資金轉帳系統，為世界上一些規模最大，最活躍的銀行傳輸和結算美元付款訂單。 CHIPS平均每天傳輸和結算價值1.5萬億美元的446,000多條"付款消息"。它每天運行20個小時，並即時匹配銀行間的交易[7]。
Fedwire	Fedwire資金服務（"**Fedwire**"）是由12家美國聯邦儲備銀行共同擁有的即時全面結算系統[8]。付款人和收款人都必須在參與Fedwire的金融機構開立帳戶，轉帳是當天不可撤銷的付款。雖然參與機構都是美國的機構，但Fedwire可以用於國際轉帳中的美國的部分。 2016年，Fedwire平均每天交易量為590,209筆交易，相當於3.05萬億美元[9]。 Fedwire服務於美國東部時間（GMT – 5）工作日前一天晚上9點開始運營至晚上6點。
ACH	自動清算所（"**ACH**"）是一個由全國自動清算所協會（"**NACHA**"）運營的電子支付網路，該協會是一個由10,000多家金融機構支持的非營利會員協會。ACH轉帳包括直接存款，工資支付和消費支付（例如保險和抵押公司）。 ACH直接借記轉帳包括消費者支付保險費，抵押貸款和其他類型的帳單。ACH覆蓋美國，相當於歐洲的SEPA（單一歐元支付區），英國有三個類似的系統：BACS，CHAPS和Faster Payments。 ACH網路每年轉移43萬億美元和250億電子金融交易[10]。

金融機構根據交易的性質使用各種支付形式。在一些情況下，單個交易中可能使用多個支付方法。

5. *https://www.swift.com/about-us/swift-fin-traffic-figures (Date: 19 December 2017)*
6. *https://www.fincen.gov/sites/default/files/shared/Appendix_D.pdf*
7. *https://www.theclearinghouse.org/-/media/tch/pay%20co/chips/reports%20and%20guides/chips%20volume%20through%20november%202017.pdf?la=en (Date: 19 December 2017)*
8. *https://frbservices.org/serviceofferings/fedwire/fedwire_funds_service.html*
9. *https://www.federalreserve.gov/paymentsystems/fedfunds_ann.htm*
10. *https://www.nacha.org/ach-network/timeline (Date: 19 December 2017)*

3) 現行資金轉移過程中的資訊

在金融行業，雙方之間的交易通常被稱為協力廠商支付。也就是說，是金融機構代表各方（個人或實體）處理交易，而這些個人或實體本身不是金融機構。除了一些主要的例外情況，這些交易通常可以分為兩種主要類型：

- 根據金融機構知情的檔處理的交易，例如在貿易融資的情況下，一個或多個金融機構可以獲得信用證，擔保和/或其他一些資訊，如提貨單和其他運輸資訊。
- 沒有擁有此類檔的金融機構參與的交易。這些交易通常被稱為“單純支付”。絕大部分協力廠商支付都屬於這種類型，在這種情況下，處理付款的金融機構對相關交易的性質的可見度相對較低。在貿易融資領域，這種交易被稱為“記帳交易”。

可能包含在金融交易中的資訊分為兩類：

- 瞭解客戶（KYC）：KYC資訊通常包括身份資訊，如客戶的姓名，位址，帳號等。
- 瞭解交易（KYT）：KYT資訊包括交易類型（例如，交易是否涉及現金，外國電匯付款或支票）和資金的收款人（包括付款人在指示時報告的位址）詳細資訊以及交易記錄中包含的細節。

4) 行業監管與ivyKoin的相關性

在過去的50年中，資金轉移越來越電子化。隨著這種進步，以及隨之而來的交易量的增加，金融機構、執法機構和監管機構面臨著越來越多的打擊金融犯罪的複雜挑戰。世界各地的司法管轄區繼續強化反洗錢（AML）法律。由於幾乎所有國家都已採用並投入越來越多的資源來執行這些類型的法律，消費者和企業習慣于金融機構要求提供KYC資訊以便在開立新的金融帳戶或經手大額資金轉移的時候驗證客戶的身份。

a. 金融機構反洗錢

以美國為例，《銀行保密法》[11]和其他規定要求金融機構執行和遵守能夠充分察覺、調查和報告可疑活動的政策、程式和控制措施。這包括可能代表洗錢，逃稅或其他犯罪活動的交易。在世界各地的發達經濟體中，類似的要求也很普遍。

用於查探可疑活動的方法通常涉及按批量審查客戶最近活動的基於規則的自動化可疑活動監視平臺。這些規則或情景會標記特定交易或交易組，以供進一步分析。這種分析通常需要金融機構人員進行人工審查，進而將被標記的活動確認為“不可疑”，或將活動升級以供進一步審查，並可能隨後向執法機構報告。

此外，某些高風險客戶經常受到定期進行的盡職調查評估，這些評估涉及對客戶在一段時間內（例如最近6個月或12個月）進行的交易的深度分析。這些盡職調查審查與自動化交易監控檢測方法具有相似的目的，即瞭解相關活動的性質，這樣金融機構可以就保留客戶關係的風險和可接受性做出決策，對識別方的帳戶進行適當控制，並根據需要報告可疑活動。

對這一領域的監管預期是，金融機構能夠進行充分的盡職調查和分析，以確認客戶活動並不可疑，如有可疑則對該活動進一步分析並向執法部門報告。金融機構應根據所有可用資訊進行這些評估：如果有更多的資訊可以提供說明，那麼金融機構需要收集這些資訊，但採取的方式不應“驚動”任何人——包括客戶或相關方——使之察覺調查已經，或可能正在進行。

11. *https://www.occ.treas.gov/topics/compliance-bsa/bsa/index-bsa.html*

b. 反洗錢法的分歧

遵守反洗錢法要求銀行有足夠的資訊來促進，執行和支持其異常檢測計畫。加密貨幣及其固有的匿名性使銀行處於一種約束狀態，因為這些交易並非自然伴隨著銀行實施他們識別欺詐或非法活動所需的資訊。為了保護自己，銀行通常暫停含有源自加密貨幣相關交易的法定存款的帳戶，並拒絕接受加密貨幣作為合法交易媒介產生的收益或結算。這個決定的一個含義是，合法的企業無法從事涉及加密貨幣的交易，因為他們無法存入收益。

c. 更多資訊的好處

無論是調查自動化交易監控系統的警報時，還是在作為持續盡職調查一部分的活動評估期間，獲得更多隨時可用的資訊可以帶來明顯的好處。額外資訊可以說明調查人員或審查員更有效地確定活動性質（包括相關方）的適當性或合法性是否值得懷疑。

這些額外資訊可以說明金融機構確定客戶是否需要被歸類為高風險，或者該機構是否違反了反洗錢法規定的義務。在日常的良性活動中，這些資訊可以讓銀行更有效地將調查資源集中在其他客戶和他們的高風險活動上。

儘管傳統的支付方式通常嵌入了有限的資訊，但這些附加資料通常可以在金融機構關於指導客戶的KYC記錄中獲得，或者由客戶直接在交易指令中提供。

前一種類型的資訊可以包括例如客戶業務性質的描述，其地理中心，帳戶可能經歷的預期活動以及關於帳戶的相關方的資訊，諸如收款方的所有者和簽署人。交易本身（KYT）可以包括與支援檔相關的資訊，例如發票，信用票據，發貨檔和交易雙方的身份資訊（這些可能包括比發起人和收款人以外的各方，例如船運公司）。它還可以包括能夠證明交易合法的檔或證明檔的證據，例如由美國財政部外國資產管理辦公室或商務部工業和安全局頒發的許可證。

將這些資訊作為支援協定的一個方面嵌入到支付指令機制中，對於說明金融機構的審查人員形成一個關於相關活動性質的更全面和清晰的圖景，可能至關重要。通過讓KYC和KYT資訊更容易獲得並消除知識差距，金融機構可以將注意力集中在調查其他應該受到嚴格審查的情況。遺憾的是，金融技術方面的一些協議發展主要集中在互通性和速度上，將監管合規性視為會產生不便之處，推遲到部署完成後期階段予以解決，這意味著很少有實現全面解決方案的承諾。

3

ivyKoin機會
高度顛覆性的先進技術

加密貨幣的好處vs 現行金融系統顯而易見：

然而，目前大多數加密貨幣固有的匿名性與當前的金融體系不相容。

ivyKoin網路將使用基於區塊鏈的加密貨幣對支援交易的KYC，KYT和AML資料進行捕獲。它將主要針對與金融機構的交易，嵌入比現行支付網路更多的合規性和更多交易審計資訊。交易資料的提供將滿足金融機構和中間機構的嚴格要求。在實施時，ivyKoin網路將比現行金融系統和競爭的加密貨幣具有明顯的優勢。

ivyKoin尋求縮小目前全球金融體系與加密貨幣的出現之間的差距，將其定位為全球支付的未來。

1) 與現行金融系統的比較

在完全開發之後，ivyKoin網路和傳統支付網路的主要區別在於ivyKoin網路：

- 通過可信任的分散式ivyKoin網路，在安全實現加密貨幣付款轉帳的同時關聯KYC和KYT資料
- 將不可變更的參照資訊安全存儲在公共區塊鏈的交易資料中；
- 比傳統的支付方式在轉帳中嵌入更多的KYT資訊；
- 比傳統的支付方式在轉帳中嵌入更多的KYC資訊；
- 將能夠被集成到現有的銀行軟體中；
- 易於集成到會計軟體中，提高記帳效率；
- 向金融機構，會計師，公司經理等根據其要求的資訊提供KYC / KYT資料的可撤銷訪問。

對於KYC和KYT，常用的現行付款形式通常支持收集相對較少的資料點。下表列出了典型交易中包含的KYC / KYT資料點的大致數量：

	SWIFT	Fedwire	Chips	ACH
KYC和AML 資料點	10	17	9	10

注意：本公司不隸屬於SWIFT，CHIPS，ACH或Fedwire。所有資訊均按一般基礎提供，並基於公司研究時的可用資訊。

在實施時，ivyKoin網路將比現有的系統和流程更具描述性。根據所執行的金融交易的類型，ivyKoin網路將允許在交易消息中包含超過120個不同的KYT資料點和超過70個不同的KYC資料點。對這些資料點進行分類的一種簡單方法是根據它們可能出自的文檔來源。

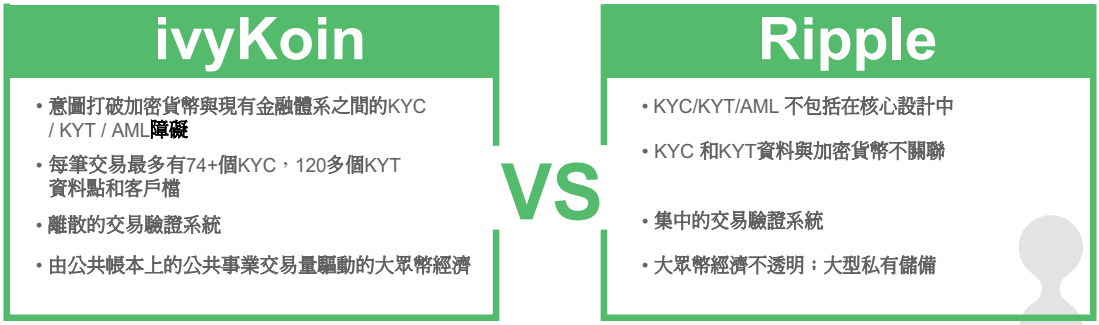
交易類型	資料點
核心交易資訊	74
其他方資訊	13
制裁聯繫	7
出口控制聯繫	7
發貨信息	21
商業發票	12
商業合同	17
審查證書	3
欠款單	10
催款單	10
配送建議	6
帳單	7
採購單	11

2) 與競爭加密貨幣的比較

代幣在充分發展的情況下，將成為一種具有以下幾個顯著特點和優勢的加密貨幣：

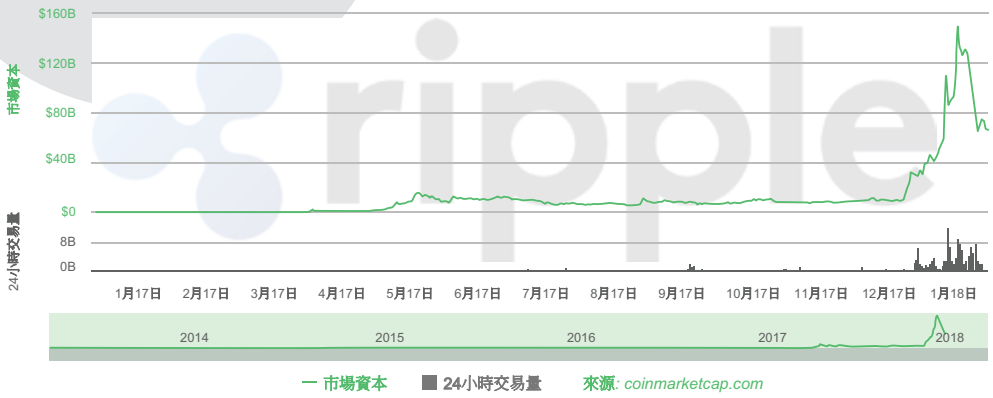
特點	描述	好處
可識別	ivyKoin網路和相關交易能將KYC / KYT / AML資料清晰整合到加密貨幣交易流程中 。	當事人的和交易的目的合法性很容易理解，並便於用於判決有關付款和存款的決定 。
可轉移	代幣作為一種加密貨幣存在，可以在公共區塊鏈上自由交易，而不會阻止金融機構和中間機構所需的相關的KYC / KYT / AML相關資訊 。	代幣的實用性便於各方可以輕鬆使用和交換，可以誠實反映其價值並取消ivyKoin.com和加密貨幣作為加密貨幣價值的唯一決定因素 。
不可偽造	ivyKoin網路交易和支援資料將有助於區塊鏈架構的使用，從而強化分配和交易資料的不變性 。	ivyKoin網路的使用者將被確保交易完整性和資料安全性，進而確保交易和支援與現金流動有關決定的資料的持久性 。
限量供應	代幣將以已知數量發行，並具有已知的初始分佈和分配 。	公共交易從與錢幣稀缺相關的經濟中受益，其中私有網路的流動準確反映了網路內貨幣流動性和流動速度 。
根據要求去匿名化	所收集的所有資料在由金融機構和仲介機構組成的私人清算網路上得到持續的保護，運輸和追蹤 。	符合資格方擁有他們在KYC / KYT / AML功能上所需的資訊 。在不影響資料的基礎安全的情況下，可以添加或移除各方 。

ivyKoin網路經充分開發後預計將比我們領先的競爭加密貨幣Ripple具有更顯著的優勢 。



具體來說，相比Ripple，ivyKoin網路是專門的去中心化驗證人網路，由金融機構和中間機構組成，他們使用代幣來溝通KYC / KYT / AML資料以及在網路上結算餘額。合規性和審計是ivyKoin網路的首要關注點。涉及代幣的交易將根據公共乙太坊網路上列出的合約被發起，使用的代幣由於能夠實現在金融機構以法定貨幣向匯款接收人支付款項而可以輕鬆被交易。這與使用XRP（核心Ripple貨幣）有很大不同，因為該貨幣除了作為交易媒介外幾乎沒有公共用途。

市場潛力得到公認。Ripple是比特幣後最大[12]的加密貨幣之一。



Ripple代幣在2017年間增值超過 28,000%。

http://fortune.com/2017/12/29/ripple-cryptocurrency-surge/

*** 參考日期2018年1月14日　　**根據籌集1500萬美元計算**

12. *https://coinmarketcap.com/ as at 14 January 2018*

4

我們的世界級一流團隊
擁有成功的記錄

公司由一支有成功記錄的世界級團隊領導。公司經驗豐富的管理團隊還有全球諮詢委員會的支持，委員會在所有專案成功所必要的垂直領域擁有無與倫比的行業知識和網路。

有關團隊的資訊，請訪問 **www.ivykoin.com.**

5

ivyKoin 運營明細

1) 運營平臺概況

a. 基本功能

我們對ivyKoin網路的設想是為最終用戶提供以下功能。該功能可通過桌面/網頁和移動體驗傳遞給其附屬成員：

發送人和接收人：

- 購買或出售代幣；
- 查看通用加密貨幣的加密貨幣兌換可能性和匯率；
- 估計網路費用並接收使用的代幣的報價；
- 查看金融機構和金融中間機構平均時間進行交易結算；和
- 查看有關個人身份資訊的KYC資料訪問日誌（針對發送人）

金融機構和金融中間機構

- 維護企業帳戶和身份資訊；
- 管理組織成員的帳戶訪問設置；和
- 查看代幣資料容器內容和訪問歷史

除上述基本功能外，公司計畫在適當的時候將以下特點、功能和解決方案整合到ivyKoin網路中：

b. 對等加密貨幣到法定貨幣網路

儘管ivyKoin網路的初始用途主要是提供企業對企業的交易，但對能夠讓個人輕鬆發送、接收和管理加密貨幣並輕鬆將其轉換為法定貨幣的簡化的支付網路也存在強大的需求。

c. 軟體集成

公司將尋求與現有的銀行軟體集成，以便KYT和KYC在各銀行系統內能夠自動分配到正確位置。

公司還打算與主要會計軟體系統集成。客戶的支付和收據（包括發票詳細資訊）的輕鬆集成將使交易資料可以直接載入到會計軟體中，從而減少客戶的管理負擔。

d. 收銀和轉換服務

公司擬發展收銀服務及轉換服務。收銀服務可以促使：

- 從銀行帳戶中提取法定貨幣並將其轉換成加密貨幣；和
- 將加密貨幣轉換回法定貨幣並將其存入銀行帳戶。

兌換服務將允許客戶將代幣轉換為一系列其他加密貨幣 。

通過提供收銀和兌換服務，公司計畫將ivyKoin網路作為一個端到端的解決方案，特別針對大額轉帳的企業 。本公司將努力：

- 促進將法幣兌換成加密貨幣；
- 促進加密貨幣在全球的轉移；和
- 使收款人能夠將加密貨幣兌換回在其銀行帳戶中的法定貨幣 。

最重要的是，根據預想，ivyKoin網路能夠在不對發送或接收金融機構造成問題的情況下做到這一點 。

e. 通過公開市場操作的固定價格轉移

加密貨幣轉移過程中潛在的貨幣損失是商家採用加密貨幣通常面臨的最大障礙之一 。公司的目標是開發一個固定價格的解決方案，消除由於加密貨幣價格波動造成的貨幣損失 。

固定價格解決方案包括使用一個國庫幣池專門用於兩個銀行帳戶間的法定美元到法定美元的交易 。通過ODFI（“原始存款金融機構”）從發送人銀行帳戶中提取法定貨幣 。然後，ivyKoin網路將使用專門為此目的而設計的場外貨幣庫來將法定貨幣轉換為代幣（**參見第7節**）。

2) 金融機構

隨著金融機構支援的增加，ivyKoin網路有可能用於以下交易，還有更多：

- 國內或國際貨物採購；
- 企業對企業服務；
- 註定要成為金融機構中法定貨幣的一般價值轉移；
- 軟體許可證購買；
- 房地產購買；
- 全球投資；
- 大額個人轉帳；
- 小額個人轉帳 。

3) 用戶功能

根據建議，ivyKoin網路將提供一個對等方之間的價值交換，其中（1）發送方試圖向接收方發送大量的加密電子錢，和（2）接收方收到該加密電子錢並使其成為銀行帳戶中的法定貨幣餘額 。

發送人和接收人都可以使用代幣將加密貨幣通過ivyKoin網路轉移到金融機構，加密貨幣可以在ivyKoin.com和主要公開交易所購買 。希望通過ivyKoin網路轉移其他加密貨幣的帳戶持有人必須先將協力廠商加密貨幣轉換成代幣 。

使用者可以通過電話或移動設備訪問ivyKoin.com，網站將為發送人提供以下核心功能：

- 帳戶開設和管理；
- 交易管理；和
- 代幣購買，銷售和轉帳

a. 帳戶開設和管理

我們預計，發送人和接收人將能夠在ivykoin.com上創建ivyKoin網路帳戶，並在註冊過程後收到獨有的發送人身份資訊。ivyKoin網路將保存所有發送人的帳號資訊，以便他們不必為後續的轉帳提供相同資訊。這個KYC信息由代表使用者身份的各種資料欄位和檔組成，例如姓名，電子郵件，電話，位址和政府身份。

完全開發後，帳戶將能夠通過 ivyKoin.com上的線上功能功能表進行管理，包括更新KYC和重複交易資料。帳戶持有人可以要求連接到其他ivyKoin網路帳戶持有人，並擴充已知和經過驗證的加密貨幣付款對端名單，這在向相同接收人頻繁發送或向新接收人快速高效發送時很有用。帳戶持有人可以在全球範圍內的ivyKoin網路上讓自己可見，並且一個帳戶持有人可以提出請求將其他帳戶持有人添加到他們自己的名單中。他們也可以使用ivyKoin網路服務轉換代幣並將其發送到自己在金融機構的法定貨幣帳戶。

i. 發送人資料驗證

ivyKoin網路意圖是將驗證基本發送人資料和銀行帳戶的合法性作為開戶流程的一部分。ivyKoin網路將使用各種協力廠商服務提供初始身份證件驗證。身份證明檔，如護照和駕駛執照預計會在幾分鐘內完成驗證。如果檔未被識別，則該帳戶將被置於待定狀態以供進一步調查。同樣，營業執照和其他註冊公司檔也能夠被迅速驗證。

為了達到同樣目的，我們打算使用一個程式來驗證帳戶持有人的銀行帳戶資訊，在這個程式裡小額存款會被存入帳戶持有人的銀行帳戶，這些存款金額將被用於獨立驗證ivyKoin網路與銀行之間的成功連接。

儘管做出了這些努力，但公司對付款的合法性或非法性不承擔任何擔保責任，儘管這種做法與現行網路非常相似。

a. 交易管理

一旦ivyKoin網路帳戶開立成功，我們預計發送人就能開始將代幣轉帳給收件人。發送人將在交易之前將特定的交易資訊輸入到帳戶中。ivyKoin網路將要求為所有轉移提供基礎級別的資訊，但根據適用的法律和法規不同可能會需要額外細節。ivyKoin網路將提示發送人提供與其交易相關的其他細節。例如，如果發送人正在進行付款以換取商品，則ivyKoin網路嵌入的轉移資訊可能包括產地，最終目的地，已支付進口關稅證明或其他識別資訊。發送人還可以選擇提供有關轉帳的其他詳細資訊 - 例如付款附帶的發票副本。此外，如果發送人知道接收人不將其視為可信來源，則還可以添加品質保證證書，批量資訊，公司章程以及其他廣泛的自願性KYT資訊等資訊。

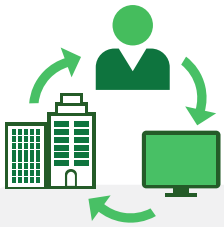
b. ivyKoin的購買，銷售和轉帳

我們預計，ivyKoin網路將促進資金和資料的安全傳輸，為發送人和金融機構帶來共同的利益。當銀行正在審查交易是否存在可以活動時，將擁有比傳統支付網路和更現代的支付轉帳替代方案更龐大的資料點來協助審查。

付款價值將可以在區塊鏈中公開查看，並且不能被刪除。KYT和KYC資料將被加密並捆綁到由發送者發送給ivyKoin網路的代幣，隨後可由接收機構和接收人訪問。此KYC / KYT / AML資料只能由交易相關方查看。

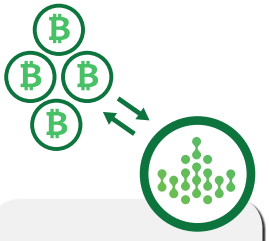
下面的圖表從發送人，接收人和金融機構的角度描述了代幣的預期流動。使用者介面簡單直觀。

ivyKoin轉換為美元的功能流程圖



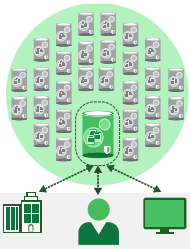
發送人通知接收人有意通過ivyKoin和ivyKoin網路將BTC付款給接收人。發送人和接收人訪問ivyKoin.com建立帳戶，提供KYC資料。

發送人提供必要的KYT資料，包括銀行要求的交易類型和檔以及接收人的監管管轄。



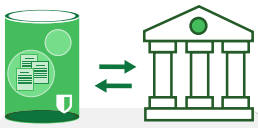
發送人在ivyKoin.com上交換已接受的密碼加上等價的ivyKoin所需的任何費用。寄件者鎖定ivyKoin最低價格來執行交易。

發送人確認發送給接收人的ivyKoin金額，並承諾發送。KYC / KYT資訊綁定到ivyKoin，並保存在ivyKoin資料容器中，同時存儲在私人分散式清算網路中。

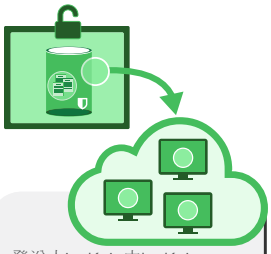


ivyKoin資料容器被轉發到ivyKoin私有網路進行後續的審查和處理。資料可供發送人，接收人和接收人金融機構查看。

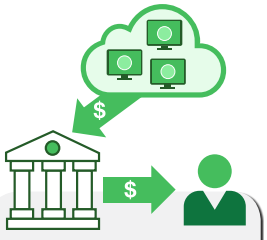
發送人的ivyKoin被託管，直到接收人金融機構批准交易。銀行為知名的發送人和接收人設立的自動接受標準可能有助於立即批准。ivyKoin在託管期間不可供發送人使用。



接收人的金融機構審查交易並批准。（如果交易被拒絕，ivyKoin將返回給發送人。）



發送人ivyKoin由IvyKoin Network兌換



發送人ivyKoin由ivyKoin Network兌換，轉換為美元並立即存入接收人金融機構。接收人金融機構在接收人帳戶中提供美元資金。

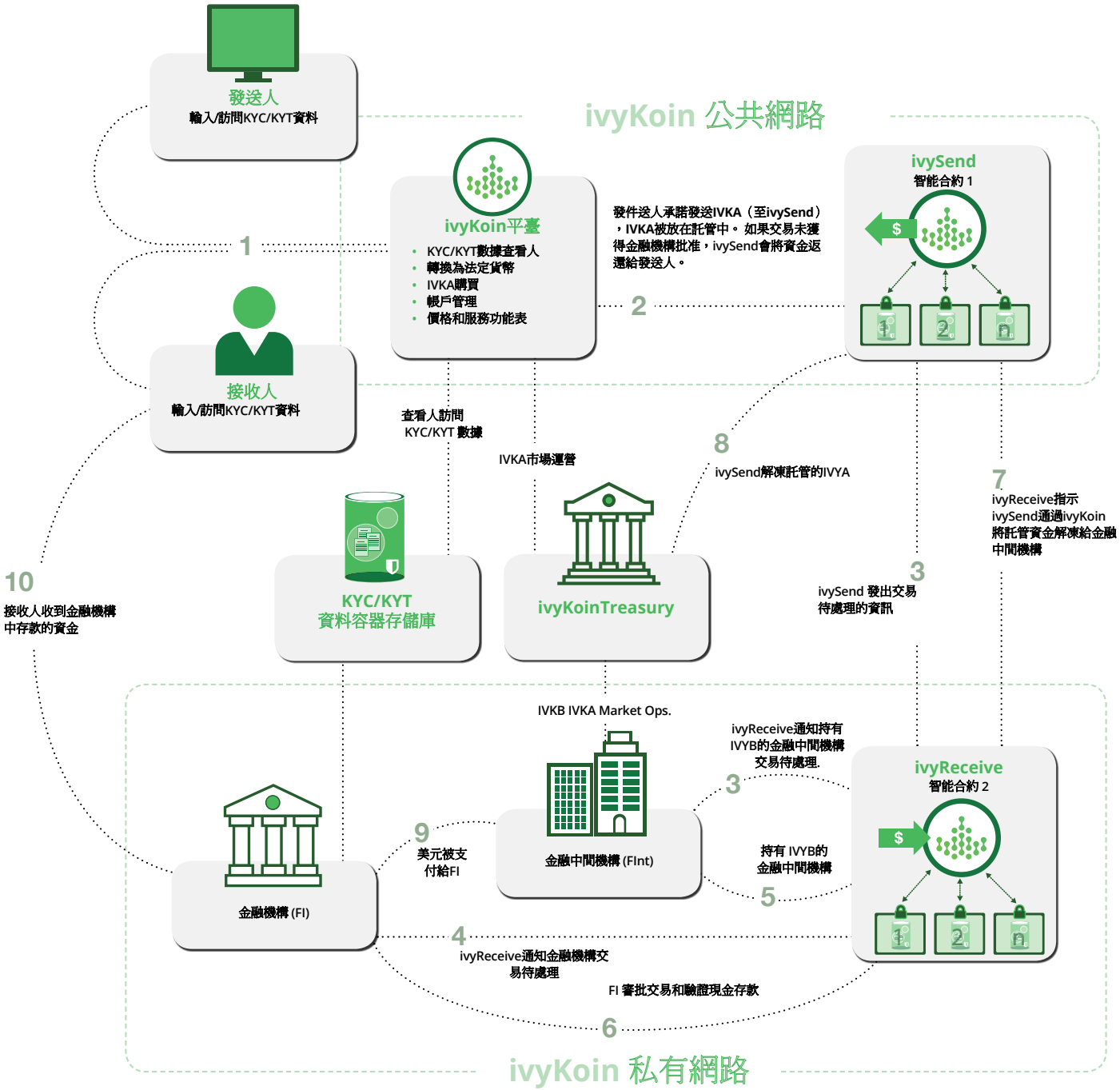
生成交易記錄並將其提供給發送人，接收人和接收人的金融機構。如果交易未獲批准，則發送人帳戶中的資金可供今後活動使用。

6

ivyKoin技術規格

1) 運營平臺概況

我們的意圖是ivyKoin網路將通過使用雙重網路架構來運行，其中代幣的發送者在公共網路（**ivyKoin公共網路**）上操作，向法定貨幣提供財務結算的參與者在私人網路（**ivyKoin 私有網路**）上操作。支援交易的KYC / KYT / AML資料將被捕獲到由ivyKoin公共網路與ivyKoin網路智慧合約交互產生的加密容器中，並且支援ivyKoin私有網路參與者實現交易結算的活動。這些資料將被儲存並提供給金融機構和法定結餘收款人的監管機構訪問。以下技術規格在充分開發時預計將各自都成為ivyKoin網路的一部分


發送人
輸入/訪問KYC/KYT資料
ivyKoin 公共網路
ivyKoin平臺
KYC/KYT數據查看人
轉換為法定貨幣
IVKA購買
帳戶管理
價格和服務功能表
發件送人承諾發送IVKA（至ivySend）
，IVKA被放在託管中。 如果交易未獲
得金融機構批准，ivySend會將資金返
還給發送人。
ivySend
智能合約 1
1
2
接收人
輸入/訪問KYC/KYT資料
查看人訪問
KYC/KYT 數據
IVKA市場運營
8
ivySend解凍託管的IVYA
7
ivyReceive指示
ivySend通過ivyKoin
將託管資金解凍給金融
中間機構
10
接收人收到金融機構
中存款的資金
KYC/KYT
資料容器存儲庫
ivyKoinTreasury
3
ivySend 發出交易
待處理的資訊
IVKB IVKA Market Ops.
ivyReceive通知持有
IVYB的金融中間機構
交易待處理.
3
ivyReceive
智能合約 2
9
美元被支
付給FI
金融中間機構 (FInt)
持有 IVYB的
金融中間機構
5
金融機構 (FI)
4
ivyReceive通知金融機構交
易待處理
FI 審批交易和驗證現金存款
6
ivyKoin 私有網路

a. 公共網路，ivySend和公共ivyKoin代幣(IVYA)

一旦ivyKoin網路投入使用，預計尋求將協力廠商電子錢發送給預期接收人帳戶的公共方必須在公開交易所中將其加密貨幣兌換成代幣，或直接從ivyKoin網路購買代幣。ivyKoin公共網路代幣（**IVYA**）將被編寫進乙太坊網路上可用的ERC20規範。代幣將被提交給乙太坊上的ivyKoin網路合同（**ivySend合同**），並在那裡被託管。託管狀態在以下兩個條件下被視為完成：a）轉帳完成，此時代幣轉移到ivyKoin網路，在二級市場或公司網站上出售，用於獲取現金或協力廠商加密貨幣，或者以其他形式燃燒；或者b）轉帳失敗，在這種情況下，向ivyKoin網路提交的全部代幣都會被退還。

預計ivySend合同將成為一個智慧合約，可以由任意數量的利益方從公共乙太坊網路調用。在初步實施時，很可能通過ivyKoin.com介面，通過網站與乙太坊網路的直接整合來提供。另外我們還設想，其他各方同樣會將此合同作為支付介面。ivySend合同意圖使用乙太坊網路開採成本激勵措施進行操作，發送人必須承擔合同的發起費用才能讓合同在乙太坊網路上進行處理。如果提交的開採成本不足以開採公共激勵，則託管合同將永不生效，保證發送人的ivyKoin網路帳戶餘額，從而可以繼續交易的其餘部分。ivyKoin網路費用也包含在ivySend合同流程的成本中（就像傳統金融機構的電匯一樣）。

我們預計，尋求使用ivyKoin網路的一方可以使用公司的網站輕鬆查看a）在各種常見的加密貨幣交易所中通用的加密貨幣到代幣匯率；b）成功執行ivySend合同預計的乙太坊開採成本收費；以及c）希望發送給預定接收人帳戶的給定法定貨幣餘額的總代幣費（法定貨幣餘額+開採成本費+傭金）。由於其中一些組成部分在總體定價中是不穩定的，通過使用公司網站，ivySend合同的用戶可以在10分鐘內收到執行報價，報價會鎖定含所報參數的給定ivySend合同交易的執行報價在ivyKoin網路表示的在給出報價時的波動上限和下限內。

通過這種方式，IVYA在完全開發後，將為其持有者提供全面的實用功能，並保護其不受合同操作時波動的影響。

b. 私有網路，ivyReceive,和私有ivyKoin 代幣(IVYB)

ivyKoin私人網路意圖通過使用私人ivyNetwork合同（**ivyReceive合同**）將資金分配到預期收款人的銀行帳戶。我們建議ivyKoin私有網路使用專用于金融機構和中間機構協調的乙太坊區塊鏈的私有鏈形式操作。

預計ivyReceive合同將託管在ivyKoin私有網路上。這將是參與金融機構和中間機構的結算帳戶通過使用私有代幣（**IVYB**）參與風險的機制，該私有代幣將是一個與乙太坊相容的ERC20代幣，在ivyKoin私有網路上運行。ivyReceive合同的目的是規定ivyKoin網路如何使用IVYB直接結算收款人帳戶的餘額。

在充分開發後，IVYB預計將成為資產支持的代幣，反映了ivyKoin私有網路帳戶持有人擁有可以將交易清算到ivyKoin網路的法定貨幣儲備金。IVYB將由本公司預先開採，只能由公司轉換為IVYA，並按照其在ivyKoin網路中的儲備比例交給ivyKoin網路帳戶持有人。至於公司對IVYB的使用方面，公司意圖對IVYB資產及負債進行公開會計處理，以顯示其在網路上的美元存款總是等於其託管和儲備的代幣持有量。

當待處理交易的資訊到達ivyKoin私有網路時，帳戶持有者必須以其IVYB押注，以獲得代表餘額的機會；這意味著ivyKoin私有網路帳戶持有人必須擁有至少等於交易金額的IVYB餘額。在這種交互中，押注代幣的過程為向金融機構或中間機構發佈KYC / KYT / AML資訊提供了支援，從中提示他們接受或拒絕資金（手動，或經預先授權自動）。這些代幣被提交給ivyReceive合同。ivyReceive合同有兩個強制放棄押注代幣的條件：

a) 顯示交易批准證明——在審查了適用的KYC / KYT / AML資訊後，適用金融機構的代理人會將批准或拒絕回復的資訊發送給ivyReceive合同。在這種情況下，有兩個可能的結果：

交易成功完成，在這種情況下，IVYB被退回，並由ivyKoin私有網路帳戶持有人在金融機構內預定接收人帳戶中存入IVYB值；或者，b）交易失敗，在這種情況下，IVYB退還給金融機構；和

b）顯示現金存款——對ivyKoin私有網路帳戶持有人銀行帳戶狀態的監控提供了一種機制，通過該機制，金融機構顯示對收款人帳戶的現金存款的已經發生。此狀態可能需要為觀察帳戶狀態進行定制集成，或使用來自供應商（如Yodlee[13]，Xignite[14]或Plaid[15]）的帳戶訪問服務進行類似操作。無論哪種方式，ivyKoin網路和金融機構之間的企業對企業的安排將規定帳戶之間資金解凍的時間限制是什麼。

如果“顯示交易批准”和“顯示現金存款”都顯示為正確，那麼在ivyKoin私人網路絡上押注IVYB的一方有資格從ivyKoin公共網路上解鎖的ivySend合同中接收付款。如果兩個條件都是錯誤的，或者在它們被設置為正確之前，ivyKoin公共網路上的ivySend合同可以由發送人來贖回。金融機構可能會拒絕批准交易，因為它試圖通過使用與ivyKoin資料容器一起提交的KYC / KYT / AML資料來清理已識別的合規要求。使用與交易和容器相關聯的中繼資料，有可能基於產地，商業中交換貨物的性質或經手金融機構或中間機構所期望的其他可配置規則來實現一定程度的自動清算。同樣，手動工作流程可能需要託管被額外保留一段時間。提交的默認行為是由發送人託管由ivyKoin私有網路上的結果決定；然而，可以設想的是，與銀行KYC / KYT / AML過程帶來的延遲以及發送者與接收者之間的通信也可能需要被適當考慮，由此在給定的延遲期之後，發送者可以通過選擇將代幣存款從託管中取出來結束這一過程。

我們的意圖是讓ivyReceive合同保持所有待處理的押注交易的可觀察餘額。IvyKoin私有網路上的許可提供了個人餘額間的獨立以及每個接收人金融機構和支持金融中間機構的待處理的結算工作流程狀態。通過這種方式，被鎖定在ivyReceive合同中的私有代幣是為了：a）提供對金融機構或中間機構考慮餘額轉移有效性的過程的可見性；b）為金融機構的業務提供一個節流閥，這樣如果沒有將交易清算到滿意的程度，他們就無法押注不成比例的交易金額。當然，這也提出了什麼迫使金融機構或中間機構根據需要進行存款的問題。為此，ivyKoin網路將能夠報告其網路中每個金融機構和中間機構的服務水準。顯然，如果一家金融機構沒有滿足客戶的需求，那麼客戶應該有能力從ivyKoin網路的其他參與者那裡考慮其他的選擇或機會，這些參與者在接收轉帳時要麼更及時，要麼更可靠。

c. 跨鏈通信和ivyKoin Oracle服務

ivyKoin網路旨在充當上述ivyKoin私有網路和ivyKoin公共網路之間的功能媒介，傾聽和回應與ivySend合同和ivyReceive合同相關的事件。

我們預計，ivySend合約的狀態變化會被參與公共乙太坊網路的授權ivyKoin驗證人觀察到。同樣，ivyKoin私有網路上的ivyKoin網路驗證人也會觀察到ivyReceive合同中的狀態更改。這兩個驗證人組合都能夠通知ivyKoin Oracle服務，該服務提供對每個託管合同狀態的認證，並有助於實現它們各自的功能。

特別讓人感興趣的是價值如何從ivyKoin公共網路分類帳餘額轉移到ivyKoin私有網路分類帳餘額。這涉及從IVYA到IVYB的價值轉移，在向ivyReceive合同發送批准消息和顯示接收人銀行帳戶到賬餘額時發生。在這兩個事件發生的時候，IVYB被釋放，而託管協定中的IVYA由ivyKoin網路要求解凍。IVYA通過使用ivyKoin Oracle服務及其中含有的對ivyKoin私有網路的驗證工具收到ivyKoin私有網路分類帳上對IVYB交易的確定。當IVYB被記入ivyReceive合同時，發送人給IVYB的公共位址將被記錄。此公開位址用於將KYC / AML資訊發送到ivyKoin交易容器。隨後，此位址將用作ivyKoin網路的結算帳戶位址，以私下結算其針對網路的交易。

13. *https://www.yodlee.com/*
14. *https://www.xignite.com/*
15. *https://www.plaid.com/*

2) 在ivyKoin網路上的身份

充分開發後，預計公司將管理ivyKoin網路上的兩種身份：發送人身份，以及金融機構和中間機構身份。

a. 發送人身份

ivyKoin 網路意圖要求寄件者在發送貨幣前在網路註冊。ivyKoin網路認為，作為開設帳戶的一部分，接收人的身份應分別由金融機構和中間機構確定。

自主權身份就足夠在ivyKoin網路上建立一個發送者帳號：然而，想要獲得ivyKoin網路授權可能需要額外的交易資訊。此資訊由發送人提交並存儲在ivyKoin網路上以建立帳戶，並允許公司為需要支援資訊的特定交易類型提供證明。發送人自主權身份資訊副本將打包在ivyKoin資料容器中，作為向預期餘額接收方金融機構和其他中間機構提交交易一部分。雖然他們的用途有具體限制，這些憑證可能會被訪問並且在交易之後一段延長時間內關聯。使用公司的網站可以持續監控這些憑證的存取時間。

b. 金融機構與中間機構身份

ivyKoin的意圖是依賴在資料通信的金融機構和中間機構的良好雇傭實踐和資訊安全實踐的警惕。想要公司跟蹤所有雇傭事件，企業和人力資源相關活動在很大程度上是不切實際的。因此，ivyKoin網路將要求金融機構，仲介機構和利益機構的相關合規人員的身份在ivyKoin網路註冊，以啟用和禁用對KYC / AML資料分散式容器的訪問。金融中間機構的相關就業行為將在ivyKoin網路及時更新。

預計金融機構經理可以登錄到ivyKoin網路來管理相關工作人員對ivyReceive合同職能和容器資料的訪問和許可權。所識別用戶的所有活動都可以集中進行跟蹤和管理，單個交易容器的歷史記錄也可以被查看。

3) 區塊鏈技術應用

分散式帳本的共識是驗證人（有時也稱為礦工）根據適當情況確定資料的準確表示以反映提交給網路的交易中正確分類帳餘額的功能。考慮到網路和系統中斷的可能，很容易預見到有些情況可能導致某些方斷開連接，並在意外缺席時錯過重要資料。

同樣，在一個分享觀點的網路中，需要建立一個確定的事實結果產生的成熟機制。在比特幣和乙太坊這樣的網路中，目前的機制被稱為“工作證明”。工作證明鼓勵驗證人根據計算能力和電力進行競爭，以驗證提交給網路的交易。擁有更多計算能力有助於驗證人解決更難的加密問題，這些問題隨後提交給網路，以便搶先將捕獲交易作為區塊添加到網路中（順便一提，這些交易區塊是根據之前提交的其他區塊的預測進行驗證的，鏈條因此產生——因此術語稱為“區塊鏈”）。隨著區塊鏈的壯大，新區塊的難度也隨之增加——驗證人為了驗證激勵和區塊獎勵的價值而花費巨大的代價進行競爭，他們希望在他們所在網路中捕獲和重新分配這些獎勵。在提供拜占庭容錯的概念的同時，這個過程對於私有網路而言既昂貴又緩慢。因此，這就是比特幣和乙太坊每秒處理少於20筆交易的原因[16]。另外，由Tendermint實施並提出的共識機制“權益證明”是對乙太坊的Casper共識的改進，將獲得添加分類帳交易區塊的權利的費用從計算和電力投資轉向了對加密貨幣本身的投資[17]。在權益證明中，擁有更多加密貨幣比例的一方在添加下一個交易區塊上也有更多比例的可能。由於每個驗證任都在網路中“押注”，網路可能由於他們的惡意行為收回他們在網路中的權益來對他們進行懲罰，這些惡意行為會導致產生虛假交易區塊的產生，這就需要網路的其餘部分進行後續校正。然而，這種方法會帶來挑戰主要有兩個原因：a）任何一方或擁有51%網路價值的串謀方更有可能獲得共識；和b）通過計算能力的投資，惡意的大多數不能被推翻，因為工作證明是允許的。此外，正如工作證明需要驗證激勵措施來使驗證者以區塊獎勵的形式捕獲交易，權益證明同樣使用激勵措施（例如“開採成本”）來防止只為網路創造工作而沒有相應財務價值的交易的提交（例如：垃圾信息）[18]

16. *http://www.altcointoday.com/bitcoin-ethereum-vs-visa-paypal-transactions-per-second/*
17. *CIT*
18. 在公共場所，潛在的垃圾資訊交易可能湧入合法交易，造成類似於拒絕服務攻擊中存在的環境；如果驗證人正在為無價值交易消耗精力，那麼有價值的交易處理起來就會更難。

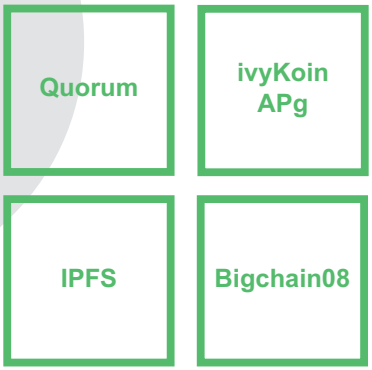
在金融支付網路中，特別是私人和被許可的網路相比公共匿名網路更容易通過利益分享而被組織和管理，因此調整激勵措施以防止可疑行為的問題會導致對實際輸送量和能夠促進準確和合規結算的協調功能的靈活性的擔憂。包括Stellar和Ripple在內的網路使用他們自己的驗證人，或者驗證人的共同參與來遮罩他們對網路結果的直接輸入[19]，因此就不太可能出現外部和惡意參與者。在這裡，他們的共識是通過他們的網路關注分散式帳本的靈活性和可用性。結果是輸送量更高[20]。

公司設想，ivyKoin私有網路將由除本身之外的實體贊助的驗證節點組成。ivyKoin私有網路將直接由獨立但有序的金融機構和中間機構進行驗證。在這種環境下，來自被許可的網路參與者的垃圾資訊幾乎不太可能，甚至首先就對他們參與ivyKoin網路的共同目標有害。網路垃圾可能性大大降低和激勵機制的調整，消除了通常用於激勵公共區塊鏈網路的區塊獎勵的需要。至於共識，使用計畫的拜占庭容錯演算法（如伊斯坦堡BFT）是最有意義的。[21]在這種共識演算法中，每個參與者都以預定的輪詢調度方式創建區塊，並將其結果提交給網路的其餘部分，必須有2/3的多數表決才能批准領導者的區塊計算。這種方法可以在網路中大約1/3的驗證人可能被證明是惡意的同時仍然證明網路的靈活性。伊斯坦堡BFT的具體基準表明其能夠每秒處理約1000次交易，[22]這反映了今天在FedWire，SWIFT和ACH之間發生的跨部門交易網路的總和。[23]

就其目的而言，我們預計，ivyKoin私有網路最初將採用Quorum，JP摩根大通實施的使用伊斯坦堡BFT共識演算法的經許可的乙太坊。[24]乙太坊的實施對於ivyKoin網路有許多潛在的好處： a）它提供了在全球金融機構範圍內驗證和改進的乙太坊區塊鏈好處；b）它提供了與智慧合約開發和投資的互通性，可以將其原型化，並可以移植到任何其他乙太坊虛擬機器（EVM）支援環境（包括Ethermint，Qtum，甚至是公共乙太坊區塊鏈）；[25,26] 和c）因為是被人熟知的金融界另類區塊鏈，其採用和使用提供了社區和支援的基線，最有可能獲得公司尋求支援其網路功能的同樣的金融機構和中間機構的支持。Quorum還支持基於主要驗證人授權的替代共識演算法，如果需要更高的交易輸送量，網路參與者的意圖的穩定性能夠減少區塊驗證開銷。

19. *CIT* - 恒星分片
20. *CIT*
21. 拜占庭容錯或（BFT）是電腦科學中解決分散式系統網路內協調問題的一個問題參考，通常稱為拜占庭將軍問題，在這個問題中，任何留在自己的設備上的單個系統參與者都被激勵為自己的利益而工作，而不是網路的真實利益。
22. *https://www.slideshare.net/YuTeLin1/istanbul-bft*
23. *CIT*
24. *https://github.com/jpmorganchase/quorum*
25. *CIT [Ethermint* 白皮書*]*
26. *CIT* [白皮書]

私有網路節點使用IPFS和BigchainDB進一步協調資料交換，以確保可用性和資料完整性. [27,28]私有網路節點的邏輯表示如下圖所示：



ivyKoin 私有網路節點概念圖

4) ivyKoin數據容器

預計ivyKoin網路將使用dxChain加密容器將KYT / KYC / AML資料存儲在日期容器（**ivyKoin資料容器**）中 。資料在使用者提交貨幣轉帳請求時通過ivyKoin應用介面被收集 。ivyKoin資料容器的這種特定容器格式如下圖所示：

ivyKoin 數據容器

ivyKoin資料容器的內容意圖涵蓋：

- 容器中繼資料
- 交易中繼資料
- 提交的交易明細
- 發送人身份資訊（如適用）
- 支援性檔和附件

使用這種格式，支援資料的每個組成部分都是獨立和持久加密的，以便在使用標準AES-256對稱加密和4096位RSA非對稱加密方法以及SHA-384消息摘要進行交換期間能夠安全訪問 。預計基於RSA非對稱金鑰的數位簽章易受Grover[29]和Schor[30]演算法對應用量子計算來確定黑盒函數輸入和大數分解上的影響，在行業有更好的理解並能提供更好支援的情況下，這些演算法將分別升級以反映量子抵抗演算法的可用性 。[31]

27. https://ipfs.io
28. https://www.bigchaindb.com
29. https://en.wikipedia.org/wiki/Grover's_algorithm

加密容器意圖為ivyKoin網路提供幾個關鍵特性：

- 提供持續控制和保護所有溝通資訊；
- 讓ivyKoin網路能夠在首次接收之後將各方添加到容器中或從容器中移除；和
- 為發送人提供保證，其與接收人交易的具體內容是保密的。

通過使用ivyKoin資料容器，可以跟蹤和驗證針對網路的個人行為。

ivyKoin資料容器意圖存儲從ivySend合同提交過程中收集的結構化和非結構化內容。在適用的情況下，ivyKoin會將ivyKoin資料容器內的資料收集標準化，以符合ISO 20022標準的資料集，代碼和格式。[32]

a. ivyKoin資料容器的生成和存儲

充分開發後，向ivyKoin網路合同提交內容時，會向ivyKoin網路發出請求以生成相關資料的容器。這項應用會將提交的KYT / KYC / AML資料發送到ivyKoin網路，並將容器標誌符返回給發送人。發送人將他們的ivyKoin存款和生成的容器標誌符提交給ivySend網路合同。

生成後，ivyKoin資料容器將被保留在託管於ivyKoin私有網路範圍內的IPFS檔案系統上。ivyKoin私有網路檔案系統將允許共用網路中的相關內容。[33]為確保檔有餘，容器對ivyKoin私有網路會有三個獨立寫入，因為在請求時只能保證提供本機複本。這些容器標誌符和ivyKoin私有網路上的物件標誌點的映射存儲在ivyKoin私有網路節點之間共用的BigchainDB網路中。[34]

檢索ivyKoin資料容器包括通過生成容器的容器標誌符來查詢BigchainDB網路，以接收用於檢索相關容器的相關物件標誌符。在ivyKoin網路中，該功能由被許可的網路上的託管服務被抽象化和維護。ivyKoin資料容器可以自由複製和存儲，而不會違反其基礎安全模型。

b. 訪問ivyKoin 資料容器

我們的意圖是讓訪問ivyKoin資料容器由網路綁定的訪問管理服務管理，該服務負責處理對ivyKoin資料容器內容特定部分的請求，並根據以下標準提供必要的存取權限（用於簡化，使用者，系統和系統進程的目的被視為使用者請求）

a) 請求得使用者組織——確定KYC資料是否與請求使用者組織發生的交易相關，或者，如果請求使用者組織是監管機構；
b) 請求用戶提交的憑證——確定請求用戶的憑證是否為ivyKoin私有網路帳戶持有者與ivyKoin身份管理環境之間的每次通信的當前資訊；和
c) 對請求用戶提交的憑證和請求的特定身份資訊類型的具體管理限制。例如，標識為個人身份資訊的特定資訊可能不能提供給所有請求的用戶。這些限制由成員金融機構的管理人員和ivyKoin網路進行協調。

成功授權給ivyKoin資料容器後，請求的內容將呈現給請求的使用者或進程。

30. *https://en.wikipedia.org/wiki/Shor's_algorithm*
31. *http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf*
32. *https://www.iso20022.org/*
33. *https://ipfs.io/*
34. *https://www.bigchaindb.com*

7 代幣生成事件後代幣結構

ivyKoin在計畫的代幣生成事件(TGE)前正在進行ivyKoin代幣的預售 。

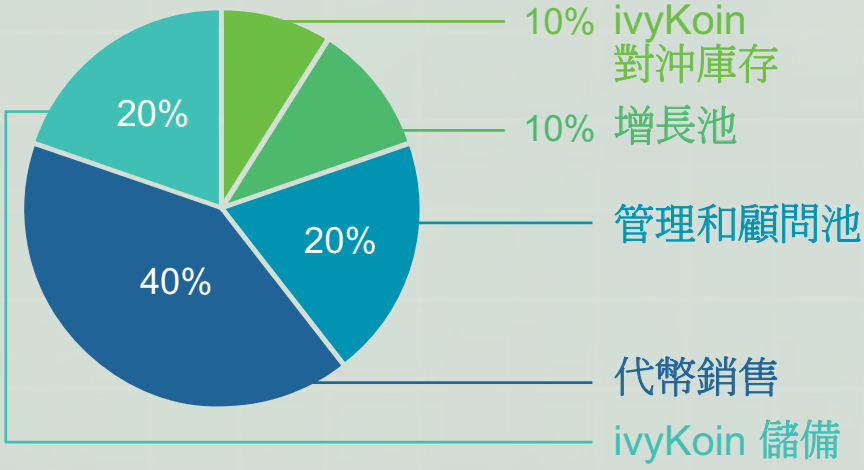
關鍵資訊	
預售開始	**2018年1月16日**
保證分配期[1]	**2018年1月29日**
預售結束[2]	**2018年2月9日**
預售代幣發售	**1.5億3**
預售代幣價格	**0.10美元**
預售籌集金額	**1,500萬美元[3]**
代幣生成事件[3]	**預計在2018年第一季度**
代幣總發行量	**約15億**
流通供應市場資本	**8,400萬美元 [4]**

*不包括交易所上市費和開價成本

1. 面向總經理接受投標的合格投資者 。
2. ivyKoin保留提早關閉預售或酌情延長的絕對自主權 。
3. ivyKoin保留全權決定更改籌集金額的權利，最高總額為15億ivyKoin供應量 。這個數字只是一個估計，公司並不保證這個數字會實現 。
4. 該數字只是一個估計值，公司並不保證這個數字可以實現 。基於TGE的1500萬美元的籌集和流通供應 。非流通供應包括為建立全球財務夥伴關係，機構合作關係，法定對沖和未來代幣銷售而保留的代幣 。

收益使用[5]

發行後持有情況 — 代幣總量



圖釋

- **代幣銷售**——包括所有出售給TGE的代幣，包括所有之前的代幣銷售和相關的代幣費用 。
- **ivyKoin儲備**——僅用於在需要時為進一步的開發和運營成本提供資金 。
- **增長池** ——用於激勵包括金融機構在內的合作夥伴來測試和採用ivyKoin.
- **ivyKoin庫**——用於促進ivySend交易和其他財務功能 。
- **管理和顧問池**——激勵現任顧問和未來管理層加入公司.

5. 此餅狀圖僅為估計，公司保留在認為合適的情況下全權決定如何使用任何和全部收益的權利 。

8

路線圖

以下日期和時間分別出於預測和展望。

近期

H1 2018:

- **代幣生成事件**(Q1 2018)
- IVYA公開可用
- 測試網路上線配合智慧合約
- KYC/KYT交易容器
- ivyKoin 公共介面上線
- 與金融機構建立合作關係
- 與美國監管機構談判

H2 2018:

- **公共網路上線**
- **ivySend上線配合傳統跨行系統**
- **ivyKoin指導IVYA銷售和市場運營上線**
- **ivyReceive上線配合IVYB跨行資金轉帳**
- **加速金融機構合作關係**

a. 代幣

私募配售完成後，公司意圖在可行情況下儘快進行代幣生成事件。想要瞭解更多資訊，請參閱公司提供的代幣生成事件的條款和條件。

b. 操作

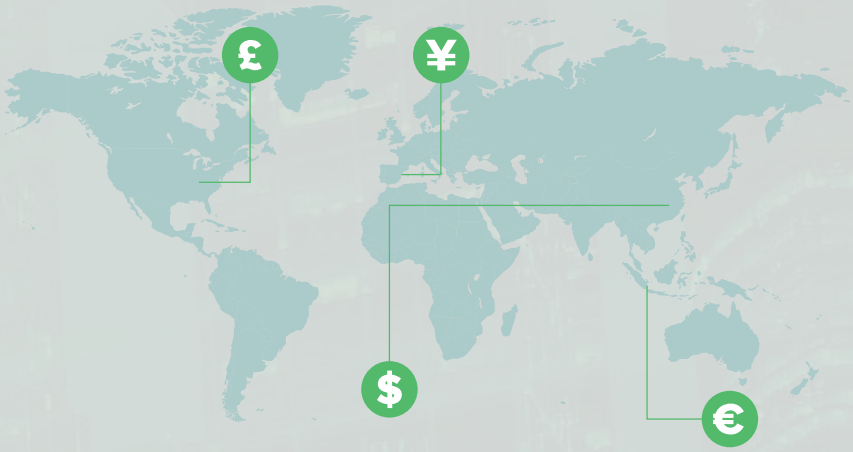
代幣發行有兩個部分：

- **代幣生成事件：** 初始代幣將被鑄造成乙太坊代幣
- **全面流通和轉換：** 功能完善的代幣在乙太坊上可用。

中期至遠期

2019

- **所有法定貨幣/加密貨幣轉換上線**
- **企業授權給容器**
- **第一批金融中間機構**



我們意圖將ivyKoin網路開發在在2018年分兩個階段進行。在ivyKoin網路開發的第一階段，通過傳統的跨行支付方式（如ACH或電匯）直接從公司收到付款。在第二階段，銀行從ivyKoin網路驗證人那裡收到付款，這些驗證人在網路上進行私人IVYB轉帳，並通過他們在那裡維持的帳戶直接付款給成員金融機構。隨著時間的推移，公司將努力：

- 在全球建立參與的金融機構網路
- 擴展轉換功能，囊括更多法定貨幣和數位資產
- 與可以從ivyKoin網路受益的組織建立夥伴關係
- 開發用於KYT / KYC / AML資料驗證的改進方法

9

風險

權利和代幣被認為是高度投機的，購買權利和代幣帶有一些風險。董事強烈建議潛在買家考慮下文所述的風險因素及本文其他部分所載的資料，並在決定是否購買權利和代幣之前諮詢其專業顧問。
如果潛在購買者不能接受以下任何風險，則潛在購買者不應購買權利或代幣。

以下列出的風險順序無意影響發生此類風險的可能性，或任何此類風險對任何特定購買者的重要性。

只有對比特幣和乙太幣以及其他基於區塊鏈的軟體系統等加密貨幣的使用和複雜性有著豐富經驗和理解的個人或實體才能購買權利和代幣。購買者應該對與其他加密貨幣相關的存儲和傳輸機制有切實的理解。

公司不提供任何建議，公司也不對由於購買者採取或不採取行動而導致的任何資金損失，權利或代幣損失負責。

失去存取權限

代幣可以存儲在錢包中，並且可以通過金鑰簽名（和其他方式）訪問。與購買者的數位錢包相關聯的必要私密金鑰丟失將導致存儲的代幣丟失。如果購買者沒有保存其私密金鑰或用於訪問其私密金鑰的密碼的準確記錄，則可能導致永久性失去對其代幣的存取權限。購買者必須將其密碼安全地存儲在與主要位置完全分離的一個或多個備份位置中。任何獲得購買者私密金鑰的協力廠商都可以訪問購買者的代幣。如果潛在購買者沒有這樣的經驗或專業知識，則不應該購買權利或代幣。

與加密貨幣協議相關的風險

代幣的基礎是加密貨幣協議。ivyKoin協定的任何故障，意外功能，分叉，故障或廢棄都可能對代幣產生重大不利影響。例如，這可能對購買者轉移或安全持有代幣的能力產生不利影響。此外，密碼學或量子計算發展的進步可能導致支援ivyKoin協定的密碼共識機制失效。任何此類影響都可能對代幣的價值產生不利影響。

開採攻擊

在驗證ivyKoin區塊鏈上的代幣交易的過程中，代幣很容易受到礦工的攻擊，包括但不限於重複消費攻擊，多數開採力量攻擊，自私開採攻擊和競賽狀態攻擊。

任何成功的攻擊都會給代幣帶來風險，包括但不限於準確執行，記錄涉及代幣的交易以及預期的適當支付操作。

駭客攻擊，網路威脅和安全弱點

駭客，個人，其他惡意團體或組織可能試圖以各種方式干擾代幣及其交易平臺，他們在平臺上的行為多種多樣，包括但不限於惡意軟體攻擊，拒絕服務攻擊，基於共識的攻擊，Sybil攻擊，“螞蟻搬家”和幌騙交易。

代碼破解的進步或量子電腦發展等技術進步可能會給代幣帶來風險，這可能會導致代幣被盜或丟失。

市場風險

公司不能完全控制任何或全部代幣購買者的行為。即使協力廠商交易所能夠實現代幣的二級交易，這種交易可能相對較新，並且很少受到或不受監管監督，因此更容易受到欺詐或操縱。此外，如果協力廠商確實認為外部交換價值屬於代幣（例如以法定貨幣計價），則此價值可能非常不穩定並且會減少至零。如果購買者選擇在交易所使用代幣，風險由購買者自行承擔。此類交易所獨立於公司，不受公司運營或控制。

交易所風險

發生代幣交易的加密貨幣交易所可能相對較新，並且很可能基本不受監管，因此可能比完善的受監管的交易所更容易發生欺詐和故障。在代表大量代幣交易的加密貨幣交易所涉及欺詐或經歷安全故障或其他操作問題時，這種加密貨幣交易所的故障可能導致代幣的價格和價值降低。

沒有保險和交易損失

與在銀行或一些其他金融機構的帳戶中持有的資金不同，除非購買者專門獲得個人保險，否則代幣一般不會獲得保險。在代幣丟失或使用代幣的能力喪失的情況下，沒有關於代幣的公共保險公司或私人保險。

如果代幣被盜或者被錯誤轉移，這些代幣可能無法收回，對此公司不承擔任何責任。因此，任何不正確執行的代幣交易可能會對代幣的價值產生不利影響。

未經交易接收人的同意和積極參與，或者理論上，若無主機區塊鏈平臺上的大多數處理能力的控制或共識，加密的代幣交易是不可逆的。一旦交易已經被驗證並記錄在被添加到區塊鏈的資料塊中，代幣的錯誤轉移或代幣的被盜一般是不可逆的，並且可能沒有針對該轉移或被盜的法律途徑或其他追索或補償。這種損失通常會對代幣的價值產生不利影響。

不確定的法規，執法行動和地緣政治事件

加密代幣，區塊鏈和分散式帳本技術的監管狀況在許多司法管轄區尚不明確或尚未確定。很難預測監管機構如何或是否可以將現有法規應用於這些技術及其應用，包括代幣。同樣很難預測的是，立法機構或監管機構如何或是否可以對影響區塊鏈和分散式帳本技術及其應用（包括代幣）的法律法規進行更改。

監管措施可能會以各種方式對代幣產生負面影響，包括僅為了說明目的，通過確定代幣是一個或多個司法管轄區中受監管的金融產品或工具，誘導對其施加披露，註冊或許可要求，或者乾脆禁止使用代幣或涉及代幣的交易。

如果監管行為或法律法規的變化導致在此類司法管轄區內運營非法，或在商業上不希望獲得必要的監管批准或為了在該類司法管轄區運營而滿足相關監管要求，公司可能會終止在某一司法管轄區的運營。

政治或經濟危機可能會刺激代幣的大規模銷售，這可能導致價格下降並對代幣的價值產生不利影響。像代幣這樣的加密代幣受供給和需求力的影響，這基於另一種去中心化的交易手段的可取性，而且這種供求如何將會如何受到地緣政治事件的影響尚不清楚。代幣的大規模銷售會導致此類代幣的流動性下降。

稅

權利和代幣的稅收特徵以及持有權利和代幣的稅收後果在許多司法管轄區尚不確定。購買者必須就購買權利和代幣尋求自己的稅務建議，這可能會對購買者造成不利的稅務後果，包括但不限於預扣稅，所得稅和稅務申報要求。購買者對購買，使用和持有代幣的任何稅收要求承擔全部責任。

不利的貨幣波動

公司意圖將銷售權利所得收益用於代幣的維護及開發。發售的收益將以美元計值。如果在發售期間或之後美元價值波動不利，公司可能無法資助代幣的開發。

極端波動

我們的意圖是不讓代幣代表任何正式或具有法律約束力的投資，並且一旦開發就不需要在任何公共市場上進行交易。此外，在公共市場上具有價值的加密代幣經常在短時間內出現極大的價格波動。這種波動是由市場力量造成的，代表了供求平衡的變化。交易所和公共市場獨立於公司並且不由公司運營。任何交易所或公開市場上的交易風險均由每位元購買者自行承擔，公司不能保證代幣的任何市場流通性或可銷售性。

此外，不同司法管轄區的不同監管要求以及某些司法管轄區公民可能無法在全球各地的交易所開立帳戶，因此代幣在不同司法管轄區的流動性可能會有重大差異。這可能會反映在市場之間巨大的價格差異上。代幣的價值也有可能在未來大幅度下降。代幣價值的任何這種下降都可能對公司籌集持續經營資金的能力產生不利影響，包括代幣的開發。

競爭的加密貨幣相比代幣對重要的加密代幣用戶群來說更為理想，或者由於技術的整體信心的下降，加密代幣的使用可能會普遍下降。任何此類事件都可能導致代幣的需求和使用減少，這通常會對代幣的價格產生負面影響。

此外，由於欺詐，企業倒閉，駭客或惡意軟體或政府規定的監管，加密貨幣交易所缺乏穩定性以及加密貨幣交易所倒閉或暫時關閉都可能導致代幣價格有更大波動。

智慧財產權索賠

協力廠商可以提出與權利或代幣相關的智慧財產權所有權和/或其原始程式碼或其他相關智慧財產權的索賠。不管任何智慧財產權索賠或其他法律行動有何好處，任何威脅的行為都可能會對代幣的價值產生不利影響。

無法預料的風險

權利和任何待開發的代幣都代表了一種新的相對未經測試的技術。

除上述風險外，還存在與購買權利或代幣，持有權利和代幣以及使用權利和代幣相關的其他風險，包括公司無法預料的風險。

無法預料的風險可能以上述或其他方式風險的變化或組合形式出現。

詞彙

乙太坊
乙太坊是一個領先的智慧合約去中心化平臺，採用Solidity程式設計語言。它是一個開源的基於公共區塊鏈的分散式運算平臺。

乙太幣
乙太坊區塊鏈平臺的價值代幣被稱為“乙太幣”。

智能合約
智慧合約是程式設計的抽象思想，明確表示各方之間交換關係的確切條款。在交易被記錄和執行之前，智慧合約條款必須被滿足並被確認為“真”。智慧合約是用Solidity這種程式設計語言編寫的。所有這些智慧合約都公開存儲在每個區塊鏈節點上。

IPFS
是一個開源的，去中心化的檔案系統協議，為文檔的創建，存儲和共用提供了永久的方法。IPFS節點構成了分散式檔共用網路的基礎。這是一個基於塊存儲模型的高輸送量。它利用散列進行檔識別，為不可改變的資料存儲創建強大的環境。

SOLIDITY

區塊鏈的智慧合約是用稱為Solidity的程式設計語言編寫的。

X509
公開金鑰證書定義的密碼標準。它是安全通信的關鍵元件，可用於驗證電子交易中的“數位簽章”。X.509由國際電信聯盟（ITU）定義，該電信聯盟是負責全球電信和標準協調工作的聯合國機構。

PKI
公開金鑰基礎設施（PKI）是創建，管理，分發，使用，存儲和撤銷數位憑證所需的一組角色，策略和過程，也是基於公開金鑰的加密系統的關鍵組成部分。

信任鏈
信任鏈是通過自下而上驗證硬體和軟體的每個元件來建立的。這可確保通過驗證鏈中的每個硬體和軟體元件，只有可信的軟體和硬體才能使用。

資料欄
交易中發送的資料量根據各方的要求以及管理交易的智慧合約的要求而異。ivyKoin不會驗證客戶資料（超出簡單的帳戶開設過程範圍）而是促進這一過程。

ivyKoin

Ivy Koin LLC
Ivy Management Group LLC

468 N. Camden Drive, Suite 200,
Beverley Hills, CA 90210

www.ivyKoin.com