Bit Gold

Nick Szabo[1]

December 29, 2005

A long time ago I hit upon the idea of bit gold. The problem, in a nutshell, is that our money currently depends on trust in a third party for its value. As many inflationary and hyperinflationary episodes during the 20th century demonstrated, this is not an ideal state of affairs. Similarly, private bank note issue, while it had various advantages as well as disadvantages, similarly depended on a trusted third party.

Precious metals and collectibles have an unforgeable scarcity due to the costliness of their creation. This once provided money the value of which was largely independent of any trusted third party. Precious metals have problems, however. It's too costly to assay metals repeatedly for common transactions. Thus a trusted third party (usually associated with a tax collector who accepted the coins as payment) was invoked to stamp a standard amount of the metal into a coin. Transporting large values of metal can be a rather insecure affair, as the British found when transporting gold across a U-boat infested Atlantic to Canada during World War I to support their gold standard. What's worse, you can't pay online with metal.

Thus, it would be very nice if there were a protocol whereby unforgeably costly bits could be created online with minimal dependence on trusted third parties, and then securely stored, transferred, and assayed with similar minimal trust. Bit gold.

My proposal for bit gold is based on computing a string of bits from a string of challenge bits, using functions called variously "client puzzle function," "proof of work function," or "secure benchmark function." The resulting string of bits is the proof of work. Where a one-way function is prohibitively difficult to compute backwards, a secure benchmark function ideally comes with a specific cost, measured in compute cycles, to compute backwards.

Here are the main steps of the bit gold system that I envision:

A public string of bits, the "challenge string," is created (see step 5).

Alice on her computer generates the proof of work string from the challenge bits using a benchmark function.

The proof of work is securely timestamped. This should work in a distributed fashion, with several different timestamp services so that no particular timestamp service need be substantially relied on.

Alice adds the challenge string and the timestamped proof of work string to a distributed property title registry for bit gold. Here, too, no single server is substantially relied on to properly operate the registry.

The last-created string of bit gold provides the challenge bits for the next-created string.

---

[1] Nick Szabo，中文尼克・薩博，一個加密社區中人盡皆知的傳奇人物。以其在智能合約和數字貨幣方面的研究而聞名於世，廣泛涉獵於電腦科學、貨幣起源、經濟和法律等諸多領域，同時是電腦科學家、法律學家兼密碼學家。1989 年分別獲得華盛頓大學電腦科學學位和喬治華盛頓大學法學學位，畢業後在弗朗西斯科・馬羅昆大學擔任名譽教授。

To verify that Alice is the owner of a particular string of bit gold, Bob checks the unforgeable chain of title in the bit gold title registry.

To assay the value of a string of bit gold, Bob checks and verifies the challenge bits, the proof of work string, and the timestamp.

Note that Alice's control over her bit gold does not depend on her sole possession of the bits, but rather on her lead position in the unforgeable chain of title (chain of digital signatures) in the title registry.

All of this can be automated by software. The main limits to the security of the scheme are how well trust can be distributed in steps (3) and (4), and the problem of machine architecture which will be discussed below.

Hal Finney has implemented a variant of bit gold called RPOW (Reusable Proofs of Work). This relies on publishing the computer code for the "mint," which runs on a remote tamper-evident computer. The purchaser of of bit gold can then use remote attestation, which Finney calls the transparent server technique, to verify that a particular number of cycles were actually performed.

The main problem with all these schemes is that proof of work schemes depend on computer architecture, not just an abstract mathematics based on an abstract "compute cycle." (I wrote about this obscurely several years ago.) Thus, it might be possible to be a very low cost producer (by several orders of magnitude) and swamp the market with bit gold. However, since bit gold is timestamped, the time created as well as the mathematical difficulty of the work can be automatically proven. From this, it can usually be inferred what the cost of producing during that time period was.

Unlike fungible atoms of gold, but as with collector's items, a large supply during a given time period will drive down the value of those particular items. In this respect "bit gold" acts more like collector's items than like gold. However, the match between this ex post market and the auction determining the initial value might create a very substantial profit for the "bit gold miner" who invents and deploys an optimized computer architecture.

Thus, bit gold will not be fungible based on a simple function of, for example, the length of the string. Instead, to create fungible units dealers will have to combine different-valued pieces of bit gold into larger units of approximately equal value. This is analogous to what many commodity dealers do today to make commodity markets possible. Trust is still distributed because the estimated values of such bundles can be independently verified by many other parties in a largely or entirely automated fashion.

In summary, all money mankind has ever used has been insecure in one way or another. This insecurity has been manifested in a wide variety of ways, from counterfeiting to theft, but the most pernicious of which has probably been inflation. Bit gold may provide us with a money of unprecedented security from these dangers. The potential for initially hidden supply gluts due to hidden innovations in machine architecture is a potential flaw in bit gold, or at least an imperfection which the initial auctions and ex post exchanges of bit gold will have to address.

比特金白皮書

一個基於公共貨幣的自治經濟架構

作者：光明博士 [Bright@utopia.country]，Version 2.1.5

前言：《比特幣白皮書》在開宗立編時，設想了“比特幣：一種點對點的電子現金系統”。事實上，Bitcoin 和區塊鏈技術通過多年的發展，已經部分地實現了這個設想，放眼 50 年後，這個設想將很有可能實現。但是在目前階段，無論是整體性能、可擴展性、交易手續費、跨文化問題、用戶體驗、安全性等多方面，均未達到了民用的標準。比特金是一個比特幣 3.0 形態的產品體系，是實現比特幣思想的全新試驗。

摘要：本文在汲取 Bitcoin 思想和歸納一些淺顯金融規律的基礎上，提出一套邏輯簡單的解決方案，宣導“新金本位制、競爭發行、公共貨幣、去中心化數字資產配置”等方法，並通過技術手段實現了：抵押比特金競爭性地發行各國法幣對應的數字貨幣（恒定幣），從而實現了共識信任底層資產和應用層流通資產，再而真正實現了數字貨幣的價值尺度、流通等價物、貯藏手段、支付仲介的能力，以去中心化智能合約廣泛應用於“價值投資、線上支付、自動清算、商業合約、物權通證化等”等經濟領域。整個嘗試過程，將通過三個大的技術步驟：1、公共貨幣運行平臺；2、數字資產自治架構；3、分佈式經濟架構。

關鍵字：公共貨幣、新金本位制、比特金、通證、良幣驅逐劣幣

1. 背景

我們可能需要一個更先進的經濟系統？

1.1. 法幣

貨幣是人類歷史上最偉大的發明，法幣是現行的貨幣，極大地推進了人類社會文化、政治、經濟、科技各領域的進步。

但是，包含現金、電子支付手段在內的各國法幣系統，以及跨國匯兌體系，其運行機制本質來說都是中心化的。人類曾經使用過的錢都或多或少存在一些不安全機制，比如偽造，盜竊，最致命的可能是通貨膨脹。歷史事實證明，“黨權民賦”的政黨統治體制並不值得人們充分信任。僅就政府壟斷的貨幣發行權而言，政府壟斷貨幣發行權之後，必然存在通過鑄幣稅方式搜刮民脂民膏的衝動，政府掌握貨幣發行權之後失信於民事件歷史上頻繁發生，也是必然要發生的。類似這樣的事件在金融類書籍裏都是查閱證實，我們不便過多和深入例證“由主權中心化發行帶來的法幣問題”，但很明顯，現有的央行式貨幣發行系統和國際匯兌系統，是發行組織的一個偉大政治工具而已，是謀取權利紅利的手段。政府擁有政權紅利已經幾百年了，並且智慧的人類正在尋求一種新的解決方案。

各個國家中央銀行的貨幣政策就是要努力創造並維護這樣的貨幣環境，並且，在更高層面上，不同的國家之間是貨幣政策是獨立的、相互隔離的，且存在複雜的競爭關係，也就是說，現行的世界法幣體系沒有共同遵守的底層共識，沒有通用資產背書，沒有共同的信仰（信用）為基礎。

1.2. 法幣發行機制

人類歷史上出現過各種的法幣發行制度，現代的制度已經是政府說著玩的制度，根本不值得討論論。我們去回顧一下曾經一定程式上公平的金本位制。

金本位即金本位制 （Gold standard），金本位制是以黃金為本位幣的貨幣制度。在金本位制下，每單位的貨幣價值等同於若干重量的黃金（即貨幣含金量）；當不同國家使用金本位時，國家之間的匯率由它們各自貨幣的含金量之比——金平價來決定。

第一，黃金生產量的增長幅度遠遠低於商品生產增長的幅度，黃金不能滿足日益擴大的商品流通需要，這就極大地削弱了金鑄幣流通的基礎。

第二，黃金存量在各國的分配不平衡。1913 年末，美、英、德、法、俄五國佔有世界黃金存量的三分之二。黃金存量大部分為少數強國所掌握，必然導致金幣的自由鑄造和自由流通受到破壞，削弱其他國家金幣流通的基礎。

第三，第一次世界大戰爆發，黃金被參戰國集中用於購買軍火，並停止自由輸出和銀行券兌現，從而最終導致金本位制的崩潰。其中，佈雷頓森林體系協議(Bretton Woods Agreement)，核心是將美元與黃金掛鉤（固定匯率），其他貨幣與美元掛鉤，是金本位制度的典型表述。

關於法幣發行機制，我們有必要再提到另外一種思想《貨幣的非國家化》，作者哈耶克教授一生堅持自由市場資本主義，以反對社會主義、凱恩斯主義和集體主義而著稱。在其晚年，哈耶克將經濟自由主義思想貫徹到底，瞄準自由經濟的最後堡壘——法定貨幣，質疑國家壟斷貨幣的法理性，提出驚世駭俗的“競爭性貨幣”理論。其思想的核心是**“由多個主體發行各自的貨幣，用市場競爭的方式來完成優勝劣汰”**。礙於當時電腦技術、政治體系等原因，這個方案實際上無法實行。即使該方案有機會實施成功，其發行者照樣擁有著全部的“鑄幣稅”——以太坊的 ERC20 Token 基本上屬於這種個體發行通證（類貨幣），是一種廣義的實現方案，它獲得了階段的市場瘋狂[2]，但也再一次印證了單一貨幣發行主體的信用問題。

1.3. 證券、積分與發行機制

證券是多種經濟權益憑證的統稱，也指專門的種類產品，是用來證明券票持有人享有的某種特定權益的法律憑證。主要包括資本證券、貨幣證券、商品證券等。狹義上的證券主要指的是證券市場中的證券產品，其中包括產權市場產品如股票，債權市場產品如債券，衍生市場產品如股票期貨、期權、利率期貨等。同理，各種企業內部績效積分、外部用戶積分等，都屬於這個通證的範疇。

而其對應的發行機制，都基於中心化權力發行，同樣有著“過程腐敗、流動許可、跨組織、跨國界流動阻隔”等問題。

1.4. 互聯網&物聯網

互聯網是基於 TCP 協議為資訊傳輸服務網絡，而區塊鏈是為價值傳輸的網路。這句話精妙地概括了，互聯網解決資訊不對稱的定位，同樣讓我們憧憬和好奇，去建一個價值自由流動的網路。

物聯網的底層其實是物權的網路化協問題，物權包括了所有權和使用權等，我們可以簡單地理想為：在含互聯網在內的通信網絡中，有形的萬物，通過所有權、使用權、監察權等的分配，而讓人與物之間的關係產生變化。換言之，如果我們能用共識的機制，讓萬物的物權量化、可交易，那麼要解決萬物聯網其實就是解決可量化的問題。

所以，如果我們的經濟系統“需要提供物權量化的能力和入口”，那將很美妙。

1.5. 區塊鏈

狹義上，區塊鏈（Blockchain）是一個分佈式的共用帳本和數據庫，具有去中心化、不可篡改、全程留痕、可以追溯、集體維護、公開透明等特點。這些特點保證了區塊鏈的“誠實與透明”，為區塊鏈創造信任奠定基礎。而區塊鏈豐富的應用場景，基本上都基於區塊鏈能夠解決資訊不對稱問題，實現多個主體間信任協作與一致行動。

在區塊鏈技術基礎上，誕生了比特幣 Bitcoin[3]、以太坊 Ethereum[4]等多個成功的案例，二者各自發展成為典型代表：比特幣成為了數字黃金的代詞，以太坊是智能合約平臺。區塊鏈技術雖然還處在早期的發展階段，但跨組織共識機制（甚至於跨國家）、統一數據協議、開放源代碼等，引發了一場世界範圍的熱潮，如 DAO（去中心化自治組織）、DeFi（去中心化金融）、DAC（去中心化協作）等。而且，似乎這樣的熱潮正在將人類文明往陌生共信社會方向引導。

我們經濟系統需要提高“跨組織（跨國）的信任共識底層”。

1.6. 比特幣

比特幣（Bitcoin），實現了前所未有的區塊鏈技術和金融現象：純技術地實現了無實物對象的共識資產；實現了數千萬倍的價格漲幅空間。它的成就舉世矚目，讓全世界的擁躉為之瘋狂。但是，比特幣和比特幣網路也存在一些問題：

- 巨大的能源消耗，其電能消耗已經達到了中等人口國家的耗電規模
- 區塊鏈性能，可容納交易量極小（相比於當前互聯網軟體）
- 延時問題，每 10 分鐘為週期
- 可擴展性問題，技術整體脆弱性
- 價格劇烈波動，無法滿足常規交易需要
- 鏈上交易手續費問題
- 鬱金香的影子，無大規模的應用場景，讓其缺少資產背書
- 技術開發可能進入了“積重難返的民主怪區”

正是基於對比特幣美好面的遵從和缺失面的反思，我們認為一個經濟系統需要“法幣”——恒定價值的貨幣。

[3] Bitcoin wiki: https://en.bitcoin.it/wiki/Bitcoin, http://www.bitcoin.org
[4] Ethereum 官方網站: http://www.ethereum.org

2. 理想

假定我們奉行的大旗是“人類總是在永不停歇地尋找更能適應和促進人類文明前行的新秩序”，那麼經濟系統該如何建立新的秩序？我們需要一個怎樣先進的經濟系統？

2.1. 理想貨幣系統

一個理想的經濟系統，首先需要一個理想的貨幣系統。

2.1.1. 理想的貨幣

因為只有完全普遍接受的價值尺度，才可能構成世界範圍的經濟大協作——履行貨幣“價值尺度、流通手段、貯藏手段、支付手段、世界貨幣”的職能，這個目標是目前任意一種單一法幣無法完成。所以，我們在尋求理想的貨幣。

加密貨幣與智能合約之父提出：如果有一種協議，能夠對"受信第三方"的依賴降到最低，線上創造出無法偽造的、有價值的數位字元，並且被安全存儲、轉賬和驗證，這就是"比特黃金"[5]——這既是比特幣的思想源頭，也是我們追隨聖賢的試圖往前一步尋找一個理想貨幣系統的動力。

理想貨幣具體的樣子非常難以定位，假設為暫定為理想貨幣是幣值長期穩定的貨幣，理想貨幣應該是既沒有通貨膨脹，也沒有通貨緊縮——不會因為“貨幣政策”而產生不公平；理想貨幣應該是現行法幣的能力之上的全球共識性一個或多個貨幣；理想貨幣應該在“耐用性、便攜性、可分割性、統一性、有限供應量和作為一種支付方式的普遍接受性”等 6 個關鍵特性上獲得更多提升。

我們可以想像一下它的樣子：

- 有底層資產背書：一種全人類共識的本位資產
- 完全自由流通：不因仲介系統（如銀行）而存在匯兌交易限制
- 適量供應（彈性供應）：需要的時候總量應需增加，反之亦然
- 價格約等於公充價值，不因總量供應影響價格穩定
- 文化與歷史的適應，符合區域文化與情感歸屬
- 不影響現行的經濟，自然並且逐步轉移

並由此推導，理想貨幣系統可能的樣子：

- 沒有一個人或群體能控制：完全去中心化
- 無仲介：沒有人為的中間手續影響交易的完結
- 自由存儲和轉移：任何個人、企業、其他組織都可以全權處置
- 自由結算：交易即結算，也就是沒有清算類的環節
- 自主隱私：有主動權選擇財務透明與隱私
- 透明可追溯可審計：用於數據抽象、可視化呈現、審計監察
- 系統開放性：充分開放系統能力，豐富接入應用場景，實現生態化自治

---

[5] The **Bit Gold** proposal, by Nick Szabo, describes a system for the decentralized creation of unforgeable proof of work chains, with each one being attributed to its discoverer's public key, using timestamps and digital signatures. It is said that these proofs of work would have value because they would be scarce, difficult to produce, could be securely stored and transferred.

為了嘗試解決法幣系統“無法自發改良，無法公平發行，跨文化使用門檻高”等問題，我們提出了基於區塊鏈的理想貨幣——公共貨幣，請見後文。

2.1.2. 理想的本位資產

其次，我們需要尋找一種“本位資產（底層資產）”。

在金本位制體系下，由於黃金總量有限、地域分佈不均、難以移動、無法可視量化、主權政治影響等其無法滿足全球經濟多樣性和快速增長的需求。

隨著互聯網、區塊鏈技術和數字經濟的發展，如果存在一種普通接受的通用資產，擁有如下幾個特點（相比於黃金），就可能可以成為新的本位資產：

- 不會被中心化組織（群體）所控制
- 有公認的價值內在：無論是信用型資產還是實體資產，需要全球全民共識
- 沒有時間空間的限制：跨國界、跨地域文化、跨時間
- 不受物理形態約束：任意交易或抵押行為，易於或者不需要物流運輸
- 沒有總量變化：底層資產應該是完全固性的，無變化量
- 易於存儲、交換、鎖押（易用性）：通過軟體終端加強易用性體驗

這種優於金屬黃金的本位資產，有可能催生統一本位制的貨幣體系。事實上，比特幣和以太幣具備了大部分如上屬性，以比特幣和以太幣為基礎的 DeFi 發速發展（去中心化金融）已經演示了去中心化貨幣體系的可行性。

所以，我們認識了“理想的本位資產”的樣子了。

2.1.3. 理想的貨幣發行機制

再次，我們需要尋找一種“發行機制”。

我們簡單回溯人類貨幣的發行機制，從物物交換，到貝殼為代表的稀有物品，到金屬貨幣，到政府信用票券，到金本位、外匯本位等，都是一個中心化集權的過程，並且伴生超發與通貨膨脹等金融經濟現金。即便到了諾貝爾獎得主哈耶克先生的多幣競爭思想和 John Nash 的《理想貨幣》，都是以一攬子商品為本位資產的解決方案——既無法與傳統利益者對抗，也無法解決發行公平性問題。

隨著電腦、互聯網和區塊鏈等技術發展，尤其是比特幣的出現、發展和階段性的成功應用後，我們已經清楚地看到了一種新的基於“電腦演算法”的發行機制。但我們之前分析過，比特幣不足以作為流通貨幣，人們已經默認賦予比特幣“數字黃金”美譽。比特幣也已經召示了一種貨幣的發行機制“礦工發行”：

- 自由創造多種公共貨幣：宏觀上可以形成多幣種競爭的態式
- 自由發行：發行公共貨幣，中觀上形成按需印鈔的格局
- 自由銷毀：銷毀公共貨幣，滿足理想貨幣的彈性供應需求
- 全民參與：沒有任何一個主體是中心，甚至主權國家都無法左右數量
- 保持健壯：發行機制需要長期保持健康運行狀態

2.2. 理想的數字資產治理

2.2.1. 通證化

要想讓經濟系統減少摩擦，自由協作，有兩三個步驟一定要實現，首要的是資訊化自動化協約，而要實現基於網路的自動化合約協作，最重要的是讓所有“價值”量化到該系統裏——“通證化”是一種理想的辦法。

廣義而言，通證其實是一種“將對象量化後的代表手段、媒介”，之前我們瞭解的貨幣是一種通證、證券債券是通證，各種可以量化介質，都是一種通證。

狹義來說，通證是以數字形式存在的權益憑證，它代表的是一種權利，一種固有和內在的價值。通證可以代表一切可以數位化的權益證明，從身份證到學歷文憑，從貨幣到票據，從鑰匙、門票到積分、卡券，從股票到債券，賬目、所有權、資格、證明等人類社會全部權益證明，都可以用通證來代表。

更粗暴的通證，其實是現在區塊鏈上的代幣（TOKEN），但的確是一種實現通證化的好辦法。所以，區塊鏈為我們帶來一個普世的機會和優秀的介質，可以簡單的進行“資產、權益的通證化”，從而帶來變革性的便利：

- 任何資產都可以進行量化拆分和打包，實現通證化
- 自由流通：增加流動性，可以無限細化和交易，並降低交易成本
- 開放市場，與資本直接連接，例如股權通證
- 優化管理方法和應用
- 可編程，實現跨組織社會化合約使用資產通證

2.2.2. 自由市場/開放式交易

自由市場是最好的配置資源的地方，自由市場或開放式交易平臺必須滿足以下要求：

- 公開透明：所有交易都應該完全公開透明，使得所有人都可以監督和信任這個交易平臺。
- 安全性：交易平臺應該採取各種措施保障交易安全，例如冷熱錢包分離、多重簽名技術、安全網絡等。
- 低成本：交易平臺應該盡可能地降低交易成本，包括交易費用、網路費用、兌換費用等。
- 大量選擇：交易平臺應該提供大量的貨幣選擇，使得交易雙方可以充分自由地選擇。
- 高靈活性：交易平臺應該提供高度靈活的交易方式，包括限價交易、市價交易、交易深度等。

基於一切有形的物品和無形的價值都可以被通證化，那麼，公平、平滑、即時、自由的通證交易就變得非常重要。換言之，在通證化成 Token 後，Token 是可以像水和空氣一樣，完全自由購買和出售。

內生式交易：發揮公共貨幣的價值信任優勢，通過智能合約，或者鏈下協商鏈上轉移的方式，不需要借助第三方的交易平臺完成數字資產交易。比如內建功能變數名稱、遊戲道具、股權、積分等，可以用公共貨幣即時完成交易過程。

去中心化交易：通常我們指撮合交易市場（Exchange），通過競價的撮合交易，達成數字資產的競爭定價與交易轉移。去中心化交所可以解決極大多數的數字資產交易所有誠信和安全問題，全部通證都可以自由交易。

第三方交易市場：通過第三方交易服務市場完成數字資產交易，實現資源按需配置。例如中心化的交易所，線下交易所，官方網站交易，社交媒介交易等。

為了實現貨幣交易的開放和自由，需要建立自由市場或開放式交易平臺，使得交易過程公開透明、交易雙方可互相信任，保障交易安全和效率，並能夠提供大量的選擇和靈活性。

通過以上要求的滿足，可以建立一個開放、安全、透明、低成本、大量選擇、高度靈活的自由市場或開放式交易平臺，推動貨幣的自由流通和全球各地的經濟合作。

2.3. 理想的組織與合作

2.3.1. 去中心化自治組織 DAO

去中心化自治組織，Decentralized Autonomous Organization。相比於基於親情關係產生的家庭，基於合夥協議產生的合夥團隊，基於員工雇傭合同產生的責任公司，基於投資協議產生的集團、財團，DAO 基於技術化的社會契約而產生一種新型組織，我們可以簡單地定義為“DAO 是由陌生成員按事務技術合約自由組合，為特定的目標進行社會化協作的松耦合型組織形式”。

我們來說明去中心化組織與中心化組織的區別：美國作家奧裏布萊福曼在一本名為《海星與蜘蛛》書中寫道，蜘蛛是中心化（細胞）組織，如果把它的頭切掉後整個身體就無法生存了；海星則是由彼此對等（無中心）的一堆細胞組成的，海星撕下的每只觸手都可成長為完整的海星。

DAO 的重點在於去中心化自治，在現有組織形式地基礎上加強了組織的社會性，即社群自治——DAO 的發起人、主創團隊就是目標制定者、協作規則策劃者，參與成員可以安照即定規則、流程、經濟報酬等參與組織，自由進出；另外根據開放程度的不同，成員參與社群事務也略有差異，優秀的 DAO 應該充許全員參與方向、戰略、規則、形象、事務等各方面。

去中心化的顯著特徵是社會化（Socialize），是一個小團體（個人）將大部分事務“外包”給陌生的人和組織，並完成目標的過程。全部或大部分事務外包的組織都可以稱為 DAO。已知的大型互聯網平臺，基於平臺軟體即規則進行協作，都是 DAO 的雛形。但真正能代表 DAO，其實是 Github 上一些著名的軟體專案團隊，是比特幣、以太坊社區這樣的社會化協作組織。成員們自發地組成了一個個“小生態”。

DAO 在共識機制和分佈式網路的共同作用下，成為一種介於產業和企業之間的組織形式。一方面，它以分佈式網路實現了資本的高效率分配，解決了資訊的不對稱問題。另一方面，通過共識機制建立起超越簡單熟人關係的信用體系，從而能夠形成以共用經濟（或者叫分享經濟）的新經濟模式，從而打破了新古典經濟中關於企業和市場關係的一系列限制，創造了新的組織結構。

在當前階段，工作量可量化、流程可標準化的組織體都可以開始進行 DAO 嘗試。而另一方面，萬能的通證（Token）是可以將任意對象通證化（Tokenize），那就意味著任意對象都可以量化——因此在通證賦能的基礎上，只要流程能夠用軟體應用來完成，就非常容易地制定組織的社會化方案。

2.3.2. 誠信協作

去信任（Trust-less）合作，即不基於信任的合作，是最少合作摩擦成本的終極目標。

在商業活動中，從古到今，都是朝著“減少欺詐，減少摩擦，共信合作”方向前進，現代商業社會以法律作為了商業活動的最低標準。實際上，商業活動還可以朝著“去信任合作”更進一步。智能合約正是這樣的產物，無論是普通的夥伴間合約，還是陌生人之間的合作規則，更或者是大型機構或全民的共同協作，都可以以智合約的形式誠信協作。

3. 實現

如何實現這個理想經濟架構？我們將繼承《貨幣的非國家化》、《Bit Gold》、《比特幣白皮書》、《以太坊白皮書》、《以太坊白皮書》等先賢著作的思想和實現，並基於 Bitcoin 和 Ethereum 現有思想去設計和運行一個新的平臺。這將是一個長期、不確定進程且永續迭代的過程，以下為 Openverse 2.0 的實現部分。

3.1. 價值協議

價值協議，Value protocol，是一個開放性價值傳輸協議，我們可以簡單理解為跟郵件傳輸一樣的開放性協議。所有區塊鏈均可通過價值協議，來交換價值，就像傳統的郵件網路一樣，myname@gmail.com 傳輸至 yourname@facebook.com 這樣，通過 Openverse 將 token/ntf 等價值資產，即時傳輸至以太坊（ethereum）、波卡網（Polkadot）等區塊鏈網路。具體請見《價值協議白皮書》及價值協議官方網站。

3.2. 核心程式 VerseCore

開源的 VerseCore 是價值協議一個 Go 語言程式實現，包括企業和個人在內的每個個體，都基於 VerseCore 可以搭建出無數的 POW/POA/POS 區塊鏈網路。

通過 VerseCore 搭建的每一個網路將生成為一個個的去中心化經濟生態，每個生態將服務於特定的行業和地域。每個生態將主張完全去中心化，為智能合約、去中心化應用提供運行平臺。

為了適應複雜社會多樣的經濟活動需求，和兼顧區塊鏈技術的發展進程，VerseCore 將分階段在基礎層實現：彈性、安全性、擴展性兼顧的區塊鏈核心。

3.3. Openverse Mainnet

Openverse.network：
是基於 VerseCore 2.0 代碼持續演進的技術網路，是包含分片結構、採用 POS 演算法、運行虛擬機的區塊網路。Openverse 定位於數字資產的運行平臺。

中樞鏈，Openverse.network：
中樞鏈指揮整個 Openverse 2.0 系統，中樞鏈的關鍵功能是管理 POS 協議以及所有的分片鏈。它有很多方面的工作要做：管理驗證者以及他們的權益；在每一步為每個分片指定所選的區塊提議者；組織驗證者進入委員會，對擬議的區塊進行投票；應用共識規則；對驗證者實施獎勵和處罰；並且，作為一個錨點，其中分片會註冊它們的狀態，以促進跨分片交易。中樞鏈不運行虛擬機、不處理智能合約。

業務鏈，Zones：
業務鏈是具體執行事務的鏈，運行虛擬機、智能合約等。各業務鏈之前通過協議的方式，與其它鏈產生價值交互。

共識演算法：
權益證明（POS），Casper FFG 是 DEE POS 共識機制的名稱。驗證者（礦工）將抵

押比特金，參與區塊的驗證，並獲得計算收益（挖礦收益）。在三元悖論[6]，Casper FFG 機制在做出決策的時候更傾向於保障安全性而非活性。

功能變數名稱系統 Universal Name Service：
Universal Name Service，即開放功能變數名稱服務，一個基於開放的可擴展區塊鏈功能變數名稱服務系統。各個區塊鏈網路/元宇宙都可以在 openverse 網路上註冊其主功能變數名稱。其主要作用是，將 Openverse 的多位亂碼式地址，翻譯成可讀、易輸入的字串。具體規規範，請見官網技術文檔。

智能合約：
Openverse 智能合約完全相容（2.0 時代為等同於）以太坊智能合約，採用 Solidity 編程。並且鼓勵社區提供智能合約範本庫。

DAO：
基於 Openverse 網路上的智能合約，任意主體都可以創建自己的 DAO。然後，以前所未有的方式進行投資、籌資、投機、交易、保險、借貸、創辦合資企業，以及進行更多的數字資產的線上管理，進行各種協作。

DEX：
基於 Openverse 網路上的智能合約，可以開設數字資產自由交易。

3.4. Openverse 數字資產歸類

Openverse 提供綜合的數字資產治理能力（發行、合約、去中心化交易），用價值量化和流通真正為跨組織（國家）經濟活動提供有用的服務。

3.4.1. 本位資產

比特金，Bitgold，簡寫為 BTG。是 Openverse 主鏈的核心資產，是經濟底層，已知的用途主要包括：成為公共資產的質押資產，交易費用，POS 共識的抵押資產，智能合約的價值源頭。

取名出發點：基於對尼克薩博先生 Bit gold 原型理解和思想繼承，基於對 Bitcoin 先鋒地位的遵從，基於對黃金在金融歷史上起到過的作用的延革——為了易於理解其在 Openverse 體系中的作用，我們將全新的本位資產名稱取為“比特金/Bitgold”。

發行總量：根據世界黃金協會（World Gold Council）提供的 2022 最新數據，自有人類文明以來，世界共開採黃金 20.48 萬噸(每年增加約 3000 多噸)；Openverse 區塊鏈約為三年減半，故以數學視角取了一個同等規模的恒定數字——2 億。即 BTG 的發行總量為 2 億枚，該數字恒定不變，所有開發者應該優先考慮小數位的移動，絕對不應該考慮數值的變動。

3.4.2. 公共貨幣

[6] FLP 不可能性（FLP impossibility）是分佈式計算領域的一個關鍵成果，其指出分佈式系統不可能同時具有安全性(safety)、活性(liveness)和完全非同步性(full asynchrony)。

公共貨幣，也可以稱為比特法幣/bitcurreny，是由公眾全員通過抵押比特金並競爭式地發行的公共資產，為了便於與以太坊的 ERC-20 命名為參照，我們取名公共貨幣標準的代號為“VRC-10”。在我們設計中，公供貨幣是一種恒定價值的數字資產，比起穩定幣來說，**我們希望人們認為它就是法幣的另外一種出現的形態，而不是競爭品**，所以我們取名和代號的時候，直接引用對應的法幣名稱。世界上目前沒有這種公共貨幣，雖然看起來相似但其實完全不同的例子如 USDT，它是 USD 的競品而非同質品；當然，更大的區別，它是由 Tether 公司中心化發行的產物。

Openverse 內嵌已發行公共貨幣是錨定於各國現行法幣的公共貨幣：

名稱	公共貨幣代號	中文翻譯	國別
U.S.Dollar	USD	美元	美國
Canadian Dollar	CAD	加元	加拿大
Indian Rupee	INR	盧比	印度
Japanese Yuan	JPY	日元	日本
Chinese Yuan	CNY	人民幣元	中國
……			

共計約兩百多種法幣[7]，涵蓋目前全球的主權國家的全部法幣，已經集成到 Openverse 主網成為公共貨幣，並且，可自由擴充更多公共貨幣。

3.4.3. 通證標準/Token

VRC-20、同質性通證/Homogeneity Tokens
同質性通證，Homogeneity Token，又可稱為通證或翻譯為令牌，狹義上它是一種區塊鏈上的同質型代幣，標準代號為 VRC-20。可以用於股權、企業積分、軟體使用天數/次數、用戶消費積分、遊戲點券等各種應用場景。

VRC-721、非同質性通證/Heterogeneity Tokens
非同質通證，Heterogeneity Token，可以理解為不可互換的通證。簡單地說，就是每個 Token 都是獨一無二不能互換的。可以用於版權、具體物權、遊戲道具、功能變數名稱等。

VRC-30、時間通證/Timing Tokens
時間通證，Timing Token，狹義上它是一種區塊鏈上的時效型代幣，標準代號為 VRC-30。具體而言，它的有效性是隨 Openverse 主鏈上的區塊序號為標準，產生、使用和滅失，一個 Token 將在某個區塊產生到某個區塊消亡。可應用於物聯網使用權等。

其他更多標準的 Token
根據未來應用情況，進行各多擴展，並通過公共智能合約範本市場，分享使用。

3.5. 公共貨幣發行機制

所以，我們分析金本位、央行法幣發行機制的缺陷，結合區塊鏈技術，提出了一種全新的設想公共貨幣發行解決方案——**公共競爭發行制度**。由於其本質上是動態抵押本位資產比特金，我們又可以稱之為“新金本位制”。

公共貨幣發行制度（Public Currency Issuance Mechanism, PCIM），通過超額抵押資產、全民參與競爭式發行公共貨幣的貨幣發行制度。PCIM 有幾個要點：

[7] https://www.iso.org/iso-4217-currency-codes.html

- 全民可參與，任何擁有本位資產的個體都可以參與競爭發行；
- 超額抵押本位資產，抵押產出公共貨幣；返還時貨幣時，解押本位資產；
- 無利息和交易成本；
- 隨時可以參與競爭發行活動；
- 高頻次，以區塊週期為時間標準進行競爭發行；
- 共同發行公共貨幣，如各種現行的法幣和未來更多需要的公共資產；

最終優勢：良幣驅逐劣幣

公共發行的貨幣，帶來了貨幣間的競爭，並且是在全球範圍內競爭，人們可以跨主權地選擇長期穩定的貨幣，最終將讓劣質的主權法幣沒有生存空間。

4. 應用場景

4.1. 比特金應用

“比特金只有一個用途：做為本位資產——如抵押發行公共貨幣”。

“雖然概率極小，但 50 年後，比特金可能會是世界統一的貨幣——假定，比特金最終價格穩定在一個水準，屆時公共貨幣將慢慢消失”。

4.2. 公共貨幣應用

“公共貨幣是法幣在區塊鏈世界的映射，是共信經濟與正統經濟的橋樑”。

“公共貨幣是 M0”。

“公共貨幣將用到法幣能用到任何地方，並且無限延展法幣的能力”。

“當比特金寵大到足夠量時，公共貨幣將自行縮減直至消失”。

4.2.1. 世界級的支付業務

以“等同於法幣的 Openverse 公共貨幣”和“企業私域穩定幣、穩定價值積分”等為代表數字資產，結合數字貨幣的其他優點，並基於完全去中心化的 Openverse 網路，無數的企業都能直接開通支付業務服務。這是有別於數字貨幣 1.0 時代的狀況（因為比特幣的價格是劇烈變化，而現有的穩定幣是中心隨性發行的）。因為公共貨幣就是法幣，所以擁有法幣支付、電子支付的優勢，又具有區塊完全自由的支付能力。同樣，在企業私域價值因企業信用背書，所以企業發行自主背書的支付通證，實現私域支付業務。

各種面對面、APP、網站直接接入 Openverse 區塊鏈，就進入世界統一的支付和結算體系。

4.2.2. 去信任的借貸業務

隨著數字貨幣應用範圍的不斷增加，利用數字貨幣直接（不需要轉換為法幣，投資的收益也以數字貨幣計價）進行投資的領域和機會逐漸增多。利用數字貨幣創造價值的人需要更多的數字貨幣，手中持有數字貨幣的人需要保值增值，數字貨幣的借貸業務需求會越來越多。

4.2.3. 無摩擦的交易仲介

公共貨幣成為 Openverse 體系內去中心化交易所的交易對仲介貨幣，以及其他中心化交易所的仲介貨幣。平滑鏈內鏈外、站內站外的交易。

4.2.4. 低匯率、即時的跨國匯兌

發揮 Openverse 主網轉賬的低手續費、即時完成、完全自主實現無管束的國際匯款、兌換用途。打破現有法幣的主權邊界，用於各種國際支付、匯兌用途。

4.2.5. 其他法幣用途

例如消費支付、員工薪水、企業支付、智能合約履約支付等。

4.3. 同質性通證應用

4.3.1. 應用於“股權”

我們可以把可能由多個主體擁有的權益進行通證化，例如企業股權、企業收益權、物品所有權、物品收益權、構成競爭關係的表決權等。以企業股權為例，在股權通證化後，可以進行通證化私募、公募、發行期權給員工，可以進行轉讓交易和公開競爭式交易等，可以結合企業上下游進行利益整合。

4.3.2. 應用於“積分”

將有一定權利、利益的非股權同質性用以通證化成“積分”，例如軟體使用次數、員工累計積分、遊戲裏消耗性積分等。且可以自由交易。

4.4. 非同質性通證應用

相比於同質性通證，異質性通證也有著廣泛的實體經濟和物聯網方面的用途。它可以代表任意的單一實物和虛擬道具，例如各種不同分隔的實體、各種證卡照、各種物聯設備、遊戲道具等，這些單一不可再分的物品道具，可以成為非同質性通證。且可以自由交易。

其中，物聯網設備，例如汽車、門禁、演唱會門票這些需要有“鑰匙”授權使用的物品，進行通證化，可以帶來更多的想像空間。

4.5. 時間通證應用

時間通證可以應用於有時效限制範圍的場景，比如對於租賃設備的使用權、投票表決權等，可以在原生網路上進行時間通證的交易。

4.6. 智能合約應用

在人類智慧的加持下，智能合約幾乎無所不能，我們可以例舉一些做為參考，並在實現過程中持續擴充（詳情智能合約範本市場）：

金融衍生品：金融衍生品合同基於標的物的價值，是公司對沖投資或交易風險的工具，如大宗商品或貨幣風險。Openverse 可從多個來源收集價格資訊，整合數據，發送至智能合約，併發送支付數據進行結算，自動執行衍生品合約。市場中的公司通常直到建倉之前都會儘量拖延付款，因此使用 Openverse 技術的智能合約非常有助於重建交易對手方之間的信任關係。

債券：先發債後償還是短期融資的理想方式。債券合約可以編寫成自動執行、無需信任且去中心化的智能合約。Openverse 可以用公共貨幣結算，同時也可消除對手方風險，因為各種去中心化認證的數據（如銀行拆借利率）將自動觸發付款

市場數據上鏈：資產在不同交易所的掛牌價格不同，因此需要將多個來源的數據匯總，以得出一項資產的準確價格。Openverse 外部資料鏈 Value Oracle 將提供足夠的數據上鏈服務，做為其他智能合約的資源。

去中心化的交易所：去中心化交易所中，資金在用戶錢包地址或者交易智能合約中，由用戶完全控制。用戶發起交易時，交易所執行智能合約來完成交易，資產劃轉在鏈上完成。交易記錄鏈上可查，公開透明。實現資源自由配置。

……

4.7. DAO 應用

DAO/DAC(Decentralized Autonomous Organization/Corporation，去中心化自治組織/企業)也許能夠衍生出人工智慧的概念。去中心化自治網路能夠在完全沒有人類干預的情況下，在預先設定的業務規則之下，在類似於公司的模式下自動運行。在 DAO/DAC 中，會有一些智能合約在區塊鏈上運行，根據預先設定的範圍，也可能是根據事件和條件的變化來自動執行預先批准的任務。

區塊鏈上，這些智能合約不僅能夠像一個自治企業模式這樣可以運作，還能夠構建一些完全和現實世界中商業模式一樣的功能。隨著比特幣交易變得越來越流行，這使得匯款市場變得更加有效率，而 DAO 和 DAC 也能夠完成相同的事情。一個匯款公司可能在面對現實世界和在與當地行政管轄區域有不少需要協調的地方，也必然會耗費許多成本，我們知道開辦企業就要與現實世界打交道，必然要考慮諸如營業許可、登記、保險、稅務等許多行政事務和監管法律，也因此會產生許多成本。而這些功能如果能夠移植到區塊鏈中，這些功能也許將變得更加有效率，而有些事務工作則完全不需要了，並且所有的業務天然就是全球化的。基於雲計算的，基於區塊鏈的自治企業實體能夠像政府在行政區內自助註冊一樣，根據智能合約和電子合同來完成任何它們

所需要的操作。每個企業首先將能變成全球性的企業，而那些受到司法管轄區域限制的商業模式也由此可能獲得更好的選擇。

5. 願景

5.1. Openverse 2.0 公共貨幣運行平臺

創建一個新的平臺，擁有類似於比特幣眾多優點的本位資產，通過競爭性地發行流通用途的公共貨幣，這些貨幣將繼承現行法幣的優點，廣泛地應用到經濟領域各個環節；再在公共貨幣強共識的基礎上，將有形無形的價值介質進行通證化，實現公共貨幣運行平臺。更進一步，通過去中心化交易所、接入支付等應用層的努力，實現數字資產運行平臺的目標。

5.2. Openverse 3.0 價值協議與交換中樞

在 Openverse 3.0 的時代，預計在 2024 年啟動規劃和啟動開發工作。在技術上，引入同質鏈群，將各種非數字資產生命週期相關事務分離到同質鏈群——是分片機制的縮減機制和延展。任何個體都可以用 Openverse 代碼運行獨立的同質區塊鏈網路，共用主網的安全性，解決私域應用性能問題；並且官方將主動資助類似同質鏈的開發和運營。與主網之間的互通性在於帳戶、本位資產、公共貨幣、本鏈主資產。各種行業協會、聯盟組織、經濟相關的生態都可以自行運行 Openverse 同質區塊鏈提供公共服務.

5.2.1. Web3 的一個基礎設施

我們正處於一個從集中式互聯網（即 Web 2.0）向去中心化 Web3 轉變的時代。在 Web 3.0 的概念下，用戶創建的數字內容的所有權明確由用戶擁有和控制，創建的價值也將根據用戶和他人簽署的協議進行分配。我們需要一個全球性的 web3 基礎設施。

5.2.2. 區塊鏈的交換中樞

在目前的情況下，每個區塊鏈網路都形成了自己的生態和小社會，是一個價值孤島。許多團隊已經開發了大量的橋接器和協議來連接各個區塊鏈網路。在此基礎上，我們正在進行下一步的研發工作。通過鏈間通信協議，不同的區塊鏈網路可以安全地進行通信。

5.2.3. 元宇宙的系列協議

就像區塊鏈網路之間的通信一樣，所有元宇宙生態系統也需要互聯互通。連接基於相互接受的標準和協議。Openverse 團隊試圖收集和整理分散的協議，形成元宇宙的統一協議系列，打破各種資訊孤島，讓用戶持有價值可以自由流動。

5.3. Openverse 4.0 分佈式經濟生態

Openverse 4.0 將支持異構鏈群的整體建設和性能的極大提升，支持第三方區塊鏈以協議的方式接入，著重於生態接入開發，形成了分佈式經濟生態的形貌。

6. 更多

如果 Openverse 體系有實現的可能性，那麼在這裏說的更多的是寄託和它慮。

6.1. 技術主張

我們需要很長時間去實現整個體系的情況下，需要在早期的時候定位一些原則。

去中心化：完全去中心化，最終實現完全不被個別意志左右
鍵壯性：任何現實世界的變故都無法停止整個網路的運行
安全性：實現分佈式共識機制，算力分佈於細支，無法發生群體性違背協議事件
簡潔性：核心只處理協議本身，不涉及應用場景的邏輯等
持久性：網路長期運行，甚至於前瞻性地考慮量子計算問題
環境保護：確保鍵壯性和安全性的情況下，不應該增加能源消耗和硬體反復投入

6.2. 運營主張

主動發展：除了主網技術持續迭代，團隊將持續開發周邊普及應用，例如豐富功能的錢包、DAO 範本、常見智能合約範本、去中心化交易所等。

追求價值：以比特金作為底層資產，所以當它的經濟總值有多大就能容納更多的實體經濟，從而加速整個發展進程。

6.3. 社會主張

我們相信 DAO 和智能合約是實現陌生主體之間資源合理整合和無信任協作的有效形式，也信相會誕生一些知名的 DAO，它們在新社會中起到了超越公司、集團、財團等線織形式的巨大的社會功能。

因而，能夠研究、策劃、設計、運營一個 DAO 的人，都會是精英和智者。也繼而可以推斷，將來的世界會是一個智者治理的社會。

6.4. 文明

文明的更迭和演進，是去除黑暗尋找光明的過程，組織間合作於共識正是這樣的過程，而經濟是文明的催化劑和推進劑，所以，我們可能也將見到“文明新進程”。所以，各種文化將會一步在新文明下進行融合和發展。

6.5. 法律

雖然我們定義 Openverse 為一場偉大的試驗，但在 Openverse 體系中，比特金嘗試成為世界金融底層資產，公共貨幣本質上是 M0 目標是部分替代法幣，都遠遠超過了現行法律所容忍的範圍。例如，Facebook Libra 在早期就遭遇了種種阻礙看來，無論從意識還是法律上，Openverse 都將無數次地面對各主權國家的法律責難。

我們應該認為它是“需要尋求既得利益群體包容和法律開恩”的偉大試驗。

6.6. 機構

Openverse 是由 Utopia Foundation[8]資助和支持的專案。

Openverse 是由 Openverse Team 主持開發和治理的專案。

[8] Utopia Foundation，一個主張“科學主義 Scientism、自由主義 Pietism、虔敬主義 Liberalism”的開放型公益組織。

參考資料

1、Nick Szabo, 《Bit gold》, December 29, 2005, https://nakamotoinstitute.org/bit-gold/

2、Bitcoin wiki: https://en.bitcoin.it/wiki/Bitcoin, http://www.bitcoin.org

3、Ethereum, http://www.ethereum.org

4、Friedrich uon Hayek,《Denationalisation of Money》

5、Zvi Bodie/Alex Kane/Alan J. Marcus,《INVESTMENTS》

6、Fank J. Fabozzi/Franco Modigliani/Frank J.Jones,《Foundations Of Financial Markets and Institutions》

7、Yuval Noah Harari, 《Homo Deus - A Brief History of Tomorrow》

8、《[The End of Money the Story of Bitcoin，Cryptocurrencies and the Blockchain Revolution》

9、N.Gregory Mankiw,《Principles of Economics》

10、ROBERT J. SHILLER,《Bubbles, Human Judgment, and Expert Opinion》

11、J. Bradford De Long, Andrei Shleifer, Lawrence H. Summers and Robert J. Waldmann, 《Noise Trader Risk in Financial Markets》