LEXEL 鏈鎖

基於區塊鏈的芯片級
數字身份認證硬件基礎設施

白皮書 V2.0

www.lexel.io

LEXEL

提供完整的個人數字資產

安全保值與增值解決方案

www.lexel.io

概述

當前互聯網的驗證操作，無論是登錄密碼、資金密碼亦或是短信驗證碼等等，黑客都可以通過程序截取甚至模擬。很多硬件層面的加密也只是內存級別，同樣可以截取並模擬。互聯網、物聯網、區塊鏈等多領域都存在嚴重的安全問題，且形勢越趨嚴峻。

LEXEL 是數字身份認證與數字資產安全解決方案提供商，基於區塊鏈技術為用戶提供個人身份認證與信任公鏈，並提供完整的個人數字資產安全保值與增值解決方案。可應用在個人可信數字身份，數字資產錢包與數字貨幣交易所等場景。

當前互聯網與金融行業數字認證（CA）應用廣泛，但傳統數字認證基於中心化企業作為認證機構，面臨信息濫用、內部管控等各種風險，也造成各家認證機構各自為政，無法被完全信任。

當前區塊鏈技術引領的價值互聯網，需要壹個可信的個人身份識別體系作為價值交換的底層基礎，基於這個基礎，才能進壹步拓展個人與機構，個人與個人的可信價值交換，LEXEL致力於成為價值交換的底層基礎，為區塊鏈應用場景的繁榮，提供可信的底層身份認證信任公鏈。

基於 LEXEL 的身份認證信任公鏈，還為用戶與機構提供完整的數字資產安全解決方案，保證數字資產的安全。更進壹步，LEXEL將面向未來，發展數字資產增值生態，在公鏈上建立智能合約，完備的解決數字資產交換問題，促進個人與個人，個人與機構之間信貸，投資生態建立。

目錄

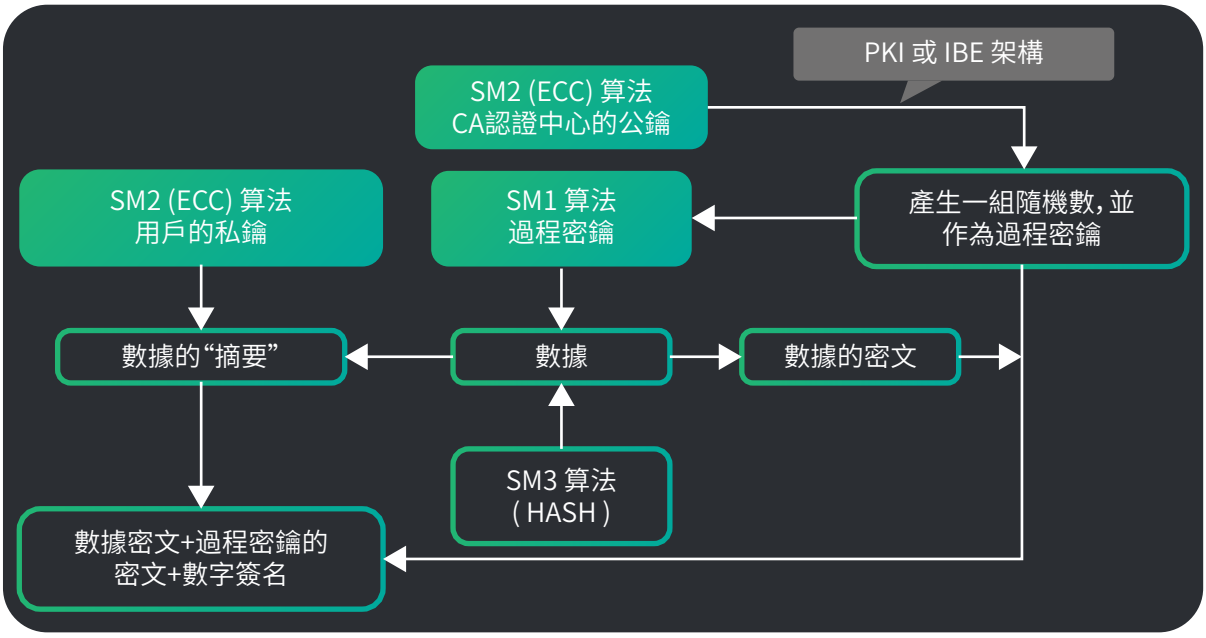
1. 市場概述

1.1 市場背景

20世紀80年代，美國學者提出了PKI（公開密鑰設施）的概念。為了推進PKI在聯邦政府範圍內的應用，美國在1996年成立了聯邦PKI指導委員會;1999年，PKI論壇成立;2000年4月，美國國防部宣布要采用PKI安全倡議方案。2001年6月13日，在亞洲和大洋洲推動PKI進程的國際組織宣告成立，它就是“亞洲PKI論壇”，其宗旨是在亞洲地區推動PKI標準化，為實現全球範圍的電子商務奠定基礎。

什麼是PKI?

PKI是Public Key Infrastructure（公開密鑰基礎設施）的縮寫，是壹種普遍適用的網絡安全基礎設施。壹些美國學者把提供全面安全服務的基礎設施，包括軟件、硬件、人和策略的集合叫做PKI，但我們的理解更偏重於公開密鑰技術。



▲ PKI 認證架構邏輯圖

數字證書是PKI中最基本的元素，所有安全操作都主要通過證書來實現。PKI的部件還包括簽署這些證書的認證機構(CA)、登記和批準證書簽署的登記機構(RA)以及存儲和發布這些證書的電子目錄。除此之外，PKI中還包括證書策略、證書路徑、證書的使用者等。所有這些都是PKI的基本部件，它們有機地結合在壹起就構成了PKI。

可提供的服務

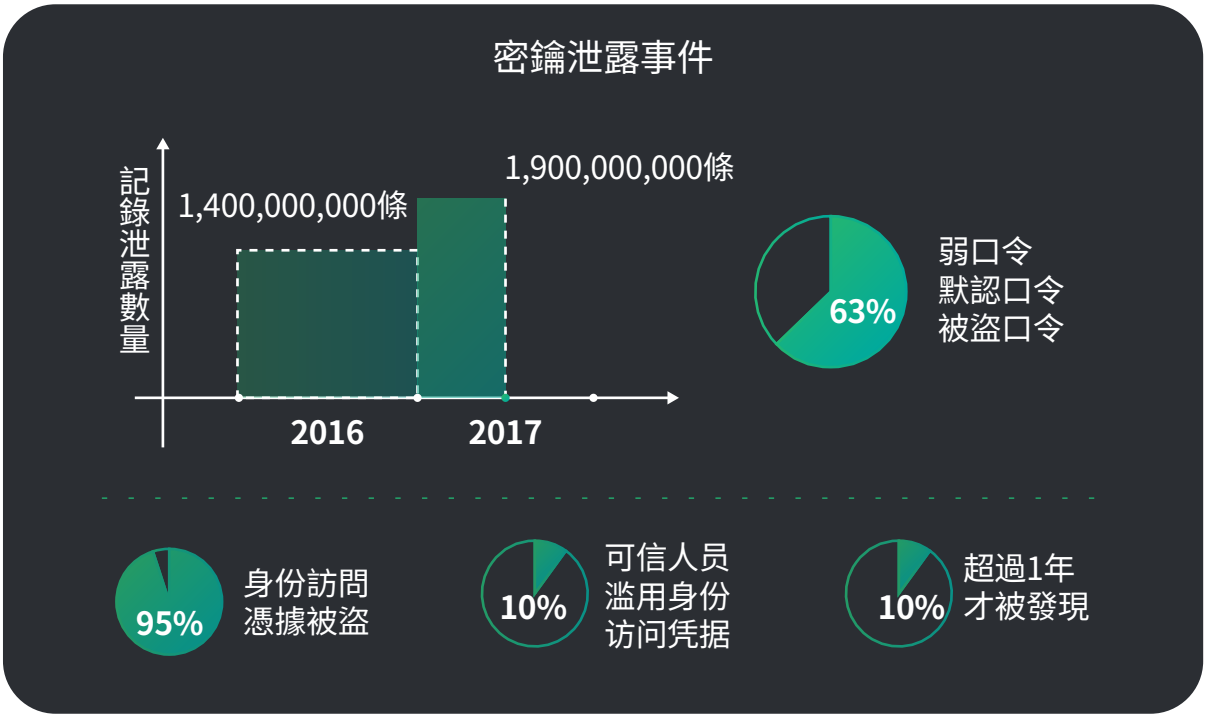
PKI已經廣泛應用在金融、電子政務等領域，如網上銀行使用數字證書確定使用者身份、企事業單位信息系統使用基於硬件的USBKEY或IC卡進行身份鑒別及其他信息保護等。其中在安全電子郵件、web安全應用（SSL/TLS）、VPN、IP/sec與電子商務上的應用尤為突出。

1.2 存在的風險

PKI的安全包括太多的方面，包括設備安全、運行安全、協議安全等。盡管PKI有如此多的應用場景，但PKI存在幾大致命問題：

• 安全性低

在當今的互聯網中，服務器認證用戶的主要方式是密碼系統。用戶在首次使用網站時創建密碼，以便在隨後的訪問中確認其身份。市面上數字簽名認證大都屬于軟件級別與內存級別的加密，密碼容易被黑客模擬或者盜取，用戶信息與資金存在較大風險。包括密碼較弱，密碼過于複雜，每個站點需要一個唯一的密碼，以及恢複被遺忘密碼的不便。



• 性能不足

PKI技術是基于RSA加密算法，需要建立CA數字認證中心，采用第三方參與的方式，密鑰采用分散生成集中存放方式。隨著用戶的增長，與滿足加密安全性的要求，PKI只能延長RSA算法的密鑰。陷入數據庫數據量愈發龐大，運行速度愈發低下的死循環。

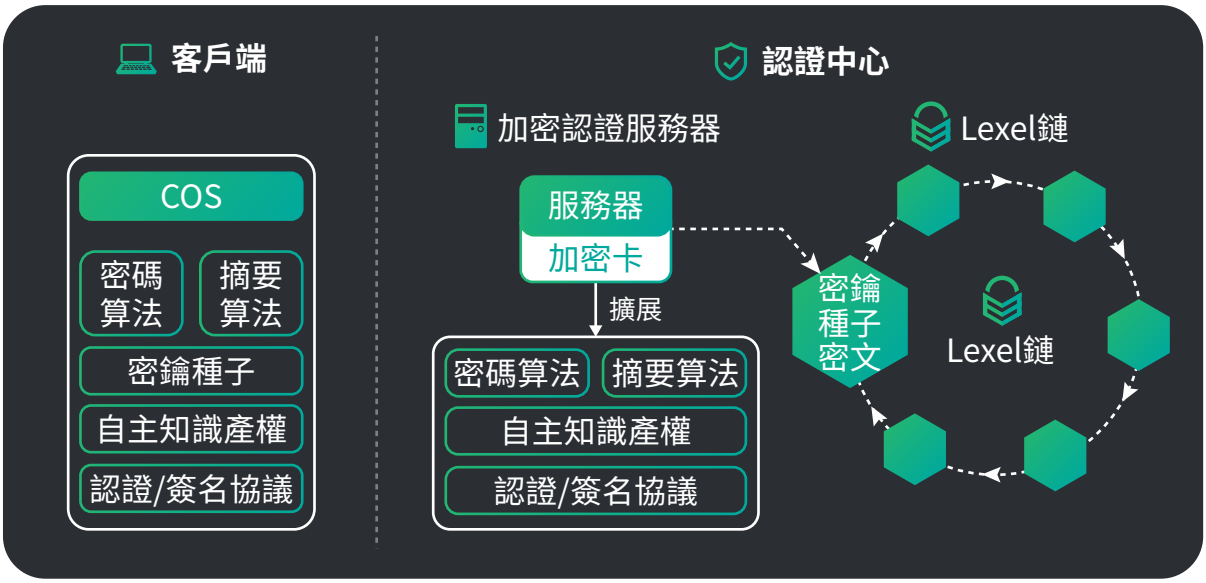
• 成本偏高

PKI的認證過程需要龐大的證書數據庫進行在線比對認證。每1000多用戶，就要建立一級CA及一套數據庫存放證書與密鑰，數據庫在線比對認證速率低，管理用戶量小。同時由于龐大的數據庫與服務器架構，需要大量的運維人員去保障設備的安全，運營負擔沈重。

2. 關鍵技術優勢

2.1 LEXEL 數字加密與安全認證技術

LEXEL 體系是由身份認證、數字簽名、密鑰交換和數據加密協議組成。通過采用自主産權算法（如：密碼算法、摘要算法），完成身份認證、數字簽名、密鑰交換和數據加密等4種功能。



▲ 加密芯片架構

其中的技術關鍵在于，如何解決單鑰密碼算法的密鑰管理世界性難題。主要具備以下特性：

2.1.1 自主可控性

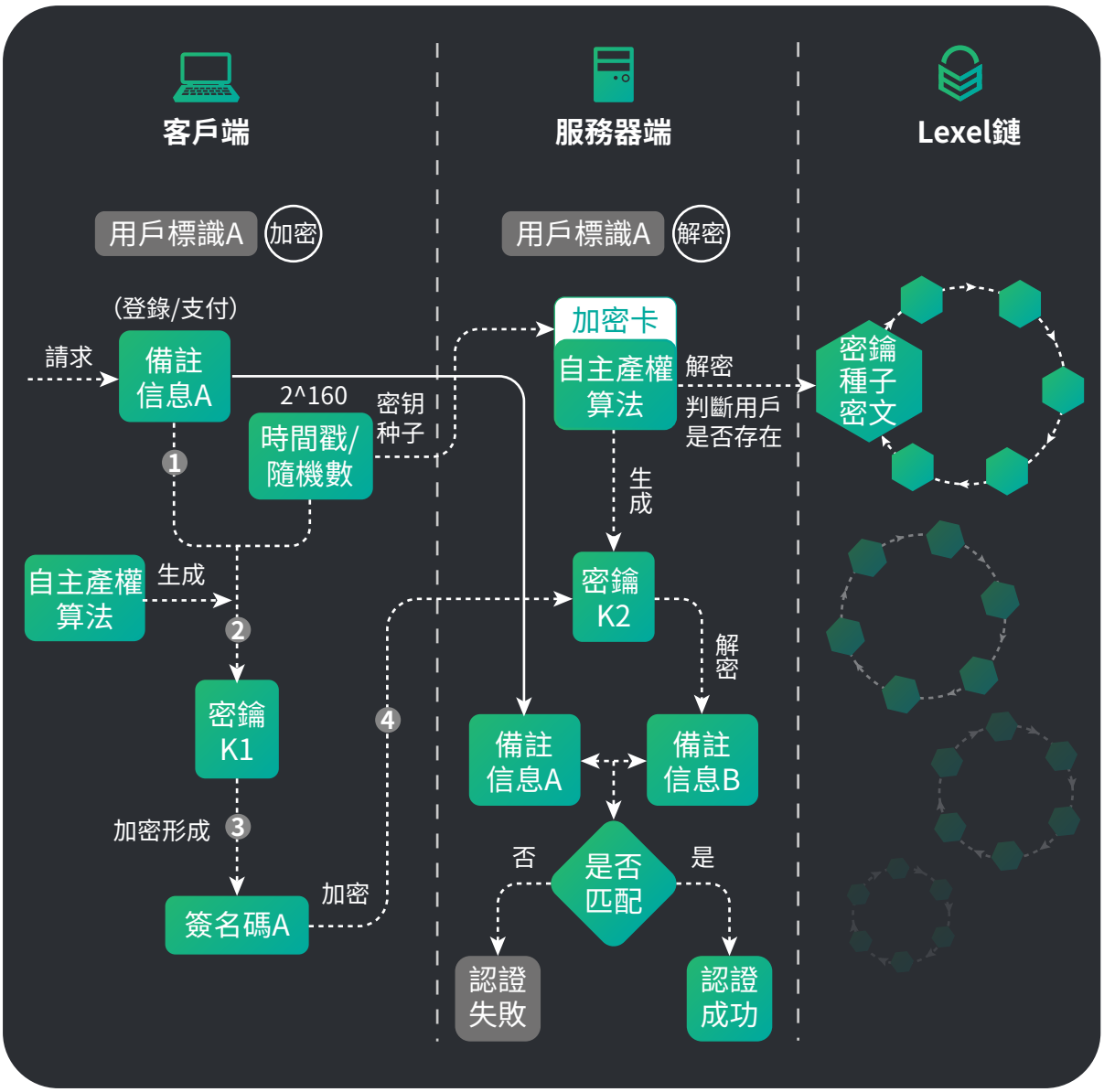
自主可控就是依靠自身研發設計，全面掌握産品核心技術，實現信息系統從硬件到軟件的自主研發、生産、升級、維護的全程可控。LEXEL 100%采用自主開發技術，從加密設備到算法，操作系統到數據庫，均采用國家級標准，是真正實現産品從硬件到軟件等個個環節都做到自主、可控。

2.1.2 與傳統認證技術對比的先進性

(1) 架構對比

PKI等傳統認證技術采用需要用2套算法，2+3次算法及調用，完成標準認證流程，密鑰與設備固定匹配；而“LEXEL”調用1次單鑰算法，即能完成所有認證流程，並且通過芯片計算，做到密鑰壹次壹變。

“LEXEL”不僅簡化了認證過程，大大提高了認證速度和並發量，更保證了認證安全性。



▲ 加密與解密過程原理圖

(2) 參數對比

性能/認證模式	LEXEL	PKI或IBE（国外技术）
安全性	高（芯片级认证）	低（内存级认证）
認證\簽名速度	比PKI或IBE快100倍-200倍	慢
認證中心管理用戶量	已证实案例达3亿， 理论可达十几级	无法保证千万数量级 以上的良好运作
認證中心建設成本	比PKI或IBE少80%	高
系統維護人員	比PKI或IBE少70%	多
核心技術	自主可控	半自主，不可控

(3) 國際對比

2011年初，奧巴馬政府為實施“網絡身份證”國家戰略，撥款5.63億美元新技術研發經費（比15年用於航天發動機研發費用高壹倍多）。期望研發新技術建立美國3億人口體量的網絡ID，但至今，新認證技術仍未問世，由於傳統認證技術的代表PKI/CA及IBE體系無法做到大並發量的商用要求，美國這壹國家戰略受到傳統技術“短板”的制約而失敗。

通過“LEXEL”技術，以3億用戶為基礎，建立壹套LEXEL系統。經《軟件產品質量檢測中心》檢測，該系統運行良好，足夠支撐3億用戶使用，並發認證達到1228.50次/秒，並發簽名驗證達到823.93次/秒，各項指標均優於傳統認證中心的上限指標。

2.1.3 技術評價、技術獎項與技術專利

“LEXEL”技術已獲得13項發明專利，系統檢測結果均為國際領先水平，並獲得中科院院士高度書面評價，通過專家組論證獲得密碼學頂尖專家團隊的高度認可，並給予“LEXEL”——“技術領先歐美至少十年”的評價。

業內國際大獎

《英國金皇冠獎》

英國國際發明博覽會最高榮譽

《韓國國際發明銅獎》

韓國國際發明展大會銅獎

《中國國際發明金獎》

中國國際發明展覽會最高獎

專利資料

“LEXEL”加密技術所獲得的發明專利清單，共13個如下所示：

No.	專利內容	數量(個)
1	密碼算法發明專利	2
2	數字簽名發明專利	1
3	密碼防盜發明專利	2
4	數據傳輸發明專利	1
5	網絡身份認證發明專利	1
6	手機認證發明專利	1
7	物聯網認證、加密傳輸和控制發明專利	3
8	銀行卡防盜加密發明專利	1
9	VPN加密發明專利	1

2.2 LEXEL 的區塊鏈核心技術

LEXEL 的区块链核心组件包括区块链基础设施、区块链协议、密码学算法等，具体而言有P2P网络通信协议、分布式计算技术、分布式存储技术、加密算法和隐私保护算法、密钥管理机制、共识机制、智能合约、标准代币协议、钱包SDK等技术。以下，我们将挑选LEXEL的重点创新模块进行阐释。

2.2.1 DPOS+BFT並行

(1) 現有區塊鏈底層的性能無法支撐商業級應用

區塊鏈作爲一套去中心化的解決方案，其核心在于共識與治理方式。比特幣誕生時間較早，估計發明者本人最初也未曾考慮過比特幣的流通範圍竟然能遍及全球，因此采用的POW工作量證明機制，要求每個節點都參與競爭式記賬（挖礦），每一個記賬節點都需要通過處理交易、維護全系統的備份，且節點還無限制地開放，導致區塊鏈的節點網絡逾日臃腫。

區塊鏈網絡擁堵造成三個顯而易見的惡果，其一，吞吐量極低。比特幣形成一個區塊的時間是10分鍾，以太坊形成一個區塊的時間是14秒左右。例如在以太貓應用上線的高峰期，以太坊積累了數百萬條未確認交易，僅僅一個智能合約的小應用已經無法承載，這也是公有鏈應用遲遲未見落地的主要原因。其二，手續費極高。由于記賬節點（礦工）處理能力有限，只能優先處理支付了高gas的交易，競爭之下，每筆交易的手續費水漲船高，導致高頻率的應用喪失成本優勢。其三，實質形成財力中心化。由于挖礦難度增加，算力逐漸集中，能源被大量浪費，記賬者開始以財力換取算力，礦機集中形成礦池，本意是去中心化的比特幣已淪爲大礦池壟斷的工具。

因此，公有鏈在2018年的最關鍵需求便是性能的提升。一方面，既要求新一代的公有鏈基礎設施能像Google、Facebook、阿裏巴巴一樣，能支持千萬級乃至億萬級的活躍用戶，支持並行計算及實現高效率低延遲的交易；一方面，又要求能低成本甚至零成本地讓個人用戶享受到區塊鏈應用的好處，從而幫助Dapp生態發展出更大的用戶規模、擴大用戶使用頻率、提高商業利

潤;另一方面,還要求能讓區塊鏈生態的創建者與最初的加入者受益最大化,而非被富有財力的後來者輕易掠奪。

(2) LEXEL 的共識設計

共識機制是區塊鏈系統中各個節點達成一致的策略和方法,是商定確定性交易順序和過濾無效交易的過程。可類比現實社會中,通過全民通過逐級的投票和評選,最終選出國家或企業領導人的過程。

在共識機制的設計層面,需要重點考慮公平與效率的均衡。公平性要確保所有的參與者都擁有記賬的權利,效率要求並不是所有的參與者無時不刻都要參與記賬,而是可以通過投票方式選擇代理人。最終,共識機制需要滿足業務場景對資源利用性、響應時間、處理時間、吞吐率和最大極限負載容量的要求。因此,LEXEL 在比較了POW、POS、BFT、DPOS等多類主流共識算法後,最終選擇采用DPOS共識。

DPOS全稱股份授權證明機制(Delegated Proof of Stake),通過引入"受托人"這個角色,降低過度競爭帶來負面影響,將記賬能力賦予專業化機構。LEXEL 賦予了給持幣人的持幣份額對應的表決權,而不是直接進行挖礦的記賬權。通過每個人持幣的比例與其擁有影響力的映射,體系的去中心化與民主得以達成。每個持幣人可以將其投票權賦予一名記賬代表(在項目前期,基金會將對記賬代表節點進行認證及甄選),獲得票數最多的前一百位代表按照既定時間表輪流產生區塊。

LEXEL 的DPOS共識算法旨在將主流主權國家的決策機制(如衆參議院、人民代表大會制等)引入區塊鏈系統,優點在于可以大幅縮小參與驗證和記賬的節點數量,實現幾秒內完成共識,同時提升效率、節省能源和確保公平。

LEXEL 的DPOS的工作原理如下:

第一,在正常操作模式下,塊生産者每3秒鍾輪流生成一個塊。假設沒有人錯過自己的輪次,那麽這將産生最長鏈。塊生産者在被調度輪次之外的任何時間段出塊都是無效的。

第二,在少數分叉情況下,不超過節點總數三分之一的惡意或故障節點可能創建少數分叉。在這種情況下,少數分叉每9秒只能産生一個塊,而多數

分叉每 9 秒可以產生兩個塊。這樣，誠實的 2/3 多數將永遠比少數（的鏈）更長。

第三，在離線少數人多重生產情況下，（離線的）少數人可以試圖產生無限數量的分叉，但是他們的所有分叉都將比多數人的那條鏈短，因爲少數人在出塊速度上注定比多數人來的更慢。

第四，在網絡碎片化情況下，導致沒有任何分叉擁有多數塊生成者。在這種情況下，最長的鏈將倒向最大的那個少數群體。當網絡連通性恢複時，較小的少數群體會自然切換到最長的那條鏈，明確的共識將恢複。

第五，在在線少數的多重生產情況下，少數節點B在其時間段內產生了兩個或更多可供選擇的塊。下一個計劃生產者（C）可以選擇基于B產生的任何一種方案繼續構建鏈條。一旦如此，這個選擇就成爲最長的鏈，而所有選擇B1的節點都將切換分叉。少數不良生產者企圖廣播再多的替代塊也無關緊要，它們作爲最長鏈的一部分永遠不會超過一輪。

此外，在缺乏明晰的生產者法定人數這種低概率的情況下，少數人還是可以繼續出塊。利益相關方可以在這些塊裏包括更改投票的交易。這些投票可以選出一組新的生產者，並將出塊參與率恢複到100%。一旦如此，少數鏈將最終超過所有其他以低于100%參與率運行的鏈。

歸根結底，LEXEL 的DPOS甚至在面對相當數量生產者舞弊的情形時也是安全的。因爲社區可以投票替換掉不合格的生產者，直到恢複100%參與率。這同時又能確保不斷優化誠實節點的數量，從而使得DPOS有能力在平均只有1.5秒的時間內以99.9%的確定性確認交易。

LEXEL的BFT共識機制進行了定制，實現秒級出塊，具備高一致性、高可用性，抗欺詐能力較強。

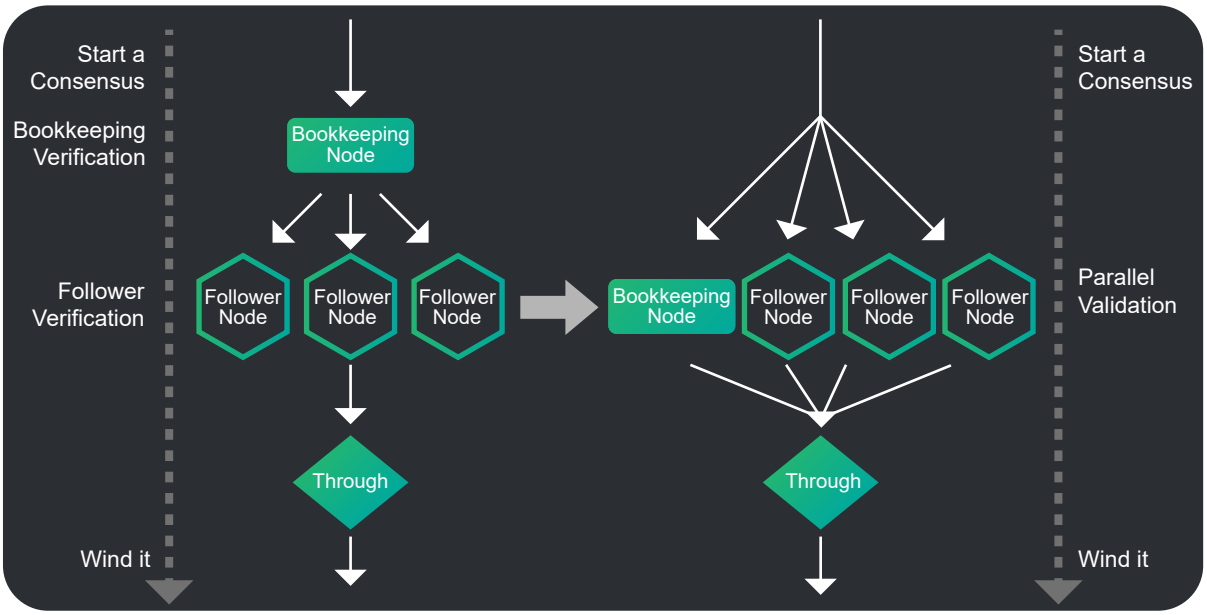
BFT算法的過程是一次提案，幾步投票直到最終確認，在這個過程中有複雜的狀態機維護過程，投票往返步驟較多，且部分流程在節點內部以及節點之間是串行進行的，每一步都會需要互相等待，在其他上一階段的計算完畢或網絡通信收集數據完成，達成階段性確認後再進入下一階段。

由于流程複雜，數據往返較多，共識過程也容易受網絡波動影響，對網路

延遲和丟包比較敏感，在狀況不理想的網絡和計算環境可能需要多次共識的嘗試才能達到最終一致性。

以上的技術挑戰給系統帶來的影響是，系統並行能力可能遇到瓶頸，或者交易的確認速度會偶發性延長。所以我們對BFT算法進行了深度的優化。

在LEXEL中，首先我們對共識過程進行了深入分析，按計算步驟，節點等維度進行分解，盡量讓所有的節點在每個階段的計算都是並行進行的，無論是議長節點還是投票節點，一個節點在運算驗證一批交易的過程中，其他所有節點也在同步運算和給出投票，不需要互相等待。



▲ 並行BFT共識流程

然後，我們對耗時較高，有次數冗余的計算過程進行了精簡，通過關鍵路徑優化，重複計算結果進行緩存等方式減少了共識過程中的每一步的耗時。

同時，我們對網絡健康度、節點存活等因素進行檢測，當發現有的記賬節點無法服務時，快速切換到下一個記賬節點，避免出現全體節點出現空等待的狀況。

最後，我們考慮到金融交易的場景常常有高峰期和空閑期的特點，在空閑期系統沒有交易流量的時候，共識機制進入心跳狀態，只維護網絡的健康狀態，不產生包含交易數爲0的空區塊數據，避免不必要的存儲浪費，以及避免空區塊的同步流量和時間消耗。

2.2.2 更安全的隱私保護算法—零知識證明

(1) 現有公有鏈的僞匿名及數據隱私泄露問題

比特幣一直以完全匿名作爲最大的賣點，但現實是，在大數據及監管科技工具之下，大部分的比特幣賬戶也是可以被完全追蹤的。雖然只要錢包地址不與個人法幣賬戶連接在一起，一個人就可以一直保護自己的隱私，但只要一旦在中心化的交易所中進行交易或提現，這個秘密就暴露了。目前，美國的執法機構已能夠在調查過程中識別特定的比特幣用戶。另一方面，由于數據在公共賬本中完全暴露，導致例如電子病曆、身份驗證數據、憑證管理、財務文件等一些需要強隱私的應用場景無法在公有鏈網絡中實現。

因此，在新一代公有鏈的隱私保護技術層面，需要重點考慮其安全需求。這可從保密性、完整性、抗抵賴性、可追溯性和真實性等角度入手。其中，保密性指區塊鏈系統確保其數據只能被授權用戶訪問的能力程度；完整性指區塊鏈系統防止未授權訪問、篡改程序或數據能力程度；抗抵賴性指區塊鏈系統針對活動或事件發生後可以被證實且不可被否認的能力程度；可追溯性指區塊鏈系統對每一個使用者的活動可以被唯一地追溯到該使用者的能力權限的程度；真實性指區塊鏈系統對目標或資源的身份標識確實能夠證實該目標或資源的能力程度。

(2) LEXEL 的零知識證明隱私保護算法

零知識證明是證明者在不向驗證者提供任何信息的情況下，使得驗證者相信他們擁有一些秘密知識。換句話說，一個程序可以有秘密的輸入，證明者不會向驗證者揭示任何東西。零知識證明提供了可用于構建隱私保護機制的基礎。零知識證明在區塊鏈隱私保護中的作用越來越重要。目前，在數字貨幣中嘗試使用零知識證明解決交易雙方的隱私問題。但是在應用模型上，已有的零知識證明方案只針對比特幣的UTXO模型，且很難推廣到以賬戶模型爲基礎的新型區塊鏈中，因此也制約了其對智能合約的支持。現有的零知識解決方案在生成證明時，先將證明內容轉化成門電路的形式，該過程需要消耗大量的計算資源和時間，因此證明只能在計算能力充足的節點（比如礦工節點）才能生成，這大大限制了其適用場景。

爲了加強匿名保護與隱私保護， LEXEL 擬將引進借鑒ZCASH的零知識證明技術以提升隱私保護強度。該零知識證明協議包含三個算法：KeyGen，Prove和Verify。KeyGen是一個隨機算法，輸入公共參數，輸出證明密鑰pk和驗證公鑰vk； Prove算法輸入證明公鑰pk,實例x以及證據a，輸出一個零知識證明π； Verify算法則輸入驗證密鑰sk,實例x以及證明π,輸出一個判定比特。零知識證明協議可以說服系統中的所有人相信，交易是正確進行的。但在賬本中不記錄交易地址，而只記錄由地址計算出來的序列號。這樣就隱藏了交易的用戶，起到保護隱私的作用。由于序列號是由交易地址經過哈希函數計算得到，根據哈希函數不可逆的性質，沒辦法逆推出交易地址，從而無法關聯同一用戶的兩個或多個交易。

此外，在區塊鏈本身的非對稱加密方面，LEXEL 通過通用的哈希摘要算法，通過在區塊中記錄上一個區塊的哈希值，確保了被記錄數據的不可篡改，並對數據完整性給予保護。對于給定的數據明文和哈希，LEXEL 可以驗證該數據明文是否被篡改。爲了防止區塊鏈的各方對記錄的數據進行抵賴。LEXEL 強化了數字簽名功能，用以確認數據單元的不可僞造性，即：確定消息確實是由簽發方簽署的。流程上，首先由簽名者用私鑰對信息原文進行處理生成數字簽名值，然後驗證者將利用簽名者公開的公鑰針對數字簽名值和信息原文驗證簽名。

2.2.3 更豐富與多樣化的智能合約應用

LEXEL 的智能合約參考了以太坊設計思想，提供一個圖靈完備的智能合約平台，讓開發者都可以編寫任意邏輯的程序。LEXEL 將定制一個用于執行合約代碼的虛擬機，智能合約的開發者可使用Solidity語言進行開發。LEXEL的CALL和CALLCODE指令的目標地址通過棧來傳遞，使得合約可以在運行時動態調用其它的合約代碼，使合約的調用路徑變爲非確定性。而智能合約可以訪問到的數據都是確定性的，使得所有節點在動態調用目標代碼時一定會獲得相同的目標地址，保證了系統的一致性。

針對目前智能合約較難進行形式化驗證的問題，一方面，LEXEL將盡可

能支持一些容易驗證的編程語言，例如Haskell和OCaml這樣的函數式語言會比C / C ++、Java和JavaScript等命令式語言更適合智能合約代碼，因爲它們的結構更容易推理和形式化驗證。一方面，在智能合約的樣板建議中，使用解釋而非編譯型語言，實際代碼在區塊鏈上可見，並且可以輕松檢查。最後，代碼永遠是難以完美的，LEXEL 將加入一定的基金會層面的治理機制，爲智能合約的升級、叠代、彌補漏洞提供一個合理的機制。

針對以太坊智能合約技術存在開發友好度不足的問題，LEXEL 將進一步深化開發出智能合約的管理器，並加入智能合約命名模塊，從而更加便于開發者進行智能合約的版本升級及命名管理。

2.2.4 SDK工具

爲了幫助更多的生態合作夥伴輕松接入LEXEL鏈鎖使用，LEXEL還將提供SDK工具，同時支持java和node.js兩種開發語言。在SDK基礎上，合作夥伴的開發者可輕松開發DAPP。屆時，生態合作的夥伴的客戶只需調用鏈上節點的功能接口，在客戶端上即可以訪問鏈上部分或全部的數據，向區塊鏈發起交易等。

在SDK的設計上，提供了簡易的接口，開發者只需關注具體DAPP的數據字段以及調用返回結果，而並不需要了解區塊鏈節點的具體部署情況，即可實現業務合約的管理、執行、交易查詢功能。這樣可以大幅度降低生態夥伴的開發門檻和成本，快速開發各種業務場景的應用。

2.2.5 LEXEL 的區塊鏈技術先進性

LEXEL的技術先進性可以從業務場景適用性、架構設計合理性、計算能力完備性、高速共識效率、超強加密與隱私安全性、可追溯與可審計性等多個維度中體現。

業務場景適用性——LEXEL將以提供更安全的基礎設施及原生幣的廣泛應用爲核心，深度改變數字貨幣行業的安全痛點，與傳統PKI不同，LEXEL將以真實的業務場景需求爲導向，保障業務流程的可靠性、時效性、穩定性。

架構設計合理性——LEXEL未來擬對鏈上有價值的可信大數據進行容災設計，實現系統、數據和鏈路的冗余備份，保證系統的可靠性和可用性，即便某個版本智能合約或DAPP的代碼出現漏洞，也不至于受到毀滅性影響，保證項目的高可用性。

計算能力完備性——價值可編程是區塊鏈技術的一個重要的本質屬性，直接決定了技術對業務邏輯的表達能力，計算能力的完備性具體體現在“智能合約”上。

高速共識效率——采用了當前最爲領先的高性能DPOS共識算法，基金會將對共識節點的配置建立高標准要求，實現秒級出塊，最高可支持百萬量級的交易並發。

超強加密與隱私安全性——涉及用戶重要隱私的數據需經過隱私保護處理，區分爲隱私敏感信息與公開信息。由于采用了硬件與軟件加密技術相結合，真正確保了用戶的信息隱私保護及資産確權，任何未受授權用戶都無法將被保護的信息解密，而只能閱讀公開信息。

可追溯與可審計性——通過區塊鏈技術的不可篡改和時間戳特點，可支持基金會進行監督管理、核查審計全部記錄並作爲相關的法律糾紛證據。

2.3 數字加密與區塊鏈的結合

傳統PKI 技術中，CA中心（Certificate Authority，證書認證機構）是信任的起點，只有信任某個CA，才信任該CA給用戶簽發的數字證書。但在具體應用中，PKI 技術存在如下問題：

- 單點失敗問題：處于核心的CA極易遭受攻擊，一旦被控制，CA根證書以及該CA 已經簽發的證書都不再可信。
- 多CA互信難問題：用戶證書只能由所屬CA的根證書進行驗證，不同CA之間不能相互驗證，現有CA互信解決方案適用性受限。

LEXEL結合區塊鏈技術的分布式數據存儲與共識機制等特點，實現去中心化認證的方式。因此，LEXEL與區塊鏈結合有以下幾點優勢：

1) 驗證節點如果遇到技術故障或遭受惡意攻擊，LEXEL不可能遭受全系統服務中斷。此外，用戶不可能在單一機構的突發事件下將其賬戶全局暫停；

2) 企業或者個人在使用驗證加密技術時，無需向傳統PKI的第三方CA申請證書或者獨立部署CA系統，只需要加入到LEXEL鏈的生態即可；

3) 結合DPOS+BFT共識，保障安全性，同時保證了TPS。

另外在當今的互聯網中，服務器認證用戶的主要方式是密碼系統。用戶在首次使用網站時創建密碼，以便在隨後的訪問中確認其身份。缺點包括密碼較弱，密碼過于複雜，每個站點需要一個唯一的密碼，以及恢複被遺忘密碼的不便。保護網絡連接的最常見機制是SSL。除了服務器證明其真實性外，SSL還在客戶端和服務器之間建立加密連接。但是，如果攻擊者可以通過使用假浏覽器根證書將自己添加到用戶浏覽器的受信任用戶列表中，則可以中斷安全連接。在公司網絡中，管理員可以將證書添加到受信任用戶列表中，然後在https連接中組織一個“中間人”攻擊。

LEXEL加密芯片是一個獨立的系統，他采用其自主産權算法結合用戶標識字段，以及行爲備注信息來自動提取用戶信息一填寫網站上的用戶配置文件，包括付款到客戶制定的帳號。分布式的算法，通過允許網站配置文件自動填充來補充的無密碼登錄。實現所有帳號登錄密碼在安全的環境下一鍵式登錄，用戶無需記錄任何信息——芯片在手，通行我有。

3. 商業模式與應用場景

3.1 商業模式

LEXEL 作爲一個去中心化的解決方案，由 LEXEL 基金會主導項目進展與開發者社區維護，專注于身份認證信任公鏈的開發，並通過技術支持與投資的方式，推進基于LEXEL 鏈上的落地項目。

LEXEL 身份認證信任公鏈設計有自己的 Token ，除作爲 GAS 消耗外，Token 可應用于身份認證信息修改、智能合約建立與維護、數字資産質押、數字資産糾紛申訴與仲裁等場景，對應場景産生的 Token 消耗將作爲獎勵提供給公鏈上的應用開發者，礦工，讓 LEXEL 身份認證信任生態更加健康。

作爲基礎公鏈，公鏈上能夠存儲完備的身份信息，信用信息，提供身份認證解決方案，與基于場景的智能合約與圖靈完備的合約編程語言言。此外作爲一個见見證人網絡，會設計完備的去中心化認證機制，防範網絡被攻擊的可能性。據此成爲價值互聯網個人身份認證信任的底層基石。

基于 LEXEL 身份認證信任公鏈，LEXEL 同時提供完整的數字資産安全解決方案，使用 LEXEL 獨有專利的數字加密與安全認證技術，將傳統的數字資産錢包私鑰存儲方式進行革新，軟硬件結合爲用戶提供更安全有保證的數字資産存儲、轉賬解決方案。

除資産保值外，LEXEL 致力于搭建數字資産增值生態，在鏈上對接開發者、服務提供商（如數字資産交易所，數字資産量化交易團隊，P2P金融理財團隊等），搭建個人對個人，個人對機構，機構對機構的數字資産借貸、投資與金金融互助等多種模式的數字資産金融生態。

簡而言之，基于 LEXEL 公鏈，開發者與服務提供商社區，我們致力于成爲未來價值互聯網的身份認證信任基礎鏈，同時提供最好的數字金融生態，讓數字資産推動未來金融發展，具有堅實的基礎。

3.2 通證設計

作爲價值交換媒介的通證（Token），是 LEXEL 公鏈上必不可少的一個環節，通證以鏈上應用的廣泛程度直接相關，另一方面也作爲 LEXEL 生態通用貨幣爲使用 LEXEL生態服務的人提供價值交換便利。通證的價值保證與應用來自于以下幾個方面：

3.2.1 數字貨幣

- 可信任網絡維護：針對見證人網絡中的見證人節點進行獎勵，保證可信任網絡平穩運行；
- 鏈上價值交換：服務鏈上各個生態價值交換場景。

3.2.2 應用邏輯

- GAS消耗：網絡轉賬等操作的 GAS 消耗；
- 硬件消耗：官方回收token，兌換成硬件發放給用戶；
- 服務消耗：與LEXEL合作的機構/交易所定期提交token給予官方，作爲技術服務費；
- 金融場景消耗：金融服務生態中各項資產交易產生的場景消耗。

3.3 應用場景

3.3.1 應用場景之一：個人可信數字身份

當前，全世界各國都在關注個人數字身份ID，如美國、德國、比利時，有些國家甚至有一個專屬網絡身份。但目前，只有愛沙尼亞基本實現了國家網絡身份證體系，成爲全球數字化程度最高的國家。但愛沙尼亞只是一個340萬人口的小國，其他各國在個人數字身份ID過程中，都遇到了大量級並發的難題。而縱觀全球，更是沒有一個可以全球迅速認證檢測的數字身份ID，因這意味著將實現全球各國的身份證頒發機構、護照頒發機構的統一聯網，難度可想而知。

而區塊鏈技術誕生之後，多樣化的共識機制與治理驗證機制，此前奢想的“讓全世界的人來證明你的身份”變爲可能。但即便如此，過去比特幣、以太坊等公鏈處理交易的效率過于低下，以及RSA、ECC等非對稱加密算法過于繁複緩慢，仍然沒有真正可以商用的個人可信數字身份技術和應用落地。

身份的安全認證，就是要確保正確的人能夠在正確的時間和正確的原因下正確訪問正確的資源。需要通過對賬號（Account）、認證（Authentication）、授權（Authorization）和審核（Audit）進行管理，即誰能夠在什麼時候獲得怎樣的授權來使用某一個應用或設備，如何去使用這樣的應用或設備，以及知道誰在什麼時候訪問了某些應用或設備等，確保合法用戶安全方便使用IT資源。

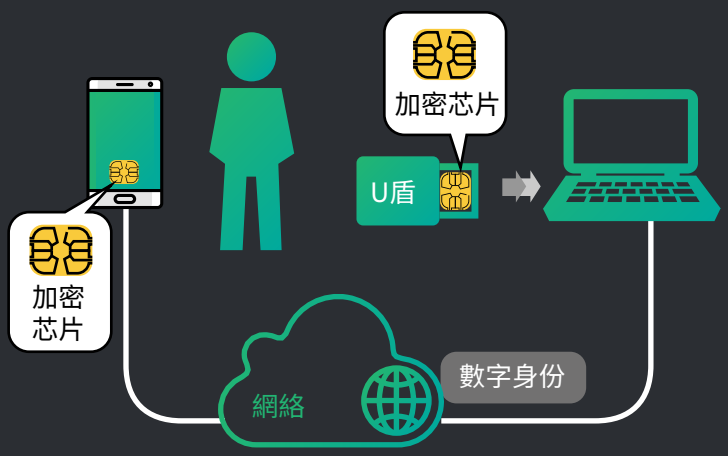
目前，LEXEL通過將加密技術與全新采用DPOS共識算法的區塊鏈技術結合，能夠完美的解決海量級交易的並發問題，並實現個人可信數字身份認證的三大功能：

一，實現個人數字身份的創建、上鏈存儲、與數字身份查詢驗證；

二，將結合硬件設備，實現個人身份與數字資產的綁定，防止黑客盜竊身份，暴力破解數字錢包密碼，盜取數字錢包賬戶資金，全面保護數字財產安全；

三，基於可信個人數字身份的電子簽章（簽名）、司法存證和證據保全等應用。

以達到萬億級體量的市場為例，即使傳統的PKI/CA傳統體系能夠突破大量級並發和區塊鏈技術落地的難題，其成本也是使用“LEXEL”的5倍以上。



3.3.2 應用場景之二：數字資產錢包

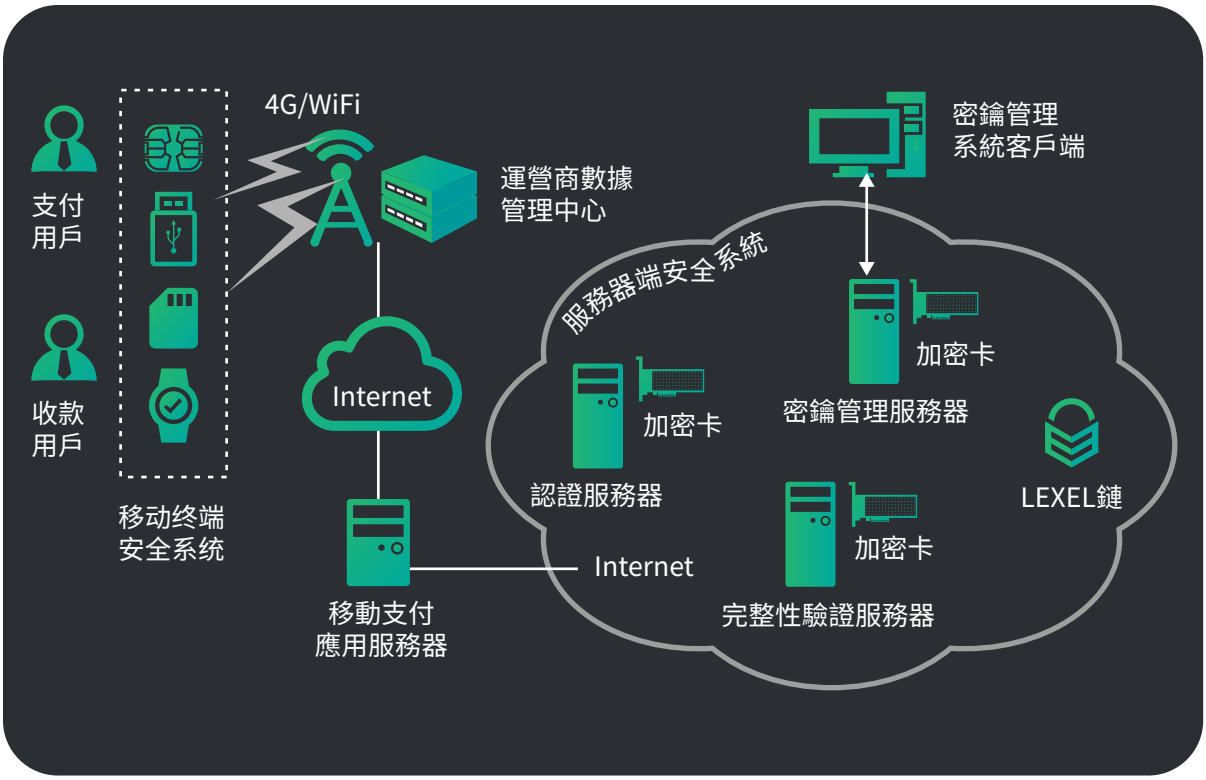
在傳統金融場景中，網上銀行、手機銀行、移動支付已經如火如荼的進入我們的生活。但即便如此，傳統金融仍然難以進行高安全級的支付，因此，國家通常采用限制支付的額度來控制風險。大額交易轉賬仍需通過網上銀行及硬件設備來配合實現。

其背後的原理是，移動支付方法都是采用驗證碼（動態口令）認證模式，如：支付寶、微信、蘋果PAY等。動態口令認證模式速度快，操作簡單，成本低廉，但其缺少簽名功能，黑客可通過截獲並替換支付單的內容，實現對移動支付協議的有效攻擊，盜取用戶賬戶中的資金。但若采用傳統PKI等傳統認證技術處理數字簽名，PKI/CA認證中心並發簽名驗證的速度較慢，加上CA認證中心建設成本偏高，市場無法接受。

而在數字貨幣的世界裏，用戶僅憑一串私鑰，就敢全權管理成萬上億級的數字資產，不僅缺乏數字簽名，甚至連動態口令認證的步驟也沒有。如此不設防備，加之各類電腦、手機終端中存在無數的漏洞及木馬後門，因此數字貨幣的投資者被黑客盜走數以億計的資產也屢見不鮮了。

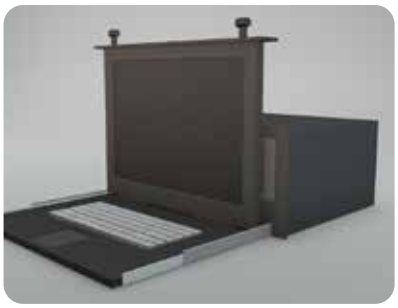
因此，LEXEL致力于改變此嚴重的行業安全痛點。

“LEXEL”技術本身在傳統場景中，就已經實現一次一密和數據加密保證個人信息安全和資金安全，數據加密傳輸速度能滿足2~3億用戶並發不延時。在數字貨幣場景中，通過與區塊鏈技術結合，首先將個人可信的數字身份存儲于區塊鏈之上，再生成對應的密鑰，部分存儲于區塊鏈賬本、部分存儲寫入于LEXEL的專用硬件中（可支持sd卡、sim卡、u盤、智能穿戴等多類存儲設備）。用戶在支付轉移數字資產時，需通過硬件設備進行驗證，黑客即便盜取了數字錢包的密碼，也無法將用戶的數字財產轉移。



3.3.3 應用場景之三：數字貨幣交易所

近期，數字貨幣交易所被黑客盜取數字貨幣資產的事件頻繁發生。其大致原因是，黑客通過攻擊交易所的大量用戶，可以盜走交易所存放在“熱錢包”中的代幣。通常而言，除了比特幣、以太幣等大幣種，絕大部分幣種都沒有被市面上的硬件冷錢包支持，一般只能通過普通的密碼和多重簽名錢包防護，盜取難度極低。


LEXEL通過加密技術，可以把關鍵的驗密過程寫入專用硬件中。與LEXEL合作的數字貨幣交易所，可以要求所有與熱錢包有關的操作（包括但不限于管理員登錄與操作權限變更、熱錢包用戶的訪問登錄、代幣資產提取、幣幣交易等）都需要一步連接專用硬件進行驗密的過程。由于黑客無法獲得硬件信息，即便破解了交易所用戶設置的所有密碼，也無法將數字資產轉移盜走。

3.3.4 應用場景之四：LEXEL 鏈鎖生態

基于 LEXEL 安全與海量並發的基本特性，形成鏈鎖的自由生態。通過智能合約形成信用機制，給予用戶使用 LEXEL 生態的各種服務時享有“特殊待遇”（根據信用積分高低決定），如：

1. 使用 LEXEL 錢包，轉賬免 Gas Fee
2. 持有者的 LEXEL 會自動增值（數字資產銀行）
3. 遊戲或者應用特權

LEXEL 鏈鎖生態務求打造一個既保障了用戶的數字資產，同時能夠給用戶的數字資產帶來增值的區塊鏈生態。

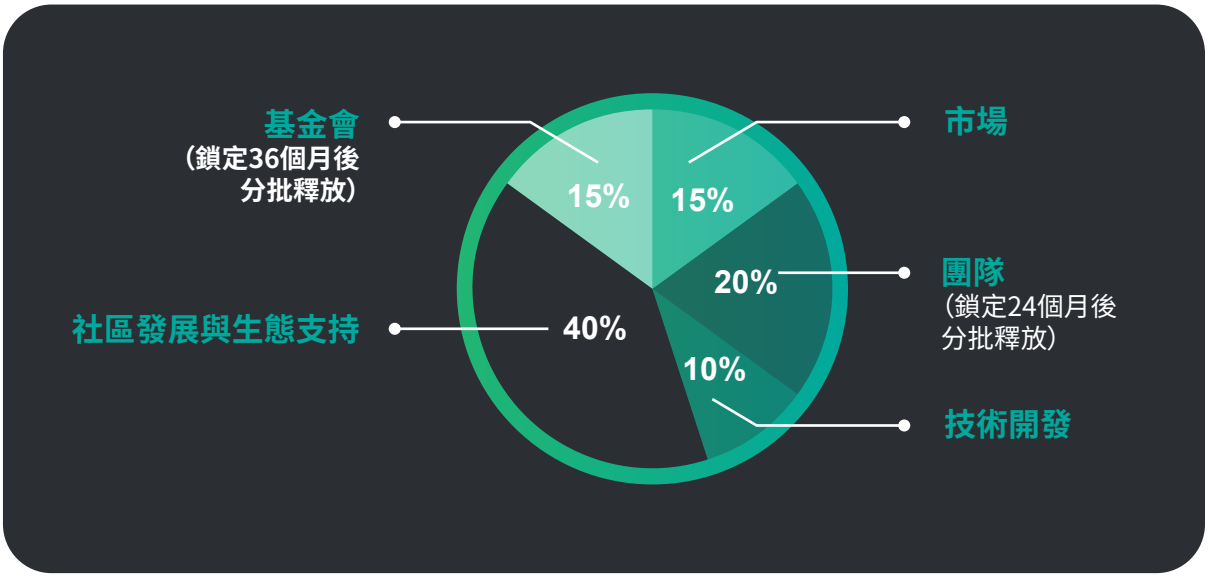
4. Token 分配

a) **代幣總量：** 10,000,000,000 LEXT（永不增發）

b) **代幣生成時間：** 2018年2月中旬

c) **交易所上線時間：** 2018年6月中旬

LEXEL不會有任何形式的公募和私募，所有代幣只對戰略投資者、社區生態貢獻者、商業合作夥伴贈送，以及基金會與技術開發團隊保留持有。禁止中國人與美國人以任何方式購買及持有，否則壹切法律後果自負！



LEXT 屆時將在LEXEL生態體系中流通使用，包括但不限於交易（事務）的記賬消耗（GAS）、個人數字身份的創建及查詢費用、安全加密存儲及支付相關服務費、可信瀏覽器廣告收入、其他數字認證場景的服務費用等。

5. 发展路线图

2011~2017

- 2011年初-2017年11月 加密認證技術研發

2018

- 2018年2月中旬 生成代幣
- 2018年6月中旬 代幣交易所上線
- 2018年6月下旬 主網投入開發
- 2018年7月~8月 關鍵硬件研發
- 2018年9月 關鍵模塊研發、主網基本完成
- 2018年12月 主網，錢包開發完成並上線

2019

- 2019年3月 智能合約應用模板推出
- 2019年6月 硬件設備接入主網開發
- 2019年8月 硬件接入主網完成
- 2019年12月 首個DApp試運行

2020以后

- 持續推進... 擴大硬件及主網的應用範圍，建立主網生態

6. 核心團隊

6.1 團隊成員

Lewis Lo

CEO CTO

10多年IT開發經驗，負責LEXEL的全局統籌與管理。近幾年鑽研區塊鏈技術的落地及應用，曾成功幫助某珠寶公司開發了一個基于聯盟鏈技術（PBFT共識機制）的珠寶銷售及防僞追溯平台。

Evangelos Rekleitis

CSO

帝國理工大學高級計算機碩士學位，自2007年起一直擔任ICT工程師和風險分析師，參與了塞浦路斯政府網絡安全戰略及其雲安全戰略的修訂，並參與了希臘政府的多項安全研究和風險分析與管理項目。2015年受聘于歐盟網絡和信息安全局；參與了大數據安全、網絡威脅、安全標准化和密碼學等項目。

Christine He

COO

畢業于北卡羅萊納州立大學，曾就職于全球最大視頻電商系統Cinsay公司，帶領團隊開展跨國業務。曾協助Cinsay合作方——Formula E車隊Andretti Autosport開發定制頁遊及運營工作。精通多國語言，具有豐富的社區運營及公關宣傳經驗。

Alog Rana

畢業于帝國理工大學，在安全交易，AML以及詐騙檢測解決方案方面有豐富的經驗。同時具備在低延遲率，可擴展性以及高可用系統設計方面的實施經驗。在金融IT方面具有貫穿整個項目生命周期的豐富的業務知識。

Soumil Verma

北卡羅萊納州立大學計算機工程與電子工程雙學位。曾擔任康涅狄格大學研究員，曾就職于食品安全檢驗局USDA擔任數據分析師，參與開展ArcGIS項目。

Anuj Sanghavi

現于Caterpillar Inc. / EASi LLC公司擔任項目工程師，負責自動化測試項目，曾是Albright Entrepreneur Village公司成員，北卡羅來納州立大學電氣及電子工程師協會聯合主席，及The Carrom Club 出納。

Todd Downing

畢業于貝勒大學，擁有超過20年的IT從業經驗，並具備多行業的業務知識，曾就職于Dell、Nexstar Broadcasting、Cinsay等知名企業。依靠豐富的技術及管理經驗，多次參與企業發展戰略的制定。在技術與業務發展方面有獨到見解。

James Kersbergen

具有超過20年的開發經驗，曾任職于Belo、Nexstar Broadcasting和Cinsay，負責技術開發及團隊管理工作。在流媒體、雲計算及數據庫技術方面有深入研究。

Serge Kononov

在IT測試領域擁有超過15年的豐富經驗，對測試技術有深入了解，擅長自動化測試。曾負責企業的自動化框架設計及搭建，確保產品快速叠代的可靠性。

Fadi el Hamdi

畢業於荷蘭阿姆斯特丹大學國際商務理財學系，曾就職於荷蘭銀行（ABN AMRO Bank N.V.）的信息科技部門。負責網絡銀行金融安全漏洞分析。為工作人員提供網絡安全工作環境與即時應對病毒木馬入侵。

6.2 專家顧問

Richard Zhang

畢業於加州大學伯克利分校電子工程和計算機科學系。曾就職於BigFix和IBM，任高級軟件工程師。現就職於AppDynamics的資深軟件工程師。曾創立過壹個網絡圖形計算器引擎和參與過文件加密軟件TrueCrypt的開源項目。專註於用戶體驗、單頁應用、加密技術、應用安全傳輸、應用安全性能管理等網絡技術。

Riad Elmnebhi

畢業於法國國立應用技術學院，信息系統架構專業。在巴黎銀行工作了11年。現在是銀行區塊鏈計劃的總監，負責創立了巴黎銀行私有區塊鏈系統。

Khalil Najjar

雲技術、企業ERP、企業數字化高級顧問；
物聯網，區塊鏈，微服務，人工智能等領域專家、架構師。

6.3 合作機構

創世資本

極點基金

鏈上資本

聚合資本

普渡大學區塊鏈研究室

三鏈資本

Africoin

引力資本

天天交易所

6.4 合作媒体

金色財經

火訊財經

耳朵財經

幣頭條

TokenBook

牛X導航

One Top

3點鐘財經

7. 風險提示

鏈鎖團隊鄭重提示您：參與者應當知曉所有區塊鏈項目皆具有風險，區塊鏈項目的價值與項目發展狀況及市場參與者的預期密切相關，參與者不應盲目相信任何區塊鏈團隊所作出的任何獲利保證，也不應盲從跟風參與，而應對項目的技術及應用發展潛力、自身的經濟承受能力和心理承受能力做出客觀判斷，壹切責任、收益、損失最終均由參與者自行承擔。

具體而言，鏈鎖和LEXT將可能存在以下風險：

(1) 信息披露不完備的風險

截至本白皮書發布之日，鏈鎖仍處於開發階段，其哲學理念、共識機制、算法、代碼等技術規範和參數可能會經常且不斷更新與變更。盡管本白皮書包含鏈鎖的特定信息，但其並不絕對完整，且出售方可能會根據特定目的不時對這些信息作出調整與更新。出售方無法，也無義務隨時告知參與者鏈鎖開發中的每個細節(包括其進度和預期裏程碑，無論是否推遲)，因此並不必然會讓參與者及時且充分地獲悉鏈鎖開發中不時產生的信息。信息披露的不充分是不可避免且合乎情理的。

(2) 監管風險

加密代幣正在被或可能被各個不同國家的監管機構所監管。出售方可能會不時收到來自於壹個或多個監管的詢問、通知、警告、命令或裁定，甚至可能被勒令暫停或終止任何與售賣、鏈鎖開發或LEXT相關的行動。鏈鎖的開發、營銷、宣傳或其他方面以及售賣均可能會因此受到嚴重影響、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鏈鎖或售賣的監管許可或容忍可能只是暫時的。在各個不同國家，LEXT可能隨時被定義為虛擬商品、數字資產或甚至是證券或貨幣，因此在某些國家之中按當地監管要求，LEXT可能被禁止交易或持有。

(3) 密碼學加速發展的風險

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（例如量子計算機的發明/改良）可能給基於密碼學的系統（包括鏈鎖)帶來危險。這可能導致任何人持有的LEXT被盜、失竊、消失、毀滅或貶值。在合理範圍內，項目方將自我準備采取預防或補救措施，升級鏈鎖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，項目方將和鏈鎖社區其他成員壹起嘗試適應密碼學和安全領域的不斷變化。

(4) 項目失敗或中止的風險

鏈鎖仍在開發階段，而非已準備推出的成品。由於鏈鎖系統的技術復雜性，出售方可能不時會面臨無法預測和/或無法克服的困難。因此，鏈鎖的開發可能會由於任何原因而在任何時候失敗或中止（例如由於缺乏資金)。開發失敗或中止將導致LEXT無法交付給售賣的任何慘與者。

(5) 收入被盜的風險

可能會有人企圖盜竊出售方所收到的募集資金（包括已轉換成法幣的部分)。該等盜竊或盜竊企圖可能會影響出售方為鏈鎖開發提供資金的能力。盡管出售方將會采取最尖端的技術方案保護募集資金的安全，某些網絡盜竊仍很難被徹底阻止。

(6) 源代碼漏洞風險

無人能保證鏈鎖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、暴露用戶的信息或產生其他問題。如果確有此類瑕疵，將損害鏈鎖的可用性、穩定性和/或安全性，並因此對LEXT的價值造成負面影響。

(7) 無準入許可、去中心化自治賬本的風險

鏈鎖底層的分布式賬本是無準入許可的，這意味著它可被所有人自由訪問和使用，而不受準入限制。盡管鏈鎖初始时是由出售方所開發，但它

並非由出售方所有擁有、運營或控制。自發形成的鏈鎖社區是完全開放、去中心化且無準入門檻即可加入的，其由全球範圍內的用戶、粉絲、開發者、 LEXT持有人和其他參與者組成，這些人大都與出售方無任何關系。就鏈鎖的維護、治理乃至進化而言，該社區將是去中心化且自治的。而出售方僅僅是社區內與其他人地位平等的壹個活躍成員而已，並無至高無上或專斷性的權力，不考慮其之前曾對鏈鎖的誕生做出的努力和貢獻。因此，鏈鎖在啟動之後，其如何治理乃至進化將不受到出售方的支配。

(8) 源代碼升級風險

鏈鎖的源代碼將逐步開源且可能被鏈鎖社區任何成員不時升級、修正、修改或更改。任何人均無法預料或保證某項升級、修正、修改或更改的準確結果。因此，任何升級、修正、修改或更改可能導致無法預料或非預期的結果，從而對鏈鎖的運行或LEXT的價值造成重大不利影響。

(9) 安全漏洞風險

鏈鎖區塊鏈基於開源軟件並且是無準入許可的分布式賬本。盡管出售方努力維護鏈鎖系統安全，任何人均有可能故意或無意地將弱點或缺陷帶入鏈鎖的核心基礎設施要素之中，對這些弱點或缺陷出售方可能恰好無法通過其采用的安全措施預防或彌補。這可能最終導致參與者的LEXT或其他數字代幣丟失。

(10) “分布式拒絕服務”攻擊風險

鏈鎖被設計為公開且無準入許可的賬本。因此，鏈鎖可能會不時遭受“分布式拒絕服務”的網絡攻擊。這種攻擊將使鏈鎖系統遭受負面影響、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鏈鎖區塊鏈的區塊之中，或甚至暫吋無法執行。

(11) 節點處理能力不足的風險

鏈鎖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鏈鎖區塊鏈網絡內屆時節點所能提供的負載，則鏈鎖

網絡可能會癱瘓和/或停滯，且可能會產生諸如“雙重花費”的欺詐或虛假交易。在最壞情況下，任何人持有的LEXEL幣可能會丟失，鏈鎖區塊鏈回滾或甚至硬分叉可能會被觸發。這些事件的後果將損害鏈鎖的可使用性、穩定性和安全性以及LEXT的價值。

（12）LEXT未經授權被認領的風險

任何通過解密或破解LEXT購買者的密碼而獲得購買者註冊郵箱或註冊賬號訪問權限的人士，將能夠惡意認領在售賣中所購買的LEXT。據此，購買者在售賣中所購買的LEXT可能會被錯誤發送至通過購買者註冊郵箱或註冊賬號認領LEXT的任何人士，而這種發送是不可撤銷、不可逆轉的。每壹購買者應當采取諸如以下的措施妥善維護其註冊郵箱或註冊賬號的安全性：使用高安全性密碼；不打開或回復任何欺詐郵件；以及嚴格保密其機密或個人信息。

（13）LEXT錢包私鑰丟失風險

若丟失或損毀了存取LEXT所必需的私鑰，這可能是不可逆轉的。只有通過本地或在線LEXT錢包來占有相關的獨壹無二公鑰和私鑰，才可以操控LEXT。每壹購買者應當妥善保管其LEXT錢包的私鑰。若LEXT購買者的該等私鑰丟失、遺失、泄露、毀損或被危及到，出售方或任何其他人士均無法幫助購買者存取或取回相關LEXT。

（14）系統分叉風險

鏈鎖是壹個由出售方發起並由社區提供支持的開源項目。盡管出售方在鏈鎖社區中具有影響力，但是其並不也無法獨斷鏈鎖的開發、營銷、運行或其他。任何人士均可以開發鏈鎖代碼的補丁或升級，而無需獲得任何其他人士的授權。壹旦部分的鏈鎖區塊鏈上驗證者接受鏈鎖的補丁或升級，這可能導致鏈鎖區塊鏈“分叉”，由此將會出現兩條分叉的網絡，直至分叉的區塊鏈合並或者其中某壹條終止出塊（這兩種情況可能永不會發生）。鏈鎖區塊鏈由於分叉而產生的每壹分支均將有其自己的加密代幣。因此，在兩條分叉

的分支上會分別存在擁有幾乎相同技術特征和功能的LEXT。鏈鎖社區可能分裂成兩批，分別支持兩條分支。此外，分叉出的鏈鎖區塊鏈分支在理論上可以進壹步無限次分叉。分叉區塊鏈的暫時性或永久性存在可能對鏈鎖運行及LEXT的價值造成不利影響。在最壞情況下，可能摧毀鏈鎖系統的可持續性。盡管鏈鎖區塊鏈上的該等分叉有可能經社區牽頭努力後將兩條分支合並而解決，但並不能保證成 功且可能耗時很久。

(15) 平臺合並的風險

技術角度而言，在特定情形下，為實現協同效應或基於其他有價值的對價，鏈鎖可能與其他區塊鏈項目合並。這種形式的合並可能導致鏈鎖區塊鏈被放棄或廢棄，以換取新創建的其他區塊鏈上壹定數量的加密代幣。該等新的加密代幣將按壹定比例分配並派發給合並前的LEXT持有者。在特定估值模型下LEXT持有者可能在該等合並中獲得的補償不足。

(16) 應用缺少關註度的風險

LEXT的價值很大程度上取決於鏈鎖平臺的普及度。鏈鎖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，鏈鎖甚至可能被長期邊緣化，僅吸引很小壹批使用者。相比之下，很大壹部LEXT需求可能具有投機性質。缺乏用戶可能導致LEXT市場價格波動增大從而影響鏈鎖的長期發展。出現這種價格波動時，出售方不會(也沒有責任)穩定或影響LEXT的市場價格。

(17) 流動性不足風險

LEXT既不是任何個人、實體、中央銀行或國家、超國家或準國家組織發行的貨幣，也沒有任何硬資產或其他信用所支持。LEXEL幣在市場上的流通和交易並不是出售方的職責或追求。LEXT的交易僅基於相關市場參與者對其價值達成的共識。任何人士均無義務從LEXT持有者處購買任何LEXT，也沒有任何人士能夠在任何程度上保證任何時刻LEXT的流通性或市場價格。LEXT持有者若要轉讓LEXT，該LEXT持有者需尋找壹名或多名有意按約定

價格購買的買家。該過程可能花費甚巨、耗時長並且最終可能並不成功。此外，可能沒有加密代幣交易所或其他市場上線LEXT供公開交易。

（18）代幣價格波動風險

若在公開市場上交易，加密代幣通常價格波動劇烈。短期內價格震蕩經常發生，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造成，這種波動也反映了供需平衡的變化。無論是否存在LEXT交易的二級市場，出售方對任何二級市場的LEXT交易不承擔責任。因此，出售方沒有義務穩定LEXT的價格波動，且對此也並不關心 。LEXT交易價格所涉風險需由LEXT交易者自行承擔。

（19）競爭風險

鏈鎖的底層協議是基於開源電腦軟件，沒有任何人士主張對該源代碼的版權或其他知識產權權利。因此，任何人均可合法拷貝、復制、重制、設計、修改、升級、改進、重新編碼、重新編程或以其他方式利用鏈鎖的源代碼和/或底層協議，以試圖開發具有競爭性的協議、軟件、系統、虛擬平臺或虛擬機從而與鏈鎖競爭，或甚至趕超或取代鏈鎖。出售方對此無法控制。此外，已經存在並且還將會有許多競爭性的以區塊鏈為基礎的平臺與鏈鎖產生競爭關系。出售方在任何情況下均不可能消除、防止、限制或降低這種旨在與鏈鎖競爭或取代鏈鎖的競爭性努力。

（20）第三方開發者風險

鏈鎖將提供壹個開放平臺適用於第三方（尤其是鏈鎖社區成員）開發的任何類型的分布式應用和智能合約程序。所有這些應用和智能合約程序可以被接入或建立在鏈鎖區塊鏈上而不受限於審查制度、限制、控制、資格預審或準入要求。出售方既不意圖也無法擔當審查員在任何程度上對任何将要在鏈鎖系统上开发或与之相关的程序进行审核。因此，在特定司法管辖区域被禁止或限制的程序，如涉及賭博、投注、彩票、乐透、色情等等的程序，

可能利用鏈鎖区块链的无准入要求来开发、促进、营销或运营。特定司法管辖区域的监管当局可能对特定程序或甚至其开发者或用户采取相应行政或司法措施。任何政府当局的处罚、惩罚、制裁、镇压或其他监管措施，或多或少会惊吓或威慑到既有或潜在鏈鎖用户使用鏈鎖系统并持有LEXT，从而对鏈鎖的前景造成重大不利影响。

(21) 其他加密資產的風險

鏈鎖中將會創建或生產並流通著各種加密資產。這些加密資產中壹部分可能是由特定人士發行的，發行人將對持有人負有特定承諾或義務。其他些加密資產可能是由鏈鎖內的智能合約創建的。這些加密資產都不會帶有和LEXT一樣或類似的功能。這些加密資產既不是出售方所出售或提供的，出售方也不會對它們負責，除非出售方另有特別說明。

LEXEL

www.lexel.io