格雷現金（GCH）區塊鏈白皮書

格雷欣實驗室/Gresham laboratory

1. 目錄

2. 引言

區塊鏈（Blockchain）的概念誕生自比特幣，最早可以追溯到 2008 年末，化名為“中本聰”的神秘人士首次提出了區塊鏈的概念。自 2009 年以來，出現了各種各樣的類比特幣的數字貨幣，得以使區塊鏈的價值被廣泛認知，比特幣開創了去中心化密碼貨幣的先河。在那之後一些區塊鏈平臺努力的支持可運作的去中心化應用，更多的企業家和開發者不斷的嘗試推廣這一技術，以便在單一的區塊鏈平臺上支持更為廣泛的應用程式。

多年的應用實踐充分檢驗了區塊鏈技術的可行性和安全性。人們發現，區塊鏈的意義在於可以構建一個更加可靠的互聯網系統，從根本上解決價值交換與轉移中存在的欺詐和尋租現象。越來越多的人相信，隨著區塊鏈技術的普及，數字經濟將會更加真實可信，經濟社會由此變得更加公正和透明。

區塊鏈技術從 1.0 數字資產“炒幣”時代到數字資產與智能合約相結合的 2.0 時代，2018 年是區塊鏈技術向 3.0 時代騰飛的一年，區塊鏈及相關行業加速發展，標誌著人類開始構建真正的信任互聯網。

區塊鏈技術帶來的無處不在的價值交換，使得社會形成一個多種設備的無縫對接的價值互聯世界。區塊鏈使得經濟不僅僅是金錢的流通，互聯網不僅僅是資訊的流通，而是進一步促進資訊、金錢、價值的有效配置和流通，使人力內耗降到最低，成為真正意義上的去中心化組織。

進一步的研究發現，區塊鏈技術具備一種“降低成本”的強大能力，能簡化流程，降低一些不必要的交易成本及制度性成本。區塊鏈 3.0 時代，是結合實體經濟、實體產業結合，也是國家大力扶持的產業鏈實體與互聯網結合生活中各個領域，大力提升區塊鏈的應用價值。

全球正在步入“區塊鏈經濟時代”，未來 3-5 年區塊鏈技術將在物聯網、金融交易、網路安全、公共記錄等多個領域大顯身手，顯著改進這些領域的服務流程，甚至顛覆這些領域內的傳統商業模式，未來發展潛力巨大。全球範圍內，區塊鏈行業應用加速推進，從數字貨幣向非金融領域滲透擴散，和各行業創新融合，技術與監管存在的衝突矛盾進一步調和，技術方案和性能不斷得到優化，區塊鏈作為一個新興的物種正發揮出其存在的巨大價值。

區塊鏈技術是世界所有人的機會。區塊鏈，將重新定義世界。

3. 關於區塊鏈

3.1. 區塊鏈簡介

3.1.1. 什麼是區塊鏈

區塊鏈是分佈式數據存儲、點對點傳輸、共識機制、加密演算法等電腦技術的新型應用模式。它是一串使用密碼學方法相關聯產生的數據塊，每一個數據塊中包含了一次網路交易的資訊，用於驗證其資訊的有效性（防偽）和生成下一個區塊。

狹義來說，它是一種按照時間順序將數據區塊以順序相連的方式組合成的一種鏈式數據結構， 並以密碼學方式保證的不可篡改和不可偽造的分佈式帳本。

廣義來講，區塊鏈技術是利用塊鏈式數據結構來驗證與存儲數據、利用分佈式節點共識演算法來生成和更新數據、利用密碼學的方式保證數據傳輸和訪問的安全、利用由自動化腳本代碼組成的智能合約來編程和運算元據的一種全新的分佈式基礎架構與計算方式。

區塊鏈技術的思想促使我們，重新思考如何去創建交易、存儲數據和交換資產。它是一場巨大變革的起點。

3.1.2. 區塊鏈發展歷史

區塊鏈的概念首次在 2008 年末由中本聰（Satoshi Nakamoto）發表在比特幣論壇中的論文《Bitcoin: A Peer-to-Peer Electronic Cash System》提出。論文中區塊鏈技術是構建比特幣數據結構與交易資訊加密傳輸的基礎技術，該技術實現了比特幣的挖礦與交易。中本聰認為：第一，借助第三方機構來處理資訊的模式擁有點與點之間缺乏信任的內在弱點，商家為了提

防自己的客戶，會向客戶索取完全不必要的資訊，但仍然不能避免一定的欺詐行為；第二，仲介機構的存在，增加了交易成本，限制了實際可行的最小交易規模；第三，數字簽名本身能夠解決電子貨幣身份問題，如果還需要第三方支持才能防止雙重消費，則系統將失去價值。基於以上三點現存的問題，中本聰在區塊鏈技術的基礎上，創建了比特幣。

區塊鏈的發展類比互聯網本身的發展，今天我們看到的區塊鏈技術實際上已經經歷了漫長的歷史演進過程。最早可以追溯到 1982 年 Leslie Lamport 提出的拜占庭將軍問題（Byzantine Generals Problem）。拜占庭將軍問題是解釋一致性問題的一個虛擬模型。拜占庭是古東羅馬的首都，由於地域寬廣，守衛的將軍需要通過信使傳遞消息，達成一致的決定。但由於將軍中可能存在叛徒，這些叛變的將軍可能會發送錯誤的消息，干擾大家的決議。

拜占庭問題的提出是為了解決在這種情況下，怎樣讓忠誠的將軍們達成一致的決議。這個問題演變到電腦領域，就是在互聯網中不同電腦通過通訊達成一致。在實際過程中有些電腦可能出現錯誤，有些電腦有可能被駭客攻擊，怎樣保證網路上的電腦對某個事物達成一致就是這個理論模型要解決的問題。

拜占庭問題是區塊鏈技術裏共識機制的基礎。正因為有了這樣的理論基礎，才使得區塊鏈技術有了發展的科學基礎。

在比特幣之前，區塊鏈經過了幾代的演進，這期間包括 e-Cash、HashCash、B-money 等相關的數字貨幣。這個期間屬於數字貨幣的發展階段。

1983 年提出的 e-Cash 是一個數位化的支付系統，但由於中心化原因導致後來失敗。

1997 年的 HashCash 是一個採用工作量機制（Poof of Work，PoW）的數字貨幣，之後被數字貨幣大量廣泛使用。

1998 年提出的 B-money 是首個提出的去中心化的數字貨幣系統，遺憾的是沒有提出具

體的實現。

直到 2009 年 1 月比特幣橫空出世，才真正實現了去中心化的、賬務公開的數字貨幣系統，正式開啟了區塊鏈技術發展。

比特幣出現後，它背後的區塊鏈技術才開始引起了大家的重視。

但比特幣本身基於腳本開發的原因，使得區塊鏈技術應用受到了很大制約。基於區塊鏈進行應用開發的呼聲越來越高，這也催生了許多牛人在智能合約方面的探索。

Vitalik Buterin 的以太坊，Daniel Larimer 的 EOS 都是區塊鏈技術在智能合約方面的研究和探索，PressOne 更是如此。

區塊鏈經歷了從加密貨幣、數字貨幣到智能合約的發展，以後還會向更複雜的智慧合約方向進軍。

隨著區塊鏈技術的不斷成熟，基於區塊鏈進行應用開發的難度會不斷降低，同時也會加速區塊鏈領域的創新和與互聯網的融合。

區塊鏈技術不僅可用於數字貨幣，還有其他更廣泛的用途。貨幣範圍的應用被稱為區塊鏈 1.0，主要解決貨幣和支付手段的去中心化。

早在比特幣創建之初，中本聰就考慮讓其具有可編程的特徵，從而可以支持多種交易類型。

以此為發端，區塊鏈技術的應用範圍超越了數字貨幣，區塊鏈 2.0 可用來註冊、確認和轉移各種不同類型的資產及合約，如各種金融交易、公共記錄、私人記錄等，從而更宏觀地對整個市場去中心化。

區塊鏈 3.0 則進一步超越了經濟領域，可用於實現全球範圍內日趨自動化的物理資源和人力資產的分配，促進科學、教育、健康、電子商務、社區、娛樂等領域的大規模協作。

3.1.3. 區塊鏈的進化歷程

- 區塊鏈 1.0——數字貨幣

是以比特幣為代表的數字貨幣應用，其場景包括支付、流通等貨幣職能。

- 區塊鏈 2.0——數字資產與智能合約

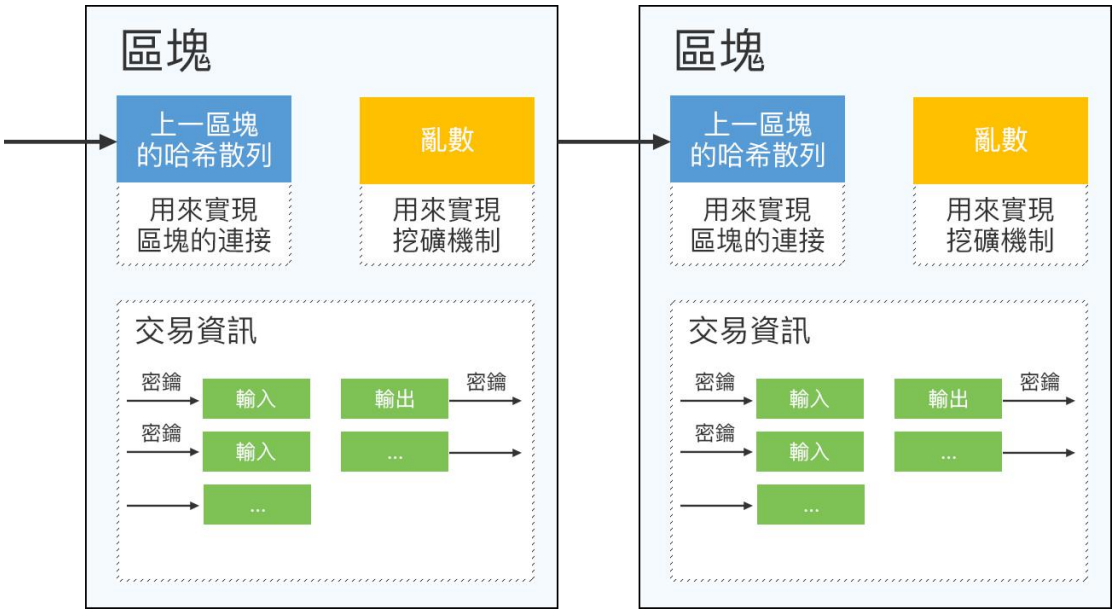
是數字貨幣與智能合約相結合，對金融領域更廣泛的場景和流程進行優化的應用。

- 區塊鏈 3.0——IFMChain，區塊鏈正式鏈接移動終端

應用範圍超出金融領域，區塊鏈正式鏈接移動終端，為各種行業提供去中心化解決方案。

3.1.4. 區塊鏈核心技術

1. 區塊鏈的鏈接



顧名思義，區塊鏈即由一個個區塊組成的鏈。每個區塊分為區塊頭和區塊體（含交易數據）兩個部分。區塊頭包括用來實現區塊鏈接的前一區塊的哈希（PrevHash）值（又稱散列值）和用於計算挖礦難度的亂數（nonce）。前一區塊的哈希值實際是上一個區塊頭部的哈希值，而計算亂數規則決定了哪個礦工可以獲得記錄區塊的權力。

2. 共識機制

區塊鏈是伴隨比特幣誕生的，是比特幣的基礎技術架構。可以將區塊鏈理解為一個基於互聯網的去中心化記賬系統。類似比特幣這樣的去中心化數字貨幣系統，要求在沒有中心節點的情況下保證各個誠實節點記賬的一致性，就需要區塊鏈來完成。所以區塊鏈技術的核心是在沒有中心控制的情況下，在互相沒有信任基礎的個體之間就交易的合法性等達成共識的共識機制。

區塊鏈的共識機制目前主要有 4 類：PoW、PoS、DPoS、分佈式一致性演算法。

3. 解鎖腳本

腳本是區塊鏈上實現自動驗證、自動執行合約的重要技術。每一筆交易的每一項輸出嚴

格意義上並不是指向一個地址，而是指向一個腳本。腳本類似一套規則，它約束著接收方怎樣才能花掉這個輸出上鎖定的資產。

交易的合法性驗證也依賴於腳本。目前它依賴於兩類腳本：鎖定腳本與解鎖腳本。鎖定腳本是在輸出交易上加上的條件，通過一段腳本語言來實現，位於交易的輸出。解鎖腳本與鎖定腳本相對應，只有滿足鎖定腳本要求的條件，才能花掉這個腳本上對應的資產，位於交易的輸入。通過腳本語言可以表達很多靈活的條件。解釋腳本是通過類似我們編程領域裏的“虛擬機”，它分佈式運行在區塊鏈網路裏的每一個節點。

4. 交易規則

區塊鏈的交易就是構成區塊的基本單位，也是區塊鏈負責記錄的實際有效內容。一個區塊鏈交易可以是一次轉賬，也可以是智能合約的部署等其他事務。

就比特幣而言，交易即指一次支付轉賬。其交易規則如下：

1）交易的輸入和輸出不能為空。

2）對交易的每個輸入，如果其對應的 UTXO 輸出能在當前交易池中找到，則拒絕該交易。因為當前交易池是未被記錄在區塊鏈中的交易，而交易的每個輸入，應該來自確認的 UTXO。如果在當前交易池中找到，那就是雙花交易。

3）交易中的每個輸入，其對應的輸出必須是 UTXO。

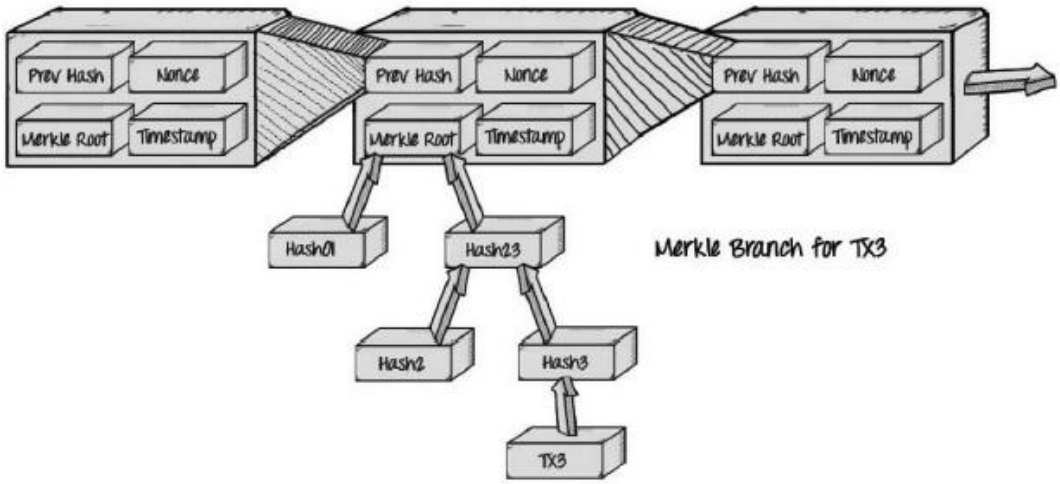
4）每個輸入的解鎖腳本（unlocking script）必須和相應輸出的鎖定腳本（locking script）共同驗證交易的合規性。

5. 交易優先順序

區塊鏈交易的優先順序由區塊鏈協議規則決定。對於比特幣而言，交易被區塊包含的優先次序由交易廣播到網路上的時間和交易額的大小決定。隨著交易廣播到網路上的時間的增長，交易的鏈齡增加，交易的優先順序就被提高，最終會被區塊包含。對於以太坊而言，交

易的優先順序還與交易的發佈者願意支付的交易費用有關，發佈者願意支付的交易費用越高，交易被包含進區塊的優先順序就越高。

6. Merkle 證明



Merkle 證明的原始應用是比特幣系統（Bitcoin），它是由中本聰（Satoshi Nakamoto）在 2009 年描述並且創造的。比特幣區塊鏈使用了 Merkle 證明，為的是將交易存儲在每一個區塊中。使得交易不能被篡改，同時也容易驗證交易是否包含在一個特定區塊中。

7. RLP

RLP（Recursive Length Prefix，遞歸長度首碼編碼）是 Ethereum 中對象序列化的一個主要編碼方式，其目的是對任意嵌套的二進位數據的序列進行編碼。

3.1.5. 區塊鏈分類

公有區塊鏈（PublicBlockChains)

公有區塊鏈是指：世界上任何個體或者團體都可以發送交易，且交易能夠獲得該區塊鏈的有效確認，任何人都可以參與其共識過程。公有區塊鏈是最早的區塊鏈，也是應用最廣泛的區塊鏈，各大 bitcoins 系列的虛擬數字貨幣均基於公有區塊鏈，世界上有且僅有一條該幣種對應的區塊鏈。

聯合（行業）區塊鏈（ConsortiumBlockChains)

行業區塊鏈：由某個群體內部指定多個預選的節點為記賬人，每個塊的生成由所有的預選節點共同決定（預選節點參與共識過程），其他接入節點可以參與交易，但不過問記賬過程(本質上還是託管記賬，只是變成分佈式記賬，預選節點的多少，如何決定每個塊的記賬者成為該區塊鏈的主要風險點），其他任何人可以通過該區塊鏈開放的 API 進行限定查詢。

私有區塊鏈（privateBlockChains)

私有區塊鏈：僅僅使用區塊鏈的總賬技術進行記賬，可以是一個公司，也可以是個人，獨享該區塊鏈的寫入許可權，本鏈與其他的分佈式存儲方案沒有太大區別。(Dec2015)保守的巨頭（傳統金融）都是想實驗嘗試私有區塊鏈，而公鏈的應用例如 bitcoin 已經工業化，私鏈的應用產品還在摸索當中。

3.1.6. 區塊鏈特徵

去中心化

由於使用分佈式核算和存儲，不存在中心化的硬體或管理機構，任意節點的權利和義務都是均等的，系統中的數據塊由整個系統中具有維護功能的節點來共同維護。得益於區塊鏈的去中心化特徵，比特幣也擁有去中心化的特徵 。

開放性

系統是開放的，除了交易各方的私有資訊被加密外，區塊鏈的數據對所有人公開，任何人都可以通過公開的介面查詢區塊鏈數據和開發相關應用，因此整個系統資訊高度透明。

自治性

區塊鏈採用基於協商一致的規範和協議（比如一套公開透明的演算法）使得整個系統中的所有節點能夠在去信任的環境自由安全的交換數據，使得對“人”的信任改成了對機器的信任，任何人為的干預不起作用。

資訊不可篡改

一旦資訊經過驗證並添加至區塊鏈，就會永久的存儲起來，除非能夠同時控制住系統中超過 51%的節點，否則單個節點上對數據庫的修改是無效的，因此區塊鏈的數據穩定性和可靠性極高。

匿名性

由於節點之間的交換遵循固定的演算法，其數據交互是無需信任的（區塊鏈中的程式規則會自行判斷活動是否有效），因此交易對手無須通過公開身份的方式讓對方自己產生信任，對信用的累積非常有幫助。

3.2. 區塊鏈前景

3.2.1. 區塊鏈應用要求

如今許多人質疑，除了炒作和投機，區塊鏈還有多少真正的價值。這項技術的處理速度太慢，無法大規模應用。第一代技術往往無法帶來轟動性的變革，要等到第二代或第三代技術。技術被採納常常要經歷這樣的過程。區塊鏈的唯一不同之處在於它的迭代過程受到了大量關注。長遠來看，區塊鏈能夠讓很多行業更加自動化、透明和分散化，區塊鏈的成熟只是時間問題。

現在很多組織和機構都在研究區塊鏈應用，一個好的區塊鏈應用，或者說去中心化應用想要更加具有普適性，需要具備以下要求：

1）大用戶量支持能力

作為一個優秀的應用，至少可支持百萬級別用戶數。無論其是中心化的還是去中心化的，其都需具備強大的多用戶支持能力。如果去中心化應用想要被主流用戶接受，那麼至少要具備支持百萬級人數的使用能力才行，所以去中心化應用需要有足夠大的擴容性。

舉例，比如我們熟知的 Facebook、Uber 等大型應用，必須具備能夠處理數千萬日活躍用戶的技術，否則應用程式無法正常工作，其又怎麼能稱作優秀的應用。區塊鏈應用也是一樣，其將來的應用場景無論是支付交易還是社交應用，都需要具備大用戶量支持能力，擁有一個可以處理大量用戶數量的平臺至關重要。現在區塊鏈應用的用戶量是相對少的，所以，哪一個應用擁有強大的擴容性是未來發展的重要一環。

2）免費的應用體驗

整個應用平臺或者操作系統，需要具備支持應用此平臺開發出免費應用軟體的能力，需提供良好的用戶體驗於用戶。即使，去中心化應用服務好處很多，也不能強迫用戶必須付費

才能使用。

很多時候，應用開發人員要靈活的提供免費服務給用戶，當用戶不必花錢就可以使用平臺，在此平臺上開發出的應用軟體數量勢必增長。同時，免費的塊鏈平臺自然會得到更多用戶的關注。當具有了足夠多的用戶規模，開發者和相關企業就可創建出更多的盈利模式。

3）簡易便捷的系統更新能力

整個區塊鏈應用操作平臺應該給參與進來的開發者，提供足夠的自由度。根據他們的想法和需求，在合適的時間去更新去中心化應用。或者讓個人根據自己的需求，選擇自己想更新的時間。

如果應用中出現了 bug 需要解決，開發人員在修補的時候，不應影響整個底層操作系統。另外，基於塊鏈的應用程式在進行功能迭代的時候自然需要能支持軟體升級。在區塊鏈底層平臺遭遇 bug 的時候，其應該具備能從 bug 中修復錯誤的能力。

4）低延遲性

區塊鏈應用或說去中心化應用除了應該具備平穩地運行能力，還應具備很低的延時性。延遲時間越久，越會影響用戶體驗，而用戶體驗的下降，將會嚴重影響並降低應用程式的市場競爭力。

5）強大的串行性能

一個良好的區塊鏈應用理應根據具體的應用場景選擇更加側重串行能力還是並行能力。比如，交易所之類的應用經常需要處理大量的串行操作，在此場景下，良好的區塊鏈架構需要具有強大的串行性能，並輔以智能的並行處理能力。

6）智能的並行性能

區塊鏈應用操作平臺要具有能讓基於它的去中心化應用同步運行的能力，這樣可以合理的分配計算量，從而節省時間。而且，大規模應用程式也是需要在多個 CPU 和電腦之間劃分工作負載的。

3.2.2. 區塊鏈的未來

區塊鏈技術發端於虛擬貨幣，自 2009 年以來，虛擬貨幣在全球範圍內興起，區塊鏈技術逐步走進人們的視野。目前，世界各國政府、產業界和學術界都高度關注區塊鏈的應用發展，相關的技術創新和模式創新不斷湧現。

趨勢一：區塊鏈行業應用加速推進，從數字貨幣向非金融領域滲透擴散

區塊鏈技術作為一種通用性術，從數字貨幣加速滲透至其他領域，和各行各業創新融合。未來區塊鏈的應用將由兩個陣營推動。一方面，IT 陣營，從資訊共用著手，以低成本建立信用為核心，逐步覆蓋數字資產等領域。另一方面，加密貨幣陣營從貨幣出發，逐漸向資產端管理、存證領域推進，並向征信和一般資訊共用類應用擴散。

趨勢二：企業應用是區塊鏈的主戰場，聯盟鏈/私有鏈將成為主流方向

目前，企業的實際應用集中數字貨幣領域，屬於虛擬經濟。我們認為，未來的區塊鏈應用將脫虛向實，更多傳統企業使用區塊鏈技術來降成本、提升協作效率，激發實體經濟增長，是未來一段時間區塊鏈應用的主戰場。

與公有鏈不同，在企業級應用中，更關注區塊鏈的管控、監管合規、性能、安全等因素。因此，聯盟鏈和私有鏈這種強管理的區塊鏈部署模式，更適合企業在應用落地中使用，是企業級應用的主流技術方向。

趨勢三：應用催生多樣化的技術方案，區塊鏈性能將不斷得到優化

未來，區塊鏈應用將從單一到多元方向發展。票據、支付、保險、供應鏈等不同應用，在即時性、高併發性、延遲和吞吐等多個維度上將高度差異化。這將催生出多樣化的技術解決方案。區塊鏈技術還遠未定型，在未來一段時間還將持續演進，共識演算法、服務分片、處理方式、組織形式等技術環節上都有提升效率的空間。

趨勢四：區塊鏈與雲計算的結合越發緊密，BaaS 有望成為公共信任基礎設施

雲計算是大勢所趨。區塊鏈與雲的結合也是必然的趨勢。區塊鏈與雲的結合，有兩種模式，一種是區塊鏈在雲上，一種是區塊鏈在雲裏。後面一種，也就是 BaaS，Blockchain-as-a-Service，是指在雲服務商直接把區塊鏈作為服務提供給用戶。未來，雲服務企業越來越多地將區塊鏈技術整合至雲計算的生態環境中，通過提供 BaaS 功能，有效降低企業應用區塊鏈的部署成本，降低創新創業的初始門檻。

趨勢五：區塊鏈安全問題日益凸顯，安全防護需要技術和管理全局考慮

區塊鏈系統從數學原理上講，是近乎完美的，具有公開透明、難以篡改、可靠加密、防 DDoS 攻擊等優點。但是，從工程上來看，它的安全性仍然受到基礎設施、系統設計、操作管理、隱私保護和技術更新迭代等多方面的制約。未來需要從技術和管理上全局考慮，加強基礎研究和整體防護，才能確保應用安全。

趨勢六：區塊鏈的跨鏈需求增多，互聯互通的重要性凸顯

隨著區塊鏈應用深化，支付結算、物流追溯、醫療病歷、身份驗證等領域的企業或行業，都將建立各自區塊鏈系統。未來這些眾多的區塊鏈系統間的跨鏈協作與互通是一個必然趨勢。跨鏈技術是區塊鏈實現價值互聯網的關鍵，區塊鏈的互聯互通將成為越來越重要的議題。

趨勢七：區塊鏈競爭日趨激烈，專利爭奪成為競爭重要領域

隨著參與主體的增多，區塊鏈的競爭將越來越激烈，競爭是全方位的，包括技術、模式、專利等多維度。未來，企業將在區塊鏈專利上加強佈局。2014 年以來，區塊鏈專利申請數量出現爆發式增長。區塊鏈專利主要分佈在北美洲的美國、歐洲的英國、亞洲的中國和韓國，未來將維持這類格局。中美專利差距在減小，中國 2016 年申請量已超越美國。可以預見，未來的區塊鏈專利爭奪將日趨激烈。

趨勢八：區塊鏈投資持續火爆，代幣眾籌模式累積風險值得關注

區塊鏈成為資本市場追逐的熱點。未來投資還將延續 2018-2020 年不斷上升的趨勢。與其他科技領域的融資模式不同，區塊鏈領域出現了一種稱為“代幣眾籌”的模式，即 Initial Coin Offering（ICO），是創業公司發行代幣、募集資金的一種眾籌方式。2016 年，全球代幣眾籌的份額已占區塊鏈相關風險投資總額的 48%，2017 年，全球代幣眾籌的份額已占區塊鏈相關風險投資總額的 49.5%，成為一個重要管道。預計 2018-2020 年還將出現 300 個以上的 ICO 案例。隨著代幣眾籌交易量攀升，其缺乏審核、價值波動巨大、處於監管邊緣等風險將隨之增大，值得關注。

趨勢九：區塊鏈技術與監管存在衝突，但矛盾有望進一步調和

區塊鏈的去中心化、去仲介和匿名性等特性與傳統的企業管理和政府監管體系不協調。但也應該看到區塊鏈給監管帶來的機遇。未來企業將積極迎合監管需求，在技術方案和模式設計上主動內置監管要求，不僅要做到合規運作，還能大幅度節約監管合規的成本。我們也認為，未來全球的監管部門也將擁抱區塊鏈這項新的監管科技，用新科技提升政府監管效能。

趨勢十：可信是區塊鏈的核心要求，標準規範的重要性日趨凸顯

在未來以區塊鏈為基礎的價值傳遞網路上，我們把將完全用演算法和軟體來構建信任基礎，但這是遠遠不夠的，還需要標準為區塊鏈增信。未來，區塊鏈的標準，將從用戶的角度出發、以業務為導向，從智能合約、共識機制、私鑰安全、許可權管理等維度，規範區塊鏈的技術和治理，增強區塊鏈的可信程度，給區塊鏈的信任增加砝碼。

4. 關於格雷欣

4.1. 關於格雷欣實驗室

格雷欣實驗室(Gresham laboratory)，新興的全球數字貨幣實驗室，支持比特幣(BTC)/萊特幣(LTC)/以太坊(ETH)/零幣(ZEC)等多種數字貨幣交易，高速撮合引擎、全方位資金安全保障及極速充提體驗。為全球數字貨幣愛好者提供最安全、便捷和專業的數字資產服務，我們一直致力於打造最專業的數字資產交易實驗與實踐平臺。格雷欣實驗室遵循以下六大價值理念（DRIVES）：

4.2. 什麼是格雷現金

格雷現金是在 ripple 的 RTXP 協議和比特幣去中心化的基礎上，採用區塊鏈技術研發的數字貨幣，是格雷現金全球數字貨幣應用生態的中心貨幣。

格雷現金未來將成為生態體系內對接多元化實體各產業鏈、價值鏈和生態鏈的流通貨幣，以及應用生態內區塊鏈大資料中心的核心資訊來源。借助資料產生的洞見，格雷現金應用生態將對交易雙方進行精准匹配，實現智慧化撮合，大幅提高成交率，降低交易成本。

格雷現金作為生態內部的資金樞紐或中心以促進內部資金調劑和集中管理，進一步將格雷現金系統進化並延伸到產業鏈、價值鏈和生態，與各類金融機構和實體產業合作，共同構建“區塊鏈＋金融+產業+消費”的應用生態。

4.3. 格雷現金的特點

區塊鏈底層技術

採用區塊鏈底層技術，擁有去中心化、公開透明、安全可靠、開放共識等特點。

擁有實體應用生態

基於格雷現金系統建立龐大的區塊鏈數字貨幣生態，與全球多種實體進行對接。

生態中心幣

格雷現金作為生態的中心貨幣，連結了人民幣與其他幣（其他數字貨幣、法幣及數字資產）的交易、匯兌、流通通道，是貫穿整個生態的潤滑劑，自身價值不可估量。

逐步增發

以智慧合約建立規則，每日增發，定期衰減。

4.4. 格雷現金錢包

錢包是格雷現金主要獲取、存儲以及平臺內各個貨幣之間轉換的重要途徑。

一個格雷現金錢包支持：

- 有一個位址像這種形式：Ox9CJAWyB4rj91VRWn96DkukG4bwdtyTh1('Ox'打頭，外加 32 位 16 進制字元)組成; 編碼地址內含校驗碼。確保不太可能發生打字錯誤。

- ✓ 收取挖礦收益；
- ✓ 收取推廣收益
- ✓ 與錢包餘額互轉
- ✓ 兌換平臺內推出的所有幣種

4.5. 格雷現金賬戶

帳戶是 格雷現金總帳裏的一個實體。通常人們擁有一個帳戶，保存著他們的格雷現金借貸記錄，期票（IOU），信任路徑和對其他帳號的信任關係。任何人知道一個帳戶的私密金鑰，就能夠授權這個錢包發起交易（也就是擁有私密金鑰就擁有該帳號的一切）。

一個格雷現金賬戶:

- ➢ 持有格雷現金交易餘額
- ➢ 可能持有另一個帳號發出的期票（IOU）
- ➢ 可以設置對另一個帳號（通常是閘道 Gateway）的信任（該帳號就可以給你發行貨幣期票）
- ➢ 可以掛單，進行貨幣兌換錢包餘額，信託額度，支付都是公開信息。
- ➢ 沒人能夠知道錢包對應誰。

每一個格雷現金賬戶都有一個位址，用於別的錢包可以：

- ✧ 發送自己其他帳戶的餘額到該帳戶
- ✧ 擴大信託額度到該帳戶

4.6. 格雷現金的發行方案

恒定發行量：6 億枚

發行時間： 6 年

預挖：格雷欣實驗室預挖 3000 萬枚，占比 5%，格雷現金（Graycoin Cash） 正式上線三年後開始釋放，分三年均等釋放完。

格雷現金將流通於各個格雷欣實驗室打造的區塊鏈應用場景之中。

4.6.1. 發行計畫

首期：發行時間 3 個月，發行數量：600 萬

第二期：發行時間 8 個月，持幣和推廣獎勵每月增長 18%

第三期：發行時間 1 年 2 個月，持幣和推廣獎勵每月增長 14%

第四期：發行時間 1 年 8 個月，持幣和推廣獎勵每月增長 10%

第五期：發行時間 1 年 8 個月，持幣和推廣獎勵每月增長 6%

4.6.2. 收益計算

服務端的主要作用用於每天根據實際計算公式，計算每個用戶可以領取的平臺幣數量，具體算力如下：

持幣利息：

計算公式：當天收益=（當天發行量/所有持幣用戶數量）*（當天持幣數量*（算力值/1000）/所有節點持幣總量）*6000（發行計畫算力值）

計算公式 ： $Di=C/U\times(Mi\times(CF/1000)/(M_1+M_2+M_3+M_4+...)\times PCF$

公式說明：C:當天發行 GCH 數量

U:所有持幣會員數量

Mi:會員當天持幣數量

CF:當天算力值

Di:當天持幣利息

M_1 、M_2 、M_3 、M_4 ： 所有持幣量

PCF：發行計畫算力值

持幣收益案例：

假設全球僅有 10000 個持幣用戶數量，總持幣量為 1000000GCH，格雷欣實驗室當天發行 50000GCH，本人持幣 50001GCH，按照第一期發行算力值 6000 計算，本人因擁有

50001GCH，所以算力值按照最高 100，代入公式計算可得：

Di=(50000/10000)*(50001*(100/1000)/1000000)*6000=150.003GCH

4.6.3. 推廣收益

計算公式(中文說明)：當天推廣收益=用戶點推廣力/所有用戶點推廣力*（當天發行量/2*(算力值/1000)）

計算公式：$Bi=Xi/(X_1 +X_2 +X_3 +X_4 +...)\times(C/2*(CF/1000))$

公式說明：C:當天發行平臺幣數量

Bi:當天推廣收益

Xi：推廣算力

X_1 、X_2 、X_3 、X_4 ：每個錢包的推廣算力

CF:當天算力值

4.6.4. 用戶點推廣力

計算公式：$Xi=Pmax^{(1/3)}+(P_1 +P_2 +P_3 +P_4 +...)$

公式說明：Xi：推廣算力

$Pmax^{(1/3)}$：最大推廣力開立方

P：所有用戶推廣力

4.7. 格雷現金發行機制的特點

4.7.1. 去中心化

格雷現金是數字貨幣，沒有中央發行機構，去中心化的格雷現金按照比例增發管理幣，所以

沒有任何支付費用。

4.7.2. 公平獲益

格雷現金是第一種真正將貨幣價值回饋給價值創造者的數字貨幣!通過格雷現金的創新的發行演算法，將貨幣發行權分配給貨幣的持有者和推廣者，以實現價值創造者獲得價值的公平的貨幣體系。

4.7.3. 保值升值

格雷現金總量限定 6 億枚，貨幣軟體後臺被閉環鎖死，永遠無法增發貨幣。解決了通貨膨脹的問題，讓貨幣保值、升值。

4.7.4. 隨時提現

沒有封閉期，協力廠商大盤撮合交易，可隨時提取本金和利息。

4.7.5. 全球發行

體量越大，價值越高，也越穩定，從而使持有者和推廣者獲得的利潤也越高，再促使推廣者更加努力的進行推廣，使持有者願意投入更多，形成一個良性迴圈。

5. 關於格雷現金系統

5.1. 系統架構

格雷現金架構共有六層，分別為數據層、網路層、共識層、激勵層、合約層和應用

5.1.1. 數據層

基於區塊鏈的高冗餘存儲機制，區塊鏈存儲對區塊鏈的擴展性和性能都有一定的影響，格雷現金框架設計有多層次的節點系統，根據不同的節點應用選擇有不同的存儲策略（分佈式記賬）：記賬節點：格雷現金的核心角色，受 BST 持有人的委託負責參與共識機制、製造區塊。全節點：負責保存完整數據，但不參與共識，偵聽並轉播交易。普通用戶直接通過介面或用戶端訪問，不保存數據。多層次節點系統的好處在於，並不希望有節點都參與記賬（挖

礦）、存儲完整數據、轉播交易。因為並不是所有節點都有共同的訴求，都希望保存完整數據，格雷現金設計讓整個系統有清晰的角色分工，專業的節點做專業的事情，既節約能源又提高了整個系統的效率。

5.1.2. 網路層

P2P 協議（P2P Protocol）支持區塊鏈網路中各節點的數據傳輸和信令交換，是數據分發或共識機制達成的重要通信保障，格雷現金系統設計中支持多種 P2P 協議、通信機制與序列化機制的配置，根據不同的場景需要迆行靈活的協議使用。在通信安全方面，可以靈活支持 HTTPS、TLS、WSS(SecureWebsockets)等安全通信協議，在需建立平臺應用對外服務介面上，可以擴展支持 OAuth 的認證集成。

5.1.3. 共識層

格雷現金選擇 PoW（工作量證明） 和 PoS（權益證明）共識演算法，是基於記賬人投票的拜占庭容錯共識演算法，具有高性能、高一致性的特點，適合於金融支付，數位化類交易數據頻繁產生，並且有較高即時性記賬要求的弱中心上層應用。傳統區塊鏈由於記賬規則的設定，需要達到一定的區塊確認數量，才能在一定概率上完成鏈的確認，也就是說在已出塊上追加區塊時並能 100%保證未來一定就是這個鏈，始終存在微小的被推翻可能。基本需要到 6 個區塊才 99.999999%的確認交易。這種模式下交易的最終性較弱，不太適合數字資產交易平臺等金融支付數位化類上層應用。而 dBFT 共識演算法可以很好的保持區塊一致性。這種共識演算法是根據權益佔有比例來選出記賬人，然後記賬人之間通過拜占庭容錯演算法來達成共識。具有一定的背書和信伕作用，因此基本不會發生超過 1/3 以上的記賬節點勾結作惡，即使發生這種情況，也可以利用密碼學證據運行事後取證追責。

這種方式的優點是：

（1）專業化的記賬人；

（2）可以容任何類型的錯誤；

（3）記賬由多人協同完成，每一個區塊都有最終性，不會分叉；

（4）演算法的可靠性有嚴格的數學證明；

dBFT 機制最核心的一點，就是最大限度地確保系統的最終性，不會分叉，非常適合於金融支付數位化類應用場景。

5.1.3.1.PoW(工作量證明)

工作量證明（Proof of Work），通過計算來猜測一個數值（nonce），得以解決規定的 hash 問題（來源於 hashcash）。保證在一段時間內，系統中只能出現少數合法提案。

同時，這些少量的合法提案會在網路中進行廣播，收到的用戶進行驗證後會基於它認為的最長鏈上繼續難題的計算。因此，系統中可能出現鏈的分叉（Fork），但最終會有一條鏈成為最長的鏈。

hash 問題具有不可逆的特點，因此，目前除了暴力計算外，還沒有有效的演算法進行解決。反之，如果獲得符合要求的 nonce，則說明在概率上是付出了對應的算力。誰的算力多，誰最先解決問題的概率就越大。當掌握超過全網一半算力時，從概率上就能控制網路中鏈的走向。這也是所謂 51% 攻擊的由來。

參與 PoW 計算比賽的人，將付出不小的經濟成本（硬體、電力、維護等）。當沒有成為首個

算出的“幸運兒”時，這些成本都將被沉沒掉。這也保障了，如果有人惡意破壞，需要付出大量的經濟成本。也有設計試圖將後算出結果者的算力按照一定比例折合進下一輪比賽考慮。

有一個很直觀的例子可以說明為何這種經濟博弈模式會確保系統中最長鏈的唯一。

超市付款需要排成一隊，可能有人不守規矩要插隊。超市管理員會檢查隊伍，認為最長的一條隊伍是合法的，並讓不合法的分叉隊伍重新排隊。只要大部分人不傻，就會自覺在最長的隊伍上排隊。

5.1.3.2.PoS(權益證明)

權益證明（Proof of Stake），2013 年被提出，最早在 Peercoin 系統中被實現，類似現實生活中的股東機制。

其原理是通過保證金（代幣、資產、名聲等具備價值屬性的物品即可）來對賭一個合法的塊成為新的區塊，收益為抵押資本的利息和交易服務費。提供證明的保證金（例如通過轉賬貨幣記錄）越多，則獲得記賬權的概率就越大。合法記賬者可以獲得收益。

PoS 是試圖解決在 PoW 中大量資源被浪費的缺點。惡意參與者將存在保證金被罰沒的風險，即損失經濟利益。一般的，對於 PoS 來說，需要掌握超過全網的資源，才有可能左右最終的結果。這個也很容易理解，三個人投票，前兩人分別支持一方，這時候，第三方的投票將決定最終結果。

PoS 也有一些改進的演算法，包括授權股權證明機制（DPOS），即股東們投票選出一個董事會，董事會中成員才有權進行記賬。

5.1.4. 激勵層

格雷現金的代幣有 20%用於共識獎勵，因為格雷現金獨特的共識機制，性能不受節點數量的影響，所以格雷現金的共識節點沒有設置上限，並且是動態發化的，任何人都可以隨時加入賺取獎勵。

5.1.5. 合約層

對於每一項智能合約，作為一項鏈上金融資產運行全生命週期管理，對智能合約的提交、部署、使用、註銷進行完整可控的流程管理，並集成許可權管理機制對智能合約操作的各項機制進行綜合性安全管理。互聯網金融行業的誠信、風控體系均通過格雷現金智能合約來設定完成，包括 P2P、眾籌、私募、互聯網金融附屬產品。比如進期合約，通過區塊鏈智能合

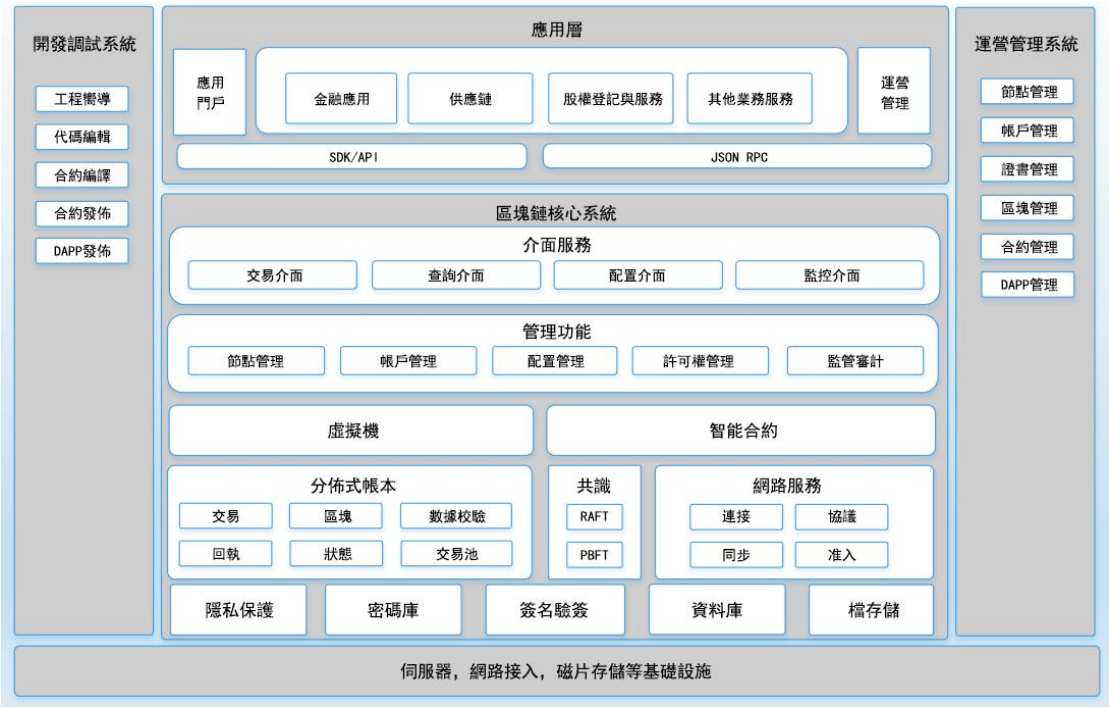
約，雙方簽名，未來指定的限期內按當日，約定出售資產合約。

5.1.6. 應用層

應用層會提供通用交易協議、支持多語言集成和功能擴展，目前已支持 C#、 Java、JavaScript、Python、PHP 等多語言，目前已開發完成通用的金融誠信協議，實際這套協議不只是應用互聯金融的誠信協議。

5.2. 平臺技術特性

不同於傳統的中心化商業模式，分佈式商業模式的發展需要由新一代數據交換基礎設施承載。格雷現金平臺是專為大規模分佈式商業設計開發的完整區塊鏈技術平臺，已經支撐了銀行、股權市場和供應鏈的多個分佈式商業場景。作為商用的新一代數據交換基礎設施，格雷現金平臺當前版本已經具有了一些領先的技術特性。



5.2.1. 功能

具備完善的商業應用所需的功能和易用性，促進應用落地的實踐。

■ 支持靈活的用戶帳戶管理功能，採用角色和許可權模型實現聯盟鏈參與者管理

■ 支持對全網所有節點同時進行靈活的配置修改，配置數據保持高一致性。

■ 基於 SDK、介面、智能合約，可快速的開發各種業務應用，將支持多種語言編寫智能合約，使業務開發過程更符合企業級軟體開發慣例。

■ 支持分組多副本方式存儲檔，並在區塊鏈中保存檔的哈希值和相關尋址資訊，提高區塊鏈的存儲和網路同步效率。

5.2.2. 性能

具備較高的交易吞吐能力和低延時特性，可平行擴容，可支持海量服務。

■ 對交易處理流程，通信流程進行優化，提升節點處理能力。

■ 實現高效共識演算法體系，採用插件式設計，支持經過優化的 PBFT 和 RAFT 共識演算法。

■ 具備並行計算架構，可平行擴容，滿足海量服務需求。

5.2.3. 安全

多層面，全面的安全防護，滿足高要求的安全標準。

- 對通信層，用戶數據等模組進行高強度的加密保護。
- 支持多種密碼學演算法，包括基於密碼學的隱私保護演算法。
- 提供安全方面的最佳實踐，保障全網安全。

5.2.4. 治理

具備規範的治理方式，保障業務合法合規，系統穩健運行

- 基於 CA 體系進行機構身份認證，具備節點准入控制機制。
- 提供監管審計的功能介面，支持監管審計接入
- 支持全面的區塊鏈指標監控，保障運營品質
- 支持全網灰度升級，確保大規模商用網路的可維護性。

5.3. 平臺技術路線

區塊鏈領域的技術形態仍在快速發展中，格雷現金平臺將以下幾個技術特性列為重點研究對象，一直在持續投入研究和開發。

5.3.1. 多鏈和跨鏈

根據業務功能、隱私保護、數據隔離、或者性能容量擴展的需求，建立多個獨立的鏈並行工作，鏈和鏈之間可以通過跨鏈服務進行交互，如發送交易，查詢交易結果，讀取配置數據等。跨鏈交互目前是區塊鏈領域的研究重點，在安全、防欺詐、數據一致性、效率等方面還需要進行深入探索。包括：

- 實現並行和跨鏈共識，提高共識效率；
- 用組合簽名替代交易執行進行區塊驗證，減少交易執行次數；
- 跨鏈通信和數據校驗、實現跨鏈安全交易，進行跨鏈對賬。

5.3.2. 分佈式存儲

現有區塊鏈實現中，每個節點存儲全量區塊鏈數據，數據冗餘度較高，且數據容量受單機存儲硬體影響，在海量服務中，如需存儲較長時間段的數據，其數據量一般不是單伺服器能容納的。

區塊鏈數據一般採用檔型本地資料庫如 leveldb，在本節點的物理硬碟上基於檔系統保存，不提供跨網路的存儲結構。而在對數據安全要求較高的機構裏，數據一般存儲在和外網隔離的安全區域裏，以保障數據的安全。同時，這些機構已經建立了成熟的數據存儲和維護方案，在基礎架構層面保障數據存儲服務的高可用、可擴容、可遷移、可維護，並和大數據平臺等系統進行整合。採用分佈式數據存儲的方案，可綜合考慮數據的容量、可維護性、安全性，支持使用現有的企業級分佈式存儲解決方案，如數據倉庫、資料庫集群等存儲區塊鏈數據。

5.3.3. 隱私保護

區塊鏈技術雖然有一定匿名性，但收發地址和金額都是可追溯的，對於某些行業應用如金融類應用，顯然缺乏隱私性。因此，格雷現金平臺考慮對以下數據進行周密的加密處理。

■ 交易身份匿名：交易中對交易雙（多）方地址進行完全匿名，滿足一次一密、不可偽造、無關聯性和可跟蹤性。

■ 交易數據加密：加密傳輸和存儲交易數據。

■ 帳戶狀態加密：加密傳輸和存儲帳戶狀態數據。

對於以上加密數據，滿足以下需求：

■ 利益相關方（交易對手方、監管方）有權利看到明文數據

■ 其他參與者沒有權利看到明文數據，但其必須可以對密文數據的真實性進行驗證

格雷現金平臺計畫實現多層次的隱私保護：

■ 身份匿名：使用群簽名進行身份匿名，同時監管方可對用戶身份進行跟蹤。

■ 數據隱私保護：已經在客戶端和智能合約上實現加法同態加密演算法，計畫增加零

知識證明用於證明加密數據的正確性（如帳戶餘額數據是否足夠用於支付）

■ 細粒度的許可權控制：基於屬性加密演算法和代理授權密碼演算法的多級訪問控制，用於控制對加密數據的隱私訪問。

5.3.4. 令牌系統

鏈上令牌系統有很多應用，從代表如美元或黃金等資產的子貨幣到公司股票，單獨的令牌代表智能資產，安全的不可偽造的優惠券，甚至與傳統價值完全沒有聯繫的用來進行積分獎勵的令牌系統。在格雷欣實驗室中實施令牌系統容易得讓人吃驚。關鍵的一點是理解，所有的貨幣或者令牌系統，從根本上來說是一個帶有如下操作的資料庫：從 A 中減去 X 單位並把 X 單位加到 B 上，前提條件是(1)A 在交易之前有至少 X 單位以及(2)交易被 A 批准。實施一個令牌系統就是把這樣一個邏輯實施到一個合約中去。

用 Java 語言實施一個令牌系統的基本代碼如下：

```
from = msg.sender

to = msg.data[0]

value = msg.data[1]

if    contract.storage[from] >= value

contract.storage[from] = contract.storage[from] value

contract.storage[to] = contract.storage[to] + value
```

這從本質上來說是本文將要進一步描述的“銀行系統”狀態轉變功能的一個最小化實施。需要增加一些額外的代碼以提供在初始和其他一些邊緣情況下分發貨幣的功能，理想情況下會增加一個函數讓其他合約來查詢一個地址的餘額。就足夠了。理論上，基於格雷欣實驗室的充當子貨幣的令牌系統可能包括一個基於比特幣的鏈上元幣所缺乏的重要功能：直接用這種貨幣支付交易費的能力。實現這種能力的方法是在合約裏維護一個格雷現金賬戶以用來為發送者支付交易費，通過收集被用來充當交易費用的內部貨幣並把它們在一個不斷運行的拍賣中拍賣掉，合約不斷為該格雷現金賬戶注資。這樣用戶需要用格雷現金“啟動”他們的帳戶，但一旦帳戶中有格雷現金它將會被重複使用因為每次合約都會為其充值

5.3.5. 虛擬機優化

格雷現金平臺計畫在下一版本支持更高性能的虛擬機，支持更主流的開發語言。計畫支持 JVM 虛擬機和 Java 開發語言。

5.3.6. 可信資訊管理

“預言機”解決方案讓區塊鏈的智能合約獲取現實世界的不確定數據資訊成為了一種可能，例如資產價格、貨幣匯率、股票指數等等。過經濟激勵與博弈機制來讓不確定的外部資訊進入區塊鏈智能合約，讓智能合約的執行能夠依賴現實世界的數據執行相關業務過程。採用特定的共識機制對提交資訊的確定性做出判斷，讓資訊知曉者在經濟利益驅動下基於區塊鏈數字身份提交現實世界的數據資訊，一定的懲罰機制也確保了資訊會向著數據的確定性和正確性方向進行收斂。

5.4. DAPP（去中心化應用）

5.4.1. 簡介

去中心化應用程式（DApps）是在 P2P 網路上而非在一台獨立的電腦中運行的應用程式，或者說，自從 P2P 網路出現以來，DApps 就一直存在。其設計目的是以不受任何單一實體控制的方式存在於互聯網上，所以，DApp 是存儲和管理任何類型數據的更可靠和安全的系統。

5.4.2. 特徵

• 公開性，DAPP 系統的設計公開透明，公開透明性是整個 DAPP 系統的基石，一個暗箱操作的組織不能作為 DAPP，現在的軟體開源精神成為公開性的一個典型範例;

• 去中心化性，沒有中心化個人和組織能控制整個 DAPP，這條特性決定了 自相似性，

去中心化特性保證了 DAPP 系統的生命力;

• 自治性，DAPP 系統可以參與，參與者都是 DAPP 系統的子公司或者單元，並從自身角度促進 DAPP 的發展。參與者的自發行為保障了 DAPP 的運行;

• 價值性，DAPP 系統必須是具有使用價值的，比如比特幣系統的國際付 网絡、匿名交易、避稅、價值儲存、不可凍結、不可監管的特性，這條 特性決定了比特幣 DAPP 系統的盈利性;

• 盈利性，DAPP 的參與者會獲得 DAPP 系統發展的獎勵，盈利性由 DAPP 本 身的價值性確定;

• 自相似性，即使在只有部分 DAPP 節點的情況下，DAPP 系統仍能正常運作併發展，部分單元節點的摧毀不會影響 DAPP 的發展，由去中心化性保證;

• 民主性，DAPP 系統核心協議的改變需要絕大多數單元的投票才能完成， 去中心化特性和自治性決定了 DAPP 必須是一個能夠民主投票的系統。

5.5. 非對稱加密演算法

非對稱加密演算法是一種密鑰的保密方法。

非對稱加密演算法需要兩個密鑰：公開密鑰（publickey）和私有密鑰（privatekey）。公開密鑰與私有密鑰是一對，如果用公開密鑰對數據進行加密，只有用對應的私有密鑰才能解密；如果用私有密鑰對數據進行加密，那麼只有用對應的公開密鑰才能解密。因為加密和解密使用的是兩個不同的密鑰，所以這種演算法叫作非對稱加密演算法。 非對稱加密演算法實現機密資訊交換的基本過程是：甲方生成一對密鑰並將其中的一把作為公用密鑰向其他方公開；得到該公用密鑰的乙方使用該密鑰對機密資訊進行加密後再發送給甲方；甲方再用自己保存的另一把專用密鑰對加密後的資訊進行解密。

另一方面，甲方可以使用乙方的公鑰對機密資訊進行簽名後再發送給乙方；乙方再用自己的私匙對數據進行驗簽。

甲方只能用其專用密鑰解密由其公用密鑰加密後的任何資訊。 非對稱加密演算法的保密性比較好，它消除了最終用戶交換密鑰的需要。

非對稱密碼體制的特點：演算法強度複雜、安全性依賴於演算法與密鑰但是由於其演算

法複雜，而使得加密解密速度沒有對稱加密解密的速度快。對稱密碼體制中只有一種密鑰，並且是非公開的，如果要解密就得讓對方知道密鑰。所以保證其安全性就是保證密鑰的安全，而非對稱密鑰體制有兩種密鑰，其中一個是公開的，這樣就可以不需要像對稱密碼那樣傳輸對方的密鑰了。這樣安全性就大了很多。

5.6. 術語

Bitcoin：比特幣，中本聰發起的數字貨幣技術。

Blockchain：區塊鏈，基於密碼學的可實現信任化的資訊存儲和處理技術。

Chaincode：鏈上代碼，運行在區塊鏈上提前約定的代碼（狀態機）。

DAO：Decentralized Autonomous Organization，分佈式自治組織，基於區塊鏈的按照智能合約聯繫起來的鬆散眾籌群體。

Distributed Ledger：分佈式記賬本，大家都認可的去中心化的帳本記錄平臺。

DLT：Distributed Ledger Technology。

DTCC：Depository Trust and Clearing Corporation，存托和結算公司，全球最大的金融交易後臺服務機構。

Fintech：Financial Technology，跟金融相關的（資訊）技術。

Hash：哈希演算法，任意長度的二進位值映射為較短的固定長度的二進位值的演算法。

Lightning Network：閃電網路，通過鏈外的微支付通道來增大交易吞吐量的技術。

Nonce：密碼學術語，表示一個臨時的值，多為隨機字串。

P2P：點到點的通信網絡，網路中所有節點地位均等，不存在中心化的控制機制。

PoW：Proof of Work，工作量證明，在一定難題前提下求解一個 SHA256 的 hash 問題。

Smart Contract：智能合約，運行在區塊鏈上提前約定的合同；

Sybil Attack（女巫攻擊）：少數節點通過偽造或盜用身份偽裝成大量節點，進而對分佈式系統系統進行破壞。

SWIFT：Society for Worldwide Interbank Financial Telecommunication，環球銀行金融電信協會，運營世界金融電文網路，服務銀行和金融機構。

挖礦：通過暴力嘗試來找到一個字串，使得它加上一組交易資訊後的 hash 值符合特定規則（例如首碼包括若干個 0），找到的人可以宣稱新區塊被發現，並獲得系統獎勵的格雷現金。

礦工：參與挖礦的人或組織。

礦機：專門為比特幣挖礦而設計的設備，包括 GPU、專用晶片等。

礦池：採用團隊協作方式來集中算力進行挖礦，對產出的比特幣進行分配。

市場深度：未成交的交易，衡量市場承受大額交易後匯率的穩定能力。

圖靈完備：指一個機器或裝置能用來模擬圖靈機（現代通用電腦的雛形）的功能，圖靈完備的機器在可計算性上等價。

6. 應用場景

6.1. 應用規劃

格雷欣致力於開發比特幣和以太坊之外的第三種區塊鏈生態系統，拓展區塊鏈技術的應用邊界和技術邊界，使普通互聯網用戶能感受到區塊鏈技術的價值。在格雷現金系統中，可以通過價值傳輸協議 RTXP 來實現點對點的價值轉移，並根據此協定，構建一個支援多個行業的（金融，電商，實體消費，社交、遊戲等）去中心化的產業流通平臺。

6.2. 應用領域

6.2.1. 網上商城

以區塊鏈為底層技術，實現去中心化，不可篡改等屬性，結合當前的電子商務和區塊鏈技術深度融合。通過區塊鏈技術打造優質商品，實現全民收益、全民監督。此外，格雷欣推出智能合約、多種簽名、數字貨幣交易、智能客服等多段無縫銜接服務，讓更多企業和客戶擁有創新的體驗和服務。

B2B2C 多用戶商城系統

幫助企業打造多種 B2B2C 盈利模式，開展多商家入駐型電商的最佳選擇。

會員管理系統

用數據幫您更好的瞭解顧客，關懷顧客，多種行銷手段提高複購率，增加營收。

O2O 門店新零售管理系統

開啟線上閒暇一體化，打造用戶主導的新型門店線上接觸客戶，促進多次到店消費。

解決方案：

小型企業融資困難、用戶貸款困難，是電商金融出現的重要因素，格雷現金為提供商提供線上的供貨結算系統，同時想小型企業和個人用戶提供金融服務產品，利用進入服務產品便捷、創新的特點，展開面向中小微企業和個人的融資、貸款業務。並提供供貨商和電商平臺牢固的捆在一起，還可以為用戶提供可持續、有效的金融服務。

1. 數字貨幣

區中心化的分佈式帳本系統，可以用戶等級和發行數位化資產、產權憑證、積分等，並以點對點的方式進行轉賬、支付和交易

2. 智能管理

商品數據、庫存、訂單，線上線下一體化管理，輕鬆對接各個平臺，匹配適應整條業務鏈的解決方案，合理應用於業態、行業及熱門電商形態。

3. 公開透明

包括生產、加工在內的供應鏈上所有環境都將通過照片和視頻的形式上傳到底層的格雷實驗室，用戶在購物時刻隨時查詢這些資訊，以驗證商家所說。

優勢：

區塊鏈上的俄數據具有不可篡改性，有利於商品的追本溯源；使用區塊鏈建立的平臺，可減少信用成本的建立。

1. 省信任成本

區塊鏈的應用使得電子商務行業中，不屬於集中市場的商家可以不用投入大量的精力、人力和廣告預算來建立信任。

2. 管理系統優化

防止了商品資訊以及在運輸過程中被動手腳的可能，一旦出現問題，可以輕易地查到是在哪個環節出現了問題，理清相關責任。

3. 數據真實性

適用於分佈式帳本模式，該模式記錄的每一筆交易都具有防篡改性，並且在全球的網路上保持著資訊的真實性，防止刷單等行為造成購買過程中的資訊不對等

4. 去中心化支付

有助於降低金融機構間的對賬成本以及爭議解決的成本，從而顯提高支付業務的處理速度以及效率

6.2.2. 遊戲平臺

遊戲產業是一個很龐大的產業，目前全球遊戲玩家已超過 10 億人，產業規模突破 1080 億美元。但是對於玩家而言，遊戲產業存在一個巨大的痛點：中心化，這樣玩家的利益就很難保障。據說以太坊的創始人 V 神，就是因為玩“魔獸世界”時，被遊戲方隨意刪除了他遊戲中的人物，一怒之下開發了以太坊。與傳統網遊、端遊等遊戲不同，區塊鏈遊戲都被分

佈式記錄在公開透明的區塊鏈上，不僅是獨一無二的。而且一旦被你擁有，就是你的個人資產，除非個人保管不善或區塊鏈所屬交易所出現問題，否則無法被任何人複製、修改或銷毀。

優勢：

1. 數據真實性

區塊鏈具備唯一性、安全性與不可篡改性的技術支撐

2. 去中心化支付

有助於降低金融機構間的對賬成本以及爭議解決的成本，從而顯提高支付業務的處理速度以及效率

3. 資產共用

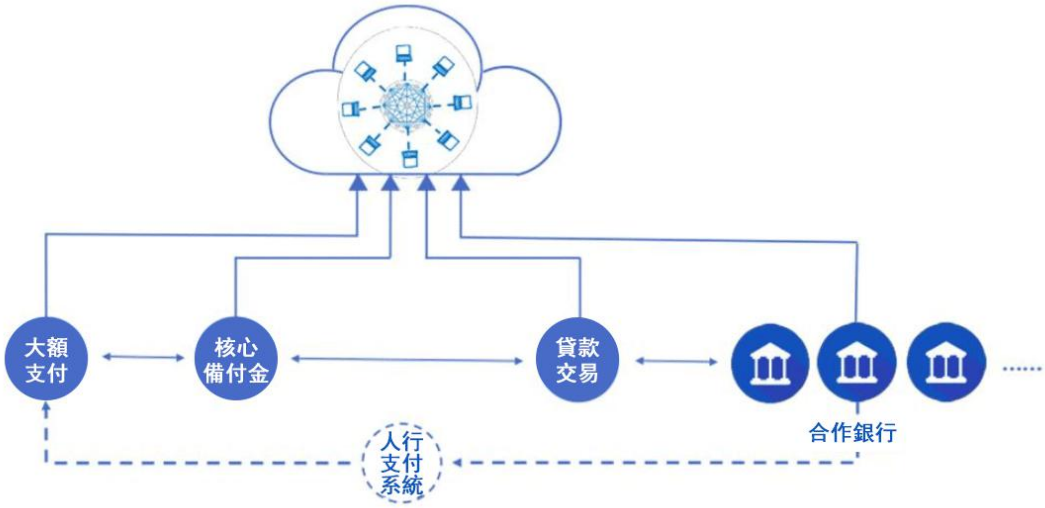
玩家角色資訊作為個人“資產”在多個遊戲世界中流通成為可能，區塊鏈遊戲裏面的數字資產都可以按照一定的協議實現跨平臺流通，這與傳統網路遊戲封閉的系統有很大差異，多個區塊鏈遊戲產品可以組成一個共識的遊戲聯盟鏈，從而實現各個遊戲資產流通及用戶共用，這種能力無疑是啟動和放大區塊鏈遊戲的數字資產價值

格雷欣實驗室（GCH）娛樂通過平臺 API 可以面向所有遊戲開放。格雷欣實驗室（GCH）快捷方便的支付系統和智慧合約的智慧機制可以實現道具交易抽成分配，使支付鏈線上娛樂提具備了加密的虛擬財產，去中心化支付，道具自由交易等優勢，獨立結算，獨立運營，保護玩家，兼顧公平，不改變原有遊戲體系，這些都將成為支付鏈線上娛樂區別於傳統系統的獨特之處。

6.2.3. 金融行業

利用區塊鏈網路，將傳統金融機構、外匯做市商、流動性提供商等加入支付網路，構建成為支付網關。通過支付網關，可以將區塊鏈上數字資產流動與現實中的法定貨幣相連接，實現法定貨幣可以轉換為區塊鏈上的數字資產，便於後續的支付轉賬。通過區塊鏈支付網路中的網路連接器可以連接傳統做市商、匯出行、匯入行等機構，摒棄中間交易環節，實現點到點快速低成本支付。

根據當前傳統的網路支付體系結構，深入分析跨境支付的交易流程，本文結合區塊鏈技術的特點，構建基於區塊鏈的跨境支付解決方案。



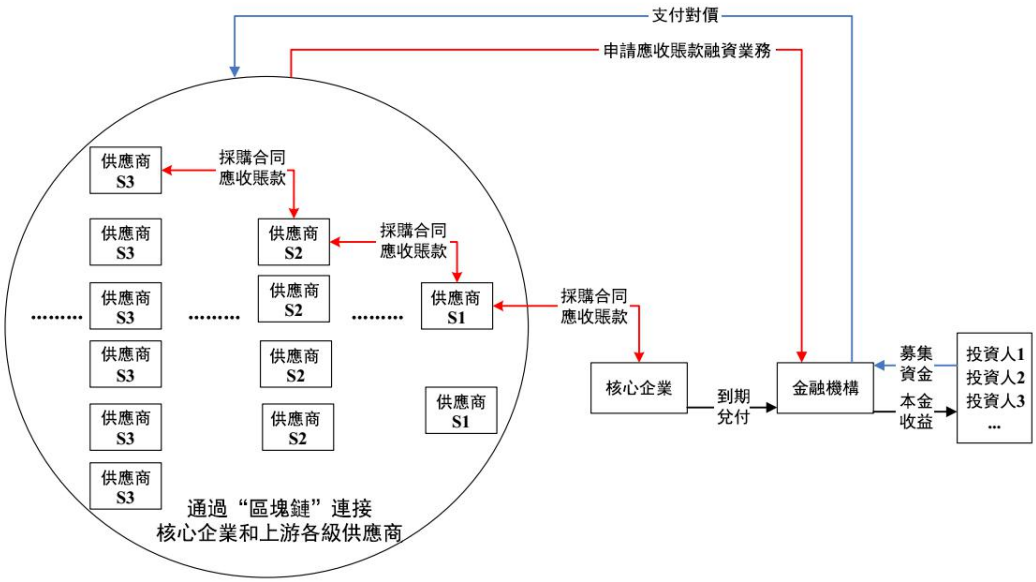
6.2.4. 影視文化

影視文化的應用主要是利用區塊鏈技術，將文化產業鏈條中的各環節加以整合，加速流通，有效縮短價值創造週期。通過區塊鏈技術，對作品進行鑒權，證明文字，視頻，音訊等作品的存在，保證權屬的真實，唯一性。作品在區塊鏈上被確權，後續交易都會進行即時記錄，實現文娛產業全生命週期管理，也可作為司法取證中的技術性保障。區塊鏈數位化證明可以保障資料的完整性，一致性，保護智慧財產權。

6.2.5. 供應鏈

供應鏈金融業務非常適合採用區塊鏈與分佈式帳本技術。首先，業務涉及多個主體，包括核心企業、供應商、金融機構、投資人等，通過區塊鏈將交易資訊在多主體間傳遞；其次，供應鏈上交易資訊通常為商業敏感資訊，區塊鏈技術可實現數據加密；最後，通過區塊鏈技術的數據不可篡改性和可追溯性，可有效杜絕供應鏈融資常見的虛假貿易現象。

總體來看，該平臺針對信用評級高、融資成本低的核心企業，運用區塊鏈技術將供應鏈交易資訊進行鏈接，將信用從中心企業向末端供應商傳遞，以提高金融資源在供應鏈屬企業間的配置效率。



6.2.6. 商業地產

傳統的房地產交易市場在交易期間和交易後流程中，存在缺乏透明度，手續繁瑣，欺詐風險，公共記錄出錯等問題。支付鏈用區塊鏈技術實現對土地所有權，房契，留置權等資訊的記錄和追蹤，並確保相關檔的準確性和可核查性。格雷現金（GCH）作為可對接全球貨幣的數字貨幣，能夠實現商業地產無紙化和即時交易。在具體操作上，支付鏈區塊鏈技術在房屋產權保護上的應用，可以減少產權搜索時間，實現產權資訊共用，避免房產交易過程中的欺詐行為，提高房地產行業的運行效率。

7. 參考文獻

1. Nakmoto,S.(2008).Bitcoin:A Peer-to-peer electronic cash System.

2. Mazieres,D.(2015). The stellar consensus protocol: A federated model for internet- level consersus. Steller Developent Foundation.

3. Brown,R.G.(2016). Introducing R3 Corda: A Distributed Ledger for Financial Services.R3 April,5.

4. UK Government Chief Scientific Adviser:Distributed Ledger Technology: beyond block chain.
5. Sachs, G.(2016). Blockchain-Putting Theory into Practice,this-blockchain.com,25-32.

6. Buterin,V.(2014).A next-generation smart contract and decentralized applicationplatform.white paper.

7. Zindros,D.,(2016).Trust in decentralized anonymous markerplaces.

8. Swan,M.(2015). Blockchain:Blueprint for a new econimy.”O’Reilly Media,Inc.”.

9. Kosba,A.,Miller,A.,Shi,E.,Wen,Z.,&Papamanthou,C.(2016,May).Hawk:The blockchain model of crytography and privacy-preserving smart contracts. In Security and Privacy(SP),2016 IEEE Sym[posium on (PP.839-858).IEEE.