基於區塊鏈的分佈式協議
OpenChat 白皮書

OpenChat 項目團隊

版本 V1.0，2017/12/01

1. 背景介紹

1.1 區塊鏈技術

區塊鍊是時下最流行的話題之一。它首先是一種社會思潮，預示著人類社會轉型、更迭的新時代的到來。凱文·凱利在《失控》一書中描述：生物邏輯的自然、社會、技術的進化規律就是從邊緣到中心再到邊緣，從失控到控制再到失控。區塊鏈的技術基礎是分佈式網絡架構，正是因為分佈式網絡技術的成熟，去中心、弱中心、分中心及共享、共識、共擔的組織架構、商業架構才有可能有效地建立起來。如今的區塊鏈技術已經發生了數次迭代：它首先是分佈式賬本，全部機構一本總賬、各項事務一本總賬；其次區塊鏈技術是一個新型數據庫，不存在中心機房，沒有運維人員，第三方按照共識算法錄入數據，使用非對稱加密算法保證數據安全；第三它是智能合約，依靠智能合約，世界就像一台精密運行的超級計算機，一切都可以事先約定，編成代碼，依照程序行事；第四它是 TCP/IP 模型裡的 Point-to-Point 價值傳輸協議，它的發明標誌著互聯網技術在過去的二十多年內幫助人們更高效地傳輸信息之後，可以不借助第三方的信任背書開始幫助人們實現價值互聯。

區塊鏈的核心價值在於其實現了不可篡改、安全可靠的分佈式記賬系統。使用區塊鏈賬本的多個參與者無需額外的第三方擔保機構即可構成多方交易的信任基礎，進而實現低成本、低延遲的信息交換和處理系統，實現數字價值的高效流通。

1.2 加密數字貨幣

加密數字貨幣是區塊鏈上的一個重要應用。顧名思義，加密數字貨幣著力採用密碼

學技術。密碼學提供一個將加密貨幣體系規則編碼到系統本身的機制，人們不但可以利用密碼學防止對系統的干擾，避免產生混淆，也能用其將新貨幣單位創造規則編碼到數學協議中。

基於 BIMP 分佈式協議的社交網絡將要使用的加密數字貨幣貫徹了這一理念。依托區塊鏈不可篡改、安全可靠的特性，為全人類創造一個使用加密數字貨幣交易、交流的點對點社區。

1.3 即時通訊軟件背景介紹

隨著智能手機的普及，即時通訊軟件(Instant Messenger)在人們的日常生活中逐漸取代了傳統的 2G 短信和語音通話。在發達國家和一些移動通訊發達的國家，WhatsApp, Telegram, WeChat 等即時通訊軟件極大地方便了日常生活和交流。在人口占據絕對優勢的新興國家，對“即時通訊+電子支付”模式的產品有很大需求。以即時通訊軟件為平台，搭建集廣告、手機遊戲、電子商務、周邊服務等多重服務的產品，構建完善的新興市場網上生態系統，打造一站式新興市場生活、工作平台是 OPENCHAT 團隊正在全力開發的方向。

在即時通訊軟件迅速發展的同時，傳統企業在運營中也逐漸暴露出一些問題。

傳統的 IM 應用通常包括三方：平台，合作商和用戶。每一方都有一個維持平台發展的角色。儘管每個人都扮演了關鍵的角色，但是這些團體的目標是以非常不同的目標進行的，目前的模式不能提供一種他們的激勵機制可以共存和協調一致的手段。由於供給方自身利益的驅使，使得未來的社交網絡變得不再安全，平台和合作商會千方百計的獲取用戶的信息，以提煉出更加適合作為推廣依據的大數據，來保證自身的生存空間，但這卻讓用戶隱私安全深陷水深火熱之中。

2013 年， Facebook、Skype、Microsoft、Apple 公司和 Yahoo!被曝參與美國國家安全局實施的“棱鏡”項目，引起一片嘩然。作為用戶，你什麼錯都沒有，但你卻可能成為被懷疑的對象，也許只是因為一次發送了錯誤的信息，他們就可以用這個項目仔細調查你過去的所有決定，審查所有跟你交談過的朋友。現今部分地區的用戶對個人隱私的重視程度還遠遠不夠，很多人不關心自己的授權被用去做什麼，也不在意 APP 中的隱私政策聲明。

2016 年，一份由 Amnesty International 公佈的「社交軟件通訊隱私排名」在社交網絡上廣泛傳播，這份名單從「人權保護」、「端對端加密」、「風險提示」、「披露後門開放情況」及「公佈加密技術細節」五個方面橫向對比了當前主流社交軟件服務，並進行了評分，作為全球主流 IM 的 Skype 和 WeChat 的評分分別只有 40 分與 0 分（滿分 100 分），可見隱私洩露風險的嚴重性。傳統的信息加密技術叫「傳輸加密」，服務商採用不同加密手段，對信息的傳輸過程進行加密。這種加密方式的最大缺陷在於：用戶之間發送的消息本身是明文的，換言之，如果負責信息傳輸的服務商自己想要偷窺用戶隱私或者不慎將消息洩漏，用戶的所有聊天記錄都將毫無保留地暴露在光天化日之下。

因此，今後可怕的不再是個人信息的洩露，而是用戶行為已經被預測出來，當科技的發展導致人工智能的建議能夠影響人的決策時，尤其是這些 AI 背後都由大公司掌控，就不知是該欣喜還是恐慌了。

區塊鍊是分佈式數據存儲、點對點傳輸、共識機制、加密算法等計算機技術的新型應用模式。區塊鏈作為數字資產的有力保障，一直以來備受業界好評，然而作為應當為用戶隱私負責的傳統 IM 卻並沒有提供任何區塊鏈的對應入口。

與此同時，傳統 IM 第三方產品的提供商為了保證自身的利益，時刻處於一種相互競爭的狀態之中，根本無法進入共生互利的狀態之中，久而久之，一些優秀和怀揣夢想

的提供商不得不接受被淘汰的命運，不僅傷害了市場的多樣化進程，還扼殺了許多優秀的創意。

1.4 電子支付背景介紹

許多電子支付方式都可以基於現金和信用兩個基本概念進行分類。

信用卡交易是目前主要的線上支付方式之一。例如用戶在亞馬遜網（www.amazon.com）上購物，結算時首先需要輸入自己的信用卡信息，亞馬遜收到賬戶信息後反饋給包括信息處理器、銀行、發卡公司及其他中介在內的支付“系統”。

如果使用 PayPal 或 Alipay 之類的第三方支付機構，用戶體驗的模式將是由中介公司收集用戶的銀行卡信息並核准每一筆交易信息，並在每個交易日結束時與賣家統一結算。

基於信用的電子支付方式很方便，但它的安全性無法得到保障。無論是買方用戶違約，或支付通道本身受到攻擊等，都會導致支付系統受到損失。而基於現金的支付系統雖然規避了由用戶直接向買方提供銀行卡信息的安全風險，卻也增加了支付系統複雜性，用戶和賣家無法直接進行交流，都得在第三方支付公司開立賬戶。

以比特幣為代表的加密數字貨幣既支持用戶和商家之間的交易，也支持用戶和用戶之間的交易。事實上，比特幣體係並不把用戶和商家區別開來，比特幣的成功很大程度上要歸功於它對用戶-用戶間交易的支持。從一開始，每位比特幣用戶都可以發給其他用戶，因為整個比特幣社區的人都努力爭取人們對比特幣的支持，並促使商家也接受它。因此，加密數字貨幣在未來很可能成為代替信用卡公司和第三方支付機構，真正實現點對點即時傳送的去信任的交易方式，成為電子支付的首要選擇。

此外，無論是基於現金還是信用的支付方式，跨境支付的高額手續費都是市場痛點

之一。據麥肯錫報告《2016 全球支付：儘管時局動盪，基石強勁不變》顯示，跨境支付交易量佔不到全球支付的 20%，但是它所帶來的交易費占到了全球支付交易費的 40％，2015 年跨境支付的收入規模為 3000 億美元。如何提升效率、降低成本，是區塊鏈技術迫切需要解決的一件事情。

2. OpenChat 生態介紹

OpenChat 項目是一套基於區塊鏈技術的分佈式協議 BIMP. BIMP 協議的首個落地應用將是基於區塊鏈跨鏈技術的移動即時通信應用（Instant Massager）附加輕錢包應用 BeeChat，未來將構建全新的社交網絡經濟生態。 BIMP 協議生成的 ChatCoin 代幣(ChatCoin，下同)將在基於 BIMP 的聊天工具中得到廣泛支持，用於聊天工具中發放紅包、打賞、付費進入小密圈等服務內容。

2.1 BeeChat 項目介紹

建立在 OpenChat 協議之上的 BeeChat，是一款真正的去中心化的，支持多重區塊鏈的平台。 BeeChat 以“即時通訊+錢包”為模式，以即時通訊軟件為平台，搭建廣告、手機遊戲、電子商務、周邊服務等多重服務，逐步構建完善的新興市場網上生態系統，為用戶打造一站式新興市場生活、工作平台。

IM 是 BeeChat 發展的根基，由於新興國家和市場很多資產還沒有數字化，如住房、汽車等，但等未來這一切都變成了數字資產的時候，IM 就可以利用與我們的 ChatCoin 形成的協議激發社區的開發能力，讓這些數字資產更好的流通，從而反過來推動 ChatCoin 的接受度。

對於大多數消費者來說，面對原始加密貨幣技術的複雜性通常是繁重的。交易費用、私鑰和字母數字地址問題，為主流用戶帶來使用障礙，其中包括首先持有加密貨幣的常見要求（只有首先持有加密貨幣，然後才能獲取和利用其他代幣）。 OpenChat 將力圖大大減少此類為啟用帶來的摩擦。在能夠與 ChatCoin 互動之前，用戶的啟用流程無需擁有加密貨幣方面的專業知識。

BeeChat 維持利益共同體原則，保障用戶和開發者的權益，讓所有人都投身到改善推動 BeeChat 的事業當中來，但 BeeChat 不代表純粹去中心化的無政府主義色彩，而是在幫助權威機構低成本地解決社會活動中的信任問題，是推動誠信社會建立的有效手段，因此 BeeChat 代表著未來，而 ChatCoin 代表著未來的行為。

2.2 基於區塊鏈的電子錢包(Bee Wallet)

使數字社區能夠使用加密貨幣所需的主要功能就是錢包。作為第一步，BeeChat 將為每個 BeeChat 用戶帳戶整合錢包。相關聯的用戶界面將允許最常見的錢包互動。通過整合錢包來支持 BeeChat 的數百萬活躍用戶，BeeChat 錢包有可能成為世界上最受歡迎、使用最多的加密貨幣錢包。

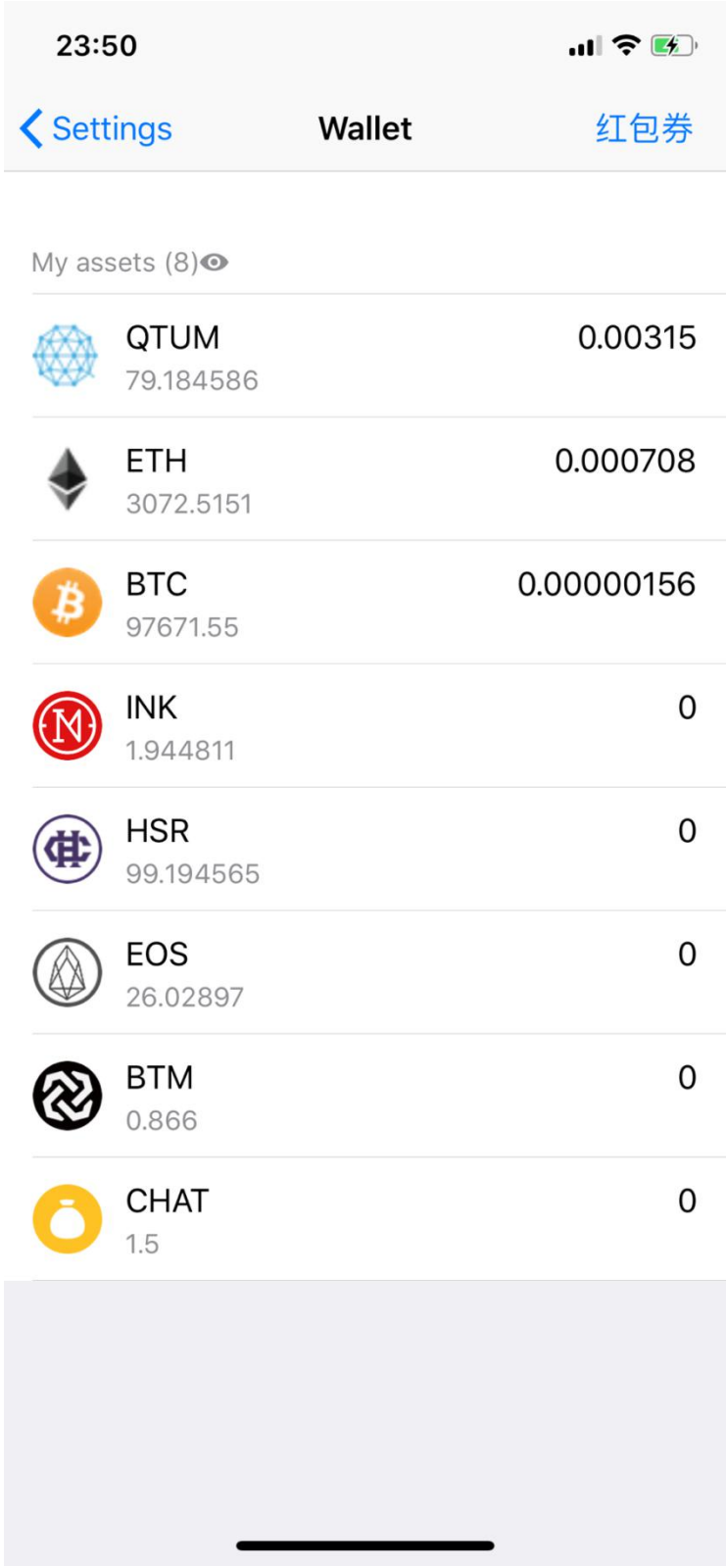
23:50
Settings
Wallet
红包券
My assets (8)
QTUM
79.184586
0.00315
ETH
3072.5151
0.000708
BTC
97671.55
0.00000156
INK
1.944811
0
HSR
99.194565
0
EOS
26.02897
0
BTM
0.866
0
CHAT
1.5
0

圖 1: Wallet 頁面

2.3 自媒體生態(Discovery)

Discovery 是 BeeChat 為用戶準備的一個集朋友圈、新聞、行情、交易於一體的動態顯示專區，用戶在關注好友動態的同時，也可以及時發現與自己利益相關的區塊鏈資訊。

Discovery 實際是 BeeChat 為了培養用戶合理規劃區塊鏈財富的習慣所作出了努力。因為很多用戶專注於 IM，對於數字資產並沒有健全的理財意識，Discovery 通過朋友圈動態與業界資訊的交替展現，讓用戶在翻閱朋友圈的同時也會注意到與自身數字資產現狀息息相關的市場變化，並針對自己的狀況做出合理的調整，真正養成合理使用和配置數字資產的習慣。

2.4 社交功能(Chat)

用戶通過 Chat 功能可以與家人、朋友時刻保持聯絡，建立自己的社交圈，將平台中其他的去中心化應用與自己的社交網絡分享。 Chat 是當今最快的集高清視頻、語音及文字於一體的移動通訊功能。它以獨有的分佈式技術，高度安全的加密服務確保免費環球暢聊，輕鬆實現無延遲、高質量的語音/視頻通話，並且支持 500 人同時在線群聊。

由於公司當前產品龐大的用戶基數，每位用戶的社交結構將隨著時間進一步與 BeeChat 融合，並通過家族社交、移民社交、工作社交不斷的傳承和擴大下去，形成全球化的 BeeChat 社交體系。

2.5 應用網絡(Network)

Network 是 OpenChat 提供的全球化的去中心化共生應用市場，用戶可以在這裡下載第三方應用開發者提供的各項產品，通過付費或提供有價值的行動來獲取該應用的使用權，開發者則通過發行去中心化的應用來賺取 ChatCoin。

OpenChat 將保持對 Network 的關注，及時調整開發者獎勵策略，保持整個共生環境的穩定性，鼓勵更多的開發者提供創新的去中心化應用。

9:13

朋友圈

热点群推荐

公众号推荐

行情

帮助和公告

小Bee圈

DAPP

创世神犬

限时领Bee

领红包券

英雄社区

个人收藏

最近通话

99+

消息

发现

设置

图 2: BeeChat 软件页面

2.6 基於 Qtum 的體系

在用戶能夠互相交流和交易之前，他們需要一個媒介來進行這些操作，傳統上這一媒介是由一名有信譽的網絡所有者提供，但隨著量子鏈公有鏈的出現，我們可以向用戶提供一種去中心化、去許可化、去信任化、具有公平訪問權限且可加密驗證協議的通道。

隨著量子鏈的發展，世界擁有建立互聯網更好模型所必需的技術。我們認為，Qtum 知識分子將繼續滲透到金融技術，法律制度，物聯網和分散應用等方面。

Qtum 最終會成為一種社會技術，為了實現其可意識到的潛力，我們需要最大限度地發揮非技術用戶的實用性，它需要無所不在，始終可以訪問，並且需要成為我們日常生活的一部分。

3. 經濟模型簡述

OpenChat 致力於打造一套開源的共生經濟體系，在這套體系下，所有的參與者（用戶，DAPP 開發者）都將成為一個利益共同體，大家必須相互協力，才能贏得共同的利益，而隨著參與者的不斷增加，這套經濟體系亦將無限制地進行擴大。

作為用戶，只要提供有價值的行為（點擊廣告，發送鏈接等）即可獲取由 DAPP 開發者提供的 ChatCoin 獎勵，這不僅增強了用戶的活躍能力，同時也降低了開發者的推廣成本，從而促進利益的共同提升。

作為去中心化應用開發者，在這套開源的共生經濟體系中，能夠相互借鑒和共享對方的技術優勢，及時發現自身的弊端並予以改正，所有開發者真正連接成利益共同體，大家都將致力於開發出更好的應用而努力。而 OpenChat 會對為技術進步做出重大貢獻的開發者提供大量 ChatCoin 的獎勵，以激勵更多開發者的熱情。

4. 業務模型介紹

4.1 全新的數字生活服務平台

BeeChat 將推出若干市場用例，促使消費者和品牌能夠使用 ChatCoin。通過實驗，BeeChat 計劃為用戶創建獨特的雙面市場的應用程序，進行產品迭代。在供給側，自動程序或內容創作者將創造獨特的體驗。在需求側，用戶將消費此類產品或服務。在不久的將來，BeeChat 的自動程序將有能力構建自己的商業模式。

4.2 應用場景

除了社交場景外，基於點對點的 Bee Wallet，用戶在交易中實現全面互通，例如：

▸場景 1：

用戶 A 是一個埃及的用戶，但是迫於生計，選擇了背井離鄉，來到阿聯酋打工。在工作之餘會使用 BeeChat 和家人打跨國電話，在領取工資之後，可以通過 ChatCoin 給家人匯款。這中間省去了高昂的貨幣兌換費用和轉賬費用。

▸場景 2：

用戶 B 是一個音樂發燒友，酷愛新發行的音樂，但是實體店的音樂由於到貨比較遲，可以通過使用 Bee Wallet 直接購買線上的音樂。

▸場景 3：

用戶 C 是一個中國用戶，打算節假日的時候帶上家人出國旅遊。在出國之前需要先

兌換大量的外幣，各個銀行會抽取一部分的手續費。在出遊的途中，會時刻擔心身上的大量現金是否安全。遊玩結束時，還需要把多餘的外幣再轉成人民幣。過程十分繁瑣。如果使用 Bee Wallet 的話，在外消費的時候，可以通過掃碼支付，將 ChatCoin 轉給對方就完成了付款。

▸場景 4：

用戶 C 打算投資房地產，但是發現國內的房子的價格已經處在階段性高點了。而海外部分國家正在吸引著越來越多的人來旅遊度假，這是一個海外置業的絕佳機會。於是用戶 C 使用了 Bee Wallet 在阿聯酋購買了一套房子。半年後房子增值 50%，於是又把房子買了，把數字貨幣存入了 Bee Wallet。

5. 項目落地情況

OpenChat 首推的 BeeChat 移動通訊軟件目前已經完成開發並已登陸蘋果應用商城（App Store）和谷歌應用商城（Google Play）。用戶可以通過搜索 BeeChat Plus 直接下載並使用。或通過登陸 BeeChat 官網（http://www.beechat.io/）下載。

6. 治理機制及風險管理

6.1 OpenChat 投資者社區

OpenChat 將建設去中心化的國際性社區，並設立 OpenChat 基金會（OpenChat

Foundation）來保證 OpenChat 投資者社區的管理、運作以及所募集資金的安全。OpenChat 基金會的組織架構將由 OpenChat 投資者社區大會，OpenChat 基金會自治委員會和執行委員會組成。

OpenChat 投資者社區大會是 OpenChat 項目的最高權力機構，由全部 ChatCoin 持有者組成，所有的持幣者都能夠通過社區大會行使自己的投票權、參與 OPENCHAT 項目重大事項的決策。

OpenChat 基金會自治委員會對投資者社區大會負責，負責對執行委員會行使管理和監督的職能。自治委員會每年根據所持代幣的數量和幣齡進行換屆。

執行委員會對自治委員會和投資者社區大會負責，由 OpenChat 項目的技術開發和日常運營團隊等構成，負責 OpenChat 項目技術開發、生態構建、運維服務、社區管理等不同層面的實際工作。

OpenChat 投資者社區大會

OpenChat 投資者社區大會由全體 ChatCoin 持有人組成，是項目的最高權力機構。具有如下職能：

（1） 修改投資者社區大會管理條例；

（2） 監督投資者社區大會管理條例的實施；

（3） 選舉和變更自治委員會委員；

（4） 撤銷自治委員會的不適當決定；

（5） 批准重大經營事項和變更事項；

社區成員作出決議需經持幣人根據持有 ChatCoin 的數量和幣齡計算權重進行投票表決通過。社區大會每年召開一次，進行項目本年度的工作進程匯報等工作。若自治委員會認為有必要，或者五分之一以上 ChatCoin 持有人提議，可臨時召開社區大會。

6.2 風險管理

ChatCoin 通過區塊鏈共識、不可篡改等技術以及數字簽名、終端用戶加密錢包等安全手段確保用戶賬戶及資金安全；用戶轉賬、紅包、內置交易平台等將通過量子鏈（Qtum）提供金融級的安全服務；將數據、交易集成到區塊鏈中，構建安全的交易環境。

6.2.1 審計

OpenChat 基金會嚴格遵守相關的法律法規和行業自律,提供完全透明的財務管理；基金會每年邀請國際知名第三方審計機構對基金會的資金使用、成本支出、利潤分配等進行審計和評估；基金會將無保留的公開第三方的評估和審計結果。

6.2.2 信息披露

OpenChat 基金會將定期披露項目開發進展、新聞資訊及資金使用情況。OpenChat 投資者社區大會將每年表決由第三方審計機構出具的審計報告和執行委員會公佈的項目年度進展情況。執行委員會也會根據項目實際發展情況，通過公告、官網、各類社交網絡平台等即時通報項目進展。

7. 項目發展時間規劃

7.1 未來展望

自互聯網技術成熟以來，人類社會開始了一次數字空間的大發現。傳統依靠土地、設備、勞動力創造財富的模式，因為資源的有限性而受到製約。而數字空間的無限可擴展性、比特結構的無限可複制性、虛擬世界的多維可塑造性可能意味著蘊藏在這裡面的待開發的財富，會數十倍於物理世界。這些新財富的表現形式就是數字資產。但是，受於巨大利益的驅使，許多的企業更加傾向於以損害用戶的權益來換取自身的快速發展，而這其中，被利用最多的當屬用戶的個人信息與隱私。

OpenChat 作為一個正在高速成長中的開源社區，希望建立一套強大的數字生活平台，服務每位 BeeChat 用戶的數字生活。 OpenChat 之後將構建一套新型的去中心化的社交經濟網絡，通過高度保護用戶隱私，自動化的用戶激勵引擎，多鏈支持的結算系統，讓億萬用戶真正進入新型的數字經濟生活當中來。

在未來，OpenChat 的用戶每天只需要拿起手機，就可以通過平台內的人工智能輕鬆發現今天最佳的賺錢途徑，而且只需要動動手指就可以將這筆財富收入囊中，如果用戶還想繼續創造價值，還可以接受其他用戶發布的任務，根據選擇不同的難易程度會獲得對應的 ChatCoin 。而每天賺取最多 ChatCoin 財富的用戶都將在朋友圈財富榜中傲居榜首，閃亮全場。

OpenChat 將致力於使數字經濟生活融入到用戶的日常生活當中去，全力推動去中心化的社交經濟網絡時代的來臨。由於坐擁巨大的用戶體量，先行的 BeeChat 必將成為下一代 IM 規則的製定人，主導著數字經濟生活的未來。

如果你想做未來數字生活的領航者，就必須掌握未來的鑰匙，而 OpenChat 有信心將這把鑰匙交到你的手中，帶領你前往未來生活的至高點。

8. 團隊介紹

8.1 團隊背景

OpenChat 背後的支持團隊是 Google 前员工創辦的開源組織，致力於跨國即時通訊應用研發和技術創新。公司匯集了來自 google，華為等公司的技術精英，已開發出多款不同功能的 APP 投放到世界各國，成為千萬級用戶日常交流的必備工具，在新興世界市場最受歡迎。

公司目前獨立研發、運營的即時通訊軟件在新興國家中佔據絕對優勢，致力於長期、深入地促進新興世界地區互聯網用戶的網絡通訊和人際交流，服務於廣大全球用戶。未來公司將繼續鞏固和發展現有的在新興國家的市場優勢，以即時通訊軟件為平台，搭建廣告、手機遊戲、電子商務、宗教周邊服務等多重服務，構建完善的新興市場網上生態系統，打造一站式新興市場生活、工作平台。並在中東、南亞、中南美洲、非洲等快速增長的新興市場，繼續宣傳推廣，提供更加高清、安全、極速的通訊服務和便捷的移動聯網生活體驗，最終實現全球戰略計劃。

8.2 團隊成員介紹

	**Oscar**
	他是一位資深的 Scrum 專家和高級軟件工程師，在團隊開發和項目管理上有多年的經驗。他的目標是開發一款頂尖的受全球認可的去中心化的軟件產品。
	**Nell**
	Java 工程師和商業化的軟件諮詢師，專精於後端開發和微服務端架構。 Nell 是我們區塊鏈解決方案的高級開發工程師。
	**George**
	後端和數據庫方面的高級軟件開發工程師，擅長軟件架構和麵向對象的設計。多年來 George 都專注於產

	品解決方案的設計。

	**Mia**
	擁有多年的法務背景，擅長幫助創業公司和中小型企業從創立伊始在融資階段中解決法務需求。在眾籌及加密貨幣領域工作多年。
	**PikaOne**
	用戶界面的數字設計師，擁有在 Google 多年的工作經驗，對於創新設計有深入的研究。
	**AC**
	品牌互動和概念設計師。擁有多年插圖和廣告設計的經驗，現在致力於數字設計開發。

參考文獻

[1] A. Narayanan. J. Bonneau. E. Felten. A. Miller. S. Goldfeder. *Bitcoin and Cryptocurrency Technology: A Comprehensive Introduction*. The China Citic Press, 2016.

[2] P. Wayner. *Digital Cash: Commerce on the Net* (2nded). Waltham, MA: Morgan

Kaufmann, 1997.