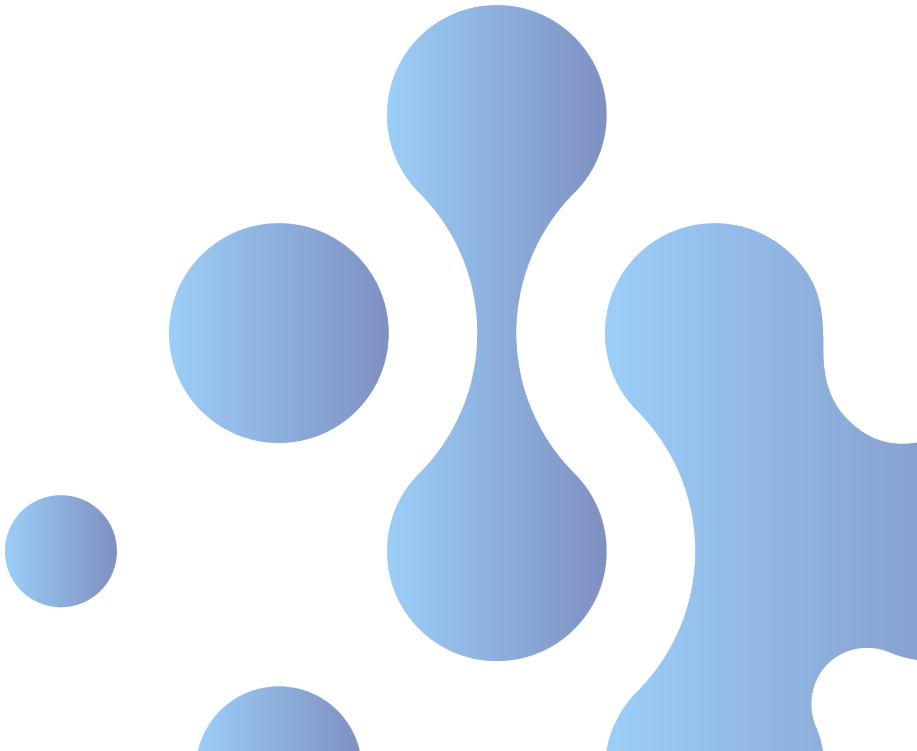
EXCRAFT

EXCRAFT存在證明通證

存在證明通證讓您放心交易



V1.0

摘要

ExCraft 是一個雲原生的香港加密貨幣交易平台，使用微服務架構以實現高安全性和高性能。為了實現去中心化並保證性能，ExCraft 將發行一種兼容以太坊 ERC20 標准的通證EXT，通過可證實的每日交易量-即“存在證明”（PoE）來獎勵交易者。額外的 EXT 通證將獎勵給那些持幣的用戶和參與交易礦池的用戶。交易礦池會為社區打造提供獨特能力的可能性。EXT 通證將為平台的去中心化自治組織提供投票機制，對社區主題進行投票。ExCraft 將持續通過利用鏈上訂單和跨鏈兼容訂單機制，以及實施建立在分布式權益證明共識上的專業主網，朝著完全去中心化的方向運行。

Kevin Chen *Senior Adviser*
kevin@ExCraft.com
Rodin Chen *Adviser*
rodin@ExCraft.com
Roy Lam kt *CEO*
roy@ExCraft.com
Benjamin Chodroff *CTO*
ben@ExCraft.com

目錄

簡介 4

中心化交易所 vs 去中心化交易所 5

EXT 通證發放概覽 6

- 存在證明（PoE）獎勵 8
- 權益證明獎勵 9
- 交易礦池獎勵 9

去中心化自治組織 10

- 權益證明代表組成的國會 11
- 交易礦池主代表組成的參議院 11

ExCraft 平台 12

- 當前架構 12
- 去中心化的能力 12
- 安全性 12
  - 基礎設施 12
  - 服務 12
  - 平台 13

團隊介紹 14

路線圖 15

引用作品 16

簡介

任何資產的價值只有通過交易才能證明。ExCraft 的建立就是為了通過交易透明度給所有的加密貨幣證明價值。世界正朝著去中心化服務的方向發展，而我們旨在創建一個專注於安全性和高性能的交易平台。我們已經創建了一套混合了中心化和去中心化的交易所服務系統。我們的中心化服務采用的是性能導向的雲原生微服務架構，而我們的去中心化服務將分階段實現。

ExCraft 交易所總部位於香港，建立在谷歌雲計算平台上。交易所的定制化構架讓其同時兼備了安全性和高性能。通過 Docker 把主要組件部署進一套 Kubernetes 管理的微服務系統，交易平台的建造既模塊化又可擴展。通過使用 Istio 保證基於 gRPC 的微服務透過服務網格互聯。不同於許多傳統的中心化交所，ExCraft 的架構通過支持交易所快速添加額外資、增加新功能同時不打亂現有交易行為的方法提高了性能。交易所平台已通過測試，能支持上千對交易對，並且整體有能力支持每秒上千萬次的交易。

另外，設計時對安全性的注重也影響了基礎設施的選擇、平台、服務、運營和總體架構。通過內部合規、外部驗證以及監管透明，ExCraft 能保證最佳安全性。ExCraft 社區將參與未來的全部開發。隨著雲、交易所和去中心化技術的提高，ExCraft 將持續改進，同時通過使用另外的去中心化服務來提供額外的安全層。

ExCraft 將創建一個傳統的去中心化服務，根據“存在證明”（PoE）機制獎勵用戶。該以太坊ERC20 兼容通證將通過以太坊智能合約發放給社區成員，其發放將基於用戶在 ExCraft 交易所中產生的 PoE 量，然後將結果發表在區塊鏈上。PoE 量有很多功能，包括為交易礦池中最高交易量的代表組成的去中心化自治組織參議院提供精英投票權，而與此平衡的是 EXT 通證持有量最多的用戶組成的國會。

為了提高交易中的透明度，ExCraft 每日將給社區獎勵一定數量的 EXT 通證，發放比例取決於每日的 POE 數額，發放數量則是以某種計算方式每日發放。交易所每日會用不少於 80%的交易費從市場上回購平台通證。這些購買到的通證將被發送至黑洞地址進行銷毀，從總供應量中刪除。通過交易得到的額外收入減去交易所的運行所需成本後，剩余費用也將用於從交易所購買 EXT 通證後銷毀。通過這種方式，所得交易費用最高達 100%都將經由 EXT 通證返還給社區。

在交易所注冊並持有 EXT 通證，或任何用以太坊私人錢包地址在與交易所鏈接後，持有 EXT 通證的注冊用戶通過權益機制（PoS）還將得到更多的獎勵。交易所將每日發放 PoS 獎勵給所有的通證當前持有者。

用戶還有第三種方法來獲得 EXT 通證的獎勵，即把其 PoE 集合到“交易礦池”中。排名前 101 的交易礦池將得到額外的通證，根據其貢獻的 PoE 平等分配給交易礦池成員。

我們的交易平台旨在提供一個將來能完全去中心化的運用，為所有交易提供存在證明，鼎力支持原子交換和跨鏈兼容，並打造一個支持靈活投票且保證高交易性能的社區。ExCraft 和其社區合伙人將爭做先鋒，運用區塊鏈技術把一個這樣的主網變為現實。

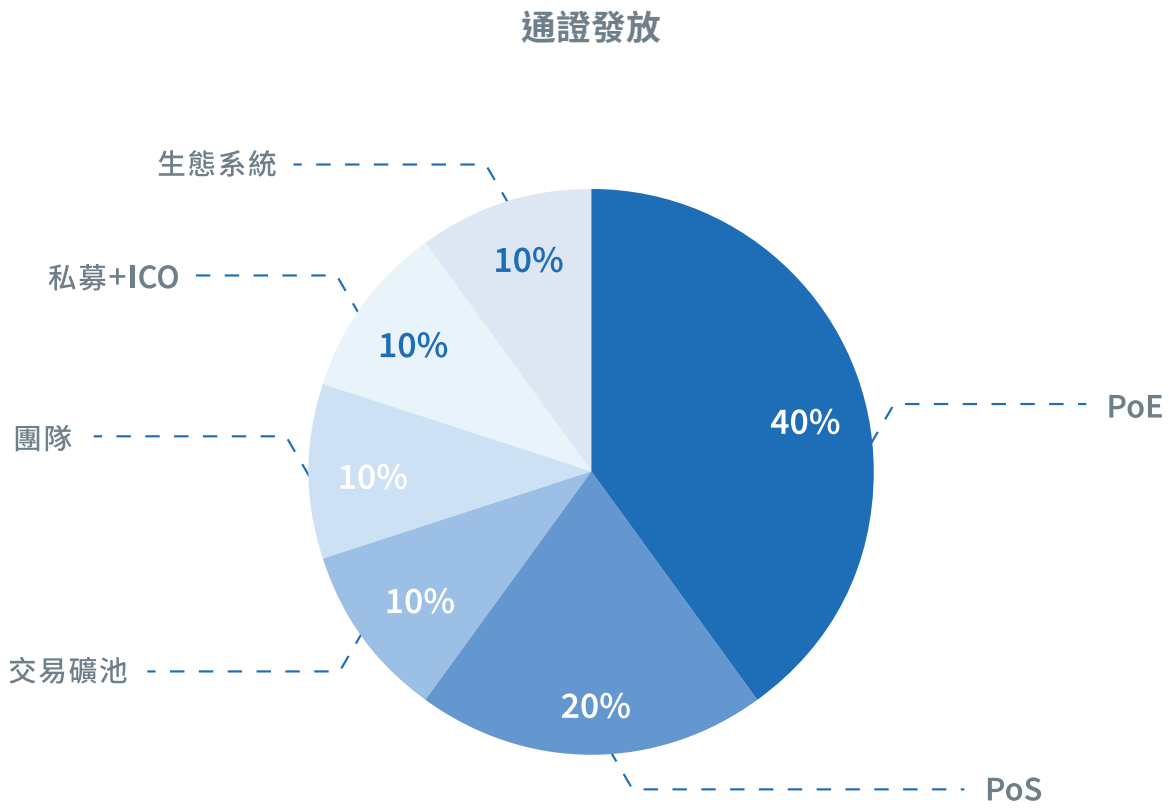
中心化交易所 vs 去中心化交易所

去中心化交易所有著勢不可擋的實現方式，能保護隱私，執行的公正度也能證明，由於這些優勢，市場在逐漸擁抱中心化交易所。不幸的是，擁有這些特征會降低當前的交易性能。由於建立這些基於區塊鏈服務所需的去中心化記賬技術相對很新，在實際確認現狀前，實施這些技術會出現延遲，通常以“分或秒”計算。(BitShares, 2018) (Komodo, 2018) 相對而言，全球頂級交易所的高頻交易會按照微秒或更短的順序來計算。大部分加密貨幣交易員並不需要按微秒的速度來交易。但是，無法處理高額交易的交易所通常在性能表現上會輸給那些可以這麼處理的交易所。

去中心化和中心化數據庫的性能差異很大，不能忽視，但這種性能的差異幅度正在加速縮短。通過內部安全、外部合規和社區參與，ExCraft 將分階段引導交易商至一個去中心化的交易所。ExCraft 將分階段支持成交訂單的 0x 項目條約，以此來促成 ERC20 兼容幣的鏈上訂單 (0xProject, 2018)。ExCraft 平台將用 Gormos 主網分階段支持 Kyber 交易網絡，來達成全部在鏈上完成的交易 (Kyber Network, 2018)。

EXT 通證發放概覽

通過在以太坊鏈上創建 ERC20/ERC223 兼容的通證智能合約，ExCraft 交易所將發放一百億枚 EXT 給不同的集團。通證的發放配置為，70%獎勵給社區，30%為內部生態構建。獎勵給社區的總額中，有40%用於存在證明的獎勵，10%用於交易礦池獎勵，10%用於私募和 ICO，而20%用於權益證明獎勵。剩余給內部的20%將平均分配給生態系統、團隊，每部分得10%。

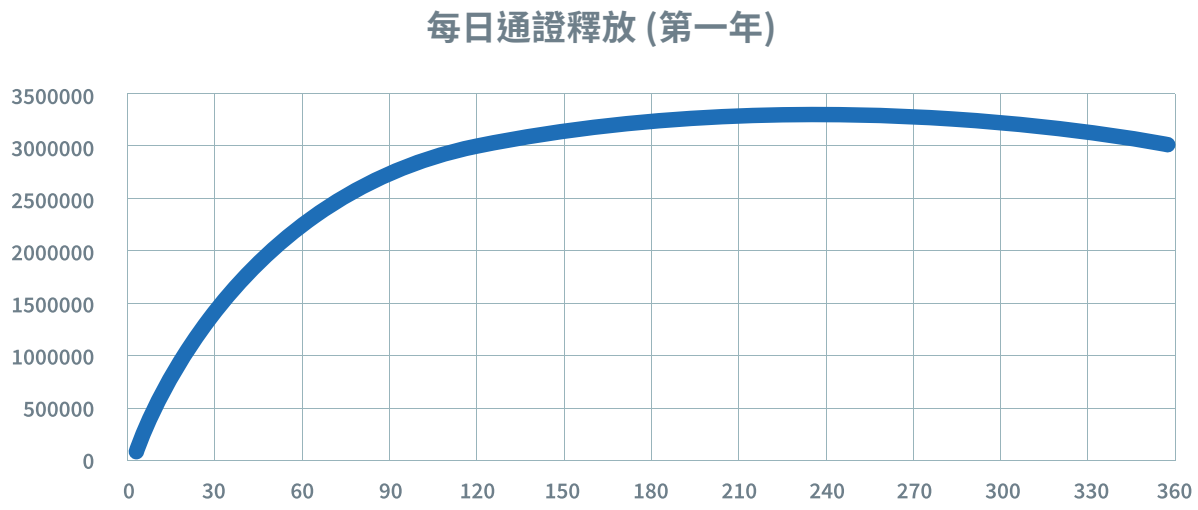


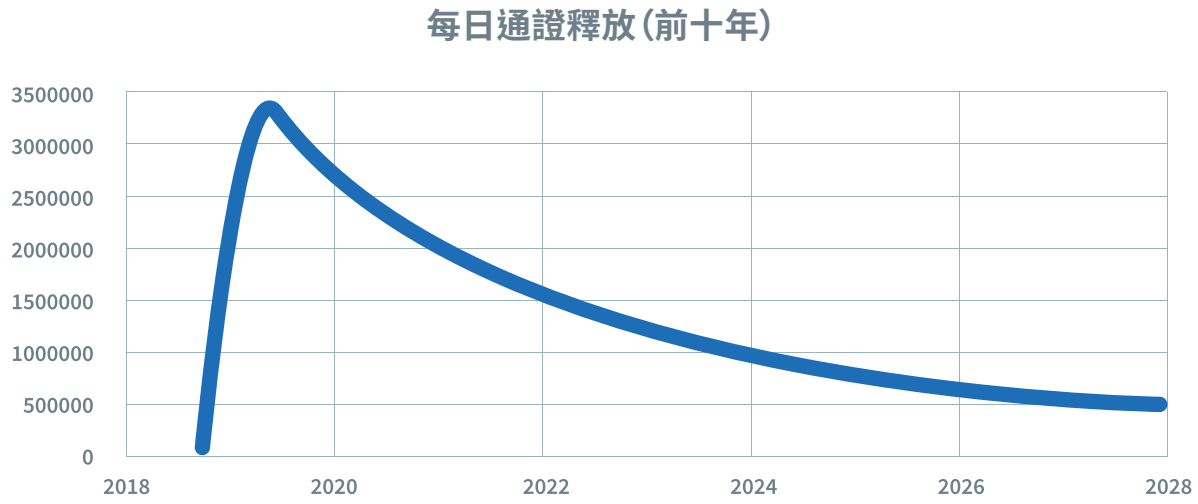
基於最終目的為減少每日獎勵的方程式，存在證明、權益證明和交易礦池獎勵設定的以太坊智能合約每出 5760 個以太坊區塊將自動獎勵通證，直至所有通證在 74037 次獎勵周期後消耗完畢。以太坊平均 15 秒出塊，因此我們可以預計這種每日獎勵可持續約 202 年。

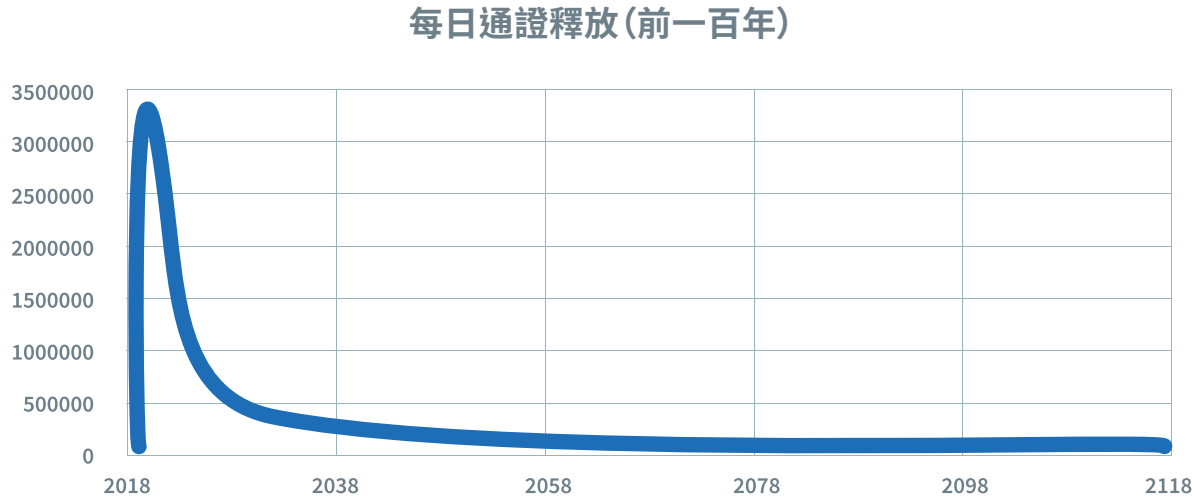
“每日”獎勵的通證計算方程式為:

$$y(x) = 3293005.88008333 * e^{-\left(\frac{\ln\left(\frac{x+5}{365}\right)+0.5}{2}\right)^2}$$

編寫該方程式是為了能讓交易所在最初十年內釋放出數量眾多的通證，但其預計使用壽命有很大的潛力。







当持有人在 ExCraft 交易所卖出 EXT 社区奖励或内部通证后，即可开始购买通证。

存在證明(PoE)獎勵

所有買家和賣家交換且包含公開交易費的資產轉移都可以視為存在證明(PoE)。通過選舉 ExCraft 將通過運用以太坊鏈來實現每產生 5760 個區塊就更新最新結果，且以“不少於每天一次”的頻率發表這些結果。

這種存在證明的價值計算取決於每筆資產的對應市值，計算方法為該階段結束時的收盤價乘以每筆交易的金額。這種方法也會用於計算單個散戶的交易行為，並寫入區塊鏈，同時用一個獨特的識別符保護用戶的隱私。計算方法還包括總買賣數除以每個注冊用戶地址，這樣可以對社區提供透明度。

用戶將可以指定外部錢包地址進行 PoE 分配，用戶如不將平台賬號與外部錢包地址鏈接起來即無法參加分配。然而，所有未鏈接外部錢包地址至交易所的用戶既無法參與社區 DAO 投票，也無法獲得獎勵或其他衍生回報。

要證明一次交易的發生，既需要記錄每個市場的買賣數量，也需要了解包含所有可能交易的交易對。這樣我們即可確保 ExCraft 交易所實現自己對 80%的交易費所做的承諾，即通過對比 EXT 市場檢查區塊鏈上交易所自己的交易，來確認是否發布的日常交易費用 80%有用於回購 EXT 通證。ExCraft 使用證偽法的鑒別方法來保證獎勵公平。通過 ID 和基於交易情況的相關獎勵，每個單獨用戶都可以查看自己在交易所上的交易量。盡管部分信息由於安全原因會進行遮掩，但所有的用戶都能查看其它用戶的日常活動和相關獎勵來鑒別交易所是否有獎勵交易額。

權益證明獎勵

用戶有機會持有通證並享有增值。在交易所賬號或在與交易所賬號相關聯的錢包地址裡持有通證的用戶每日將因為持有通證而獲得額外獎勵。

盡管通證的供應量是固定的，但除去交易所運營成本，ExCraft 會特意依照當前市價把更多交易收入花在回購 EXT 通證上。這些通證會發开給鎖定的智能合約來減少即時通證總供應量，並為整個社區提高交易所通證的價格。

交易礦池獎勵

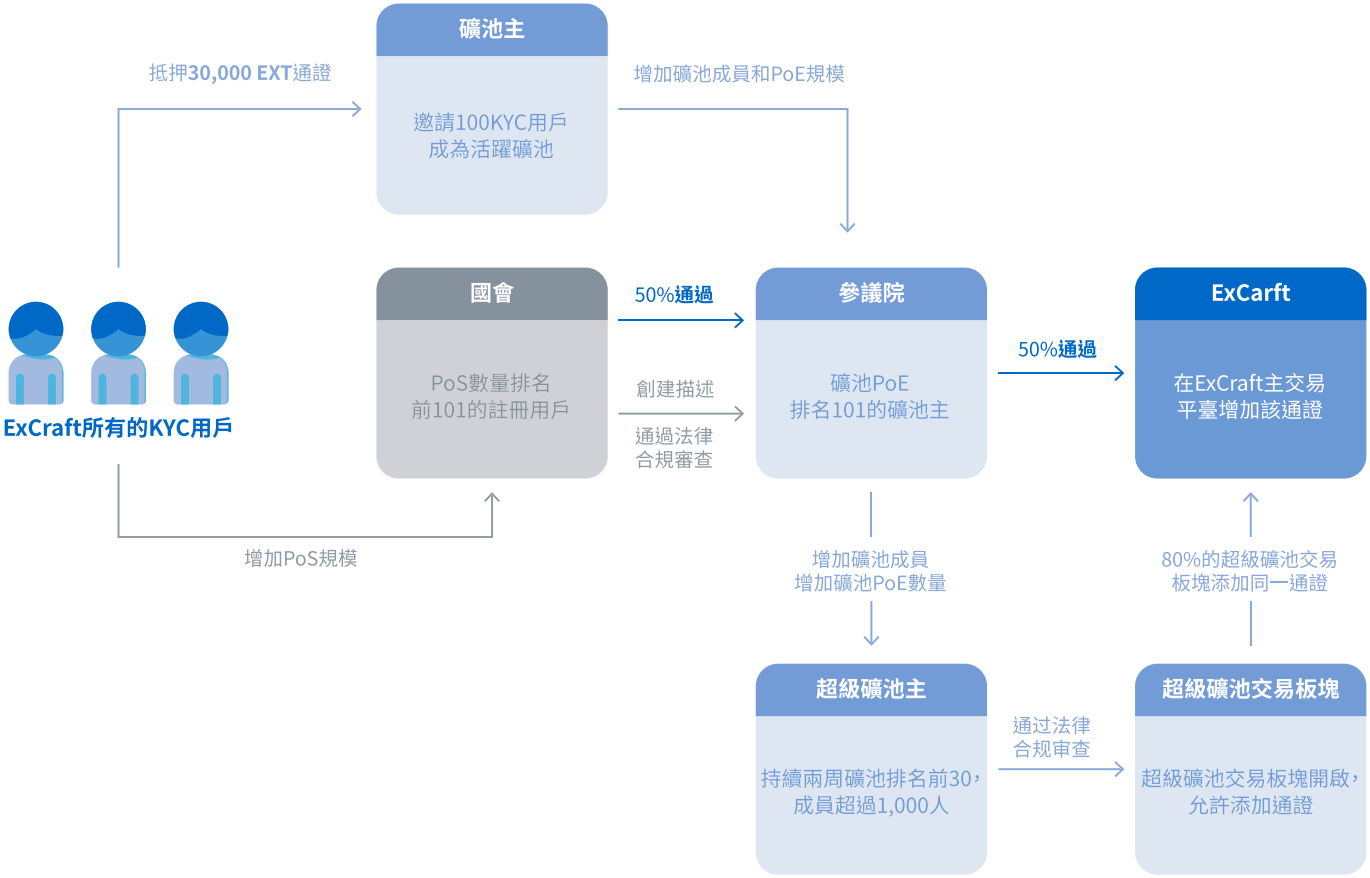
用戶可以加入其它用戶的交易礦池來增加獲得發放更多每日通證比例的機會。任何用戶可以抵押 30000 枚 EXT 通證來創建自己的礦池，並被委任成為一個礦池主。任何用戶隨即可以加入該礦池，並把自己的 PoE 計入該礦池的總 PoE。當一個礦池包含了至少 100 個 KYC 用戶，且該礦池所有成員的 PoE 相加後該礦池 PoE 總量排名能位於 ExCraft 前 101 位時，該礦池即有資格領取礦池獎勵。根據 PoE 貢獻量，該交易礦池會自動按 PoE 比例發放獎勵給所有的交易礦池成員，但是，交易礦池主可以通過選舉保留一定比例的獎勵。通過每個用戶交易行為或鼓勵其他用戶在自己的交易礦池內交易，用戶將增加其 EXT 投資組合供應和最終的估值。

用戶可隨時選舉加入不同的交易礦池，但出於計算原因，他們的 PoE 將鎖定在單個交易礦池中最長達 24 小時。通過這種方式，我們希望鼓勵交易礦池主能公平發放獎勵，同時鼓勵交易礦池成員用 PoE 總量來獎勵交易礦池主。

一個礦池主可以解散礦池並在解散後 24 小時內返還成員抵押的通證。礦池主既可以強迫其礦池裡的所有成員廿到礦池外來解散礦池，也可以選擇自動把所有的礦池成員轉移到任何其他礦池來解散自己的礦池。

去中心化自治組織

基於真實交易的存在證明既可以讓智能合約的投票基於 KYC（了解你的客戶）系統已核實的用戶賬號，也可以讓精英投票系統建立在單個或者加入了交易礦池的用戶交易量上。用戶可以對交易所是否上線新項目進行投票。ExCraft 社群重視所有用戶的投入，也注重交易最為頻繁的用戶。因此，所有的投票將會由一個國會和一個參議院投票來決定。



權益證明代表組成的國會

權益證明代表組成的國會將是精英管理，其管理成員為根據智能合約顯示的持有 EXT 通證數量在前 101 名的用戶。任何國會的現任代表都可以提出一個投票主題。其他用戶必須聯系國會的一名現任代表來提出投票主題。

用戶也可以在 dApp 網頁進行投票，用注冊公匙通過 Metamask 的瀏覽器插件或者其他合適的區塊鏈客戶把自己的投票寫入智能合約。投票完成後，投票結果將在 ExCraft 交易所展出，也可以很容易地通過區塊鏈簽名進行驗證。

每個投票都必須以“通過”或者“不通過”的方式執行。如果國會通過一個提案，則該提案會被提交至參議院進行二輪投票。

交易礦池主代表組成的參議院

沒有存在證明的 ExCraft 平台是無法可持續運行的。即便人數較少，但那些直接投入了存在證明的，或者在一個交易礦池中聯合他人的，都是不容忽視的股東。國會通過的所有投票都將以新智能合約的方式提交給參議院。該參議院由成員持有的 PoE 數量排名前 101 名的交易礦池池主組成。

第二階段的流程將力求平衡，有能力通過立法的參議院必須執行民主制。相反，只獲得一票的人必須說服那些有存在證明的交易礦池參議院來通過他們的立法。如果該參議院沒有通過，則該國會成員完全可以換一個交易礦池，在新一輪投票中把 PoE 投票權轉移給新的交易礦池。

投票伊始，參議院的智能合約就會追蹤所有可用的白名單交易礦池中的 PoE。一旦投票開始，就不會再考慮創建新交易礦池來投票。每天，每個交易礦池的 PoE 都將用於投票。每個礦池的運營方可以基於對問題進行投票當天的礦池可用 PoE 來投票。每個投票都必須以“通過”或者“不通過”的方式執行。如果參議院以 50%的同意率通過該議案，則該議案將由交易所代表社區進行實施。

PoE 排名前 30 的參議員礦主，保持 1000 名 KYC 用戶兩周之後既有資格成為超級礦池主。如果兩周後跌出前 30 名，則該超級礦池主的資格將在跌出榜單後的 180 天後失效。除了礦池主以及參議員的所有權利外，超級礦池主還擁有成立超級礦池交易板塊的權利，能讓ExCraft 團隊給其超級礦池交易板塊上幣其無需 DAO 事先投票通過。盡管該請求流程仍需要經過 ExCraft 團隊法律審核和實施的同意，但至少可以給超級礦池主一個選擇，即比交易所其他方更快上線新通證。如果一個超級礦池主的任期到期，則所有上線的定制通證都將停止交易，除非 DAO 代表整個 ExCraft 社區同意該通證，或超級礦池主復任，或前超級礦池主加入現任超級礦池主運營的礦池，後者可選擇是否繼續上線該定制通證。

如果80%的超級礦池主（即 24 位超級礦池主）同意上線一個定制通證，則該通證就可以自動並永久由所有的 ExCraft 交易所用戶使用，且無需 DAO 投票。

ExCraft 平台

當前架構

ExCraft 交易平台部署在谷歌計算平台上，通過 Docker 以及 Kubernetes 管理的微服務架構實現模塊化和可擴展性。主機托管平台的特定硬件所限制的中心化架構會產生擴展性問題，而雲原生的方法可以讓 ExCraft 解決這一傳統問題。交易平台上可以用各種語言，包括 Python，Go，和 C 語言。

去中心化的能力

隨著 ExCraft 團隊持續開發實施主網，我們的目標也將從中心化的主要交易平台服務向去中心化的架構轉移，可靠性和規模水准不變，也不會降低安全性和性能。主網可以跨鏈兼容，通過智能合約為支持的交易對提供原子交換，而無需第三方的參與。另外，用戶將全權控制私鑰，以此解決隱私和風險問題。

安全性

要想讓用戶信任自己的服務，一個交易平台的安全性至關重要。如果用戶無法信任底層平台執行，他們完全可以去別處交易，這樣平台將會失去流動性，最終失去競爭力。因此，盡管本書並不提供對所有安全政策和實施的詳細描述，但 ExCraft 在設計之初就設立了一個把信任貫穿整個基礎設施、服務、平台、運營和總體架構的安全模型。

基礎設施

在基礎設施層面，谷歌雲提供了高信任度和可靠的物理基礎設施，並用於構建安全雲服務平台。ExCraft 依靠很多物理和底層基礎設施服務來確保多方安全性，包括數據中心合規、encryption at rest、私鑰管理、入侵檢測和預防，全球負載均衡，以及用於選擇備份網址的災備（disaster recovery）區(Google, 2017)。我們還和 CloudFlare 建立合作關系，以此預防拒絕服務（DoS）攻擊、強制執行帶有強大密碼和關鍵優勢的外部加密、並阻隔攻擊 (CloudFlare, 2017)。

服務

我們提供的服務不僅使用 Docker 提高運營效率，通過網絡隔離和資源管理還可以劃分關鍵服務（Critical Service）來減少安全風險 (RedHat, 2017)。如果在某項服務中找到弱點，我們會使用 Kubernetes 加強版的 Docker 容器來強制執行“默認拒絕”，以此減少攻擊者利用其它服務篡改另一項服務的可能性。

平台

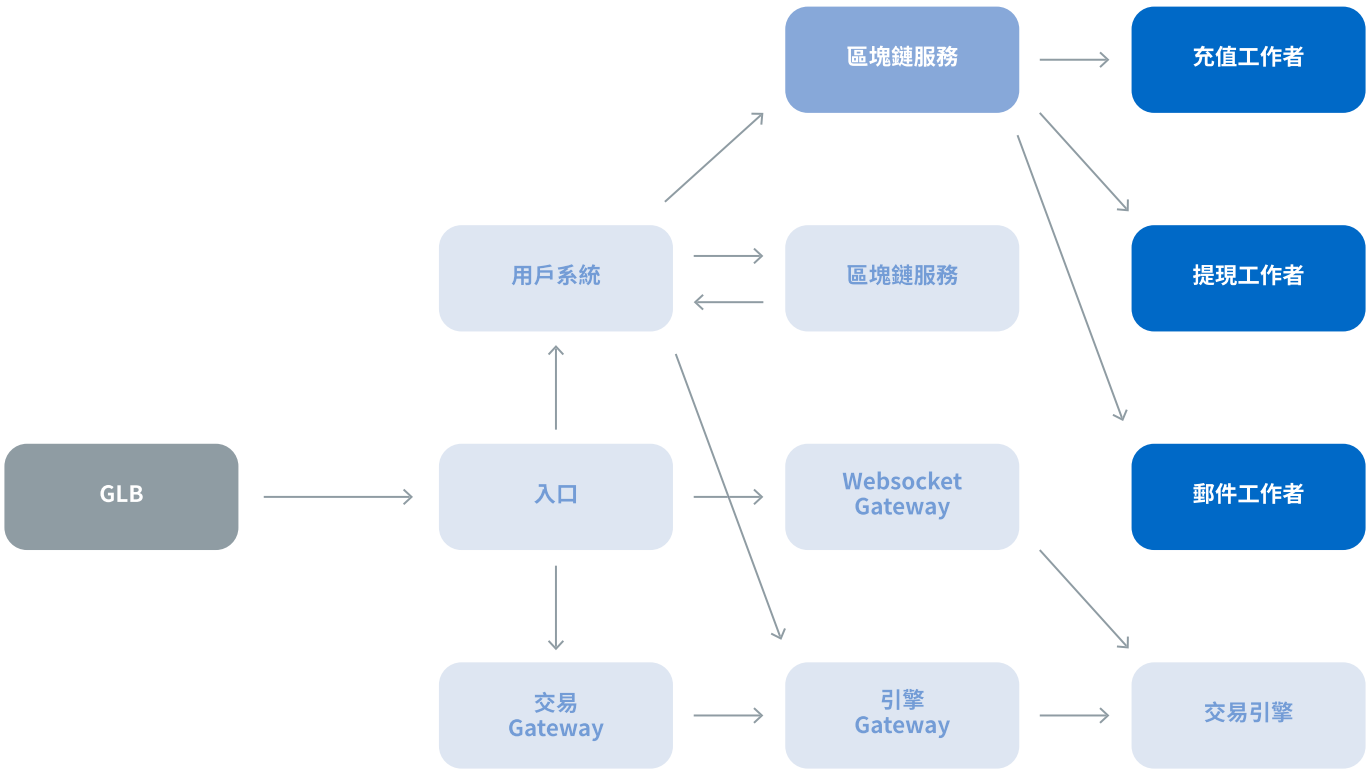
我們底層設施和特制的服務結合後，最終建立的平台連接了融合 Istio 和 GRPC 的輕量級進程（LWP）。

弱點管理

ExCraft 利用第三方提供商，通過結合商業用途和特制的室內工具、自動和人工集中滲透強度、保質流程和軟件安全評估和外部審計，積極掃描安全威脅。安全團隊負責追蹤並跟進變化的弱點。一旦查到需要改進的弱點，就寫入日志，並根據嚴重程度分配給負責人。弱點管理團隊會不斷追蹤並跟進這個問題，直到確認該問題得到修復為止。ExCraft 還會和安全研究社區成員保持聯系和溝通，來跟進 ExCraft 服務報告的問題和開源工具。

監測

ExCraft 采取的是一套穩健的主動被動相結合方案，來收集內部交易系統的指標、見解和弱點。這些數據的分析包括解析和自動通知的商業和開源工具。如果出現未解決的威脅或運營問題，將自動和人工啟動流程通知我們相關的運營和安全團隊員工。



團隊介紹

Roy Lam kt

CEO

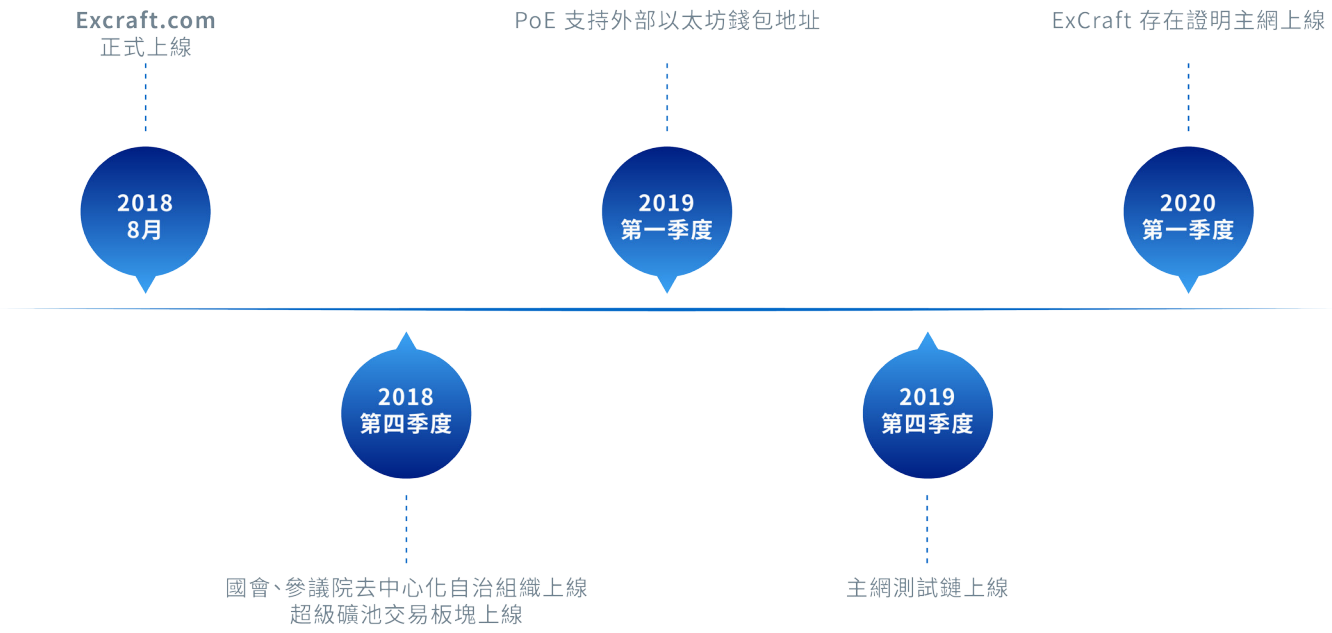
林建東是早期比特幣投資者、投資基金經理、世界頂級高智商協會門薩會員。他是中國收視冠軍的大腦科研節目江蘇衛視《最強大腦》中的中國隊隊長，被譽為全香港最聰明的人。他早期曾在“2010威爾士公開記憶力錦標賽”榮登“亞洲記憶王”。同時他也是一名TEDx 演講者。

Benjamin Chodroff

CTO

Benjamin Chodroff是ExCraft的首席技術官，負責監督所有技術層面和戰略方面的規劃。他有著超過十年的經驗，在擔任IBM的高級IT架構師和ClearObject物聯網和雲解決方案開發的首席技術官時獲得了多項專利。他從2013年開始就一直從事分布式分類帳技術的工作，他在2010年開始就對比特幣有著很濃的興趣。他在凱斯西儲大學獲得了計算機工程學士學位。

路線圖



1. 2018 年 8 月 – ExCraft.com 正式上線
2. 2018 年第四季度 –國會、參議院去中心化自治組織上線
3. 2018 年第四季度 – 超級礦池交易板塊上線
4. 2019 年第一季度– PoE 支持外部以太坊錢包地址
5. 2019 年第四季度 – 主網測試鏈上線
6. 2020 年第一季度 – ExCraft 存在證明主網上線

引用作品

(2018). Retrieved from 0xProject: https://0xproject.com/pdfs/0x_white_paper.pdf

(2018). Retrieved from Kyber Network: https://kyber.network/

BitShares. (2018). Retrieved from BitShares - Your share in the Decentralized Exchange: https://bitshares.org/

CloudFlare. (2017). *Cloudflare Advanced DDoS Protection*. Retrieved from https://www.cloudflare.com/media/pdf/cloudflare-whitepaper-ddos.pdf

Google. (2017). *Encryption in Transit in Google Cloud*. Retrieved from https://cloud.google.com/security/encryption-in-transit/resources/encryption-in-transit-whitepaper.pdf

Komodo. (2018). *Decentralized Exchange*. Retrieved from Komodo Platform: https://komodoplatform.com/decentralized-exchange/

RedHat. (2017). Retrieved from TEN LAYERS OF CONTAINER SECURITY: https://www.redhat.com/cms/managed-files/cl-container-security-openshift-cloud-devops-tech-detail-f7530kc-201705-en.pdf