為醫療保健的未來打造信任的基礎：
BitMED 醫療協議（BXP）概述

博．凡加斯（Bo Vargas）與李希．瑪多（Rishi Madhok, MD）
BitMED 公司, BitMED.io
2018 年 3 月

摘要

BitMED 開發的 BitMED 醫療協議（BXP）是為未來醫療數據交易與管理建立一個安全基礎的區塊鏈聯盟協議與代幣生態系統。BXP 利用現有的區塊鏈協議，包括以太坊（Ethereum），星際檔案系統（IPFS）和超級賬本（Hyperledger），並且添加功能以滿足全球醫療保健市場的需求。BXP 建立於開源分佈式共識賬本、互聯網協議和原生的 BXM 代幣。BitMED 能夠提供即時的、安全的、廉價的、任何規模的醫療服務。本協議支持分佈式應用程序和智能合約，可預防雙重支付，並且允許健康結果的納米支付。

備註：BitMED 是未完工的項目。有關系統更新的新白皮書將發佈在我們的知識庫。若有任何意見或詢問，請通過 BitMED. io/contact 網頁與我們聯繫。

目錄

1. 簡介

BitMED 開發了一個數字醫療平台，讓全球可獲得易用、個人化並可負擔的醫療保健服務。我們的區塊鏈和實用代幣 BXM 搭建了一個激勵醫療保健生態系統的架構，其主要特徵為：

- 照護：無論在世界各地，成員透過 BXM 代幣能夠獲得美國董事會認證的各專科醫療服務。
- 社群：無論是與人工智能系統、街坊鄰居或是有相似經歷的人，成員被激勵與他人聯繫並溝通健康事宜。
- 內容：成員被激勵去創造、驗證、分享以及使用準確的醫療保健信息。
- 數據：BXP 利用智能合約保持機密性、完整性和可用性。
- 提供者：提供者被激勵提供身份和從醫證明，從而最大化醫療專業人士的供應。
- 治療：患者無論何時何地均可獲得藥物、設備和治療，同時保持使用權與知識產權。
- 保障：智能合約能在有需要時為任何一方提供價格、範圍和服務的透明信息。

BitMED 正在重新分佈其關係與角色，以反映醫療行業裡必要的改變。隨著去中心化模式和用戶對健康數據的個人參與倍增，醫療保健獲得恢復到原始的理想目標的機遇。

醫療問題複雜且頻繁，而技術性的解決方案若未考慮到管制、法律和文化等挑戰與需求，就不算是解決方案。作為技術性解決方案，BXP 是 BitMED 通往全新醫療保健及醫療數據管理基礎路線圖中的一部分。若您想攜手共建未來，請加入我們的行列。加密貨幣社群對未來的旅程至關緊要。

本白皮書的範圍包括 BXP、其作用及其運作方式。本白皮書不包含 BitMED 公司的使命，但您可訪問 BitMED.io 查詢更多詳情。

本白皮書適用於誰

本白皮書的主要目標受眾是密碼學及加密貨幣群體。讀者應對區塊鏈技術有一定的認識。初學者可參考尼克．卡斯托迪歐（Nik Custodio）為 freeCodeCamp 社群撰寫的文章《向五歲的我解說比特幣》（Explain Bitcoin Like I'm Five）或區塊鏈學習網。

2. 醫療保健為何需要自己的區塊鏈協議

對我們而言，每一天都是我們與人們分享我們使命和計畫的新機遇。在密碼學、安全與隱私領域中，幾乎所有人都有類似的反應：

> 「為何不用以太坊？」
> 「你形容的不就是超級賬本嗎？ 就用它吧。」
> 「為什麼要建立自己新的區塊鏈？ 為什麼不用已存在的呢？」

沒錯，現有的區塊鏈系統用於各種敏感信息的交易已足夠堅固，那為什麼不適用於醫療數據呢？ 簡短來說：用現有的區塊鏈協議交易醫療數據是違法的。

為了更詳細解答這個問題，我們首先簡單地解釋醫療界最迫切的一些問題。隨後，我們會簡單說明現有的區塊鏈，及其為何無法用於安全地儲存、更新與交易世界各地的醫療數據。

2.1 醫療保健產業的相關問題概述

醫療保健所面對的眾多問題，本白皮書不足以覆蓋。作為醫療服務提供者、企業家和科技專家，BitMED 的創始團隊親身經歷過許多。符合我們研究目的最主要的問題是體制中的各方對彼此缺乏信任。

醫療保健是零信任

醫療保健體制運行的方式使任何一方都無法信對方。每一筆交易或協議都被緊急和昂貴的程序拖住，但為了有一定的保障和信心，這些程序卻是必不可少的。

- 服務提供者不信任保險公司會賠償手續費，而逐漸常見的是，公司甚至從最初就不包含此類保障。隨著美國的醫療保健市場不斷更新政策，許多診所和醫院每年也更換它們接受的保險。
- 保險公司不信任服務提供者，經常對報銷有異議，加重了提供者的行政負擔。據美國醫學會（AMA）估計， 由於報銷處理效率不足導致的收益損失 10-14%[1]。
- 患者對醫生和其他醫療專業人士的信任取決於很多指標：地理因素、社會經濟地位、文化、年齡層等等。患者對健康保險的信任更為直接，哈里斯民意調查自 2003 年的年度調查結果始終顯示這是最不受信任的產業之一，僅僅險勝石油和煙草產業[2, 3]。

舉個例子：資格認證。如果一名醫生想到另一個較缺乏醫生的州屬去工作，她申請並且被接受了。那麼她下個月可以開始在那兒上班了嗎？不，因為醫生的資格認證按新州屬的規定需要平均六個月的時間處理。這些規定是為了保護患者而設立的，你不可能要看一個沒有資格行醫的醫生。但是對於醫生而言，工作遷移的難度比大部分的專業人士要高，並且構成全球缺乏醫生的問題。美國醫學院協會的報告指出，到了 2025 年，單單美國就將缺乏 90400 名醫生[4]。

此外，患者首先必須了解事先核准機制——保險單所覆蓋的是誰、是什麼、是什麼時候的護理——很多時候，這會限制或延遲患者獲得服務。美國醫學會發現：「90％的受訪醫師表示事先核准有時、經常或始終會延遲患者獲得醫療照護的時間[5]」。然而，我們所獲得的照護是昂貴的，而且價格不斷增長。2017 年 CMS 的報告指出美國預計 2025 年的國內生產總值（GDP）會有整整 20%消費在醫療保健上[6]。

患者必須承擔他們所接受的服務各方面的相關費用，如資格認證和監管程序的費用。隱藏在醫療帳單上含

糊的字眼背後，是驗證、認證和監管他們醫療照護的每一步所涉及的時間與開銷，均由他們負擔。

法律和監管壁壘防止了創新和獲得醫療保健服務的能力

全球醫療保健體制中原來旨在保護患者的法律與監管壁壘，現在在某種程度上妨礙著實施護理中嚴重缺乏的創新。

數十年來，不完整的醫療保健管理方式成為了昂貴且日益增長的問題。2010 年，世界衛生組織發佈了一項醫保體制融資的全球性研究，發現：「按保守估算，花費在醫療保健上的大約 20～40％資源被浪費，這些資源可轉用於致力達到全民醫療保健。」[7]他們發現，罪魁禍首是藥物——品牌藥物價格遠高於通用藥物、抗生素與注射過度使用、惡劣的存儲設備和差異極大的價格——但資源浪費也包括了效率過低的醫院程序、醫療失誤、未被充分利用或有效利用的技術，以及服務提供者獲得報酬的方式。以服務計酬的報酬架構往往傾向於多服務那些負擔能力較強的人，少服務那些負擔能力較低的人。此外，每個地方的法律法規也對當地生產及記錄的醫療數據有所限制。更多詳情請查閱第 2.2 部分。

醫療數據碎片化、不可存取，並且不完整

數據是醫療保健創新的洞見與發展之基礎。然而，與其他產業比較，醫療保健的成效緩慢，原因是一個根深蒂固的問題——數據不完整，並且不可跨組織存取。

直到近年，醫療記錄一路以來完全以紙質形式儲存，但現在電子儲存方式逐漸增加。這些電子醫療記錄（EHRs）儲存在醫療保健系統當中，由醫院掌控數據，而不是患者。然而，醫療保健消費者是流動的。他們在自願或非自願的情況下有可能到不同的機構看不同的醫生。很不幸的，他們的數據卻不會與他們一起流動。事實上，數據隱私權的制度雖然旨在保護患者，但卻導致了大量的醫療廢物，也因治療延誤與失誤、過度檢查和不當檢查，對患者造成傷害。

值得一提的是電子醫療記錄的結構和重點不在於準確、有效的患者數據和健康記錄，而是在於醫療賬單。電子醫療記錄與紙質系統相比，固然提升了醫療溝通和患者醫療事件的數據記錄，但這過程仍然與理想相隔千里。

當醫療保健的各機構沒有分享數據的動機時，患者若需要服務提供者迅速交換他們的資料，就必須在照護的每一步之間付出等待的代價。由於過時的行政流程，服務提供者之間交換數據的時間有可能高達數週。

此外，電子醫療記錄也面臨系統不完整的可悲情況。醫療保健的消費者不住在醫院裡，他們在離開醫師的辦公室後依舊過著各自的生活。患者在每一次看醫生之間，通過電子健康產品和服務收集的健康數據日益增多，這些數據很少被綜合到患者的治療計畫中。現有的電子醫療記錄大部分必須進行大型翻修才能夠允許此類功能。

2.2 現有的區塊鏈不適用於醫療保健

現有的區塊鏈無法滿足醫療保健的需求，而兩大原因是：1）所有醫療保健服務必須遵循的法律與監管框架，以及 2）已有的區塊鏈協議每秒交易量的限制與醫療市場所需的規模有落差。

法律和監管條規

全球許多國家，包括美國[8]、德國[9]和加拿大[10]的法律規定個人健康信息不得離開其國家。在人們考慮使用區塊鏈交易的數據種類當中，健康數據往往需要進一步限制。僅因此故，現有的區塊鏈不適用於醫療保健，因為這麼做是違法的。

就以太坊而言，輸入智能合約的數據會與以太坊區塊鏈上任何地方的每一個人分享。此數據的跨國分享違反了許多國家的隱私權保護法。超級賬本利用認許制操作模式，應對功能可伸縮性及隱私的問題，具體應用消逝时间量证明（PoET）和工作量證明（PoW）的共識機制，還有細粒度權限控制。然而，為了符合醫療保健的法律和監管條規，仍然需要調整。

舉例美國一項法規，即可看見以上所述：健康保險攜帶和責任法案（HIPAA）。1996 年 HIPAA 法案通過後，美國衛生及公共服務部（HHS）因此制定了 HIPAA 隱私規則和 HIPAA 資安規則[11]。這是醫療保健產業裡保護醫療信息的第一組公認標準。

HIPAA 法規適用於美國所有醫療保健服務提供者、醫保計畫及醫療保健清算所。
受保護的醫療信息包括[12]：

- 姓名
- 出生日期、死亡日期、治療日期、入院日期及出院日期。
- 電話號碼和其它聯繫信息
- 地址
- 社會安全號碼
- 醫療記錄號碼
- 照片
- 指紋和聲波紋
- 任何其它身分識別號碼

根據 HIPAA 隱私規則，患者擁有的權利包括：

- 接受任何醫療保健服務提供者、計畫或清算所的隱私慣例通知的權利。
- 查閱受保護的醫療信息並持有副本的權利。
- 要求更換記錄、更改錯誤或添加信息的權利。
- 擁有受保護醫療信息透露名單的權利。
- 要求保密溝通的權利。
- 投訴的權利。

這些規定為患者的醫療數據給予大量的保護，但其應用並不涵蓋所有接觸個人健康信息的個體。需遵循 HIPAA 規則的機構包括明顯的醫療保險計畫或公司、大部分醫療保健提供者以及被涵蓋機構的「商業夥伴」，包括醫療賬單與醫療記錄公司[11]。然而，不需遵循 HIPAA 的機構包括[11]：

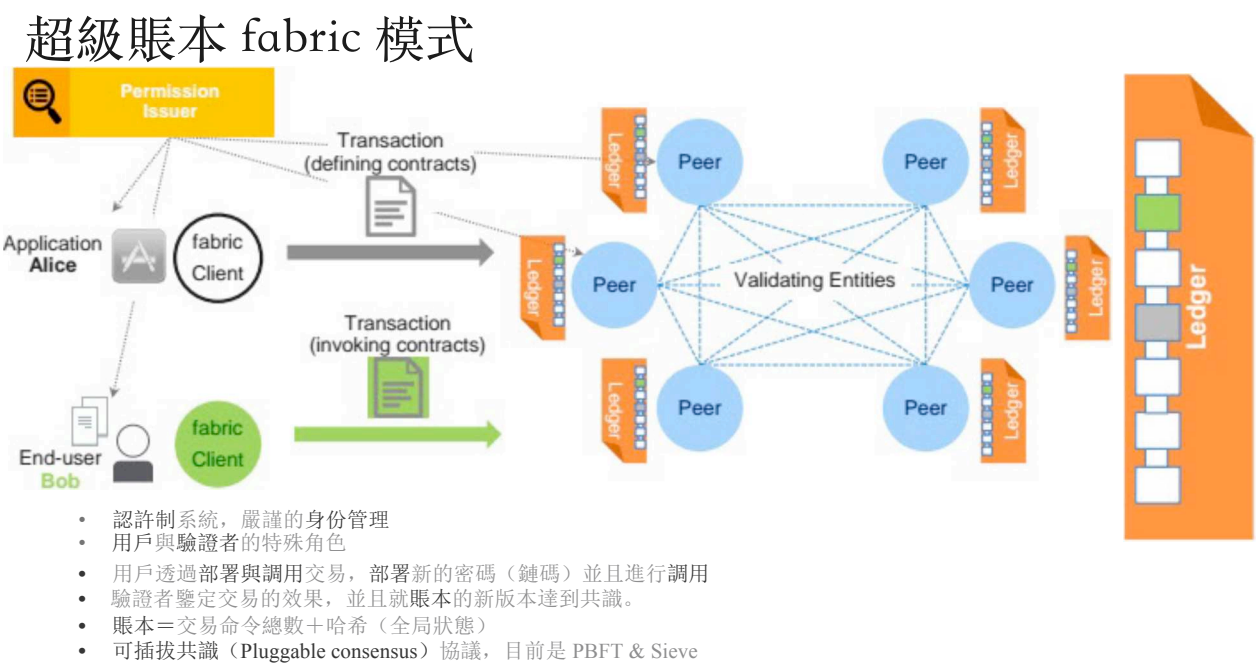
- 人壽保險公司
- 雇主
- 雇員賠償保險公司
- 多數學校及校區
- 多所政府機構，如：兒童保護服務機構
- 多數執法機構
- 多所市政辦公處

因此，法規雖然出於好意，卻未能達到其保護患者的最佳效果。我們的 BitMED 協議致力於利用智能合約和去中心化應用程序（dApps）的實行，程序化地確保各地所有醫療保健消費者的隱私權受到保護。

規模問題

根據 CDC，2014 年僅僅在美國，到醫師辦公室的拜訪有 8 億 8 千 470 萬趟，也就是每秒大約 28 趟[13]。為全球醫療保健打造的區塊鏈必須能夠達到每秒支持 10 萬筆交易的能力。截至撰寫此文之時，現有的區塊鏈無法承擔全球上百萬用戶的應用。

例如超級賬本 Fabric——最初由 Digital Asset 和 IBM 貢獻的一個開源超級賬本項目，旨在加強企業級安全[15]。Fabric 擁有認許制，其用戶和驗證者在系統中各盡其職[16]。節點依據客戶端（clients）、同伴（peers）或命令者（orderers）區分[17]。客戶代表最終用戶啟動並調用交易。他們與同伴節點和命令者節點溝通。同伴節點維持賬本，並且向命令者接受更新信息，以在賬本上提交新交易。背書節點（endorsers）是一種特別的同伴節點，任務是認可交易，檢查交易是否足以符合條件，例如提供了所需簽字。命令者向客戶和同伴提供溝通渠道，讓含有交易的信息能通過此渠道被廣播。至於共識，這些渠道將確保所有連線的同伴節點收到一模一樣的、邏輯順序相同的信息。



圖一、超級賬本 Fabric 模式

此時，如果多個命令者互不信任，就會引起錯誤信息的傳送。為了跨越任何可能發生的錯誤（如：信息命令不一致）而達到共識，必須使用共識算法，使分佈的賬本能夠無誤的被複製。Fabric 的算法是「可插拔」的，也就是說，依據各應用需求，各種算法可被使用來達到共識和提供成員服務[15]。舉例來說，要應對隨機或惡劣的複製失誤，可用拜占庭容错算法的一種替代算法。此外，渠道裡的信息流動是被區分開來的，意味著客戶只能看見與他們有連結的信息和相關交易，而對於其它渠道不會知情。這樣一來，交易信息的存取權限於相關人士，而結果就是共識只需在交易級別達到，而不是像以太坊一樣在賬本級別。

此實行方式對許多商業案例來說是最優的。然而，交易量目前最高達到每秒 1000 筆交易左右[18]。

3. BitMED 醫療協議（BXP）簡介

3.1 如何運作

BitMED 醫療協議是一個開源的分佈式共識賬本，擁有原生貨幣，BXM 代幣。它可支持智能合約及 dApps，又稱為去中心化應用程式，並且保護醫療數據和個人可識別信息（PII）。它的設計防止醫療保健體制中雙重支付的發生，並且激勵患者參與在健康事宜中。此系統著重於以下成分：

1. go-Ethereum

使用以太坊協議 Go 編程語言的基礎層（go-Ethereum）[19]。

2. BXM 協議

- 交易管理——允許私人交易中加密交易數據的存取，管理本地數據存儲和與其他交易管理人之間的溝通。
- 加密區域——負責私鑰管理和私人交易數據的加密與解密。
- 網絡管理——控制網絡存取，建立一個認許制網絡。
- BXM 鏈——以投票為基礎的紅腹區塊鏈（Red Belly Blockchain）協議，使用以太坊的核心功能來驗證並在網絡中傳播選票。
- 隱私管理——執行治理、合規、建模和 PII 風險。
- 臨床管理——管理臨床工作流程、觀察、治療、照護服務以及藥物。
- 專業管理——支持臨床決定、人工智能和報告代理。
- 財務管理——報銷、福利和付款的存取與授權。

3. BXM 代幣

BitMED 平台上的產品與服務都是由 BXM 代幣驅動的。

成員
成員的個人檔案設置若允許數據貢獻，就可依據市場需求賺取代幣。成員隨時可在貢獻數據和不貢獻數據之間更換權限設置。成員也可貢獻內容並參與社群，以賺取代幣。

激勵成員的參與
一種因果難定的情況迅速出現：網絡需要有人才會有價值，而一個空置、無價值的網絡人們沒有原因加入（即梅特卡夫定律）。在過去兩年期間，BitMED 透過各種各樣的合作聚集了 2250 萬名正在等待加入的成員，而流水線中另有 1 億名。為了引導成員、利用生態系統並使其增長，我們設計的第一輪激勵代幣分佈是最高額的。在第一年以後的每一年，它將減少一半。根據系統的設計，夥伴機構越早帶入成員，其獲得的價值就越高。這是以對數計算的。

網絡與交易費用
BitMED 網絡會遵循梅特卡夫定律：網絡價值「以節點數量或終端用戶數量的平方的速度增長」。據發現，比特幣、以太坊和達世幣網絡都遵循了這項法則。

處理交易所需的能量必須從用戶社群當中獲取，這些用戶也從他們參與的生態系統中獲益。為了負擔生態系統的運作成本，生態系統的每一筆交易將包括一個小浮動基點費（即煤氣）。我們的目的是要隨著需求的增長，激勵驗證者把更多資源介紹到網絡上來，同時為網絡用戶提供更佳的服務。

4. BXM 代幣挖礦

比特幣、以太坊等區塊鏈的運作基於工作量證明：解決一個問題，計算下一個區塊，獲得酬報。這是一種開放、高參與性及零信任的機制。它在計算上也是非常密集的，每秒平均進行 3 到 20 筆交易，目前無法擴展到醫療保健所需的規模[22]。

與其使用此機制，BitMED 選擇的是權益證明（proof of stake）機制。為了促進交易量並達到（醫療保健應用所需的）每秒 10 萬交易，我們引進了經過嚴格審查的驗證者或挖礦者，他們可從中獲得真正的收益與風險。

雖然賬本是開源並且公開的，但只有 BitMED 審查過的挖礦者可驗證賬本。這運作就像通訊社似的，系統中所有人都能讀取，但只有某些用戶是允許更新的。驗證者是必須遵循醫療保健有關機密性、完整性和可用性要求的公有及私有機構。

成為驗證者是有一定成本的，因此為了激勵優質的驗證者，我們計畫在最初給予他們一定數額的代幣。然而，他們還未賺取代幣。通過 BXM 代幣挖礦，驗證者每筆交易可賺取代幣。他們也可以為更大的賞金與數個驗證者競爭。然而，如果驗證者被發現違反任何條規，他們有可能失去的不僅僅是交易，而是競爭更大賞金的機會。若行為過份惡劣，即失去所有收益。最重要的一點是，驗證者承擔著違犯各自國家法律的附加風險。舉例來說，美國的驗證者若泄漏一例醫療記錄，即需承擔民事處罰（罰款一萬美元）及刑事處罰（長達 10 年監禁）的風險。

但若驗證者依條規完成交易，則贏得賭注。每一次勝利讓驗證者累積賭注，並使其與贏得大賞金離得更近。這種機制會激勵挖礦者準確地生產及驗證數據，承擔著真實的風險。

5. 去中心化應用程式，或稱 dApps

BitMED 生態系統最初期將包含四個主要的去中心化應用程式：照護、策展內容、社群和數據。

照護

BitMED 讓成員能以實時信息的形式，與有專業資質認證的醫療服務提供者溝通。成員可通過我們的信息平台與其對話，也可預約現場視頻咨詢。成員可選擇如何獲取我們的醫療服務：給予數據或代幣。使用 BitMED 的電話醫療服務無需付定額手續費或費用。

策展內容

皮尤研究中心（Pew Research Center）在 2013 年報導 72%的互聯網用戶在過去一年中曾經在線上搜索健康信息[23]。很不幸的，谷歌醫生並沒有上過醫學院。BitMED 把有醫學認可的內容與成員所關注和感興趣的主題相配。內容直接傳遞至各成員的個人頁面，讓其過目、儲存，並與他們的社群或醫生分享。

社群

BitMED 社群中，成員可討論共同興趣、分享經歷、提供精神支持，並且不斷學習如何應付日常的健康情況。社群可使用 BXM 代幣交易來開設。在社群中的積極參與，包括領導和主持，都會獲得 BXM 代幣為

獎勵。

數據
BitMED 的生態系統以獎勵的方式激勵所有利害關係者之間的數據交易。數據將依據提供者所設定的條件被匯集、去識別化及存取。數據可用於患者照護、醫療報告結果、研究、臨床試驗、算法開發、精算分析和消費者行為的深入了解。當數據被存取時，利害關係者在智能合約所明確的時期內，可使用 BXM 代幣獲取數據。

使用代幣的例子

為了用範例說明如何使用代幣，讓我們假設一些虛構的機構與角色。

- Acme 公司是一個醫療系統，擁有從 1990 年至 2010 年的紙質患者醫療記錄 2500 萬例。維持這些紀錄存儲一年的成本是 20 萬美元。
- Star 公司是一個醫療系統，擁有從 2000 年至 2017 年的患者醫療記錄 500 萬例，以綜合形式存儲。維持紙質與電子紀錄一年的成本是 5 萬美元。
- 一家 Johns Hopkins 的初創企業 Quanttus 公司需要 20 萬例患有心房顫動（AFib）或心肌梗死（MI）的病患醫療記錄，並且要在至少兩周前有心電圖（EKG）的記錄。Quanttus 有一項突破性的心房顫動早期發現警告算法，一旦經過美國食品藥品監督管理局的批准，預計每年能拯救 20 萬條生命。
- Safe 公司是一家病歷存儲公司，隨著企業轉向電子醫療記錄，正在尋找新的收入來源。

過程
Safe 公司向美國所有公司提議，以每張 50mBXM 的價格電子化的紙質醫療記錄，提供三年匿名字段的存取則折價 40mBXM，並且給每位允許同步現有記錄的患者發出 20mBXM。智能合約可能如以下範例：

```
type contract = {
        uint public value;
        address public to;
        address public from;
        enum State { Created, Locked, Inactive }
        State public state;
        modifier condition(...){ /* rules of contract */ }
        function validatePatientContent(Address add){...}
        function computePayment(...) { /* payments to parties */}
        function storage(...) { /* data storage access, location, and conditions */)
    }
```

圖二、BXP 智能合約範例

Star 和 Acme 同意讓 Safe 電子化所有紙質記錄。此外，Star 告知所有患者，他們現在可通過 BitMED 生態系統存取自己的醫療記錄。成員們可以完全掌握自己的醫療記錄，若選擇授予存取權限則可獲得補償。

Quanttus 設立了新合約，在 BitMED 生態系統上要求 20 萬個 Afib 或 MI 的圖表。為每一個符合條件的記錄，Quanttus 提出的價格是 2BXM。若沒有 BitMED 生態系統，Quanttus 需要用長達兩年的時間累積所需的記錄，總成本超過 1000 萬美元，更別提在數據收集過程中所喪失的生命。

Star 公司能完成 15 萬項記錄的要求，也知道另一家醫療系統公司 Dawn 擁有 1 千萬項記錄，估計從中可獲得其餘的 5 萬項。然而，Dawn 公司的數據是紙質的，還需解決保留系統。Star 向 Dawn 提出以無預付費的方式，電子化所有的記錄，並要求在五年期間可存取這些記錄的匿名字段。Dawn 同意此條款，但條件是
Star 公司必須協助它現代化，並把所有成員及未來記錄遷移到 BitMED 生態系統上。有了這些額外的記錄，Dawn 公司現在擁有可完成 Quanttus 公司合約的 20 萬項記錄。

3.2 擷取可用的，創建欠缺的

BitMED 的目標並不是要重複前人的發明，BXP 利用現有技術的一部分，再連接、添加所需的部分，以解決全球醫療保健市場所面對獨特的法律條規的挑戰。

超級賬本 / Quorum 分叉

BitMED 區塊鏈的基礎是超級賬本、Quorum 和星際檔案系統（IPFS）技術，這些技術應付了非認許制賬本、規模和存儲的問題，同時確保交易級別的隱私和網絡透明度，並且允許個別定製以滿足商業要求。

- 所有公開與私人智能合約及總體系統情況取自一個單一、共享、完整的區塊鏈，其交易是由全球網絡的每一個節點驗證的。
- 私人智能合約情況則僅限合約各方及批准的第三方，如監管機構，知情與驗證。
- 為現有的以太坊應用撰寫的智能合約將在 BXM 網絡上保持透明度。
- 為了滿足不同的隱私需求加強現有的智能合約設計，是簡單且直接的。

通過高達 200 個可信節點的認許制分布式賬本的實行，我們降低交易成本，每秒處理上千筆交易，達到 PII 對於機密性、完整性和可用性的標準，並且為已有的健康標準與協議提供向前發展的方向。

即使超級賬本能提供企業級安全，HIPAA 和其它地理性的醫療數據法律還有額外的要求。BXP 和超級賬本的主要差異在於，HIPAA 已覆蓋的數據字段不會在整體區塊上複製。我們利用的是 IPFS 的 IPLD 機制，指出信息可尋獲的地點。記錄即時被匿名化，只有患者居住國家節點會擁有 HIPAA 字段。總的來說，這就是使用分片技術（shard key）為 HIPAA 字段進行垂直分區。

紅腹區塊鏈（RBBC）算法

BXP 利用 Crain, Gramoli, Larrea 和 Raynal 開發的紅腹區塊鏈和二元拜占庭共識（binary Byzantine consensus）算法[24]。他們的算法是為了順應共識有效性的延伸意義，並且由兩部分組織而成：

1. 從多元共識減少至二元共識。這是完全非同步的，並且「不使用隨機化機制、最終領導者或簽名」[19]。它「總是決定二元共識 0(1)序列中的一個非預定值。此算法只會等待最早終止的併發可靠廣播實例，隨之發出二元共識實例。由於它假定 t < nl3，其中 n 是過程數量，t 是故障過程數量的

上限，因此這種減少算法是彈性最好的」[24]。

2. 二元拜占庭共識（BBC）算法 它也不需要隨機化、最終領導者或簽名[24]。從計算上來說，除了傳輸延誤不斷增加的情況外，它總是會終止的。若所有非故障過程都提出同樣的值，則 BBC「總是終止於 0(1)時間，否則它可能仍然在恆定時間內終止，但保證在 0(T)時間內終止，這是最優的」[24]。

其結果不僅是彈性最優(T < n!3)，而且時間最優，因為它終止於 0(1)[19]。

3.3 好處

BXP 為兩大目標設計：1）滿足目前醫療保健的需求，以及 2）為安全、開放的生態系統打好基礎，以促使未來醫護服務中降低成本與創新的機會得以實現。

提高照護的可獲取性

現有的公司不再需要建立自己的醫療保健業務。受審查的醫療保健公司可利用 Care dApp 及 BitMED 的醫療服務提供者，或構建自己的 dApp 與服務，以達到降低再入院率或解讀醫療數據或結果等目標。

提高準確健康信息的可獲取性

BitMED 提供一個核心地點，讓所有人能夠獲取與個人相關、醫學驗證的健康信息或內容。內容創作者及輔助人員，如編輯和翻譯員，也可為他們的工作獲得報酬。

在降低成本的同時強制執行協議

BXP 利用生態系統中的合規協議及其它受審查的醫療機構之去中心化應用程式（dApps），不必面對典型的審計、合規與入職所涉及的時間、開銷等問題。此協議將強制執行並且防止任何人違反規定。

遵循 HIPAA 規定的成本取決於一個機構或業務的大小和需求，有可能處於數千美元到 5 萬美元，甚至更多，的範圍內[25]。若違反規定，成本則比守規高很多，但這無疑是一筆成本，不僅僅是金錢上的損失，也包括因此被阻礙的醫療研究[26]。當協議本身強制執行合規性時，這筆成本的減少是所有人共享的。

降低交易成本，減少欺詐

生態系統排除耗時的手動過程（如：多個單獨賬本之間的和解、行政流程等），因而降低成本。通過時間戳條目和網絡共享的共同、不可變的賬本，欺詐也可減少。這可預防醫療保健系統中常見的雙重支付問題。

安全儲存醫療數據，保護個人可識別信息（PII）

BXP 是一個開源、認許制的網絡，它使所有患者、服務提供者以及公有與私有機構的醫療數據得以儲存。各機構無需花費資本與合規成本去構建自己的安全方案，即可確保數據的安全。BXP 利用以下現有的衛生資訊科技及安全標準：

- FHIR
- Health Level 7

- ISO 27001
- HITRUST
- FISMA
- 隱私盾（Privacy Shield）

這些標準固然必要，但也很快變得過時，其代表的僅僅是在設立之時已知的現有威脅的簡短說明。BXP 協議使最佳安全措施能夠持續適應生態系統每日面對的威脅，同時使網絡上的各方從中受惠。

規模可根據醫療保健的需求伸縮

如以上第 3.2 部分所述，BXP 使用紅腹區塊鏈（RBBC）擴展至醫療保健所需的規模，這是經證實「可以在單個數據中心的 300 台機器上每秒處理 66 萬筆交易」的多元拜占庭共識模式[27]。我們利用著 Crain、Gramoli、Larrea 和 Raynal[24] 每秒可處理數十萬筆交易的開發成果。相比之下，Visa 網絡每秒可處理 56000 筆交易。

RBBC 算法對 BXP 和其他區塊鏈聯盟是理想的，其共識不完全私有，亦不完全公開，但由經審查的驗證者執行。能夠達到如此高的交易量是因為它「在二元共識 0(1)序列中決定一個非預定值」。[24]這是通過結合「將掩碼（bitmask）應用於一系列提議的，多元減少至二元共識的算法，以及構建這個掩碼的二元共識」，從而產生並行的二元共識實例[24]。

激勵數據分享

美國醫療保健體制開發的時候，人們認識自己的醫生，並且長期看同一個醫生。現在，服務提供者來來去去，唯有患者一生不斷與醫療系統互相交流。保持對自身健康數據的掌控對每個人來說比以往更為重要。

BitMED 生態系統不僅給人這種程度的個人健康數據掌控，還給予每個人靠著自己數據掙錢的能力。若成員同意讓家人或第三方公司存取他們的數據也可這麼做。第三方甚至有可能構想出對某些群體更佳的應用程序或服務。

一句從 70 年代隨著媒體進化流傳至今的說法是：「如果你沒有為之付出，你就不是客戶，而是被賣的產品。」臉書（Facebook）就是一個實例——即使利用你的資訊數據賺取廣告費，他們卻沒有把這盈利的任何一部分支付給你。BitMED 異象中的系統是每一個人的數據只要被視為有價值，就可選擇使用它獲益。

有一個重要的區別，就是通過 BitMED 生態系統接受的服務不要求支付當地貨幣，但是服務提供者與成員之間的諮詢服務是需要用 BXM 代幣的。成員可以實時與美國專業資質認證的醫生以信息溝通，使用短信聊天平台，或預約現場視頻諮詢。

4. 總結

BitMED 的協議及生態系統讓所有成員有機會獲取照護、內容與社群。它也在患者、服務提供者、研究人員、產業夥伴以及醫療服務提供過程中的各利害關係者之間促使受激勵的、安全的、可靠的數據合作。這意味著一種轉變，從原來的生病了才注意醫療保健，到維持健康，甚至達到醫療個人化與最優化的終極目標。

目前，BitMED 正透過我們已有的渠道夥伴處理 2250 萬名全球成員的加入過程。我們的目標是要在 2018 年結束前觸及 1 億名未加入者。我們會在 2018 年中旬逐步擴大 BitMED 平台的存取。在下階段的發展中，BitMED 欲將所有現有的產品與服務重建在 BitMED 生態系統上，以加強其可伸縮性，並且構建新的產品與服務。我們對於加密貨幣群體成員的加入格外興奮。

我們正在開發數據研究的智能合約，並且在發佈此白皮書後將發行 BitMED 區塊鏈源碼及 BXM 代幣。請瀏覽此網站 https://www.BitMED.io/roadmap/ 了解更多有關 BitMED 路線圖的詳情。BitMED 是一項未完成的項目，隨著更多研究結果被發掘，我們會不斷把最新消息告訴社群。[17]

參考文獻

[1] M. T.E. Sullivan, "Administrative Simplification in the Physician Practice," [Online], Available: https://www.ama-assn.org/sites/default/files/media-browser/public/about-ama/councils/Council%20Reports/council-on-medical-service/i 11 -cms-administrative-simplification-physician-practice.pdf. [Accessed 2017],

[2] The Harris Poll, "Oil, Pharmaceutical, Health Insurance, Tobacco, Banking and Utilities Top The List Of Industries That People Would Like To See More Regulated," 21 December 2012. [Online], Available: http://www.theharrispoll.com/politics/Oil__ Pharmaceutical__ Healthlnsurance____Tobacco _ Banking_and_Utilities_Top_The_List_Of_Industries_That_People_Would_Like_To_See_More_Regulated.html.

[3] R. Xu, "The Health Care Industry's Relationship Problems," 28 October 2015. [Online], Available: https://www.newyorker.com/business/currency/the-health-care-industrys-relationship- problems.

[4] L. Bernstein, "U.S. Faces 90,000 Doctor Shortage by 2025, Medical School Association Warns," 3 March 2015. [Online], Available: https://www.washingtonpost.com/news/to-your-health/wp/2015/03/03/u-s-faces-90000-doctor-shortage-by-2025-medical-school-association- warns/.

[5] S. Morse, "Prior authorization needs streamlining, new healthcare coalition including AMA, MGMA says," 25 January 2017. [Online], Available: http://www.healthcarefmancenews.com/news/prior-authorization-needs-streamlining-new-healthcare-coalition-including-ama-mgma-says.

[6] The Advisory Board, "CMS: US health care spending to reach nearly 20% of GDP by 2025," 16 February 2017. [Online], Available: https://www.advisory.com/daily- briefmg/2017/02/16/spending-growth.

[7] World Health Organization, "Health systems financing: the path to universal coverage," 2010. [Online], Available: http://www.who.int/whr/2010/en/.

[8] Office for Civil Rights, U.S. Department of Health and Human Services, "HIPAA for Individuals," 17 June 2017. [Online], Available: https://www.hhs.gov/hipaa/for- individuals/index.html.

[9] Team EU-PATIENTEN.DE, "How are my medical data protected in Germany?," 1 September 2017. [Online], Available: http://www.eu-patienten.de/en/behandlung_deutschland/datenschutz/datenschutz.jsp.

[10] Office of the Privacy Commissioner of Canada, "The Personal Information Protection and Electronic Documents Act (PIPEDA)," 9 September 2016. [Online], Available: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/.

[11] U.S. Department of Health and Human Services, "Your Rights Under HIPAA," 1 February 2017. [Online], Available: https://www.hhs.gov/hipaa/for-individuals/guidance-materials-for-consumers/index.html.

[12] ASC Communications, "50 things to know about healthcare data security & privacy," ASC Communications, 9 June 2015. [Online], Available: https://www.beckershospitalreview.com/healthcare-information-technology/50-things-to-know- about-healthcare-data-security -privacy. html.

[13] H. E. O. T. Rui P., "National Ambulatory Medical Care Survey: 2014 State and National Summary Tables," 3 May 2017. [Online], Available: https://www.cdc.gov/nchs/data/ahcd/namcs_summary/2014_namcs_web_tables.pdf.

[14] F. Ehrsam, "Scaling Ethereum to Billions of Users," 27 June 2017. [Online], Available: https://medium.eom/@FEhrsam/scaling-ethereum-to-billions-of-users-f37d9f487dbl.

[15] The Linux Foundation, "Hyperledger Fabric," [Online], Available: https://hyperledger.org/projects/fabric.

[16] R. Strukhoff, "How Hyperledger Fabric Delivers Security to Enterprise Blockchain," 14 November 2016. [Online], Available: https://www.altoros.com/blog/how-hyperledger-fabric-delivers-security-to-enterprise-blockchain/.

[17] Hyperledger, "Architecture Explained," 26 July 2017. [Online], Available: hyperledger-fabric.readthedocs.io/en/latest/arch-deep-dive.html.

[18] C. Gutierrez, "Hyperledger's Sawtooth Lake Aims at a Thousand Transactions per Second," 13 March 2017. [Online], Available: https://www.altoros.com/blog/hyperledgers-sawtooth-lake-aims-at-a-thousand-transactions-per-second/.

[19] The go-ethereum Authors , "Go Ethereum Homepage," [Online], Available: https://ethereum.github.io/go-ethereum/. [Accessed 2017],

[20] K. Alabi, "Digital blockchain networks appear to be following Metcalfe's Law," Electronic Commerce Research and Applications, vol. 24, pp. 23-29, July-August 2017.

[21] H. R. V. Carl Shapiro, Information Rules, Boston: Harvard Business Press, 1999, p. 184.

[22] J. Vermeulen, "Bitcoin and Ethereum vs Visa and PayPal - Transactions per second," 22 April 2017. [Online], Available: https://mybroadband.co.za/news/banking/206742-bitcoin-and-ethereum-vs-visa-and-paypal-transactions-per-second.html.

[23] M. D. Susannah Fox, "Health Online 2013," 15 January 2013. [Online], Available: http ://www.pewinternet. org/2013/01/15/heal th-online-2013/.

[24] V. G. M. L. M. R. Tyler Crain, "(Leader/Randomization/Signature)-free Byzantine Consensus for Consortium Blockchains," 2017.

[25] T. Ferran, "How Much Does HIPAA Compliance Cost?," 6 April 2015. [Online], Available: http://blog.securitymetrics.com/2015/04/how-much-does-hipaa-cost.html.

[26] The National Academy of Sciences, "Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research," 4 February 2009. [Online], Available: http://nationalacademies.org/hmd/reports/2009/beyond-the-hipaa-privacy-rule-enhancing-privacy-improving-health-through-research.aspx.

[27] J. Peterson-Ward, "University of Sydney's super-fast blockchain gets even faster," 25 October 2017. [Online], Available: https://sydney.edu.au/news-opinion/news/2017/10/25/university-of-sydneys-super-fast-blockchain-gets-even-faster.html.

[28] R. Guerraoui, "Indulgent Algorithms," in Proceedings of the nineteenth annual ACM symposium on Principles of distributed computing, New York, 2000.

[29] C. N. a. V. Gramoli, "The blockchain anomaly," in Proc. 5th IEEE hit 7 Symposium on Network Computing and Applications (NCA '16), 2016.

[30] Ethereum, "Solidity," 2016-2017. [Online], Available: https://solidity.readthedocs.io/en/develop/.

[31] Protocol Labs, "IPLD Homepage," [Online], Available: https://ipld.io/. [Accessed 2017],