# 綠色比特幣GreenBTC:

# 全新的挖礦邏輯

# V1.0

admin@greenbtc.top

2022年10月22日

## 1. 導言

在全球BTC開採能耗超標的情況下，同時BTC因環境問題受到世界各國政府的嚴厲打擊。我們是不是該做些改變？FIL，一種所謂的硬碟分佈式存儲系統，裏面充斥著垃圾檔。與此同時，XCH也退化為與市場上各種PoS專案的硬體競爭。我們是不是該做些改變？在PoW方面，PoS和PoC受資本和欲望驅動。那些正在逐漸遠離區塊鏈的初衷。我們是不是該做些改變?

深挖當下主流加密數字貨幣，BTC挖礦並不環保。被多國抵制，而ETH轉為PoS後的前景至今尚未明朗。更不用說，FIL暫時還無法解決投入成本和存儲有效數據的問題。我們還擔心的是，Chia的門檻太低，造成了不公平的壟斷。於是，挖礦業陷入僵局，似乎後繼無人。

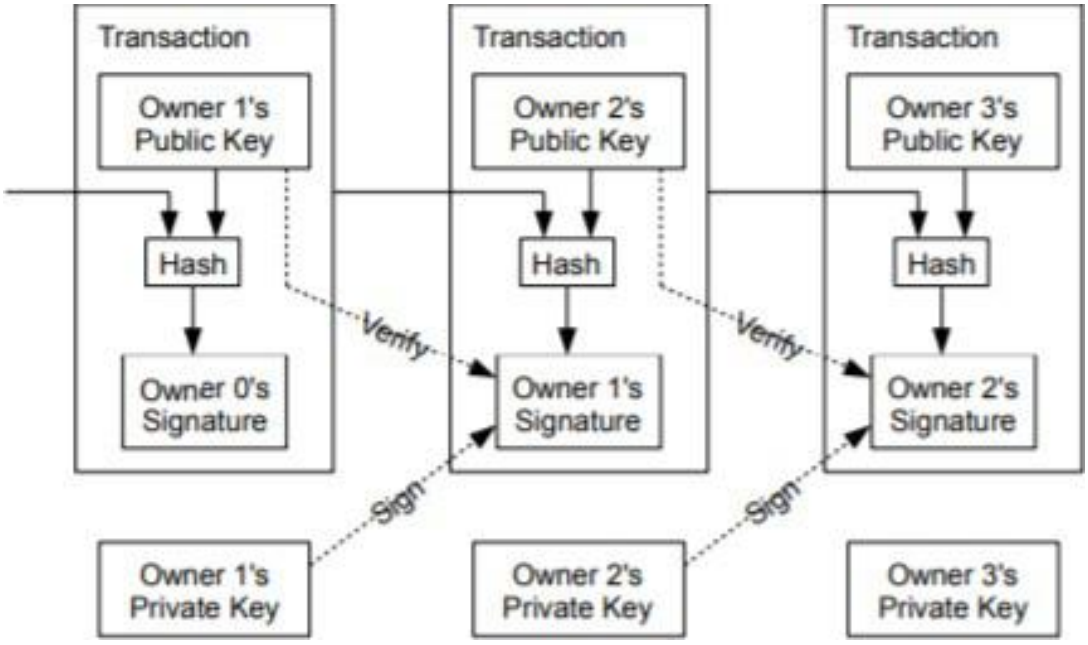
在當前Web3的環境下，區塊鏈世界迫切需要一個更加環保、智能、公平的去中心化網路生態。於是，綠色比特幣GreenBTC因應運而生。綠色比特幣GreenBTC的誕生是為了推翻傳統的採礦機制。它通過形成一種新的、獨特的挖掘邏輯，結合了上述傳統方式缺陷的解決方案。它旨在真正平衡PoW和PoS，符合BTC和Chia的初衷：用普通設備挖礦，讓區塊鏈真正去中心化。也許這一點小小的努力，只能慢慢引起一點微小的變化，但這些變化卻可能引發翻天覆地的改變。

2022年，綠色比特幣社區誕生。綠色比特幣GreenBTC的技術團隊對Chia代碼進行了深入研究，得出結論：Chia非常適合轉化為PoW+PoS。但考慮到Chia的缺陷，比如門檻低，綠色比特幣GreenBTC團隊決定在Chia的基礎上進行二次開發，實現PoW和PoS共識機制的結合。沒錯，這是綠色比特幣GreenBTC在極客和朋克思維的碰撞下，幾個名不見經傳的程式員和礦工想出了一個瘋狂的主意：顛覆並重建整個區塊鏈礦業世界。在區塊鏈這樣一個內部有連接的野蠻系統中，一點細微的初始能量就可能引發一系列連鎖反應，就像多米諾骨牌效應一樣。

## 2. 技術概述

### 2.1. 交易記錄

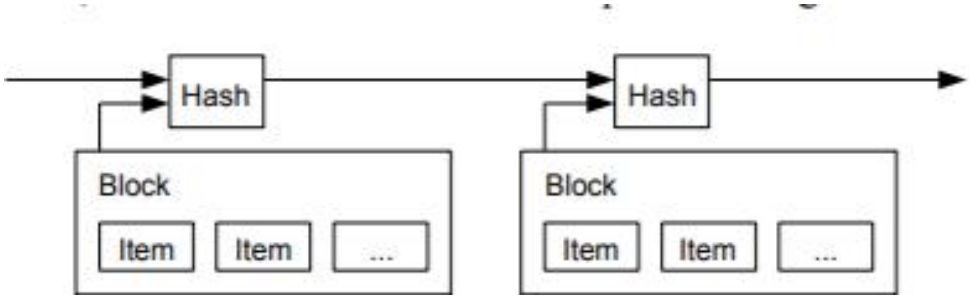
我們將數字貨幣定義為數字簽名鏈。每個所有者將硬幣進行轉移時，通過對先前交易的哈希和下一個所有者的公鑰進行數字簽名把這些加到硬幣的末端。收款人可以驗證簽名以驗



問題是，收款人無法核實是否有一個所有者雙重消費數字貨幣。一個常見的解決方案是引入一個可信的中央機構，或鑄幣局，檢查每一筆交易的雙重消費。每次交易後，硬幣必須返回鑄幣局發行新硬幣，只有直接從鑄幣局發行的硬幣被認為不會被重複使用。這種解決方案的問題是，整個貨幣系統的命運取決於經營造幣廠的公司，每筆交易都必須經過它們，就像銀行一樣。我們需要一種方法讓收款人知道以前的所有者沒有進行任何早期的交易。在我們看來，最早的交易才是最重要的。我們不必擔心以後會有人試圖加倍花錢。確認不存在事務的唯一方法是瞭解所有事務。在以鑄幣局為基礎的模型中，鑄幣局知道所有交易，並決定哪一筆交易先到。為了在沒有可信方的情況下實現這一點，交易應該公開宣佈。此外，我們還需要一個系統，使參與者能夠就接收順序的單一歷史達成一致。收款人需要證明在每次交易時，大多數節點同意它是第一個接收的。

### 2.2. 時間戳伺服器

我們提出的解決方案從時間戳伺服器開始。時間戳伺服器的工作原理是獲取要標記時間戳的專案塊的哈希值，並廣泛發佈該哈希值，例如在報紙或部落格帖子中。時間戳證明了數據在那個時間必須存在，顯然，為了進入哈希。每個時間戳都在其哈希中包含前一個時間戳，形成一個鏈，每個附加的時間戳都會加強其前面的時間戳。



### 2.3. 平衡證明

類似比特幣的區塊鏈使用工作量證明（Proof-of-Work，PoW）機制，如果大部分計算能力都在誠實用戶的控制之下，那麼安全性就保持不變。然而，這一假設最近受到了嚴重挑戰，如果違背了這一假設，類似比特幣的系統就會失敗。綠色比特幣GreenBTC提出了一個新的區塊鏈結構，在這個方案中結合了PoW和股權證明（PoS）機制。我們的分析表明，只要誠實的用戶控制了大部分的集體資源（包括計算能力和股權），該鏈就是安全的。特別是，即使對手控制了超過50%的計算能力，如果誠實的一方在系統中持有足夠高的股份，安全性仍然保持。作為一項附加價值，我們的區塊鏈還能抵禦適應性強的對手。

因此，綠色比特幣GreenBTC網路結合了PoW和PoS的優點，提出了一種新的PoB（Proof-of-Balance）共識機制。綠色比特幣GreenBTC網路採用自己的技術，基於經濟模型和傳統的PoW機制，實現了可接受的硬幣生產方法。此方法自動調整挖礦的難度，並逐漸減少區塊獎勵。同時，結合PoS的共識機制降低能耗需求，避免了計算能力過度集中的悖論。解決了上述問題後，綠色比特幣GreenBTC終於平衡了工作量與資金、巨頭與散戶、利益與貢獻。我們稱之為PoB共識機制。通過這種方式，結合了基於資源和基於令牌的共識機制的優點，保證了攻擊者從共識的安全性上獲得資源和資金的雙重優勢。從機制的公平性上講，人人都有機會參與到綠色比特幣GreenBTC網路中來。

在綠色比特幣GreenBTC網路中採礦並不強制要求進行質押GBTC。為了避免資源和資金壟斷帶來的過度集中，綠色比特幣GreenBTC的挖礦機制鼓勵中小礦工貢獻整個網路的算力。他們不需要入股或過度入股就能取得採礦收入。當單個礦工帳戶的計算能力達到一定閾值時，就會有一個注標要求，而且是線性加權注標。也就是說，在公鑰下的質押GBTC越多，贏得塊的機會就越高。在這種機制下，大用戶需要極高的成本才能壟斷算力，這將損害中小礦工的

利益，危及綠色比特幣GreenBTC的安全。不能因為設備資源或巨額資金而過度佔用網路資源。中小礦工可以低門檻甚至零門檻加入穩健的綠色比特幣GreenBTC網路，為更去中心化、更公平的區塊鏈網路貢獻力量，獲得利益。

### 2.4. 採礦系統

目前，很多專案在出塊機制上存在缺陷，存在諸多隱患。以Chia為例，其正在搭建基於時空證據的區塊鏈平臺。然而，空間和時間的證明究竟是什麼？在某種程度上，這是一種新型的方式。在徹底研究了Chia的代碼之後，綠色比特幣GreenBTC的技術團隊得出結論：Chia的礦業系統非常適合用它來做工作量證明，我們可以增加一個投注功能來完成股權證明部分。

但是，Chia在檢測繪圖檔時遇到了一些問題，它導致了假的計算能力。Chia網路並沒有對繪圖檔的當前狀態進行詳細檢測。

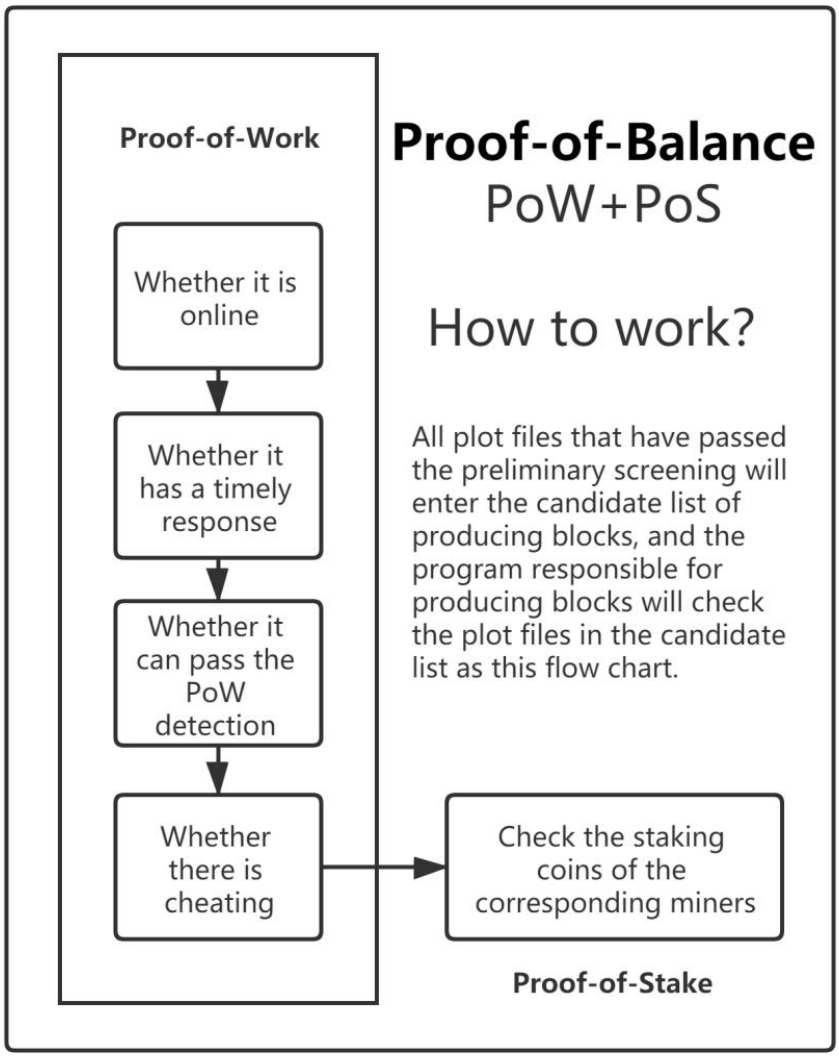
例如，在生成塊時，它無法檢測是否有人在當前繪圖檔上作弊。因此，如何保證Chia網路的效率和公平性是一個具有挑戰性的問題。

對此，綠色比特幣GreenBTC設計並優化了產塊檢測機制。在綠色比特幣GreenBTC網路中，所有通過初篩的地塊檔都將進入生產區塊的候選列表，負責生產區塊的程式將按照以下順序對候選列表中的地塊檔進行詳細檢查：

- 是否線上
- 是否有及時的回應
- 是否能通過工作量證明檢測
- 是否存在作弊行為（如重複挖礦）

- 檢查相應礦工的投注幣

圖塊生成程式將自動排除不符合上述檢查表要求的繪圖。在這種情況下，確保了綠色比特幣GreenBTC網路的高速運行，並消除了不必要的隱患。



### 2.5. 節點數

節點是更廣泛網路中的設備或數據點。例如，在網路中，節點可以是連接點、重新分發點或通信端點。節點是區塊鏈中的一個開源、跨平臺的，運行時，它允許開發者創建各種服務。綠色比特幣GreenBTC網路的節點參與共識，存儲數據的副本和更多的服務，並在鏈中提供一些指定的服務，為此他們獲得獎勵。我們將其命名為應用節點。這些節點的任務在每個階段都不同。

在綠色比特幣GreenBTC網路中，應用程式節點是timelord。但是，眾所周知，如果timelord不是在chia網路和綠色比特幣GreenBTC這兩個最快的硬體上，就沒有任何好處。

最後但並非最不重要的一點是，在mainnet啟動後，應用程式節點將支持鏈上的更多服務。最顯著的優點之一是應用節點可以發起DAO提議，並且持有GBTC令牌的用戶參與輪詢。另一個優點是應用庫由多個應用節點組成的特定組管理，由GBTC持有者選擇這些應用節點。

### 2.6. 隱私權

隱私一直被認為是加密貨幣社區最有價值的特性之一。綠色比特幣GreenBTC團隊誕生於社區之中。 它非常注重社區成員的隱私和安全。一方面，匿名性是可替代性的前身，廣泛使用的貨幣形式將需要這一特徵;另一方面，大多數社區成員不希望資產和交易記錄得到充分披露，這也符合分權的理念。在區塊鏈領域，匿名的難點在於如何在不洩露用戶資訊內容的情況下，正確驗證用戶資訊的準確性，防止惡意攻擊。在目前為區塊鏈提供隱私保護的各種加密方案中，以ZK-SNARK（Zero Knowledge-Succinct Non-interactive Argument of Knowledge）和ZK-STARK（Zero Knowledge-Scalable Transparent Argument of Knowledge）為代表的零知識證明演算法逐漸被大眾所重視，並被眾多專案和專業人士所接受。

不過，考慮到開發的時間和難度，綠色比特幣GreenBTC將採用混幣系統，該系統設置在鏈外，以實現匿名性。

零知識證明演算法最顯著的優點是它提供了簡化的易記密碼證明，允許用戶向另一個用戶證明他的聲明的真實性，而不洩露任何超出聲明有效性的資訊。所涉及的各方通常被稱為證明者和驗證者，他們所持有的密鑰被稱為證明。這些功能的主要目的是允許雙方之間盡可能少的數據交換。這無疑為隱私提供了一個強大的特徵集，相對較少證據的驗證可以快速有效地完成大規模計算的驗證。因此，零知識證明演算法可以為分佈式交換協議提供一個更好的分佈式保持規模，同時提高事務處理效率。經過社區創業成員的慎重考慮和投票，綠色比特幣GreenBTC決定採用可擴展性和安全性更強的ZK-STARK，以確保綠色比特幣GreenBTC網路的匿名性和安全性。

### 2.7. 系統架構

在鏈上交易頻率上升到一定程度後，以太坊等公共鏈在表現上出現的擁堵、高氣等一系列問題也隨之顯露出來。為此，綠色比特幣GreenBTC系統就是要採用分層設計的理念來解決上述痛點。分層邏輯是在不同的層次上完成不同的操作。這些層通過介面進行交互，而每一層本身也是一個或多個區塊鏈。這可以顯著地提高整體TPS能力，並且通過區分每層的功能，可以擴展程式的計算能力和處理效率和能力，並且可以降低相應的成本（費用）。另外，在層間隔離後，還可以進一步提高安全性。即使上層出現問題，也不會影響下一層的安全。

綠色比特幣GreenBTC系統由四個部分組成：鏈上交互層、計算服務層、零知識證明和用戶UI介面。

- 鏈上的交互層

在綠色比特幣GreenBTC系統中，操作與用戶資產相關，例如存放令牌、投注和挖掘，以及系統狀態記錄和驗證，例如計算層狀態更新和相關證明。它們都是由鏈上相關的智能合約來執行的。因此，鏈上交互層可以看作是連接鏈上和鏈外的關鍵樞紐。

- 計算服務層

計算服務層可以被認為是綠色比特幣GreenBTC網路中的第2層協議，它是一個程式模組，用於處理在該鏈下運行的所有事務。計算伺服器通過WebSocket介面與用戶交互，並監視鏈上交互層中的事務。所有合法的事務請求都被放入綠色比特幣GreenBTC記憶體池中，然後最終由綠色比特幣GreenBTC引擎處理。Block Proposer將事務匯總以生成新塊，而State Keeper將更新第2層中所有令牌的狀態。接下來，State Keeper將狀態發送給Commuter，後者負責與Prove伺服器通信並獲取相應的交易證明。最後一個階段將通過發送方將狀態和相應的STARK證明發送到鏈上的XXSwap智能合約。

- 零知識證明系統

綠色比特幣GreenBTC的零知識證明系統採用分佈式架構，並採用最安全的零知識證明演算法STARK來生成證明。Prove伺服器支持多個Prover。它主動查詢Prove伺服器中的證明任務，然後生成證明並將其發送回Prove伺服器。 STARK不依賴於數學問題假設，也不需要信任初始化。它被認為是量子抗性的。同時，得益於極高的驗證效率，STARK具有更實質的可擴展性。

- 前端用戶介面

方便易用的可視化前端用戶介面，可以方便用戶完成交換、發送、接入、加注等一系列功能。

## 2.8. NFT模組

NFT是Non-Fungible Token的縮寫。同質化一詞最初是經濟學中用於描述商品特徵的技術術語，意思是廣泛的相似性。與同質化的含義相反，獨特性和稀缺性是NFT資產的重要屬性。

NFT和區塊鏈技術在很多方面是一致的。區塊鏈可以保證NFT的稀缺性，並使其價值最大化。NFT和DeFi不僅是極具創造力和發展潛力的組合，也是綠色比特幣GreenBTC功能拓展的重要方向。NFT與DeFi結合的核心價值在於資產版圖的拓展和流動性的增強。理論上，NFT可以實現將現實世界中的各種稀缺資產映射到區塊鏈上的意圖，這可以幫助DeFi進一步將資產方法延伸到現實世界，比如藝術品、土地、房產等。這些都是可以用作抵押、貸款、典當等的資產，同時，一個設計合理的DeFi系統，能夠相對增強這些稀缺資產的流動性。將資產映射到資產鏈上，不僅可以避免資產的真實性，而且可以平衡資產鏈上的時間成本和價值損失。

集中式交易仲介結構

在NFT方面，綠色比特幣GreenBTC創造性地提出了NFT開發模組的概念，旨在降低用戶生成和使用NFT的門檻。NFT開發模組程式可以使用智能合約對任何NFT進行參數化，這意味著即使你完全不熟悉電腦編程代碼和NFT製作流程，你仍然可以根據自己的喜好和需求，在範本中設計和填寫NFT參數。然後，只需單擊一下即可生成NFT。

**3.令牌分發**

GBTC是綠色比特幣GreenBTC的協議令牌。就綠色比特幣GreenBTC的分散化和社區而言，GBTC總量的大部分將通過持續的採礦活動產生，並分配給維持系統運行的社區參與者。GBTC的輸出和分配規則如下：

- **輸出量**

GBTC的總金額沒有上限。綠色比特幣GreenBTC網路約每18.75秒生成一次塊。GBTC的輸出規則如下：

區塊獎勵階段 1（區塊高度 0-999,999）： 1 個 GBTC

區塊獎勵階段 2（區塊高度 1,000,000-1,999,999）： 0.6 個 GBTC

區塊獎勵階段 3（區塊高度 2,000,000-2,999,999）： 0.4 個 GBTC

區塊獎勵階段 4（區塊高度 3,000,000-3,999,999）： 0.2 個 GBTC

區塊獎勵階段 5（區塊高度 4,000,000-19,999,999）： 0.1 個 GBTC

區塊獎勵階段 6（區塊高度 20,000,000 開始）： 0.05 個 GBTC

30 年發行總額：≈10,000,000

- **發展基金**

開發基金預計將補償參與維護綠色比特幣GreenBTC核心代碼的貢獻者。開發基金用於獎勵貢獻代碼並幫助改善綠色比特幣GreenBTC網路的人員。

### 4.1 使用案例

GBTC令牌有三個不同的用途：管理網路，支持DeFi應用，為GreenBTC網路提供支持。

- **數據訪問對象**

GreenBTC是一個由社區領導的去中心化公共鏈。由於GBTC是平臺上的唯一令牌，它應該成為社區參與治理的憑證。

持有一定數量GBTC令牌的應用節點可以發起升級提案，如股權加權係數、開發計畫調整等。所有GBTC令牌持有者都可以對提案進行投票。以獲得過半數選票者為通過。開發團隊將很快跟進實施工作。

- **DeFi應用擴展**

DeFi是GreenBTC團隊非常重視的賽道。 隨著主網2.0的正式推出，GreenBTCSwap交換協議的設計和開發將提上日程。在這種情況下，GreenBTC將正式進入DeFi賽道。屆時，GBTC的應用場景將得到極大拓展。持有GBTC的用戶，可以通過投票或下注的方式實現貨幣上市，也可以利用GBTC進行便捷的跨鏈兌換。

GreenBTC團隊還將聯繫線下合作夥伴，宣傳GBTC的價值，以擴大GBTC的線下金融支付能力。

- **NFT部分**

不可互換令牌（NFT）是存儲在數字帳本（稱為區塊鏈）上的數據單位，它證明數字資產是唯一的，因此不可互換。NFT可用於表示諸如照片、視頻、音頻和其他類型的數字檔之類的專案。

在NFT方面，GreenBTC創造性地提出了NFT開發模組的概念，旨在降低用戶生成和使用NFT的門檻。NFT開發模組程式可以使用智能合約對任何NFT進行參數化，這意味著即使你完全不熟悉電腦編程代碼和NFT製作流程，你仍然可以根據自己的喜好和需求，在範本中設計和填寫NFT參數。然後，只需單擊一下即可生成NFT。