LIGHTCHAIN
WHITE PAPER

2018 / v1.0

光鏈白皮書

一 什麼是光鏈

LightChain (簡稱「光鏈」或「Light」) 是世界上第一個雙層鏈， 致力於開發比特幣和以太坊之外的第三種區塊鏈，以解決高速發展中的區塊鏈世界中日益突顯的性能及擴展性問題。只有有效解決了這兩個問題，海量的應用場景才能真正上鏈，平行世界才能真的與現實世界握手前行。Ligh 首創的雙層鏈結構，在技術上和經濟模型上都是巨大的創新，擁有革命性的優勢。

二 光鏈分析

1 技術分析

Light 創新性地構建了雙層鏈結構，有效地保持了超級賬本的核心功能--記錄不可被篡改或銷毀，同時實現 10wQPS(Query Per Second，每秒請求數) 以上的系統性能。Light 的雙層鏈分為父鏈和子鏈。 父

鏈有且僅有一個，子鏈有一個或多個且相互獨立，數量可以任意擴展。父鏈與傳統的公鏈類似，通過分布式的方式保證記錄不可被篡改或銷毀，且對大眾透明。子鏈基於 PoM（Proof of Machine）validation 方式，結合 In-Memory 數據庫緩存，實現性能的大幅提高。子鏈的交易記錄週期性的與父鏈同步，如 1 小時、6 小時或 1 天等，以保證父鏈有全網的完整的交易記錄。同步過程以 batch updat 的方式進行打包操作。包中的記錄在子鏈中已被檢查，父鏈無需進行檢查直接更新即可。

2 經濟分析

在宏觀經濟學中，一個經濟體在增長過程中造成通貨膨脹是不可避免的。經濟的持續增長必然帶動需求的強勁，而需求的強勁必然帶來物品價格的提高。這時，貨幣的適度超發就成為必然選擇。實際上，適度的通貨膨脹是經濟市場強勁的表現。而比特幣在設計之初就數量恆定，是一種緊縮式貨幣。在使用過程中，人們發現持有比特幣會獲得更好的經濟收益，進一步限制了比特幣的市場流通性。因此，比特幣本身與經濟發展所需的貨幣要求是相背離的。在 Light 的雙層結構中，子鏈是組織化部署的，由機器控制的，可以通過自身數字貨幣超發來

滿足所在領域經濟發展的需要。而父鏈通過激勵機制建立去中心化的分布式網絡，實現對經濟生活關鍵數據和交易透明且不可被篡改的記錄。消除信息不對稱的情況，保證信息面前人人平等，避免不必要的人為泡沫。两者结合提供了一个信息公开透明的、公平公正的、具备充分经济发展活力的模型。

三 光链的愿景

光鏈，讓世界有光。Let there be light. --- 《聖經》

通過 Light 革命性的雙層鏈結構，讓區塊鏈技術及理念得以大規模且高效應用，使平行世界與現實世界握手前行，從而推動人類社會的進步，正如上帝創造光一樣。

四 光鏈的設計理念

1 面對的問題

2008 年 10 月 31 日比特幣的出現，真正意義上解決了數字貨幣 double-spend 的問題，並首次提出了 utxo 的設計。2013 年 11 月，以太坊的出現實現了圖靈完備的智能合約。這些進步雖然對人類社會意義重大，但都無法真正填平現實世界與平行世界的鴻溝。現實場景的多樣性和複雜性如一座大山橫亙在區塊鏈面前，阻礙了區塊鏈的廣泛使用。原因如下：

- 在一次交易中，transaction 需要被廣播給全網的所有節點進行記錄。在接收側，礦工將其緩存，而後記錄於自己挖掘的 block 中。
- 每個 block 被加入 Blockchain 之前需要根據 Proof-of-Work、Proof-of-Stake 或其他原則，完成 block 生成的 validation。

綜上所述，比特幣當前的交易週期約為 1 - 3 小時，使得實時握手場景無法被滿足，以至於區塊鏈如此優秀的理念無法規模性的應用在人類社會當中。

2 解決思路

解決思路非常明確。

- 在接受側，引入可靠的 In-Memory 數據庫將 transaction 記錄進行緩存，有效提高緩存環節吞吐量，達到 10 萬 QPS (Query Per Second，每秒請求數) 級別。目前的 In-Memory 數據庫均能簡單完成這個目標。
- 在 Validation 環節，優化 validation 效率，提升 Block 的產生速度，以保證緩存的記錄能夠及時消化出去。

目前已知的區塊鏈 validation 方法有三種。

- Proof-of-Work：工作量證明是通過較高的生成成本和很低的驗證成本來有效應對拒絕服務攻擊和其他服務濫用的策略。其優勢突出，但弊端也很明顯，它太浪費了。比特幣網絡每秒完成 600 萬億次 SHA256 運算，而最終這些計算沒有任何實際或科學價值。這些運算存在的唯一目的是用來解決工作量證明問題，而為了使惡意攻擊者不能輕易地偽裝成幾百萬個節點和打垮網絡，這些問題被故意設置得很難。隨著挖礦節點數的增加，這種無端的電量

消耗快速增長，最終會嚴重衝擊整個生產生活的用電情況。因此有效抑制 PoW 節點的快速增長勢在必行。

- Proof-of-Stake：股權證明機制已有很多變種，但基本概念是產生區塊的難度應該與其在網絡里所佔的股權(所有權佔比)成比例。授權股權證明機制(DPoS)表示每個股東按其持股比例擁有影響力，51%股東投票的結果將是不可逆且有約束力的。其挑戰是如何及時而高效的方法達到 51%批准。在確信度為 99.9%的情況下，DPoS 的平均 transaction 記錄週期為 1.5 秒。較 PoW 有大幅提高，但依然低於 10 萬 QPS 的性能要求。
- Proof-of-Machine：已有若干團隊探尋出了在機器上建立 TEE (Trusted Execution Environment) , 以確保基於其執行的智能合約和其他協議是足夠安全的，記錄是不可被更改的， 滿足 Blockchain 的超級賬本核心訴求。TEE 提供了主處理器中的隔離執行環境，以執行操作系統無法觀察或更改的代碼，並確保策略和控件按預期執行。 TEE 是可以被驗證並被證明在參考條件下運行的安全環境。多年來，全球 ARM 和 Intel 架構處理器都提供 TEE 功能。

當前普通服務器的基礎運算週期在納秒級別， 使用 Proof-of-Machine 的 validation 方式，結合 In-Memory 的數據庫緩存，可以在保證安全的前提下有效地將系統性能提升至 10wQPS 以上。

然而 Proof-of-Machine 帶來了一個新的問題: 儘管 PoM 機制使用後，類似於我們放飛了一個上帝， 和我們無關地自行執行最高階的任務，俯瞰眾生， 但 PoM 是有組織的部署的， 也可以被有組織銷毀。這就使得儘管鏈上記錄無法被修改，但鏈本身可以被有組織銷毀，最終導致所有記錄被有組織清除。

3 解決方案

為了有效保持超級賬本的核心功能-記錄不可被篡改以及銷毀， 同時實現 10wQPS 以上的系統性能，我們提出了一個新的革命性的區塊鏈—光鏈。 Light 是一個雙層鏈分為父鏈和子鏈。 父鏈有且僅有一個，子鏈有一個或多個且相互獨立，數量可以任意擴展。 父鏈與傳統的公鏈類似，通過分布式的方式保證記錄不可被篡改和銷毀，且對大眾透明。子鏈基於 PoM (Proof of Machine)validation 方式， 結合 In-Memory 數據庫緩存，實現性能的大幅提高。子鏈的交易記錄

週期性的與父鏈同步，如 1 小時、6 小時或 1 天等， 以保證父鏈有全網的完整的交易記錄。同步過程通過 batch update 進行打包操作。包中的記錄在子鏈中已被檢查，父鏈無需進行檢查直接更新即可。

Light 的雙層鏈結構，具有巨大的彈性優勢，適用於各類應用場景。實現了從性能問題入手，真正解決整個區塊鏈行業的易用性問題。Light 的圖示如下。

4 細節分析

4.1 數據的完整性

子鏈的交易記錄週期性的與父鏈同步，以保證父鏈有全網的完整的交易記錄。在子鏈被摧毀前，必須強制執行一次與父鏈的同步，以確保數據無丟失。

4.2 數據的一致性

由於子鏈與父鏈的同步是週期性的， 子鏈常常具有新的記錄。 在閱讀記錄時，我們遵照如下步驟，以確保讀出的數據是最新的。

檢查某子鏈是否存在

如存在且未被摧毀，從子鏈中讀取相應記錄

如存在且被摧毀，從父鏈中讀取相應記錄

如不存在，則忽略子鏈的名稱及ID等metadata存放於父鏈中，在子鏈創建時被寫入。當子鏈被摧毀時，相應的記錄也寫入父鏈。

4.3 子鏈的隔離性

在光鏈的雙層結構中，子鏈是相互隔離的。 某子鏈的硬件及軟件資源只用於該子鏈內部，不會被其他子鏈爭搶。 這樣資源和業務在子鏈間相互隔離，避免了單鏈結構中資源被不同業務惡性爭搶的問題。也在系統架構層面，為業務的優化和治理提供了有效的前提和保障。

4.4 子鏈的獨立性

在光鏈的雙層結構中，子鏈是相互獨立的。參與一個 transaction 的雙方必須屬於同一子鏈，不能也無需跨鏈交易。因此，交易記錄也僅屬於一個子鏈，不必在多個子鏈中重復存儲。當我們將子鏈大小不斷縮減後，很容易發現最小的原子性子鏈就是一個 DApp。

4.5 系統的可擴展性

理論上，光鏈的子鏈數是可以無限擴展的，這使得整個系統的可擴展性是無限的。在父鏈吞吐量有限的情況下，系統可以通過調整子鏈的同步頻度來容納更多的子鏈接入父鏈，實現系統擴張。

4.6 安全性

子鏈與父鏈的同步過程通過 batch update 方式根據智能合約進行打包操作。包中的記錄在子鏈中已被檢查，父鏈無需進行檢查直接更新即可，以獲取更好的性能。這樣，子鏈的安全等級投射到了父鏈之上，使得整個系統的安全性更大程度上受到了子鏈的影響。

4.7 分布與集中

父鏈是去中心化的分布式的，有效地構建了記錄不可被修改和摧毀的超級賬本。子鏈採取組織化部署 TEE 的方式，獲取了高的系統性能。兩者的結合使得我們有效構建了高性能的超級賬本，且完整透明的對公眾開放。

4.8 流量模型

超級賬本遵循傳統的一次寫入多次讀出的流量模型， 只是寫入是通過廣播給全網的所有節點來完成的。這導致系統付出過多的流量成本來保證記錄的多備份及安全性。在通常的大數據系統中，數據備份總是在內網中實現的。外網的廣播式記錄和備份被認為是極其浪費的。

將整個網絡分成若干子網是降低這種廣播式記錄和備份成本的有效方法。在一個 MxN 的單層網絡中，我們需要對 MxN-1 個節點發送廣播消息來完成備份。當我們把網絡劃分為 M 個包含 N 個節點子網時，僅需同步所處子網的所有節點以及父網的骨幹節點即可。這些節點總數為（N-1）+ (M-1)個。

很明顯，光鏈的兩層結構能夠有效降低廣播式記錄和備份的帶寬成本。

4.9 激勵機制

在傳統的區塊鏈設計中，激勵機制是去中心化分布式運行的制度基礎。在光鏈的雙層結構中，父鏈完整地保留了這樣的激勵機制，保證參與者有足夠的激情建立各自的節點。而子鏈由機器控制，有組織化部署，無需任何激勵機制去創建新的節點。

五 經濟模型

在 Light 的生態體系中，我們定義和生成了固定數量的 LightCoin。其流轉方式如下。

- 礦工基於優化的 PoW 方式挖掘出父鏈 Block 後，獲取一定的 LightCoin，這和比特幣及以太坊基本一致；
- 每個子鏈在和父鏈同步數據時要根據數據包中的記錄數交付摩擦費。 摩擦費最後交付給礦工作為激勵；
- 每個子鏈創建時，需要交給父鏈一定數量的 LightCoin 來進行抵押，否則無權創建子鏈。抵押的 LightCoin 可以作為摩擦費被子鏈使用， 抵押數量會隨著時間推移逐步增長。

六 光鏈實施及迭代

1 光鏈上線的時間規劃

光鏈項目的主要時間節點包括:

第一階段

2015: 團隊開始研究區塊鏈性能問題

2016: 團隊進行了大量 PoW、PoS、PoW 的性能及安全性測試

第二階段

2017:「光鏈」項目正式啓動

第三階段

2018 Q1: 光鏈基金會成立

2018 Q2: 光鏈內測

2018 Q3: 光鏈公測

2018 Q4: 光鏈 v1.0 正式版本發佈

2018 Q4: 光鏈正式對 DApps 開放

第四階段

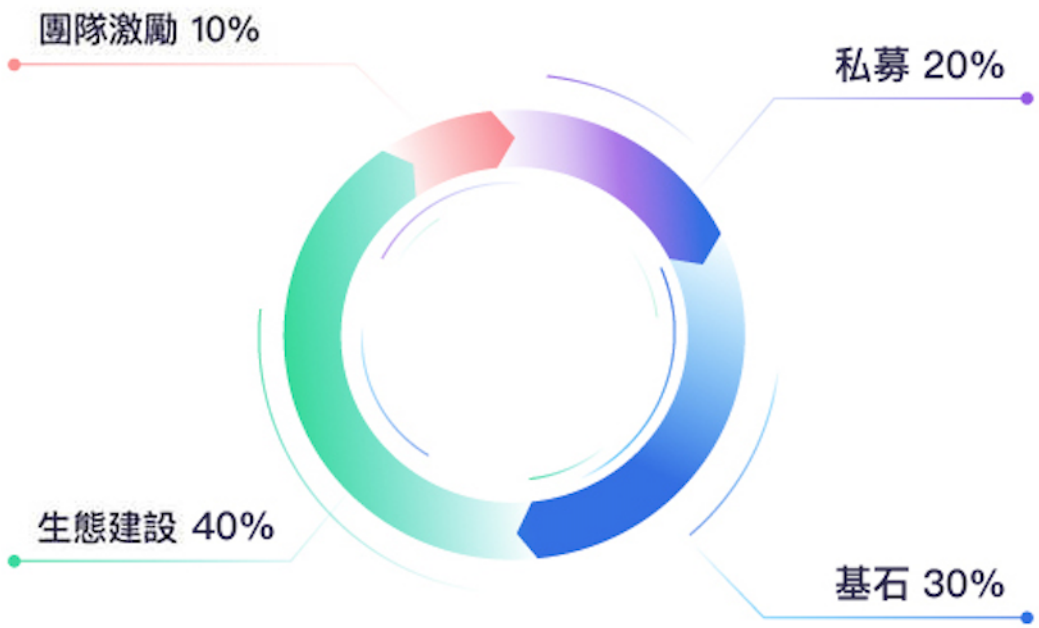
光鏈生態系統建設

互換細則

1 互換詳細規則

光幣數量總計 2100 億枚，其中：

- 基石：30%
- 私募：20%
- 生態建設：40%
- 團隊：10%



代幣分布圖

2100 亿枚

2 時間

2018 年 1 月

3 互換方式

光鏈可以接受以太坊 (ETH) 的互換

八 光鏈團隊

光鏈擁有一個經驗豐富的國際化研發團隊。這支研發團隊由 40 多名對區塊鏈、數字貨幣等領域具有多年經驗的科學家及工程師組成。團隊的核心成員曾主導開發多個全球知名的大規模數據存儲和處理系統，併發規模在萬台服務器以上。 光鏈項目開發團隊共有 21 位核心開發者, 由 Jason Jia 帶領。主要團隊成員及經歷如下：

姓名 & 经历

Jason Jia
曾任百度電商首席架構師，
百度鳳巢高級科學家，
盛大創新院副院長，
應用彙 CTO

Shaoyang Erh
曾任百度遊戲副總裁，
運營多款日活超千萬頂級移動互聯網產品，
資深的比特幣專家

Franklin Weldon
畢業于美國麻省理工大學，
之後一直從事區塊鏈技術與數字貨幣加密
技術研究工作

Kristina Bliadze
區塊鏈工程師，
曾在Microsoftware軟件開發公司12年，
後轉戰區塊鏈領域至今6年

Alexius Lee
數字貨幣與智能合約專家，
曾就職于全球區塊鏈研究中心，
中國數字商務部

Aniket Jindal
全棧開發人員，
在分布式區塊鏈領域擁有超過5年的
工作經驗

Monica Desai
完成哥倫比亞大學MBA，
曾在美國一知名區塊鏈企業
（Auxesis Group）工作

九 法律法規

1 運營主體

光鏈在新加坡建立基金會（Light Chain Foundation），該基金會主要的任務就是公開、公正、透明的不以盈利為目的地運營及維護光鏈生態，並對光鏈的開發團隊進行支持。光鏈基金會將由新加坡會計與企

業管理區（ACRA）批准建立, 受新加坡公司法監管, 該基金會由具備受該基金會由具備受託資格人組成的受託董事會或管理委員會獨立管理運營並獨立於政府之外。新加坡以穩定而健全的法律、金融環境著稱, 光鏈基金會是在新加坡成立的非盈利組織(Non-Profit Entity), 依照新加坡法律, 該基金會是為支持或參與公共利益或私人利益的活動, 而不具任何商業利益的合法成立的組織。基金會所獲得的「利潤」被稱為盈餘, 將被繼續保留作為其他活動的經費, 而不在其成員中分配利潤。

2 免責條款

光鏈基金會目標轉變為非營利組織, 鏈上用戶獲取的是光鏈的使用權。購買者應明白在法律範圍內, 光鏈不做任何明示或暗示的保證, 並且 LightCoin 是「按現狀」購買的。此外, 購買者應明白 LightCoin 不會在任何情況下提供退款。

十 風險提示

1 政策性風險

目前國家對於區塊鏈項目以及互換方式融資的監管政策尚不明確，存在一定的因政策原因而造成參與者損失的可能性；市場風險中,若數字資產市場整體價值被高估, 那麼投資風險將加大, 參與者可能會期望互換項目的增長過高, 但這些高期望可能無法實現。

2 監管風險

包括 LightCoin 在內的數字資產交易具有極高不確定性，由於數字資產交易領域目前尚缺乏強有力的監管，故而電子代幣存在暴漲暴跌、受到莊家操控等情況的風險, 個人參與者入市後若缺乏經驗, 可能難以抵御市場不穩定所帶來的資產衝擊與心理壓力。雖然學界專家、官方媒體等均時而給出謹慎參與的建議，但尚無成文的監管方法與條文出台, 故而目前此種風險難以有效規避。

不可否認, 可預見的未來, 會有監管條例出台以約束規範區塊鏈與電子代幣領域。如果監管主體對該領域進行規範管理，互換時期所購買的

代幣可能會受到影響，包括但不限於價格與易售性方面的波動或受限。

3 團隊風險

當前區塊鏈技術領域團隊、項目眾多，競爭十分激烈，存在較強的市場競爭和項目運營壓力。光鏈項目是否能在諸多優秀項目中突圍，受到廣泛認可，既與自身團隊能力、願景規劃等方面掛鈎，也受到市場上諸多競爭者乃至寡頭的影響，其間存在面臨惡性競爭的可能。光鏈基於創始人多年行業積累的人脈，匯聚了一支活力與實力兼備的人才隊伍，吸引到了區塊鏈領域的資深從業者、具有豐富經驗的技術開發人員。團隊內部的穩定性、凝聚力對於光鏈的整體發展至關重要。在今後的發展中，不排除有核心人員離開、團隊內部發生衝突而導致光鏈整體受到負面影響的可能性。

4 技術風險

首先，本項目基於密碼學算法所構建，密碼學的迅速發展也勢必帶來潛在的被破解風險；其次，區塊鏈、分布式賬本、去中心化、不同意篡改等技術支撐著核心業務發展，光鏈團隊不能完全保證技術的落地；

再次, 項目更新調整過程中, 可能會發現有漏洞存在, 可通過發佈補丁的方式進行彌補, 但不能保證漏洞所致影響的程度。

5 安全風險

在安全性方面, 單個持幣者的金額很小, 但總人數眾多, 這也為項目的安全保障提出了高要求。電子代幣具有匿名性、難以追溯性等特點, 易被犯罪分子所利用,或受到黑客攻擊, 或可能涉及到非法資產轉移等犯罪行為。目前未可知的其他風險：隨著區快鏈技術與行業整體態勢的不斷發展, LightCoin 可能會面臨一些尚未預料到的風險。請參與者在做出參與決策之前, 充分瞭解團隊背景,知曉項目整體框架與思路, 合理調整自己的願景, 理性參與代幣互換。

6 免責聲明

本文檔僅作為傳達信息之用, 文檔內容僅供參考, 不構成在光鏈、光鏈基金會、及其相關公司的任何形式的建議、教唆或邀約。此類邀約必須通過機密備忘錄的形式進行, 且須符合相關法律規定。本文檔內容不得被解釋為強迫參與互換。任何與本白皮書相關的行為均不得視為參與互換, 包括要求獲取本白皮書的副本或向他人分享本白皮書。參

與互換則代表參與者已達到年齡標準, 具備完整的民事行為能力, 與光鏈簽訂的合同是真實有效的。所有參與者均為自願簽訂合同, 並在簽訂合同之前對光鏈進行了清晰必要的瞭解。