BACCHUS

酒神

佳釀區塊鏈：可追溯性的佳釀生態系統

酒神白皮書

酒神
BACCHUS

重要聲明

請仔細閱讀本白皮書免責聲明部分，並諮詢法律和財務專家以獲得進一步的指導。

本白皮書是一份初步草案，將在 BACCHUS 酒神代幣可供兌換之可能前進行修訂，其中包括有關以下方面的訊息:

- 兌換 BACCHUS 酒神幣可能受到限制的國家（若有）；和
- 兌換 BACCHUS 酒神幣相關的其他風險。

白皮書的最終版本將在 BACCHUS 酒神代幣可供兌換之前上載在 BACCHUS 酒神網站，以供任何人士兌換決定之前的全面審查。

本白皮書草案不應被誤解為兌換或徵求兌換的方案。本白皮書草案中列出的人員不是也不會兌換 BACCHUS 酒神代幣。進行 BACCHUS 酒神代幣可供兌換的法定公司名稱將稍後披露。

BACCHUS 酒神代幣並不打算在任何司法管轄區構成證券。本白皮書不構成任何類型的招股說明書或要約，也不構成對任何司法管轄區證券或招攬投資證券的要約。本白皮書不構成兌換或徵求兌換 BACCHUS 酒神代幣的任何意見或任何意見的一部分，也不構成任何合同或投資決定的基礎或依賴于任何合同或投資決定。

兌換 BACCHUS 酒神幣可能受到限制的國家

投資於 BACCHUS 酒神團隊涉及風險，僅適合擁有富裕資金的人士參與，而他們對 BACCHUS 酒神團隊中投資的流動性亦沒有迫切的要求，他們亦對 BACCHUS 酒神團隊所涉及的風險完全瞭解並願意承擔，且有足夠的財務資源來承受這些風險。投資者必須能夠承擔他們在 BACCHUS 酒神團隊中全部投資的損失。團隊中的權益不存在公開市場，且在預期的未來亦不會出現。團隊亦對投資者退股或轉讓權益有諸多限制。

權益僅售予在認購協議中作出（其中包括）以下陳述的投資者：

(a) 他自承費用且僅出於投資目的而購買權益，且不會轉售或分派

(b) 他明白權益並無依照美國《證券法》或外國類似證券法進行登記，而其轉讓權利受美國《證券法》及美國、州和國外基金相關法律條文所限制，且當中權益並不存在市場；

(c) 他是：

i. 一名美國《證券法》D 條例中的“受信投資者”；

ii. 且不是一名美國《證券法》S 條例中的“美國人”。

團隊將要求身為合夥企業、集團公司、有限責任公司、信託公司或其它實體的潛在投資者做出陳述，其內容旨在使團隊豁免作為一家投資公司根據投資公司法進行註冊。各潛在投資者均須簽署和交付一份認購協定，作出其它陳述，並符合認購協議所述其它標準。可按投資者要求向其提供一份認購協定以及一份合夥協定。若干司法權區的投資者或須符合所在司法權區的證券法規提出的其它要求或標準。與本項目無關。

上述適當性標準為潛在投資者的最低適當性要求。各潛在合資格投資者以及其投資、稅務、法律、會計顧問和其它顧問徵詢意見確定此投資是否適合該投資者。

1 **對於開曼群島投資者：**

于開曼群島不可向公眾發售本權益或邀約認購權益。

2 **對於中華人民共和國投資者：**

不可向中華人民共和國公眾直接或間接發售權益，不可向中華人民共和國公眾提供本文（並無提交給中國證券監督

管理委員會）和本文所載有關團隊權益的發售材料和資訊，上述 BACCHUS 酒神團隊不可用於向中華人民共和國公眾進行認購發售或出售權益。BACCHUS 酒神團隊權益只可發售或出售予獲准進行外匯業務及在中國以外進行離岸投資業務的中國機構。根據中國相關外匯管制規定，中國投資者須遵守外匯管制批准和備案的規定。投資者須負責從中華人民共和國相關政府部門取得所有相關的政府批文、審核、許可或登記（若有），這些部門包括但不限於國家外匯管理局、中國證券監督管理委員會、中國銀行業監督管理委員會、中華人民共和國商務部、國家發改委和其它相關監管機構。投資者須遵守中華人民共和國的相關規定，包括但不限於相關外匯規定（例如返程投資的規定）及/或海外投資規定。

3 **對於香港投資者：**

本白皮書並未提交給相關公司註冊處進行註冊，香港監管機構並未審閱其內容。香港證券及期貨事務監察委員會並未批准此團隊。因此：

(a) 不可在香港通過任何形式向香港證券及期貨條例（香港法例第 571 章）定義的“專業投資者”以外的人士發售或出售權益，本白皮書亦不可依據上述法例的任何規則，或對照公司條例（香港法例第 32 章）列出的定義而構成“招股書”，或在按公司條例規定未構成向公開募集的其它各種情況下發售或出售權益；及

(b) 除非權益僅針對或打算針對香港之外的人士或“專業投資者”發售，任何人均不得在香港或其它地方對香港公眾發佈或為發佈之目的而留存任何與權益相關的邀請、廣告或其它檔（除非按照香港證券法規的要求可以這樣操作）。香港監管機構並無審閱本私募備忘錄的內容。建議閣下處理發售時須謹慎。若閣下對本文內容有疑問，閣下應聽取獨立的專業意見。

4. **對於日本投資者：**

權益發售並無且將不會根據日本證券及交易法進行登記，除非依據日本證券及交易法和其它日本相關法規所提供的豁免，不可在日本直接或間接向其居民發售或出售權益。

5. **於韓國投資者：**

團隊和投資經理均無根據韓國法律規定就本白皮書的接受者購買權益的資格作出相關陳述；韓國相關法律包括但不限於外匯交易法和相關規定。權益並無根據韓國證券及交易法或韓國間接投資資產管理法進行登記。除非跟從韓國相關法例，權益將不可在韓國直接或間接提供、出售或派發、或提供、出售或派發予重新提供或轉售之任何韓國居民。

6. **對於盧森堡投資者：**

根據盧森堡證券及期貨法第 289 章第 304 條的規定，本白皮書所述發售或邀約只可對機構投資者或其它人士進行，而根據第 305 條的規定則只可向資深投資者而非普通公眾發售或邀約。根據上述盧森堡法例，本白皮書並非招股書，因此，有關招股書內容的法定責任並不適用。潛在投資者須仔細考慮投資是否適合他們。本白皮書並無在盧森堡金融管理局登記為招股書，因此，本白皮書和其它與發售或出售或邀約認購或購買權益之有關檔或材料不可分發給盧森堡普通公眾，或對盧森堡任何普通公眾

發售或出售或邀約認購或購買此權益，除非發售或出售或邀約認購或購買予

(a) 機構投資者或其它人士（根據盧森堡證券及期貨法第 304 條規定的條件；

(b) 資深投資者（根據盧森堡證券及期貨法第 305 條規定的條件；或

(c) 其它人士（根據盧森堡證券及期貨法其它適用條文規定的條件。除非通過法律效用，上述盧森堡人士認購或購買的權益不可轉讓。）

7. **對於臺灣投資者：**

團隊並無且不會在臺灣政府機構進行登記。在臺灣出售權益須遵守當地法律規定和限制。不可在臺灣出售、發行或公開發售權益，及只可以私募形式對在臺灣的資深投資者出售。臺灣並無任何人士或公司實體被授權發售或出售權益，或就權益的發售和出售提供意見或作為仲介提供服務。

8. **對於泰國投資者：**
   編制本文的目僅計畫對泰國機構投資者發售權益。本文並非招股書。不可在泰國公開發售權益。

9. **其它司法權區：**
   於沒有遵守登記規定或其它法律規定而進行權益發售或邀約認購或購買權益屬於非法的司法權區，本文並不構成發售權益或邀約認購或購買任何權益。本文不會在任何司法權區根據相關證券法律登記為招股書。若干司法權區可能禁止分發本文，取得本文的人士必須知曉和遵守這些限制。

本文中討論的某些事項涉及我們未來的業績，包括但不限於 BACCHUS 酒神未來的收入、收益、策略和前景。所有非依據歷史性資料所做的陳述均構成“前瞻性陳述”。這些前瞻性陳述存在風險和不確定性，可能會導致實際結果與預期不符。這些陳述是基於管理層的信念以及管理層依據目前獲得的資訊所做的設想。在本文中，“預期”、“打算”、“估計”、“相信”、“期望”、“應該”、“潛在”、“預測”、“項目”或類似這些用詞的使用，旨屬前瞻性陳述。

謹請讀者注意，不要過分依賴這些前瞻性陳述而作出任何個人決定。儘管我們盡一切努力確保本白皮書中所有資訊的準確性和最新性，但這些材料絕不構成專業意見。 BACCHUS 酒神既不保證也不承擔對本文內容的準確性、可靠性、當前性（如本白皮書）或完整性的責任。有意投資此平臺的個人應在徵求本文所載任何資訊之前尋求獨立的專業意見。本白皮書中列出的任何資訊並沒有受到監管機構審查或批准。本白皮書沒有或將要根據任何司法管 轄區 的法律、監管要求或規則，採取這樣的行動。本白皮書的發佈，分發或傳播並不意味著己經遵守適用的 法律、法規要求或規定。

藉由您接受或依賴本白皮書或其任何部分而產生或與之有關的決定，在適用的法律、法規和規則允許的最大範圍內，BACCHUS 酒神及其關聯公司和代幣發行合作夥伴不承擔任何形式的侵權、合同或其他方面的任何間接、特殊、附帶、間接或其他損失（包括但不限於收入，收入或利潤的損失，以及使用或資料的丟失）。BACCHUS 酒神及其附屬公司和代幣發行合作夥伴不會以任何形式向任何實體或個人作出或聲稱做出任何陳述、保證或承諾，包括與真相、準確性有關的陳述，保證或承諾以及本白皮書中提供的任何資訊的完整性。

酒神
BACCHUS

內容提要

傳統企業做區塊鏈的設計，不是一拍大腿弄個分佈式賬本，發個幣就可以的，而是要結合企業的現狀進行產業的資產和關鍵問題分析，作為新的生產關係一定是要解決企業的問題，產生增量價值的，而不是弄個空氣幣出來。

可永續的區塊鏈用例非常稀少。儘管事實存在，但是有很多人給加密貨幣帶來了價值，不顧「可用東西」的數量仍遠遠低於 2,000 億美元的市值。ICO 產業面臨的主要挑戰就是如何彌補這個差距，並使其達到市值的實際價值。

BACCHUS 幣是一個代幣經濟下的新系統。本白皮書將解釋的一些核心例如:分佈式帳本系統

- 分佈式帳本系統
- 如何解決行業痛點
- 防偽驗證系統
- 區塊鏈防偽企業方案
- 幣的用途及信用

BACCHUS 將會為世上所有酒生產商提供數字貨幣買賣酒的商城。當中的佳釀全部都是真品。在本區塊鏈的發明之下運作，消費者才能於商城上以 BACS 對換成酒。

BACCHUS 核心是以區塊鏈技術分享作生意模式，幫助中美澳歐四大酒類出口國家中的酒庄能快速建立區塊鏈技術，以這個生意模式獲利，並讓所有投資者和區塊鏈使用商獲利。即使有酒庄已經使用了他們的區塊鏈，BACCHUS 酒神系統更希望最終會發展成一個酒類區塊鏈的路由器，可以透過本系統直接找到其他系統中的佳釀。而且酒神系統獲合作伙伴致真庫團隊授權使用香港特別行政區政府知識產權署專利註冊處的註冊專利，用於運作一個區塊鏈溯源的系統，專利編號 Patent No. :HK1246582 。

本團隊位於香港，一個既擁有紅酒文化，又擁抱內地的白酒文化和歐洲烈酒文化的交點，有能力將 BACCHUS 酒神理念推動區塊鏈技術普及至國際化的重要核心。

酒神 BACCHUS

目錄

酒神
BACCHUS

摘要

由於偽造、摻假和過量使用防腐劑及危險化學品在近年急劇增加，行業對佳釀供應鏈可追溯系統的需求至關重要。為了克服這些問題，各類酒行業需要一種新系統為消費者提供保障，以驗證從酒原料例如小麥、葡萄種植者到零售商的每批酒的成份和釀造過程。酒神目前的系統是基於區塊鏈系統的一套加密專利而的衍生的生意模式，舊有的系統依然可以根據需要去偽造存儲的信息，因為有大量的人依附在酒廠周邊。

在本白皮書 BACCHUS 團隊提出一種基於區塊鏈的酒類供應鏈溯源系統，其中每個交易都被記錄為鏈中的一個區塊，並且可讓相關參與者看到。因為對記錄信息的任何改變都會打破區塊鏈的記載，所以這些信息塊相信是不可改變的，也不能被刪除，節點的有效性也可以追溯。

除了提供高質量的信息管理框架外，本白皮書建議的可追溯性系統還可以實現從原料到瓶子的整個過程的透明度，問責制度、安全性和可靠性。

商城的設計是用 woocommerce 加上以太坊智能合約及 metamask 插件作商城，第一階段的商城是 OFFCHAIN 離鏈但可以和 metamask 溝通的。 第二階段將會讓整個商城上鏈，讓整個區塊鏈中的溯源訊息，可以與酒神幣買賣成品酒的商城進行溝通，並且對應酒神系統以外的智能合約。

保護產品
產品認證和保證與區塊鏈真實性

信任
消費者瞭解更多關於的瓶子，通過從圈到瓶子的品牌認證提高了意識和忠誠度

高速擴展及相容性
酒莊只要登記成為合作夥伴，即可免費享有些系統區塊鏈的使用權

跟踪和認證
每一瓶酒釀造過程到產酒的地理區域都經過跟蹤並認證所有資訊

酒神 BACCHUS

I. 介紹

傳統上，優質酒都是以信任的方式買賣：賣家提供一瓶佳釀加上它的資訊，例如是罕見的，舊的，或來自標誌性的製造商；並提及一個好的出處或故事，以確定酒是真實的並且已經正確儲存。但佳釀行業在過往十年中發生了巨大的變化。

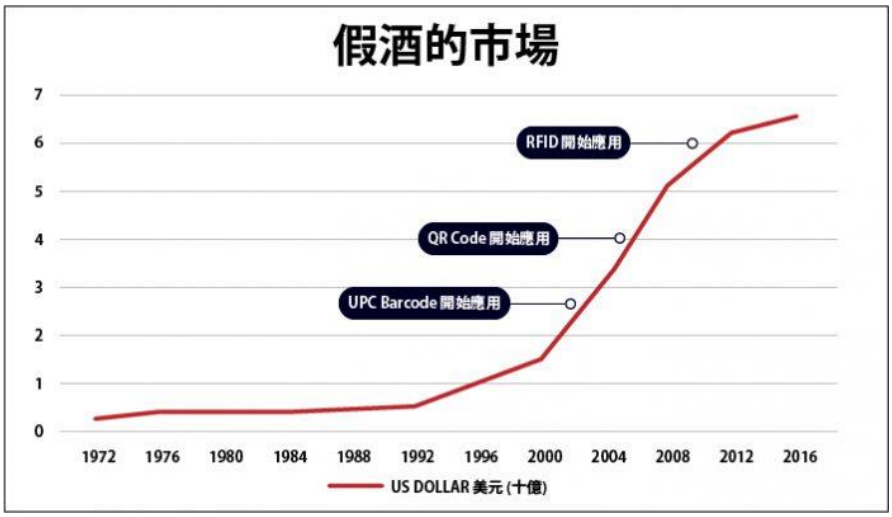
自 20 世紀 90 年代初以來，葡萄酒的假冒產品迅速增加，欺詐性假酒佔全球二級市場的近 5%，達到 150 億美元[1]。在各種各樣的葡萄酒欺詐行為中，將廉價葡萄酒偽造和重新標記為昂貴且高度可收集的葡萄酒是最常見的欺詐類型。最近，葡萄酒行業通過實現葡萄酒供應鏈的可追溯性，更加注重防止假酒。可追溯性是一種方法，通過該方法，任何人都可以驗證整個過程，包括原料，運輸和儲存條件，加工，分銷和葡萄酒供應鏈中的銷售。2008 年，本傑明華萊士[2]的真正犯罪事件“億萬富翁的醋”揭露了一位德國音樂經理和葡萄酒收藏家的故事，據稱他曾欺騙其他富有的收藏家購買假冒葡萄酒，以某種方式摻假的葡萄酒，經常在一個更昂貴的品牌下過世，包括他聲稱屬於 Thomas Jefferson 的幾瓶酒。

華萊士的書成為“紐約時報”的暢銷書，並在各地的收藏家心中埋下了一大堆懷疑。

五十年後，葡萄酒世界再次動搖，當葡萄酒收藏家變成葡萄酒偽造者 Rudy Kurniawan 因欺騙高端收藏家至少 2000 萬美元而被判十年徒刑。 （關於整個故事，請查看 Peter Hellman 的新書 In Vino Duplicitas。）在“魯迪事件”之後，拍賣行開始撤回大量可疑來源的葡萄酒。隨後提起訴訟，還有一位著名的收藏家 - 億萬富翁比爾科赫，他成為魯迪和華萊士的書“哈迪羅登斯托克”的受害者 - 甚至開始討論假酒，僱用一支專家團隊並花費他的 2000 多萬美元有錢揪出造假者。

事實上，美國政府還以不大相同的美酒假冒定義估計全球美酒假冒產業為 50 億元美金，比 10 年前(2008)高出 17 倍。同樣地，IACC 於 2012 年的報告中，表明假冒美酒每年造成 60 億美元的問題，實際上這個問題在過去二十年中增長了 10，000%以上，部分原因是消費者需求以及應用於葡萄酒行業的標籤技術的有限效果。 下圖顯示了從 1972 年開始兩個組織對葡萄酒假冒市場規模的估計，以及之前的估計。

1. 假酒問題



現今已經開發了許多可追溯系統和標準來自動化供應鏈活動。特別是條形碼(barcode)，射頻識別（RFID），QR 碼，電子產品代碼（EPC），EPC global，無線傳感器是最具吸引力的技術和供應鏈可追溯性範例。“Global standard 1”（GS1）系統提供全球通用標準，以便於識別公司及其產品並交換有關它們的信息[4]。 GS1 在生產和分銷的每個階段實施編號或編碼方案，以唯一地識別產品和服務。數字或條形碼的機器可讀表示用於指定分配給它的項目。最近的 GS1 標準化開發也為使用 RFID 支持的 EPC 提供了行業標準。

I. Expsito 團隊提出了一個使用 RFID 和無線傳感器網絡的葡萄酒供應鏈可追溯系統[5]。在葡萄園中部署了無線傳感器網絡以收集氣象數據和植物健康信息，而 RFID 標籤用於記錄收穫，傾析，發酵和保存過程的數據。在[6]中提出了另一種基於 RFID 的可追溯系統，該系統依賴於普遍的移動架構。所提出的系統提供了過程跟踪的事務視圖，其示出了系統中數據記錄的生成和管理。此外，還提供了系統的架構視圖，以使跟踪過程能夠遠程檢索記錄的信息。

Kreshnik 團隊提出了一種數據模型和系統原型，以支持通過加密條形碼技術移動訪問葡萄酒信息[7]。數據模型是 GS1 標準的改編版，代表參與實體及其活動，如灌溉管理，葡萄園中的葡萄監測，過程監控和酒窖中的轉向。為了防禦假冒產品，參與實體的身份最初被加密，編碼並打印在稱為 QR 碼圖像的瓶子標籤上。只有授權實體才能使用 Web /移動應用程序和解密密鑰檢索全局可跟踪性標識符。最近 IBM 商業價值研究院對基於區塊鏈的食品供應鏈管理系統的研究表明，通過跟踪供應鏈中食品的來源和流動，可以確保從供應商到消費者的產品的安全性和真實性。該研究側重於區塊鏈可以實現重大突破的三個關鍵方面：擴展可見性，動態優化和開放預測[8]。

大多數葡萄酒供應鏈可追溯系統使用條形碼和/或 RFID 標籤在供應鏈的不同階段存儲信息。 手動檢索該信息並將其存儲在中央數據庫中。 最後，開發 Web 或移動界面以向最終用戶顯示信息。 現有可追溯性系統的主要問題之一是源信息的真實性，因為它易於有機會被創造假信息。 除此以上方法外，世上暫時沒有更有效的方法來識別假冒瓶子，因為這些瓶子總是伴隨著偽造的起源歷史。 因此，酒行業需要一種解決方案來確保其生產的每瓶酒的真實性和來源。 而區塊鏈對優質高價酒市場的信任問題帶來了希望。

中國急速增張的假酒市場:[3]

- 美酒市場的需求越來越多
- 儘管有 120 個國家在生產美酒， 但當中只有大約 15 個國家在全球化的美酒當中擔當重要的角色
- 近年中國作為生產者、進口者及消費者在全球美酒界中迅速崛起。在 2011 年，中國的美酒生產區已成為世界 4 大並且仍在繼續增加生產區的規模。
- 中國為世界第 5 大美酒消費國，並且第一次成為紅酒最大消費國，領先於法國和意大利。
- Vinexpo 最近的一項研究更表明，中國和香港已成為全球第二大貴價美酒市場
- 在 2012 年至 2016 年間，中國美酒消費量在預期中上升了 40%，增至 8.58 億瓶。這使中國成為美國與俄羅斯之上的最快增長市場。
- 中國正積極開發新本地美酒，它的一些葡萄酒技術缺陷很少，質量也在提高。

REFERENCES

[1] P. Schmitt, "How much fake fine wine is in the market?," https://www.thedrinksbusiness.com/2016/12/how-much-fake-fine-wineis-in-the-market/, 2016.

[2]The Billionaire's Vinegar: The Mystery of the World's Most Expensive Bottle of Wine https://www.amazon.com/Billionaires-Vinegar-Mystery-Worlds-Expensive/dp/0307338789

[3]6,000 BOTTLES OF FAKE WINE BUSTED IN CHINA https://www.thedrinksbusiness.com/2017/08/6000-bottles-of-fake-wine-busted-in-china/

[4] GS1, "Wine Supply Chain Traceability: GS1 Application Guideline," http://www.gs1.org/docs/traceability/GS1 wine traceability.pdf, 2015, pp. 1–28.

[5] I. Expsito, J. A. Gay-Fernndez, and I. Cuias, "A Complete Traceability System for a Wine Supply Chain Using Radio-Frequency Identification and Wireless Sensor Networks [Wireless Corner]," in IEEE Antennas and Propagation Magazine, vol. 55(2), 2013, pp. 255–267.

[6] M. G. C. A. Cimino and F. Marcelloni, "Enabling Traceability in the Wine Supply Chain," in Methodologies and Technologies for Networked Enterprises: ArtDeco: Adaptive Infrastructures for Decentralised Organisations, Springer Berlin Heidelberg, 2012, pp. 397–412.

[5] K. Vukatana, K. Sevrani, and E. Hoxha, "Wine Traceability: A Data Model and Prototype in Albanian Context," in Foods Journal, vol. 5(1), http://www.mdpi.com/2304-8158/5/1/11, 2016.

[6] IBM Institute for Business Value, "Trust in trade- toward stronger supply chains," IBM Corp., 2016.

[7] K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the IoTs," in IEEE Access, Special section on the plethora of Research in IoT, 2016, pp. 2292–2303.

[8] K. Biswas and V. Muthukkumarasamy, "Securing Smart Cities Using Blockchain Technology," in IEEE 14th International Conference on Smart City, 2016, pp. 1392–1393.

2. 假酒行業最核心的痛點

本團隊認為很多防偽技術出現，依然不能阻止假酒出現，甚至年年急速增加，是因為傳統的物流鏈以筆記型電腦為核心，管理非常複雜，核心企業對上下游的延伸和掌握有限。上下游可能存在競爭關係，存在資訊流作假，市場供需變化無法及時傳遞。很多人依附在酒的物流鏈上下游，篡改後存在的訊息差，令衍生假酒的問題沒有得到解決。

3. 甚麼是區塊鏈

即(a)分佈式帳本及(b)交易透明度和可靠性。區塊鏈雖已存在多年，但由中本聰所提出及創造之比特幣系統[9]卻開

a. 分佈式帳本

區塊鏈是一種分佈式，分散的分類賬，或不斷更新的交易清單，記錄協議，合同和銷售。最初開髮用於支持加密貨幣，這種點對點系統可用於任何形式的交易而無需中介。區塊鏈技術的安全性取決於強大的加密方案，可以驗證每個交易塊並將其鏈接在一起。攻擊者必須妥協 51%的系統才能超越目標網絡的哈希能力。

b. 交易的透明度和可靠性

篡改存儲在區塊鏈中的交易在計算上是不切實際的。以下示例演示了區塊鏈技術的工作過程。讓 A 和 B 成為基於區塊鏈的支付系統的兩個參與者，並且 A 想要向 B 匯款。該交易在系統中表示為包括諸如塊號，工作證明，前一個塊和交易細節之類的信息的塊。並且該塊被廣播給網絡中的每個參與者。其他被稱為礦工的參與者驗證該區塊，如果超過 50%的礦工驗證該區塊，則交易被批准並添加到鏈中。之後，資金從參與者 A 轉移到參與者 B 的賬戶。

4. 為何區塊鏈在供應鏈中是一個絕對的遊戲改變者

區塊鏈的應用有望提高透明度，更新可行性，減少不一致性，提高支付處理準確性，並消除合規性問題。儘管該技術仍然是新技術，但需知道其潛力不容忽視。

5. 開創價值物聯網時代

傳統物聯網（Internet of Things，簡稱 IoT）是讓所有能行使獨立功能的普通物體實現互聯互通的網路，它通過網路技術將感測器、控制器和客觀實體連通起來，實現智能化管理和控制。例如通過射頻識別（RFID）、紅外感應器、全球定位系統、鐳射掃描器等資訊傳感設備，按約定的協議把任何物品與互聯網連接起來，進行資訊交換和通訊，以實現智能化識別、定位、跟蹤、監控和管理。

物聯網作為互聯網的延伸，進一步強化了機器與機器、人與機器的連接，實現了數據在資訊世界的全生命週期的流通管理。

隨著技術的不斷進步，物聯網技術的發展和應用在最近幾年取得了顯著的 成果，目前在世界範圍內已經有數十億個感測器和智能控制器投入使用，預計 在未來幾年這個數字還會成倍的增長。但是，物聯網技術也面臨著許多問題和 挑戰，比如感測器數據的採集缺乏標籤身份認證，中心化存儲的數據風險高， 金融領域

物聯網應用的安防成本太高，這些問題有可能成為物聯網在未來發展 和應用的巨大障礙。而由區塊鏈技術引領的價值物聯網，可以給這 些問題提供解決方案。 價值物聯網的技術實現，是通過以 RFID 晶片為核心構築的底層硬體平臺， 將現實世界中的物品標籤、事件標籤、人物身體標籤等實體標籤與互聯網的虛 擬世界進行連通，並結合區塊鏈技術這條傳遞價值、構造信任的紐帶，實現真 正意義上的萬物互聯。 由資訊互聯網、傳統物聯網向基於 RFID 技術和區塊鏈技術的價值物聯網轉型，其發展速度可能會遠遠超過目前人們的普遍預期，當價值物聯網真正實現 萬物互聯互通的時候，RFID 技術和區塊鏈技術將得到更大的發揮。

6. 區塊鏈 1.0 到 3.0 的啟示

區塊鏈 1.0

是指比特幣所運用的分散式帳本技術 (Distributed Ledger Technology)，這個電子現金系統是依靠分散式網路的「共識機制」運行。在當時金融海嘯的背景下，創造者中本聰賦予數位貨幣「去中心化」、「不可竄改」、「可追蹤性」、「匿名性」的特性。儘管上述特性都有可能，特別強調只是「可能」被破解，但仍造就了能夠不經由第三方，完成點對點支付的第一代加密貨幣。

區塊鏈 2.0

則以智能合約為發展核心，能夠用來寫 DApp 和發 ICO。智能合約是以程式碼構成，並運行在區塊鏈上的程式。只要滿足在智能合約中事先設定好的條件，就會自動執行，不再需要第三方憑證，如銀行、律師、公證人...等等。其中最具代表性的是以太坊，建立可編程的區塊鏈，使任何人皆可使用區塊鏈技術建立去中心化應用

區塊鏈 3.0 及區塊鏈 3.0 會帶來什麼改變

目前仍沒有統一的說法，但概念大致分為兩種：將分散式帳本技術應用到更多實際場景，或是解決目前區塊鏈 2.0 碰到的技術問題，例如擴容與儲存限制。與物聯網的結合是滿多人探討的領域，許多人較熟悉的是 IOTA。以 IOTA 為例，他們試圖讓「物與物」可自由溝通，也就是數據交流，再結合數位貨幣的領域，數據交流就可以達成「幣流」，也就是金流。

以太坊，2017 年開始崛起，帶動了 2017 年 ICO 片地開花，也慢慢地開始有人開發到區塊鏈中加入去中心化的程式，以太坊是一個分散式的電腦，有許多的節點，其中的每一個節點，都會執行位元組碼--智慧合約，然後把結果存在區塊鏈上。由於整個網路是分散式的，且應用就是一個個的狀態組成，存儲了狀態就有了服務；所以它就能永不停機，沒有一個中心化的結點，任何協力廠商不能干預。

酒神
BACCHUS

II. 商城

1. 酒神幣

第一階段本酒神系統將於以太坊公有鏈上發行，以 ERC-20 制式為第一階段 ICO 代幣。

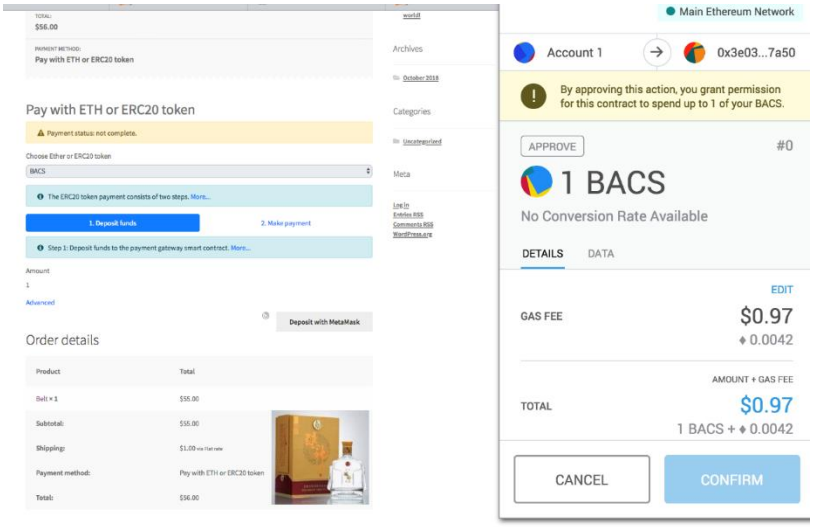
Contract:	0x0618822550a8483176e7b8cf7ce57cc26294a927
Decimals:	0
Function:	approve,transferFrom,transfer,approveAndCall
Total token issuance:	600,000,000BAC
Soft Cap:	20000 ETH
Hard Cap:	100000 ETH
Price level:	1ETH = 1000BAC/ 1BAC=1CNY
Token for sale:	50 0,000,000BAC
Lockup period	NO

2. 酒神 BACCHUS 商城

酒神幣可以應用予商城中消費，第一階段下的商城是半離鏈的，可以由以下網址中用酒神幣換取特選的佳釀:

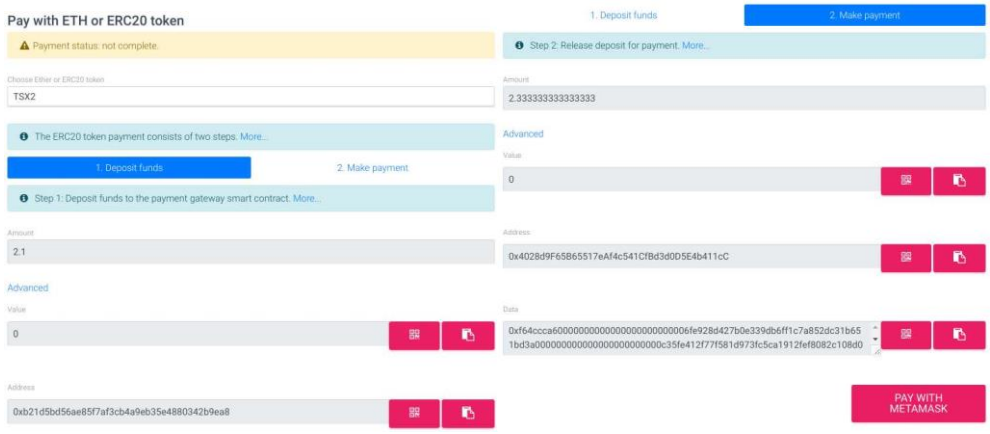
http://commerce.bacc.tech/

從以上商城演示到利用以太坊外部插件，配以 woocommerce 系統的線上商城的整個交付系統，下圖示範了從 metamask 授權使用 BACS 從商城中支付的介面及操作。用戶需要安裝瀏覽器的 metamask 錢包插件，馬上可以開始在商城買酒，過程就像在 Amazon 填寫好所有的訊息後，再通過 Paypal 支付。



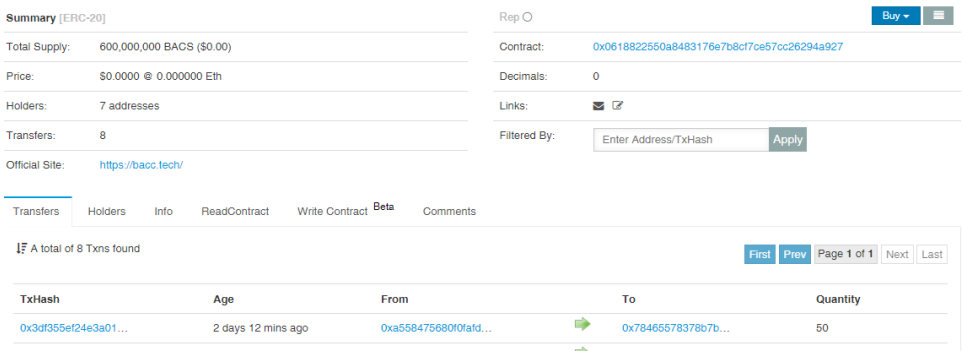
Metamask 是去中心化錢包，購買訊息填好後在回饋功能上會通知商城已完成付款。交易會顯示在區塊上，我們使用以太坊瀏覽器 Etherscan 便可以驗證每一筆交易。有 BUG 出現令交易內容無法證實時，遇上任何無效購買時，酒神幣將會退回原有地址的持有人手上，所有交易記錄都會公開在區塊上。

用戶需在 http://commerce.bacc.tech/ 上的完成注冊，然後就可以在酒神商城中購物。相信隨著區塊鏈應用的普及，支付方法會更簡便。



圖/METAMASK PLUG-IN

以上圖表列出了從酒神幣到 woocermence 商城的智能合約，讓酒神幣從個人錢包發送到指定的地址時，商城能從中得到完成支付的訊息。從而通知酒分銷商發貨。而存在於區塊上的酒神幣 BACS 交易記錄，可以用作核實交易是否已經完成。



圖/以太坊瀏覽器 etherscan，BACS 內容截圖

第一階段，酒神幣及商城系統不能與整個溯源系統溝通，但是能完成用幣換酒的功能，智能合約會回饋訊息到商城中。酒神幣的交付記錄會記載於以太坊瀏覽器 Etherscan 上。

而當酒神區塊鏈系統到了第二階段，整個 ERC20 系統的酒神幣會上主網，將會能夠與整個酒神溯源系統互相溝通。

第二階段，酒神系統會全面上線自己的區塊鏈主網，會由 ERC-20 轉出到一個私有鏈，這個私有鏈可以結合以下的區塊鏈發明專利到酒神幣、商城及酒的區塊鏈身分證互相溝通。攻能:防偽、記錄交易(資產上鏈)、增加收藏價值、開源、去中心化錢包、交易金額能和溯源系統溝通、整體升值的系數。

商城系統中發售的酒

五糧液釀神六十年酿神封藏限量酒(40,000 酒神幣)

商城當中酒的價值就已經被充分肯定了，而且非常有賣點，中國銀行更將五糧液六十周年建廠釀神六十九度收藏酒推出成另類理財產品[15]，在<<中國名酒收藏>>一書中，釀神更是位列於第一頁的名酒[16]。另外亦會將收藏證書放上區塊鏈中。

茅台百家姓酒(400 酒神幣)

茅台集團獨家訂製百家姓，以“做好茅臺服務型行銷、承載中國酒文化傳播”為使命，以搭建綜合性行銷服務平台為基礎，通過優質服務和文化宣導培育具有“強粘性”的酒友群體，圍繞消費者構建多元化的圈子生態文化，努力成為中國傳統行業成功擁抱互聯網的標杆企業。本項目與其合作為酒神區塊鏈系統試行區塊鏈溯源，能為不同的人士提供獨特的個性化服務。是宴客，收藏，送禮各方面其中一個最佳的選擇。酒神官方預測此款酒在市場有一定的需求，相信此款酒的銷量會佔整個酒神區塊鏈商城中最高銷量。同時也是酒神幣有人搶購的原因，維持酒神幣的市場價格。

茅台十二生肖頭首收藏限量酒套裝 共 12 支(100,000 酒神幣一套)

與茅台集團合作，酒神商城獨家訂製，根據圓明園十二生肖頭像設計，全球限量 2 萬套。圓明園十二生肖頭像原來是清朝皇家園林圓明園海晏堂前噴水池的一部分，由義大利耶穌會會士清朝宮廷畫家郎世寧設計，由法國耶穌會神父蔣友仁監督修建，由清朝宮廷匠師製作。該噴水池稱為水力鐘和十二生肖報時噴泉，十二生肖形象的 12 件獸首人身像以八字形分列在噴水池兩旁，南邊為子鼠、寅虎、辰龍、午馬、申猴及戌狗，北邊為丑牛、卯兔、巳蛇、未羊、酉雞及亥豬。十二生肖銅像每日都會依次序輪流噴水，每到一個時辰，相應的獸首銅像口中就會噴水達兩小時[15]。茅台十二生肖頭首收藏限量酒套裝，一套十二款，每瓶裝有 500ml 茅台最頂級之佳釀，這款收藏酒別具收藏價值。

比頓山紅葡萄酒(400 酒神幣)

比頓山莊園由 17 世紀的一個西班牙家族創立，於 1864 年建成並完工。莊園位於世界著名優質葡萄酒產地 – 法國西部波爾多市中心之東南部，佔地約二十二公頃，當中包括城堡、酒莊和釀酒車間。酒莊位列法定產區葡萄酒 AOC 級別，產地名略高於「波爾多和優級波爾多」酒莊。葡萄園土壤以礫石，石灰及粘土為主，土壤的多樣性，賦予比頓山酒莊葡萄酒極大個性。絕佳的環境種植出優秀的葡萄，使其 2013 年釀製的葡萄酒，獲得 2015 年巴黎農業大賽的金獎（Medaille d'OR）。母公司為大唐西市酒業控股有限公司是大唐西市絲路投資控股有限公司之子公司（香港聯交所股份代號：0620）

Reference

[15] 圓明園十二生肖銅獸首下落及追索大事記，新華網，2009

[16] 网贷天眼 APP, “中国银行推五粮液限量酒另类理财产品”, https://www.p2peye.com/thread-2082174-1-1.html

[17]王邦華, “中國收藏酒名錄”2012，2012 年

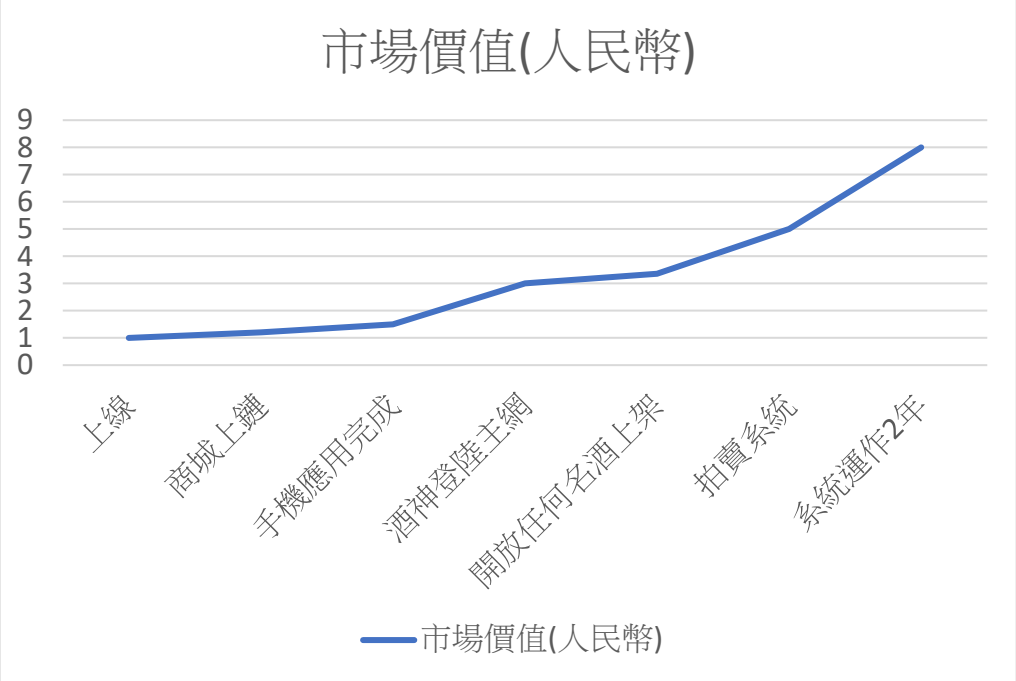
酒神
BACCHUS

未來預測

考慮到酒產業的經濟量，本系統只產生 6 億個酒神幣，在未來將會愈來愈有價值，酒神商城中的價格會隨 BACS 市場價值上升，商品所索取的 BACS 會漸漸減少，如果得到市場認同，每個 BACS 幣的價值都是無法想像的。

隨著酒神系統推出一浪一浪的好消息，例如商城連接區塊鏈(啟動完全去中心化)，手機應用程式開發，主網映射，開放予任何酒庄，拍賣系統，更多的機構合作，BACS 幣的價值會進一步推高。

酒神幣被設計成沒有小數點，必須要整顆的轉移，因為團隊認為不能拆分成小數點，這有助在酒神幣在初期建立價值。在進行主網映射後，會加入 8 個位數的小數點，酒神團隊希望酒神幣能在市場按需求自由反映價格，只會保留 10%予員工及股東。



III.區塊鏈技術實施細節

本酒神區塊鏈發明已獲提出一種產品資訊錄入與訪問的方法、裝置、存儲介質(區塊鏈)及終端設備，其中所述方法包括，接收廠商錄入產品的掃描識別碼；所述掃描識別碼用於設置在所述產品的包裝上以錄入或訪問所述產品的資訊；回應所述掃描識別碼的錄入，生成所述產品的解密私密金鑰和加密公開金鑰；其中，所述加密公開金鑰與所述解密私密金鑰配對，所述加密公開金鑰用於分配給所述產品的授權方，以在所述授權方訪問時對所述授權方錄入的所述產品的資訊進行加密；所述解密私密金鑰用於在通過所述掃描識別碼訪問所述產品的資訊時，對由所述加密公開金鑰加密的資訊進行解密。採用本發明，能夠使消費者識別其購買的產品是否為仿冒品。

機密性，完整性和可用性，也稱為 CIA 三元組，是一個旨在指導組織內信息安全策略的模型。該模型有時也被稱為 AIC 三元組（可用性，完整性和機密性），以避免與中央情報局混淆。三合會的要素被認為是安全的三個最重要的組成部分。本發明符合 CIA 三元組所定

在這種情況下，機密性是一組限制信息訪問的規則，完整性是信息可靠和準確的保證，可用性是授權人員可靠地訪問信息的保證。

機密性

保密性大致相當於隱私。為確保機密性而採取的措施旨在防止敏感信息傳達給錯誤的人，同時確保合適的人實際上能夠獲得信息：訪問必須限於那些有權查看相關數據的人。同樣，數據根據損壞的數量和類型進行分類是很常見的，如果數據落入非預期的手中。然後可以根據這些類別實施或多或少的嚴格措施。

有時，保護數據機密性可能涉及對此類文件的人員進行特殊培訓。此類培訓通常包括可能威脅此信息的安全風險。培訓可以幫助授權人員熟悉風險因素以及如何防範這些因素。培訓的其他方面可以包括強密碼和密碼相關的最佳實踐以及有關社會工程方法的信息，以防止他們以良好的意圖和潛在的災難性結果來彎曲數據處理規則。

用於確保機密性的方法的一個很好的例子是在線銀行業務時的帳號或路由號碼。數據加密是確保機密性的常用方法。用戶 ID 和密碼構成標準程序;雙因素身份驗證正在成為常態。其他選項包括生物識別驗證和安全令牌，密鑰卡或軟令牌。此外，用戶可以採取預防措施，以最大限度地減少信息出現的位置數量和實際傳輸完成所需事務的次數。對於極其敏感的文檔，預防措施，例如僅存儲在氣隙式計算機上，斷開連接的存儲設備，或者對於高度敏感的信息，僅採用硬拷貝形式，可能會採取額外措施。

完整性

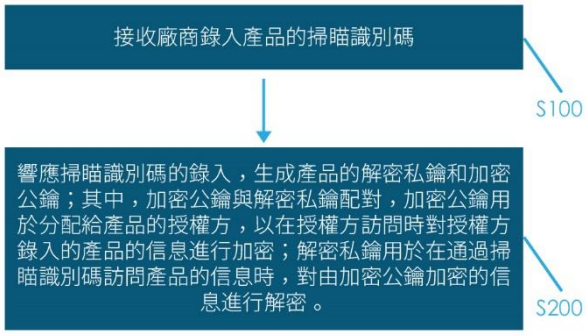
完整性涉及在整個生命週期內保持數據的一致性，準確性和可信賴性。數據不得在傳輸過程中更改，並且必須採取措施確保未經授權的人員不會更改數據（例如，違反保密規定）。這些措施包括文件權限和用戶訪問控制。版本控制可用於防止授權用戶的錯誤更改或意外刪除成為問題。此外，必須採取一些措施來檢測由於非人為引起的事件（如電磁脈衝（EMP）或服務器崩潰）而可能發生的任何數據變化。一些數據可能包括校驗和，甚至是加密校驗

和，用於驗證完整性。必須有備份或冗餘才能將受影響的數據恢復到正確的狀態。

可用性

通過嚴格維護所有硬件，在需要時立即執行硬件維修以及維護沒有軟件衝突的正常運行的操作系統環境，可以最好地確保可用性。保持當前所有必要的系統升級也很重要。提供足夠的通信帶寬並防止出現瓶頸同樣重要。冗餘，故障轉移，RAID 甚至高可用性群集可以減輕硬件問題發生時的嚴重後果。對於最壞的情況，快速和自適應災難恢復至關重要;該容量依賴於全面的災難恢復計劃（DRP）的存在。防止數據丟失或連接中斷的保護措施必須包括不可預測的事件，如自然災害和火災。為防止此類事件造成數據丟失，備份副本可能存儲在地理位置隔離的位置，甚至可能存放在防火防水保險箱中。額外的安全設備或軟件（如防火牆和代理服務器）可以防止由於拒絕服務（DoS）攻擊和網絡入侵等惡意操作導致的停機和無法訪問的數據。

摘要附圖



圖

專利實施內容

i. 一種產品資訊錄入與訪問的方法，其特徵在於，包括：

(a) 接收廠商錄入產品的掃描識別碼；所述掃描識別碼用於設置在所述產品的包裝上以錄入或訪問所述產品的資訊；

(b) 回應所述掃描識別碼的錄入，生成所述產品的解密私密金鑰和加密公開金鑰；其中，所述加密公開金鑰與所述解密私密金鑰配對，所述加密公開金鑰用於分配給所述產品的授權方，以在所述授權方訪問時對所述授權方錄入的所述產品的資訊進行加密；所述解密私密金鑰用於在通過所述掃描識別碼訪問所述產品的資訊時，對由所述加密公開金鑰加密的資訊進行解密。

ii. 如權利要求 i 所述的產品資訊錄入與訪問的方法，其特徵在於，所述授權方包括所述廠商，所述加密公開金鑰包括多個公開金鑰，所述方法還包括：

(a) 接收所述廠商錄入的所述產品的生產資訊；

(b) 所述生產資訊包括所述廠商以及所述產品的產品編號、廠商位址、出廠日期、產地、原材料中的至少一者；

(c) 從所述加密公開金鑰中選取公開金鑰作為所述產品的廠商加密公開金鑰；以及

(d) 根據所述產品的廠商加密公開金鑰，對所述廠商錄入的所述產品的資訊進行加密，並將加密後的資訊存儲于區塊鏈中。

iii. 如權利要求 ii 所述的產品資訊錄入與訪問的方法，其特徵在於，所述授權方包括代理商，所述方法還包括：

(a) 接收所述廠商錄入的所述產品的代理商的資訊；以及

(b) 從所述加密公開金鑰中選取公開金鑰作為所述產品的代理商加密公開金鑰。

iv. 如權利要求 iii 所述的產品資訊錄入與訪問的方法，其特徵在於，所述方法還包括：

(a) 接收所述代理商的代理訪問請求；

(b) 其中，所述代理訪問請求是包括所述產品的掃描識別碼和所述代理商的簽名資訊；

(c) 根據所述掃描識別碼和所述代理商的簽名資訊，查找所述產品的代理商加密公開金鑰；

(d) 判斷所述產品的代理商加密公開金鑰是否為首次被查找到；

(e) 當所述產品的代理商加密公開金鑰首次被查找到時，生成所述代理商已取貨的資訊；以及

(f) 根據所述產品的代理商加密公開金鑰，對生成的所述代理商已取貨的資訊進行加密，並將加密後的資訊存儲于區塊鏈中。

v. 如權利要求 iv 所述的產品資訊錄入與訪問的方法，其特徵在於，所述方法還包括：

(a) 接收所述代理商錄入的所述產品的分銷商的資訊；

(b) 從所述加密公開金鑰中選取公開金鑰作為所述產品的分銷商加密公開金鑰；以及

(c) 根據所述產品的代理商加密公開金鑰，對所述代理商錄入的資訊進行加密，並將加密後的資訊存儲于區塊鏈中。

vi. 如權利要求 v 所述的產品資訊錄入與訪問的方法，其特徵在於，所述方法還包括：

(a) 接收所述分銷商的分銷訪問請求；

(b) 其中，所述分銷訪問請求包括所述產品的掃描識別碼和所述分銷商的簽名資訊；

(c) 根據所述掃描識別碼和所述分銷商的簽名資訊，查找所述產品的分銷商加密公開金鑰；

(d) 判斷所述產品的分銷商加密公開金鑰是否為首次被查找到；

(e) 當所述產品的分銷商加密公開金鑰首次被查找到時，生成所述分銷商已取貨的資訊；以及

(f) 根據所述產品的分銷商加密公開金鑰，對生成的所述分銷商已取貨的資訊進行加密，並將加密後的資訊存儲于區塊鏈中。

vii. 如權利要求 vi 所述的產品資訊錄入與訪問的方法，其特徵在於，所述方法還包括：

(a) 接收所述分銷商錄入的所述產品的出售資訊；以及

(b) 根據所述產品的分銷商加密公開金鑰，對所述產品的出售資訊進行加密，並將加密後的資訊存儲于區塊鏈中。

viii. 如權利要求 vii 所述的產品資訊錄入與訪問的方法，其特徵在於，所述方法還包括：

(a) 接收消費者的銷售訪問請求；

(b) 所述銷售訪問請求包括所述產品的掃描識別碼；

(c) 根據所述掃描識別碼，從區塊鏈中提取由所述產品的加密公開金鑰加密的資訊；

(d) 根據所述產品的解密私密金鑰，對提取到的由所述產品的加密公開金鑰加密的資訊進行解密，獲得明文資訊；以及

(e) 將所述明文資訊返回給所述消費者。

ix. 如權利要求 viii 所述的產品資訊錄入與訪問的方法，其特徵在於，所述產品的解密私密金鑰存儲在解密伺服器中，則所述根據所述產品的解密私密金鑰，對提取到的由所述產品的加密公開金鑰加密的資訊進行解密，獲得明文資訊，包括：

(a) 將提取到的由所述產品的加密公開金鑰加密的資訊發送給所述解密伺服器；

(b) 接收所述解密伺服器返回的明文資訊；

(c) 其中，所述明文資訊是所述解密伺服器根據所述產品的解密私密金鑰對接收到的由所述產品的加密公開金鑰加密的資訊進行解密而獲得的。

x. 如權利要求 ix 所述的產品資訊錄入與訪問的方法，其特徵在於，所述方法還包括：

(a) 將加密後的資訊存儲于區塊鏈之後，接收所述區塊鏈返回的索引；

(b) 其中，所述索引與所述產品的掃描識別碼關聯；以及

(c) 所述根據所述掃描識別碼，從區塊鏈中提取由所述產品的加密公開金鑰加密的資訊，包括：

- 查找與所述所述掃描識別碼關聯的索引；
- 根據查找到的索引，從從區塊鏈中提取由所述產品的加密公開金鑰加密的資訊。

xi. 一種產品資訊錄入與訪問的裝置，其特徵在於，包括：

(a) 識別碼接收模組，用於接收廠商錄入產品的掃描識別碼；

(b) 所述掃描識別碼用於設置在所述產品的包裝上以錄入或訪問所述產品的資訊；

(c) 金鑰生成模組，用於回應所述掃描識別碼的錄入，生成所述產品的解密私密金鑰和加密公開金鑰；

(d) 其中，所述加密公開金鑰與所述解密私密金鑰配對，所述加密公開金鑰用於分配給所述產品的授權方，以在所述授權方訪問時對所述授權方錄入的所述產品的資訊進行加密；

(e) 所述解密私密金鑰用於在通過所述掃描識別碼訪問所述產品的資訊時，對由所述加密公開金鑰加密的資訊進行解密。

xii. 一種實現產品資訊錄入與訪問的終端設備，其特徵在於，所述終端設備包括：

(a) 存儲裝置，用於存儲一個或多個程式；

(b) 當所述一個或多個程式被所述一個或多個處理器執行時，使得所述一個或多個處理器實現如權利要求 i-x 中任一所述的產品資訊錄入與訪問的方法。

xiii. 一種電腦可讀存儲介質，其存儲有電腦程式，其特徵在於，該程式被處理器執行時實現如權利要求 i-x 中任一所述的產品資訊錄入與訪問的方法。

xiv. 一種實現產品資訊錄入與訪問的終端設備，其特徵在於，所述終端設備包括：

(a) 中央伺服器，用於執行如權利要求 i-x 中任一項所述的產品資訊錄入與訪問的方法；

(b) 區塊鏈伺服器，用於存儲所述中央伺服器加密後的資訊；

(c) 解密伺服器，用於存儲解密私密金鑰，以及根據所述解密私密金鑰對由與所述解密私密金鑰配對的加密公開金鑰加密的資訊進行解密。

產品的代理商加密公開金鑰，即分配給代理商。該代理商加密公開金鑰可以與代理商的資訊關聯，方便後續代理商在訪問產品的資訊時，查找到代理商的加密公開金鑰。

在一種可能的實現方式中，廠商將產品交付給代理商，代理商在收到產品後，會對該產品包裝上的掃描識別碼進行掃碼。此時，伺服器可以接收到代理商的代理訪問請求；其中，代理訪問請求包括有產品的掃描識別碼和代理商的簽名資訊。當代理商為該產品的授權方時，那麼伺服器是可以根據掃描識別碼和代理商的簽名資訊，查找到產品的代理商加密公開金鑰，如若查找不到，則說明該代理商不是該產品的授權方。當查找到了產品的代理商加密公開金鑰的時候，判斷該產品的代理商加密公開金鑰是否為首次被查找到；若是，則說明該產品已被授權了的代理商取貨了。此時，可以生成代理商已取貨的資訊，以及通過代理商加密公開金鑰對代理商已取貨的資訊進行加密，並將加密後的資訊存儲于區塊鏈中。

在本實施例中，每一個授權方加密的資訊可分別存在相應區塊當中，在後加密存儲的區塊與在先加密存信的區塊前後連接或前後索引。

在本實施例中，非授權方加密的資訊也可存儲在區塊鏈中，但是由於其經非授權方的加密公開金鑰進行加密，其所建立的索引無法被在產品的查詢過程檢索到。即，在檢索過程被丟棄。以及，即使被檢索到，由於無法被相應的解密私密金鑰進行解密，其資料也會被丟棄。

在一種可能的實現方式中，代理商可以將產品分銷給分銷商進行銷售，例如華南區的代理商將產品分銷給該區的某個市的一個超市。那麼代理商在確認該產品的分銷商後，可以對產品的掃描識別碼再次掃碼，進入資訊錄入，具體地：中央伺服器接收代理商錄入的產品的分銷商的資訊，然後，從加密公開金鑰中選取一個公開金鑰作為產品的分銷商加密公開金鑰，即分配給代理商。該分銷商加密公開金鑰可以與分銷商的資訊進行關聯，方便後續分銷商在訪問產品的資訊時，查找到分銷商的加密公開金鑰。以及，根據產品的代理商加密公開金鑰，對代理商錄入的資訊進行加密，並將加密後的資訊存儲于區塊鏈中。

在一種可能的實現方式中，代理商將產品交付給分銷商，分銷商在收到產品後，會對該產品包裝上的掃描識別碼進行掃碼。此時，伺服器可以接收到分銷商的分銷訪問請求；其中，分銷訪問請求包括有產品的掃描識別碼和分銷商的簽名資訊。當分銷商為該產品的授權方時，那麼伺服器是可以根據掃描識別碼和分銷商的簽名資訊，查找到產品的分銷商加密公開金鑰，如若查找不到，則說明該分銷商不是該產品的授權方。當查找到了產品的分銷商加密公開金鑰的時候，判斷該產品的分銷商加密公開金鑰是否為首次被查找到；若是，則說明該產品已被授權了的分銷商取貨了。此時，可以生成分銷商已取貨的資訊，以及通過分銷商加密公開金鑰對分銷商已取貨的資訊進行加密，並將加密後的資訊存儲于區塊鏈中。

在本發明實施例中並不僅僅包括廠商、代理商、分銷商等授權方，還可以包括多個級別的代理商或多個級別的分銷商，其訪問或錄入產品的資訊的方式也是類似的，在此不再贅述。

在一種可能的實現方式中，分銷商將產品銷售給消費者，此時分銷商再次對產品包裝上的掃描識別碼進行掃碼，並進行產品已售出的資訊的錄入，包括售出時間、售出價格等。伺服器在接收到分銷商錄入的產品的出售資訊時，可以根據產品的分銷商加密公開金鑰，對產品的出售資訊進行加密，並將加密後的資訊存儲于區塊鏈中。

在本實施例中，如圖 2 所示，中央伺服器將加密後的資訊存儲于區塊鏈，區塊鏈將會返回的一個索引，中央伺服器將索引與產品的掃描識別碼關聯，並存儲在索引伺服器或索引資料表中。

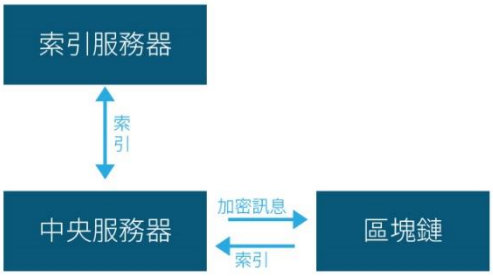


圖 2

在一種可能的實現方式中，消費者購買到產品時，可以利用移動設備，例如手機、IPAD 等，對產品包裝上的掃描識別碼進行掃碼。此時伺服器通過掃描識別碼接收消費者的銷售訪問請求。然後根據掃描識別碼，從區塊鏈中提取由產品的加密公開金鑰加密的資訊。並根據產品的解密私密金鑰，對提取到的由產品的加密公開金鑰加密的資訊進行解密，獲得明文資訊。以及，將明文資訊返回給消費者。

本實施例中，產品的解密私密金鑰一直存儲在解密伺服器中，無法被提出到解密伺服器之外。如圖 3 所示，消費者對產品資訊的查詢可以是：消費者向中央服務發送請求。中央伺服器根據掃描識別碼，向索引伺服器查找與掃描識別碼關聯的索引。中央伺服器根據返回來的索引從區塊鏈中提取由產品的加密公開金鑰加密的資訊。然後，中央伺服器將提取到的由產品的加密公開金鑰加密的資訊發送給解密伺服器。解密伺服器根據產品的解密私密金鑰對接收到的由產品的加密公開金鑰加密的資訊進行解密獲得明文資訊，並返回給中央伺服器，中央伺服器將明文資訊返回給消費者。

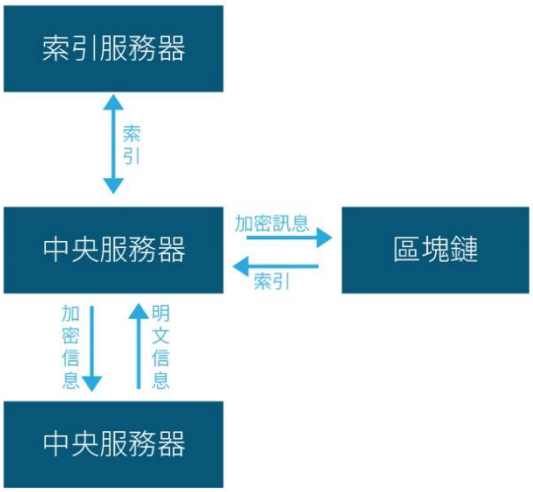


圖 3

在一種可能的實現方式中，消息在購買到產品後，對銷售小票或發票進行拍照，並掃碼上存於伺服器中。伺服器可以根據銷售小票或發票上的資訊錄入產品的購入資訊，方便轉售，杜絕重新包裝或二次售賣。

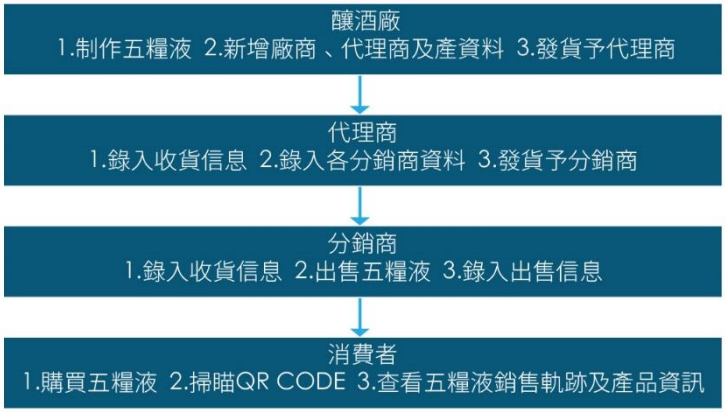


圖 4

請參閱圖 4，其是本發明提供的產品資訊錄入與訪問的方法的應用實例的示意圖。該方法以五糧液酒銷售流程為例，進行詳細的描述：

a）釀造廠把釀制完成的一瓶五糧液酒後進行包裝，每枝五糧液的包裝上都有獨有的 RFID。每枝五糧液在出廠前會被釀造廠進行掃碼，以把產品編號、廠商位址、出廠日期、代理商資料等錄入區塊鏈。在掃碼錄入資訊的過程中生成解密私密金鑰和多個加密公開金鑰。其中，加密公開金鑰分別為釀造廠和代理商分配一個，並存在伺服器當中。

b）代理商收貨後，把每個 RFID 掃描一次以訪問伺服器，代表代理商已取貨，這資訊會被代理商的加密公開金鑰加密，並錄入到區塊鏈（格物鏈）。

c）代理商為五糧液進行分配分銷商，以便分發到相應的分銷商中。此時代理商再次掃描產品特有的 RFID，以錄入各分銷商的資料。此資訊也會被代理商的加密公開金鑰加密，並錄入到區塊鏈中。由於此前沒有分銷商的資料，而分銷商作為授權方，其也在錄入分銷商資料的同時，被分配一個相應的加密公開金鑰。

d）分銷商收貨後也會對產品的 RFID 進行掃描，伺服器記載分銷商已取貨的資訊，該資訊由分銷商的加密公開金鑰進行加密存儲于區塊鏈中。分銷商在售出一枝五糧液酒的同時，也會對售出的五糧液酒的 RFID 進行掃描，以錄入五糧液酒已出售的資訊，該五糧液酒已出售的資訊由分銷商的加密公開金鑰進行加密存儲于區塊鏈中。

e）消費者可以掃描五糧液酒的 RFID，追縱其買入的五糧液酒的產品資訊及銷售軌跡。如若發現代理商已取貨、分銷商已取貨或產品已出售這些資訊沒有被錄入，即可認為此五糧液酒是仿冒品。

本實施例具有的特點：

a）廠商、代理商及分銷商等授權方均會獲得不同且獨有的加密公開金鑰，以取得錄入或更改資訊的許可權。

b）區塊鏈本身有著不可複製及不可造假的特性，仿製商無法更改區塊鏈中的資訊。

c）只有廠商，代理商及分銷商等授權方有權更改區塊鏈資訊，其他持份者及不法之徒只能查到區塊鏈中的產品的資訊。

本實施例具有的有效效果：

a）有效地進行打假活動，減少企業花費巨額的律師費等打假所需費用，提高利潤。

b）隨著打假活動成功，將會締造良好的營商環境，讓企業對其拓展的市場有更大信心，減少擴大經營的風險。

c）打破現有的區塊鏈技術只能用於虛擬貨幣的交易中的模式，使得區塊鏈深入日常生活中。

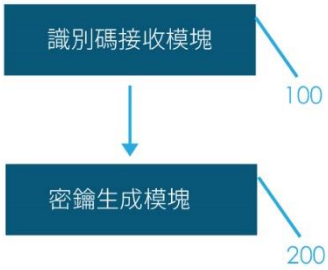


圖 5

如圖 5 所示，本發明實施例還提供一種產品資訊錄入與訪問的裝置，包括：

a）識別碼接收模組 100，用於接收廠商錄入產品的掃描識別碼；

b）所述掃描識別碼用於設置在所述產品的包裝上以錄入或訪問所述產品的資訊；

c）金鑰生成模組 200，用於回應所述掃描識別碼的錄入，生成所述產品的解密私密金鑰和加密公開金鑰；

d）其中，所述加密公開金鑰與所述解密私密金鑰配對，所述加密公開金鑰用於分配給所述產品的授權方，以在所述授權方訪問時對所述授權方錄入的所述產品的資訊進行加密；

e）所述解密私密金鑰用於在通過所述掃描識別碼訪問所述產品的資訊時，對由所述加密公開金鑰加密的資訊進行解密。

所述裝置的功能可以通過硬體實現，也可以通過硬體執行相應的軟體實現。所述硬體或軟體包括一個或多個與上述功能相對應的模組。

在一個可能的設計中，產品資訊錄入與訪問的結構中包括處理器和記憶體，所述記憶體用於存儲產品資訊錄入與訪問的裝置執行上述第一方面中產品資訊錄入與訪問的方法的程式，所述處理器被配置為用於執行所述記憶體中存儲的程式。所述產品資訊錄入與訪問的裝置還可以包括通信介面，用於產品資訊錄入與訪問的裝置與其他設備或通信網路通信。

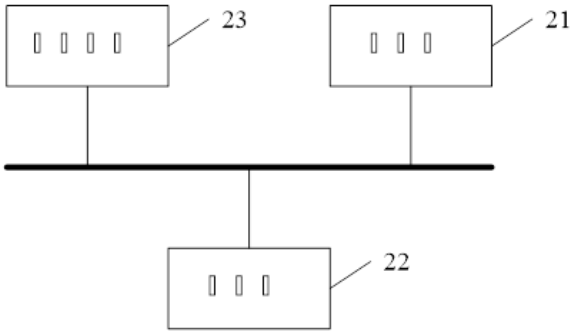


圖 6

本發明實施例還提供一種終端設備，如圖 6 所示，該設備包括記憶體 21 及處理器 22。記憶體 21 內存儲有可在處理器 22 上運行的電腦程式。處理器 22 執行電腦程式時實現上述實施例中的產品資訊錄入與訪問的方法。記憶體 21 和處理器 22 的數量可以為一個或多個。

該設備還包括通信介面 23，用於處理器 22 與外部設備之間的通信。記憶體 21 可能包含高速 RAM 記憶體，也可能還包括非易失性記憶體（non-volatile memory），例如至少一個磁碟記憶體。

如果記憶體 21、處理器 22 和通信介面 23 獨立實現，則記憶體 21、處理器 22 和通信介面 23 可以通過匯流排相互連接並完成相互間的通信。匯流排可以是工業標準架構（ISA，Industry Standard Architecture）匯流排、外部設備互連（PCI，Peripheral Component）匯流排或擴展工業標準架構（EISA，Extended Industry Standard Component）匯流排等。匯流排可以分為位址匯流排、資料匯流排、控制匯流排等。為便於表示，圖 6 中僅用一條粗線表示，但並不表示僅有一根匯流排或一種類型的匯流排。

可選的，在具體實現上，如果記憶體 21、處理器 22 及通信介面 23 集成在一塊晶片上，則記憶體 21、處理器 22 及通信介面 23 可以通過內部介面完成相互間的通信。

在本說明書的描述中，參考術語“一個實施例”、“一些實施例”、“示例”、“具體示例”、或“一些示

例”等的描述意指結合該實施例或示例描述的具體特徵、結構、材料或者特點包含于本發明的至少一個實施例或示例中。而且，描述的具體特徵、結構、材料或者特點可以在任一個或多個實施例或示例中以合適的方式結合。此外，在不相互矛盾的情況下，本領域的技術人員可以將本說明書中描述的不同實施例或示例以及不同實施例或示例的特徵進行結合和組合。

此外，術語“第一”、“第二”僅用於描述目的，而不能理解為指示或暗示相對重要性或者隱含指明所指示的技術特徵的數量。由此，限定有“第一”、“第二”的特徵可以明示或隱含地包括至少一個該特徵。在本發明的描述中，“多個”的含義是兩個或兩個以上，除非另有明確具體的限定。

流程圖中或在此以其他方式描述的任何過程或方法描述可以被理解為，表示包括一個或更多個用於實現特定邏輯功能或過程的步驟的可執行指令的代碼的模組、片段或部分，並且本發明的優選實施方式的範圍包括另外的實現，其中可以不按所示出或討論的順序，包括根據所涉及的功能按基本同時的方式或按相反的順序，來執行功能，這應被本發明的實施例所屬技術領域的技術人員所理解。

在流程圖中表示或在此以其他方式描述的邏輯和/或步驟，例如，可以被認為是用於實現邏輯功能的可執行指令的定序列表，可以具體實現在任何電腦可讀介質中，以供指令執行系統、裝置或設備（如基於電腦的系統、包括處理器的系統或其他可以從指令執行系統、裝置或設備取指令並執行指令的系統）使用，或結合這些指令執行系統、裝置或設備而使用。

就本說明書而言，“電腦可讀介質”可以是任何可以包含、存儲、通信、傳播或傳輸程式以供指令執行系統、裝置或設備或結合這些指令執行系統、裝置或設備而使用的裝置。

本發明實施例的電腦可讀介質可以是電腦可讀信號介質或者電腦可讀存儲介質或者是上述兩者的任意組合。電腦可讀存儲介質的更具體的示例至少（非窮盡性列表）包括以下：具有一個或多個佈線的電連接部（電子裝置），可携式電腦盤盒（磁裝置），隨機存取記憶體（RAM），唯讀記憶體（ROM），可擦除可編輯唯讀記憶體（EPROM 或閃速記憶體），光纖裝置，以及可携式唯讀記憶體（CDROM）。另外，電腦可讀存儲介質甚至可以是可在其上列印程式的紙或其他合適的介質，因為可以例如通過對紙或其他介質進行光學掃描，接著進行編輯、解譯或必要時以其他合適方式進行處理來以電子方式獲得程式，然後將其存儲在電腦記憶體中。

在本發明實施例中，電腦可讀信號介質可以包括在基帶中或者作為載波一部分傳播的資料信號，其中承載了電腦可讀的程式碼。這種傳播的資料信號可以採用多種形式，包括但不限於電磁信號、光信號或上述的任意合適的組合。電腦可讀的信號介質還可以是電腦可讀存儲介質以外的任何電腦可讀介質，該電腦可讀介質可以發送、傳播或者傳輸用於指令執行系統、輸入法或者器件使用或者與其結合使用的程式。電腦可讀介質上包含的程式碼可以用任何適當的介質傳輸，包括但不限於：無線、電線、光纜、射頻（Radio Frequency，RF）等等，或者上述的任意合適的組合。

應當理解，本發明的各部分可以用硬體、軟體、固件或它們的組合來實現。在上述實施方式中，多個步驟或方法可以用存儲在記憶體中且由合適的指令執行系統執行的軟體或固件來實現。例如，如果用硬體來實現，和在另一實施方式中一樣，可用本領域公知的下列技術中的任一項或他們的組合來實現：具有用於對資料信號實現邏輯功能的邏輯門電路的離散邏輯電路，具有合適的組合邏輯門電路的專用積體電路，可程式設計閘陣列（PGA），現場可程式設計閘陣列（FPGA）等。

本技術領域的普通技術人員可以理解實現上述實施例方法攜帶的全部或部分步驟是可以通過程式來指令相關的硬體完成，的程式可以存儲於一種電腦可讀存儲介質中，該程式在執行時，包括方法實施例的步驟之一或其組合。

此外，在本發明各個實施例中的各功能單元可以集成在一個處理模組中，也可以是各個單元單獨物理存在，也可以兩個或兩個以上單元集成在一個模組中。上述集成的模組既可以採用硬體的形式實現，也可以採用軟體功能模組的形式實現。集成的模組如果以軟體功能模組的形式實現並作為獨立的產品銷售或使用時，也可以存儲在一個電腦可讀存儲介質中。存儲介質可以是唯讀記憶體，磁片或光碟等。

以上，僅為本發明的具體實施方式，但本發明的保護範圍並不局限於此，任何熟悉本技術領域的技術人員在本發明揭露的技術範圍內，可輕易想到其各種變化或替換，這些都應涵蓋在本發明的保護範圍之內。因此，本發明的保護範圍應以權利要求的保護範圍為准。

優化網路成本

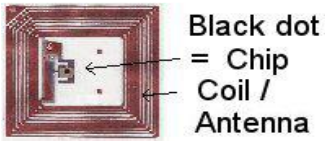
為了支撐 BACCHUS 的運作，優化使用網路的成本非常重要。

每個單獨的供應鏈在以太坊上使用各自的交易 和合約配置以在物件於供應鏈上移動時處理資料。在以太坊上進行交易已變得相當昂貴，而我們的自訂的這套區塊鏈解決了這個問題。 BACCHUS 使用的主要交易網路是 BACCHUS 區塊鏈，這是以太坊的一個私人版本，而不是用以太坊為主。注意“私人”在這裡可能具有潛在的誤導性，因為 這個網路是公開的，且可以被任何人接入。這個術語僅用於區分 BACCHUS 區塊鏈和以太坊主網路。所有與 BACCHUS 協議有關的智慧合約將在 BACCHUS 區塊 鏈上運行，為了進一步認證會週期性地複製到以太坊主網路上。 酒神代幣一開始的眾籌會在以太坊區塊鏈上進行，BACCHUS 區塊鏈建成之後代幣會被轉移至 BACCHUS 網路。

NFC 驗證部份

為了構建整個系統，需要有一堆軟件和硬件來實現它; 例如，構建數據庫服務器和認證應用程序所需要的軟件，應縮小 NFC 標籤和支持 NFC 的智能手機等硬件，以便將這些數據庫和應用程序集成到硬件中，使整個系統運行得以實現。

經過多年的發展，13.56MHz 以下的 RFID 技術已相對成熟，目前業界最關注的是超高頻 RFID，它在860MHz～960MHz 頻率下工作，具有支持快速讀寫、多目標識別、非視距識別、移動定位及長期跟蹤管理、作用距離遠（通常是 3m～10m）和通信速度快等優點。超高頻 RFID 技術已成為業界發展的熱點，超高頻無源 RFID 標籤和系統應用也因此得以迅猛增長。

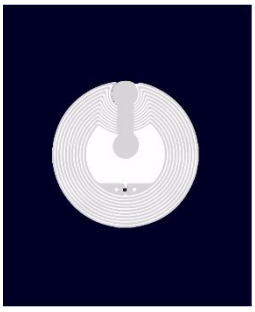


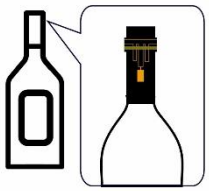
在現今市場上，就只有Android平台平台可以兼容NFC技術。這意味著所有支持NFC的智能手機實際上都在運行Android操作系統，而不是Apple的IOS，所以我們需要的是模擬整個BAC，就是採用NFC功能的智能手機，以便利用硬件NFC技術的應用， 因此，可以在這款支持NFC的智能手機上構建和運行。

事實上，市場上有114款支持NFC的智能手機。但是我們應該如何確定哪種智能手機最適合？該以什麼標準去選擇一部NAS手機？這裡有5大要點去滿足。首先，手機應植入最新的NFC芯片和控制器型號。其次，NFC的芯片需與市場上的大多數NFC裝置兼容。第三，智能手機必須在2011年秋季之後發布，這是獨一無二的通用NFC標籤 - NTAG203的發布季節。第四，所選的支援NFC的智能手機必須與通用NFC標籤兼容 - NTAG 203和其他2型NFC標籤。第五，智能手機必須具備基本的技術要求，如使用四核處理器植入，至少在Android 4.3（Jelly Bean）上運行，內置Wi-Fi和藍牙等。

然後我們縮小範圍，選擇了三星最新發佈的手機 - 三星Galaxy Note 8（型號SM-N9500）作為主要支持NFC的設備和我們建立NFC相關的所需智能手機，因為Note 8符合所有標準 BAC所需要的。三星Galaxy Note 8是Galaxy Note系列的最新型號，它支持NFC，其NFC控制器也兼容恩浦NTAG203，可滿足所有剩餘要求。

NFC智能手機所需的NFC控制器芯片將是Broadcom BCM20793S。為了與NFC標籤兼容，NFC控制器芯片支持Type 2 NFC標籤。為了與NFC標籤兼容，NFC控制器芯片支持Type 2 NFC標籤。雖然還有一些支持NFC的智能手機符合BAC的標準，但不及三星Galaxy Note 8那樣適合。





NFC標籤是不涉及電力而且需要被動開啟的，包括NFC PCB芯片和基板中的天線。標籤具有相對較低的RF（射頻等於13.56MHz），對於強烈的交互而言太弱。當暴露於具有更強大RF場的“啟動器”（讀取器，寫入器或智能手機）時，標籤的RF場會被加強，然後可以進行讀取或寫入。大多數NFC標籤包含標準化的NDEF訊息，這些訊息在屏幕上進行解析和顯示，格式化為易於閱讀的內容。NDEF嚴格來說是一種訊息格式，是NFC論壇兼容標籤和設備以及標籤的通用數據格式

這裡有一組五個選擇標準，以便縮小範圍為整個BAC選擇最合適的NFC標籤，1）與所選NFC智能手機的

NFC控制器芯片的兼容性，2）應用標籤的材料，3）標籤尺寸，4）標籤存儲器容量，以及5）NFC標籤的寫入耐久性。還有一些小的標準，即價格和購買的便利性。

關於為BAC選擇的NFC智能手機的兼容性，我們選擇用Galaxy Note 8， 該智能手機的NFC控制器芯片是前面提到的Broadcom BCM20793S。（對於我們帶到美國以外的地區）基於NFC論壇類型標籤平台，NFC標準，產品存在及其規格。（請參閱附錄2），我們意識到那些帶有NFC論壇類型標籤平台 - 類型2標籤的NFC標籤將適合併兼容植入三星Galaxy Note 8的NFC控制器芯片。簡而言之，我們的目標NFC標籤僅限於“Type 2 Tag”組。

基於第一個標準，我們已經提出了這樣一個事實，即只選擇2型標籤進行進一步篩選，即Mifare Ultralight（UL）， NTAG203，Mifare Ultralight C，Kovlo 2Kb RFID等

對於標籤物理尺寸，如果這些標籤可以是圓形並且直徑約為25-35mm，厚度最多為0.5mm，對於0.75升的葡萄酒則更好。雖然寫標籤存儲器容量應該更好144個字節（對於類型2標籤，只有48字節或144字節這兩種選擇），寫耐久性應至少10000次。通過整合上述所有標準，選擇並購買了四個NFC標籤，這些標籤全部由恩智浦半導體生產，並從上海和深圳購買，其中三個屬於第二類性質，一個屬於第七類性質。對於這三個Type-2 NFC標籤，其中兩個實際上是NFC鐵氧體標籤，這令NFC標籤使得整個BAC能夠在金屬環境下工作和操作，例如圍繞大多數瓶頸的箔包裝，這些都是在 改進階段，以便在可用性研究後進一步改進BAC。

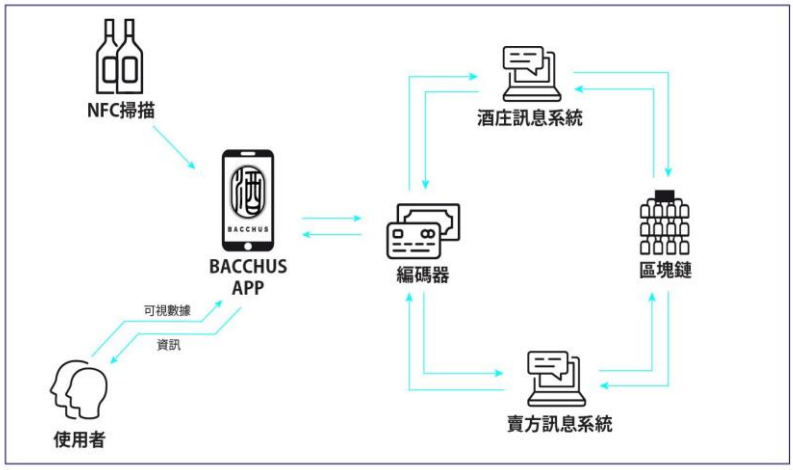
NTAG203是世界上最通用的NFC標籤，它與大多數支持NFC的智能手機或設備的型號兼容並支持，這很適合我們開發的BAC。

對於Mifare Ultralight（UL）C，它是針對有限使用應用而開發和設計的，例如身份驗證和NFC論壇標籤類型2應用程序，這是一種更安全的Mifare Ultralight（UL）版本，具有3DES加密功能。根據ISO / IEC 14443的智能防衝突功能允許同時在現場操作多張卡，防衝突算法獨立選出每張卡並確保正確執行所選卡的交易執行，而不會因現場其他卡而導致數據損壞。因此，不會同時讀取2個NFC標籤。

對於Mifare Class 1K，MF1ICS50專為簡單集成和用戶便利而設計，可以在不到100毫秒的時間內處理完整的票務交易。在進行一系列針對不同情況，用戶案例和標籤類別的測試後，將進一步確定最合適的BAC。而出於控制實驗的目的，將購買該標籤以確定NFC控制器芯片是否可以與該Type-7標籤兼容。

系統設計

下圖是BAC的一般操作結構。 對於由葡萄酒生產商獨家擁有的基於網絡的葡萄酒數據庫，主要有兩個信息系統模塊，1）生產者信息系統 和 2）葡萄酒賣家信息系統。前者實際上是一個由葡萄酒細節，用戶反饋，葡萄酒評論等組成的系統，它只會存儲有關葡萄酒的信息，葡萄酒製造商將在其中輸入信息來更新系統，作為回報，該系統可以為釀酒師提供有關葡萄酒的信息，以進一步改進產品和更好的產品管理實踐。而後者雖然包括特定葡萄酒產品的交易記錄，供應鏈合作夥伴的詳細信息，可能是釀酒商的分銷商，批發商和經銷商。但項目的細節著重於釀酒師和特定供應鏈之間的美酒的銷售。然後，兩個模塊將通過局域網（LAN）連接和集成在一起，形成一個Microsoft SQL數據庫2012，這正是特定釀酒師擁有的基於網絡的美酒數據庫。網絡數據庫實際上與區塊鏈連接，這是一個葡萄酒區塊鏈數據庫與在支持NFC的設備上運行的應用程序通信的平台。



在用戶端，美酒消費者只需在零售點使用支持 NFC 的智能手機上運行執行特定葡萄酒認證的步驟，或者當葡萄酒供應鏈中的下一個節點接受葡萄酒時，通過開放的 ScanWINE。供應鏈合作夥伴還可以打開在其 NFC 設備上運行的 ScanWINE，使用 NFC 技術掃描附在葡萄酒瓶頸上的 NFC 標籤。同時，NFC 標籤基於存儲在標籤中的 WID（Wine ID 是標籤值的基本元素）作為橋接來連接應用程序和後端數據庫。通過 WID，特定的葡萄酒記錄可以由應用程序定位和引用，對於該應用程序，通信，例如從應用程序發送的基於掃描的 WID 的特定葡萄酒記錄信息的請求以及從後端返回的葡萄酒記錄 wine 數據庫，可以使用 JSON 格式通過 HTTP 與 Web 服務平台下的應用程序控制器構建，使用該地區的 ISP 提供的 Wi-Fi 或 GPRS。

每當美酒在供應鏈中生產併轉移時，美酒記錄如交易記錄便會自動同時更新於酒瓶頸上的標籤。當供應鏈合作夥伴使用 NFC 裝置掃瞄便可以立即看到美酒最新資訊。例如，當供應鏈合作夥伴採用 BAC 並使用支持 NFC 的智能手機掃描 NFC 標籤，同時他們接受釀酒師的葡萄酒情報時，設備上運行的 ScanWINE 應用程序將連接到後端的身份驗證控制器 – 由釀酒師擁有的最後端美酒數據庫，交易記錄將自動更新。

BAC 的系統結構流程圖顯示了沿特定葡萄酒供應鏈。事實上，BAC 包括五個重要的控制器來執行不同的功能，1）供應鏈信息控制器，2）交易歷史控制器，3）認證控制器，4）酒譜系統控制器，和5）不成功的記錄控制器， 都是在後端數據庫中設置的。

供應鏈信息控制器負責收集和管理公司信息，與釀酒師過去的合作項目記錄以及供應鏈合作夥伴持有的葡萄酒。例如，當整個供應鏈中的釀酒師發送這些葡萄酒產品並且後續供應鏈合作夥伴通過閱讀 NFC 接受時，可以同時更新協作項目中涉及的葡萄酒產品組合的信息。 連接標籤，ScanWINE 在其支持 NFC 的設備上運行。在第一筆交易記錄發送到 Wine Pedigree Server 之前，這些信息應由供應鏈合作夥伴預先註冊並由主辦公司進行驗證。

交易歷史記錄控制器對葡萄酒譜系至關重要，因為它們構成了供應鏈特定節點中葡萄酒產品歷史的全貌，並將收集和管理所有節點交易歷史記錄，包括葡萄酒信息和發布記錄。 釀酒師和那些交易記錄，甚至是後續供應鏈合作夥伴提供的銷售記錄，它還構成了在懷疑偽造品出現時追查問題的基礎。隨著葡萄酒產品沿著供應鏈移動，每個供應鏈合作夥伴應該使用他們的 NFC 設備讀取貼在葡萄酒瓶頸上的 NFC 標籤，該設備應該通過 HTTP 與交易歷史控制器通過 BAC 連接到互聯網，以便每個節點都可以更新。反過來，存儲在釀酒師葡萄酒數據庫中的匯總信息可以自動更新，根據該數據，釀酒師不能手動修改交易記錄，這也是 BAC 的安全考慮因素。

驗證控制器分別從交易歷史控制器和供應鏈信息控制器驗證那些節點交易歷史和那些更新的供應鏈信息。認證控制器篩選出供應鏈中的可疑活動; 例如葡萄酒上的 NFC 標籤不是原始的會被發現。然後將篩選的記錄發送到 Bacchus 進行存儲並在 Wine Database Layer 中進行查看。對於那些無法通過認證控制器並被視為可疑葡萄酒假冒的葡萄酒記錄，當“WID”（標籤的組成部分）時，該葡萄酒的“葡萄酒狀態”將從“有效”變為“無效”。 存儲在由供應鏈合作夥伴或葡萄酒消費者掃描的 NFC 標籤中的價值被發現與釀酒師擁有的後端數據庫中無法比擬，相關的葡萄酒記錄將被發送到不成功的記錄控制器進行存儲， 由相應釀酒師共享的其他供應鏈合作夥伴進一步審查和未來參考。供應鏈合作夥伴還將負責向釀酒師報告此類案件，並將“無效”葡萄酒送回原釀酒師，因為擔心懷疑的葡萄酒假冒產品仍將存在於市場中。儘管如此，存儲在不成功記錄控制器中的“無效”葡萄酒記錄也將被分享給供應鏈信息控制器以更新特定葡萄酒供應鏈下的記錄，報告疑似葡萄酒假冒案例，以供釀酒師進一步記錄和參考。

供應鏈合作夥伴還可以通過向 Bacchus 存儲合法葡萄酒記錄的請求來驗證從製造點到整個供應鏈的前任所有者的部分美酒酒譜系，而葡萄酒譜系控制器又從交易歷史中檢索交易記錄，然後從交易歷史控制器檢索交易記錄以及從供應鏈信息控制器獲取公司信息，以從 Bacchus 生成所需的譜系。他們應該拒絕任何涉及服務器的可疑部分血統的葡萄酒。此外，葡萄酒譜系控制器和認證控制器也負責協同工作，其中前者存儲部分合法美酒記錄，而後者包含一系列用於驗證美酒記錄的業務邏輯，於生成完整的葡萄酒譜系，接收來自 BAC 的這些用戶的請求並以 JSON 數據格式將其響應到其 NFC 設備以傳輸防偽值。當葡萄酒消費者通過使用 BAC 對真正的葡萄酒感到滿意並且已經確認付款時，BAC 將自動將銷售記錄更新到交易歷史記錄控制器，隨後將其發送到 Bacchus。此後，標籤將不再可行，並且在銷售記錄更新後使用相同的葡萄酒檢測到任何進一步的閱讀過程將被視為可疑。

潛在的系統攻擊

Sybil 和 outsourcing 攻擊

理論上，創建多個（Sybil）身份將允許惡意節點假裝存儲相同數據的更多副本，但是只需要存儲一次並在需要證明他們提供服務時從存儲位置快速獲取它們。通過建立與應用於圖形的 Filecoin 白板中引入的複制證據類似的機制來解決此問題，同時考慮到 OriginTrail 中的數據是公共設計的。有了這些先決條件，加密就被用來證明復製而不是用來模糊數據 - 在將數據輸入系統之前，由數據創建者加密他們需要隱藏的輸入信息。因此，OriginTrail 中的每個節點都需要定期證明它們是存儲圖的特定編碼，其中每個編碼是可區分的不可壓縮的。編碼功能必須是可緩慢的 PRP（偽隨機使用密碼塊鏈接的排列）：

- 足夠慢，以便很容易區分誠實和時間之間的時間惡意響應，因為攻擊者需要先加密然後傳輸通過網絡。
- 在運行時間方面可任意調整，運行於，在哪裡每個圖元素在繼續下一個之前加密的次數（順序加密，其中輸入每個加密元素的結果加密下一個元素）並且是圖中元素的數量。
- 可公開驗證，這是通過使用基於的唯一加密密鑰實現的點公鑰
- 具有快速反向解碼功能，可以快速完成解碼（使用並行化）

51%的攻擊

51%的攻擊通常被定義為在分散系統中控制絕大部分（至少 51%）功率的能力（即以太坊中的散列能力），然後授予操縱數據的能力。就 OriginTrail 中的數據完整性而言，這樣的攻擊不是問題，因為對於每個圖，通過將從 DH 節點提取的散列與區塊鏈層中的加密指紋進行比較，確定性地可驗證數據未被改變。另外，DH 節點被激勵以其適當的形式存儲，以便能夠證明存儲和接收補償。如果節點未能提供可檢索性/複製的證據，則數據創建者可以很容易地用系統中的另一個節點替換它。

拜占庭式容錯

拜占庭故障被定義為由節點引起的故障，通過不可用或具有不正確的數據響應來提供供應鏈圖形數據。不正確的響應被定義為無法通過 OriginTrail 的區塊鏈層上的適當散列指紋驗證的響應。由於數據管理共識是在數據持有者節點中復製圖數據（其中是不同供應鏈數據創建者節點的數量），因此交付所涉及節點的數量顯著減少了傳遞所請求數據的失敗概率。當 DH 節點未能在所需的時間段內提供服務時，數據分發協議用於查找新的候選節點並複制數據以在網絡上保持所需的副本數量。

Eclipse 攻擊

通過使所有出站連接到達惡意節點來將節點或多個節點與網絡隔離，稱為 eclipse 攻擊。這可以通過在 Kademlia 中使用公鑰哈希作為節點 ID 來解決。為了捕獲網絡上的節點，攻擊者必須生成密鑰對，這些密鑰對將自己在 Kademlia 中更靠近目標節點定位，而不是最近的非惡意鄰居，並在新節點與更近的 ID 連接時保持該位置。隨著越來越多的節點被引入網絡，這個問題越來越複雜，並且本質上呈現出一種工作量證明問題。

人質數據攻擊

惡意節點可能拒絕提供某些圖表數據，以便勒索數據所有者以獲取其他令牌。通過在多個節點上複製圖數據來減輕這種可能性。

IV. 項目總結

BACCHUS 酒神的進一步可能改進:

事實上，BAC 的開發實際上只是基於一個釀酒師或釀酒廠，更不用說將有大量類似的 ScanWINE 應用程序加載到消費者的 NFC 智能手機上，如果有更多的個體釀酒師不希望利用 BAC，情況將很混亂，使 BAC 無效。因此，如果有任何中央葡萄酒數據庫，甚至是由政府或任何知名組織開發和建造的中央酒系統，例如香港葡萄酒商會（HKWMCC）促進優質葡萄酒的開發，會更好產品，存儲在中央數據庫中來回輸入和出口的葡萄酒產品的所有標準化葡萄酒記錄，並允許供應鏈的所有節點更新供應鏈上關於可信度，有效性的葡萄酒譜系。存儲的所有葡萄酒記錄的準確性，中央葡萄酒數據庫，甚至提供給葡萄酒消費者或經銷商的交易前使用的應用程序。

BACCHUS 的想法應該擴大，而不是僅僅基於一個釀酒師，但是它們的集群或集中式數據庫應該由政府，一些專業的葡萄酒組織或一組葡萄酒品牌的戰略聯盟帶頭建立，能有更好提供的效率，有效性和防偽價值，而不是讓美酒消費者和佳釀供應鏈合作夥伴在每次需要處理其他品牌的酒產品時下載新的應用程序。

不可否認，將 BAC 視為世界上最安全的防偽系統尚不成熟甚至為時尚早;然而，這個想法是 BAC 可以為美酒行業增加一層安全保障。每個人都知道，標籤技術的組合肯定比僅將其中一種應用於酒行業更加安全和復雜。總是很好的說 BAC 只是基於 NFC 技術，，但現實是包括更多的標籤或其他防偽技術可以使 BAC 更多為用戶提供安全和可信賴的功能，例如將二維碼或條形碼掃描功能添加到 Bacchus App 中。我們還應該推薦那些美酒品牌除 NFC 標籤外還應使用代碼，以便吸引最多的客戶。

工程師正在設計和構建更多有用的功能。開發計畫包括：

- 完全上鏈的的應用程式商店，構建應用程式並於無形中支援所有的加密貨幣。
- BACS 完全從 ERC-20 代幣中分離出去，擁有自己的私有鏈。
- 將收藏証書上鏈，令每一收藏酒都在區塊鏈上找到它的身份證。
- 酒神幣交易、商城和酒的身份證的智能合約可以互相溝通。
- 商城支援以太坊經典和比特幣。
- 適用於 Android 和 iOS 的手機商城，錢包，手機端區塊鏈追蹤器。

ACKNOWLEDGMENT

This research is partially funded by the Institute for Integrated and Intelligent Systems, Griffith University.

REFERENCES

[1] P. Schmitt, "How much fake fine wine is in the market?," https://www.thedrinksbusiness.com/2016/12/how-much-fake-fine-wineis-in-the-market/, 2016.

[2]The Billionaire's Vinegar: The Mystery of the World's Most Expensive Bottle of Wine https://www.amazon.com/Billionaires-Vinegar-Mystery-Worlds-Expensive/dp/0307338789

[3]6,000 BOTTLES OF FAKE WINE BUSTED IN CHINA https://www.thedrinksbusiness.com/2017/08/6000-bottles-of-fake-wine-busted-in-china/

[4] GS1, "Wine Supply Chain Traceability: GS1 Application Guideline," http://www.gs1.org/docs/traceability/GS1 wine traceability.pdf, 2015, pp. 1–28.

[5] I. Expsito, J. A. Gay-Fernndez, and I. Cuias, "A Complete Traceability System for a Wine Supply Chain Using Radio-Frequency Identification and Wireless Sensor Networks [Wireless Corner]," in IEEE Antennas and Propagation Magazine, vol. 55(2), 2013, pp. 255–267.

[6] M. G. C. A. Cimino and F. Marcelloni, "Enabling Traceability in the Wine Supply Chain," in Methodologies and Technologies for Networked Enterprises: ArtDeco: Adaptive Infrastructures for Decentralised Organisations, Springer Berlin Heidelberg, 2012, pp. 397–412.

[5] K. Vukatana, K. Sevrani, and E. Hoxha, "Wine Traceability: A Data Model and Prototype in Albanian Context," in Foods Journal, vol. 5(1), http://www.mdpi.com/2304-8158/5/1/11, 2016.

[6] IBM Institute for Business Value, "Trust in trade- toward stronger supply chains," IBM Corp., 2016.

[7] K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the IoTs," in IEEE Access, Special section on the plethora of Research in IoT, 2016, pp. 2292–2303.

[8] K. Biswas and V. Muthukkumarasamy, "Securing Smart Cities Using Blockchain Technology," in IEEE 14th International Conference on Smart City, 2016, pp. 1392–1393.

[9] S. Nakamoto, "Bitcoin: a peer-to-peer electronic cash system," http://bitcoin.org/bitcoin.pdf, 2008.

[10] G. Greenspan, "Multichain private blockchain," White paper, http://www.multichain.com/download/MultiChain-White-Paper.pdf, 2015, pp. 1–17.

[11] D. Gilbert, "Bitcoins Big Problem: Transaction Delays Renew Blockchain Debate," in International Business Times, http://www.ibtimes.com/bitcoins-big-problem-transaction-delays-renewblockchain-debate-2330143, 2016.

[12]Euromonitor International, Illegal Alcohol: Trends & Challenges, October 2013.

OECD Task Force on Charting Illicit Trade (TF-CIT), Sub-Group on Alcoholic Beverages Stakeholders' contribution to the Assessment of the Size, Impacts and Drivers of Illicit Trade in Alcohol, February 2014, p. 3.

[13]Stéphane Dubois, "Lecture géopolitique d'un produit alimentaire mondialisé: le vin" [Geopolitical reading of a globalized food product: wine], Revue internationale et stratégique 1/ 2013 (no. 89), p. 22. 5 Ibidem, p. 26.

[14]Scheherazade Daneshkhu, "China overtakes France as biggest consumer of red wine", Financial Times, 29

January 2014.

[15] 网贷天眼 APP, “中国银行推五粮液限量酒另类理财产品”, https://www.p2peye.com/thread-2082174-1-1.html

[16]王邦華, “中國收藏酒名錄”

酒神
BACCHUS

附件: 專利

香港特別行政區政府知識產權署專利註冊處
Patents Registry, Intellectual Property Department
The Government of the Hong Kong Special Administrative Region

專利註冊紀錄冊 REGISTER OF PATENTS
註冊紀錄冊記項 REGISTER ENTRY

專利編號 Patent No.	:HK1246582
類別 Type	:短期專利 Short-term Patent
申請編號 Application No.	:18107087.9
提交日期 Filing date	:30.05.2018
法律程序所用語文 Language of Proceedings	:Ch
發表編號 Publication No.	:HK1246582
專利說明書首次發表日期 Date of first publication	:07.09.2018/A

發明名稱 Title
產品信息錄入與訪問的方法、裝置、存儲介質及終端設備
PRODUCT INFORMATION RECORD AND ACCESS METHOD, DEVICE, STORAGE MEDIUM AND TERMINAL DEVICE

申請人 Applicant
何泓達
香港
新界大埔

發明人 Inventor
何泓達
香港
新界大埔

分類 Classified to :G06Q

送達地址 Address for Service
香港知識產權代理有限公司
香港新界
白石角香港科學園第三期
科技大道西12號2樓230室

代理人地址 Agent's Address
香港新界白石角香港科學園第三期科技大道西12號2樓230室

批予專利日期 Patent grant date :07.09.2018

專利所有人 Proprietor
何泓達
香港
新界大埔

酒神
BACCHUS

附件　收藏家協會證書，及中國名酒收藏 2012

五粮液建厂六十周年特别酿造
“五粮液酒厂六十年酿神封藏限量酒”
收藏证书

“五粮液酒厂六十年酿神封藏限量酒”是五粮液股份有限公司集中优势资源倾力打造的一款战略性高端旗舰酒，是一款主打人文历史和投资收藏理念的顶级收藏白酒。

“五粮液酒厂六十年酿神封藏限量酒”净含量1000毫升，酒精度数为69度原浆酒。“五粮液酒厂六十年酿神封藏限量酒”依托五粮液股份有限公司特有的酿造工艺和品牌内涵，以五粮液建厂六十年和缅怀五粮液历史上最重要的三大名人为产品历史背景，以国酒大师的特别监制为酿造之保障，以国家工艺美术大师特别艺术创作的产品组合为载体，通过先进的白酒投资收藏营销理念推广，其全新的创意核心和价值核心必将支撑起中国白酒界的第一号投资收藏型白酒。

“中国的五粮液，世界的五粮液”，五粮液素有中国白酒大王的美誉，在国人的心目中也是顶级白酒的代名词，其品牌价值连续15年保持中国白酒品牌价值之冠，这样一个白酒王国的巨人，倾力打造了这一款惊世之作。“五粮液酒厂六十年酿神封藏限量酒”的影响力已不仅仅局限在传统白酒行业，其投资收藏的创新理念更是开创了弘扬中国收藏文化的新思路、新渠道，新市场。它既是一款可以饮用的极品白酒，又是一款奉献给时代精英、时代主角的投资理财产品，这种收藏界与高端白酒联姻的价值创新，将引领着中国顶级白酒进入收藏酒的元年，代表着中国传统名酒的一种人文及价值回归。同时，也是一次将中国传统的白酒文化推动到世界级奢侈品收藏领域的文化盛事。

宜宾五粮液股份有限公司“五粮液酒厂六十年酿神封藏限量酒”立意深远，品质卓越，是民族白酒工业的骄傲和代表，具有极高的的品鉴价值，收藏价值，历史文化价值，值得永久鉴藏。

特颁此证，荣耀共赏！

宜宾五粮液股份有限公司“五粮液酒厂六十年酿神封藏限量酒”全球限量3000瓶。

宜宾五粮液股份有限公司董事长
签名：

宜宾五粮液股份有限公司出品（章）
2011年2月28日

中国收藏家协会

五粮液建厂六十周年特别酿造
“五粮液酒厂六十年酿神封藏限量酒”
收藏证书

在五粮液建厂六十年之际，缅怀五粮液历史上最重要的三大名人：杨惠泉、邓子均和范玉平，由宜宾五粮液股份有限公司集中优势资源倾力打造的一款战略性高端旗舰白酒，是一款主打人文历史和投资收藏理念的“顶级收藏白酒”——“五粮液酒厂六十年酿神封藏限量酒”首次向全球限量发行。

“五粮液酒厂六十年酿神封藏限量酒”净含量高达1000毫升，酒精度数为69度原浆酒。“五粮液酒厂六十年酿神封藏限量酒”依托五粮液股份有限公司特有的酿造工艺和品牌内涵，以五粮液建厂六十年和缅怀五粮液历史上最重要的三大名人为产品历史背景，以国酒大师的特别监制为酿造之保障，以国家工艺美术大师特别艺术创作的产品组合为载体；通过先进的白酒投资收藏营销理念推广，其全新的创意核心和价值核心必将支撑起中国白酒界的第一号投资收藏型白酒。

五粮液素有中国白酒大王的美誉，在世界范围内也是顶级白酒的文化符号之一，其品牌价值连续15年保持中国白酒品牌价值之冠，作为白酒大王五粮液倾力打造的这款投资收藏酒，堪称五粮液六十年绝版神酿。“五粮液酒厂六十年酿神封藏限量酒”的影响力已不仅仅局限在传统白酒行业，其投资收藏的创新理念更是开创了弘扬中国收藏文化的新渠道，新市场。这种收藏界与高端白酒界联姻的价值创新，将引领着中国顶级白酒进入收藏酒的元年，代表着中国传统名酒的一种人文及价值回归。

为确保收藏者投资收藏的价值，发行数量的真实，可靠，以及发行活动的严肃，权威，每瓶“五粮液酒厂六十年酿神封藏限量酒”在瓶底和防伪证书上都有一致的唯一数字编号，还均配有五粮液股份有限公司董事长唐桥签名和加盖公章的专用防伪收藏证书，限量发行公证书，各类质检报告，以及五粮液系列酒特有的专用防伪标识。

经中国收藏家协会鉴证，宜宾五粮液股份有限公司“五粮液酒厂六十年酿神封藏限量酒”，立意深远，品质卓越，既是一款可以饮用的极品白酒，又是一款奉献给时代精英、时代主角的投资理财产品，它将中国传统白酒文化推动到世界级奢侈品收藏领域，是民族白酒工业的骄傲和代表，具有极高的的品鉴价值，收藏价值，历史文化价值，值得永久鉴藏。

特颁此证，荣耀共赏！

宜宾五粮液股份有限公司“五粮液酒厂六十年酿神封藏限量酒”全球限量3000瓶。

中国收藏家协会会长
签名：

中国收藏家协会
2010年12月31日

1100014197