BICA

BITCAPITAL COIN

Light Paper

Document Vision 1.0

May 2019

BITCAPITAL COIN

穩定幣契機

加密貨幣市場的劇烈波動

2018年，全球加密資產市場總市值縮水接近90%

投資者迫切需要價值穩定，波動性小的加密數字資產

USDT信任危機

多篇文章表示Tether涉嫌超發，與Bitfinex有利益關聯

甚至聯手操縱 比特幣價格

審計主體，內容未達到正式審計標準

加劇了市場對於透明，可信任的穩定幣的需求

缺乏充足資產擔保

發行資產是否有充足或硬通貨來支持整個生態體系

BITCAPITAL COIN

打破陋習

打破發行方也是管理方的迷失及陋習

打破只有銀行或金融機構才能發行貨幣

人人都是發行方

所有資產受基金會(管理方)及各國第三方公司管理

基金會的模式，在各國深根落地

遵守當地政府法規，更符合跨國跨領域

BITCAPITAL COIN

發行模式

由中心化組織，管理穩定幣發行贖回相關的智能合約

其本質是發行人以自身資產做抵押，發行可以贖回標的資產“借據“(IOU)

發行時需要有法幣、黃金或實物資產作爲抵押品，

使得每個穩定幣都具備對應等值實際資產的能力

發行方承諾每發行1美元穩定幣就向儲備機構

存入1美元現金或等值美元的抵押物，以保證每個穩定幣和 美元1：1錨定

抵押物以超額抵押方式折算，例如超額比例爲50%

目前，與該模式類似的美元穩定幣，

包括USDT 、 TrueUSD 、 GUSD 、 PAX等

BITCAPITAL COIN

涉及主體

管理方

以基金會形式，負責穩定幣相關的技術支持與業務管理，
指定信託公司或銀行，盈利主體

發行方

所擁有之資產達到信託公司或銀行的標準，
通過KYC審核後具備發行或銷毀穩定幣能力的主體

用戶

穩定幣購買與轉帳的使用者

各國第三方資產管理公司(託管公司或銀行)

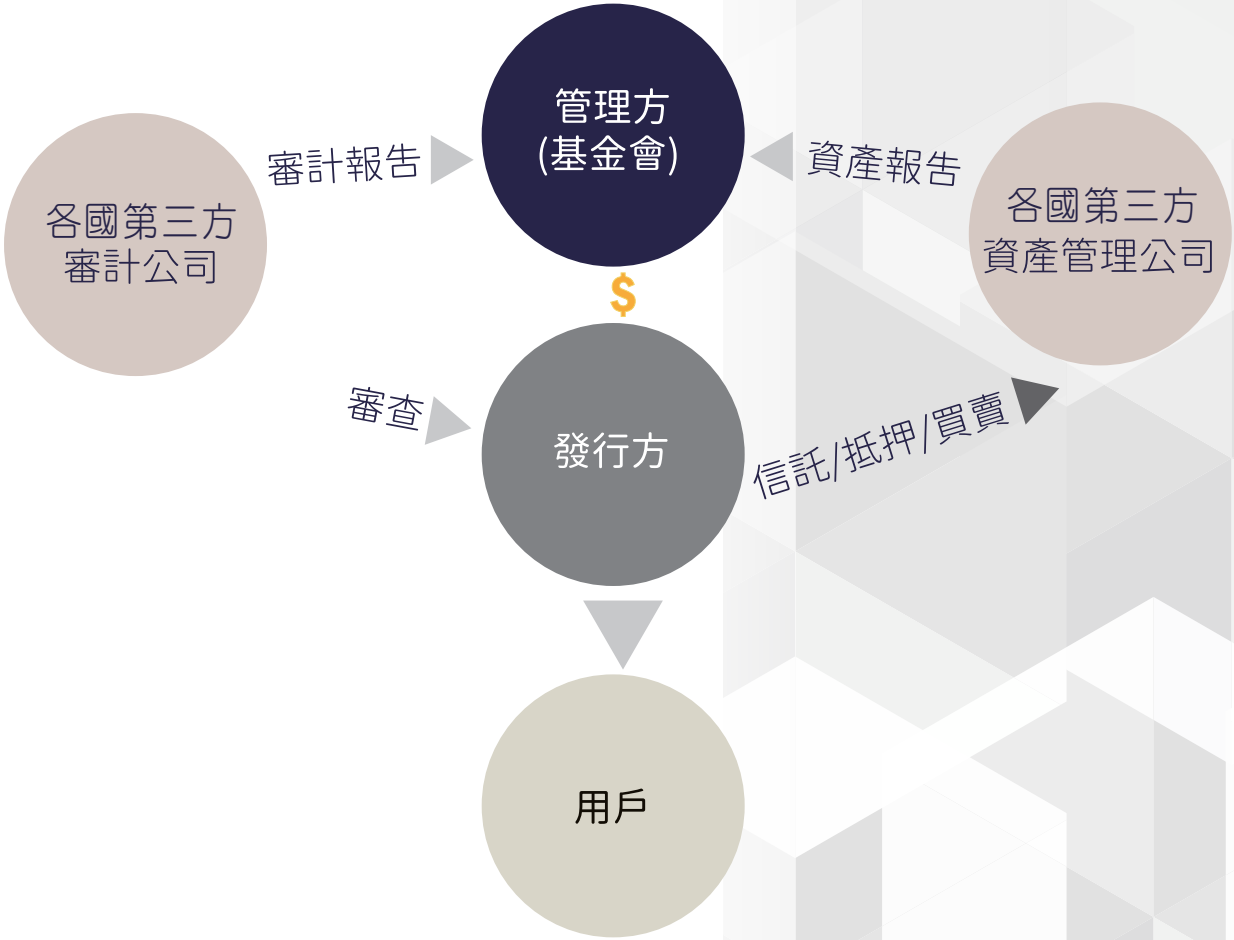
出具託管協議， 負責發行方KYC及託管所有兌換穩定幣的美金和抵押物
(爲穩定幣持有人提供定期審計和強有力的法律保護)

各國第三方審計公司

對託管帳戶的資金餘額及抵押物進行獨立審計並發布報告

BITCAPITAL COIN

涉及主體角色



BITCAPITAL COIN

抵押產權債權

信託、抵押、買賣的資產不是加密貨幣

而是代幣化的證券、大宗商品及地產…等高保值 高價值之資產

由獨立第三方公司完成資產評估及審計

BITCAPITAL COIN

接受資產

BITCAPITAL COIN

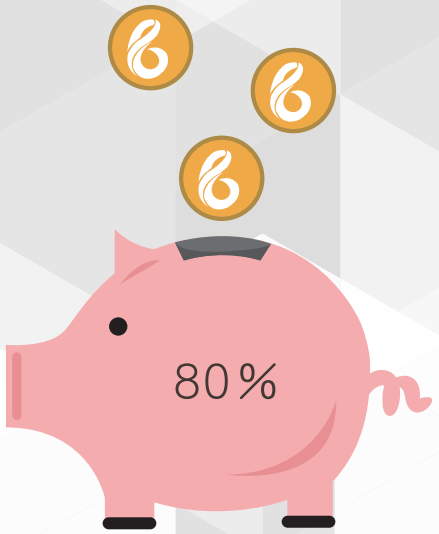
不接受資產

BITCAPITAL COIN

資產抵押利息

每個發行個案，基金會將向發行方，收取一定利息費用
基金會將從每個發行個案，所支付的利息當中80%
透過簽約合作交易所，發放給全球持有BICA的持幣者

其餘的20%做為基金會運作基金



BITCAPITAL COIN

盈利模式

持有收入- 用戶

用戶透過簽約合作的交易所，可獲得每個發行個案抵押利息

利息收入- 管理方

隨著穩定幣需求的增加，管理方手中會積累大量法幣及抵押物，

這就帶來了利息收入的可能性：

1. 一方面是存入銀行的利息
2. 通過投資低風險短期國債或貨幣市場基金獲利
3. 向發行方收取資產抵押利息

做市-發行方

發行方可以在加密資產交易所充當做市商，靠穩定幣的買賣價差獲利。

不過，隨著交易量擴大，買賣價差將會縮小，發行方這項收益也會受到擠壓

BITCAPITAL COIN

流通場景

BITCAPITAL COIN

回購機制

可通過盈利回購市面流通的穩定幣，

從而減少流通量，在低於錨定價格時使價格升高。

BITCAPITAL COIN

技術框架

BICA是發行於乙太坊公鏈上的代幣，

完全相容目前廣泛認可的ERC20代幣標准

具有1:1的可備付(等值)美元資產抵押作爲代幣的價值背書

BICA系統由鏈上與鏈下兩部分組成：

鏈上

運行於公有區塊鏈上的智慧合約物件集合，以技術背書保障鏈上信任，

利用乙太坊公鏈基礎設施提供代幣的發行、銷毀、轉帳、授信和解授信等功能

鏈下

完備機制以保障法幣的抵押、贖回以及審計、監管合規等過程

以透明合規確保鏈下信任。

BITCAPITAL COIN

技術框架

乙太坊

乙太坊是一個具有智慧合約功能的公有區塊鏈平臺
將可程式設計性質帶入到公共分散式帳本之中
其提供的圖靈完備的程式設計語言與執行環境
讓公共帳本的使用不僅限於底層功能，讓上層的去中心化應用變爲可能
也讓基於區塊鏈的應用生態變得更加豐富

ERC20

乙太坊的出現讓代幣的發行和轉移變得更加便捷
代幣的自由發行也暴露了低門檻下缺乏規範的弊端
爲了統一代幣發行,乙太坊社區制定了ERC20代幣合約
這也是目前運用最爲廣泛的代幣標準
其中定義了代幣的基本屬性、核心帳本集合等

BITCAPITAL COIN

可升級的智能合約

智能合約本質上是可執行的電腦程式，區塊鏈賦予了它更豐富的概念

智能合約部署到區塊鏈之後將不可修改，且不由任何一方控制

這使得所有使用者可以信任資料和邏輯的眞實性

電腦程式的可升級性在商業場景下是重要

實現穩定幣智能合約作爲現實金融世界與數位元世界的最佳媒介必定是監管友好的

設計具備可升級的智能合約系統是十分重要

BITCAPITAL COIN

可升級的智能合約

可升級的智慧合約主要思想是：

1. 存儲與邏輯相分離
2. 資料存儲永久繼承
3. 邏輯可升級

邏輯可升級

通過部署新的邏輯合約實體，解除舊的邏輯合約與代理合約和存儲合約之間的關聯，並將二者與新的邏輯合約相關聯來實現。

除了繼承可升級智能合約之外，BICA還具備：

邏輯升級嚴格管理，在嚴格監管與審計下完成邏輯合約升級

用戶應用的接入點永久不變，使得調用BICA系統的DApp持續穩定

BITCAPITAL COIN

技術實現

BICA在乙太坊上共有4個實體：

3個核心模組

其中Proxy, Ledger, Logic是可升級智慧合約所需要的核心模組，用來實現ERC20標準的查詢、轉帳、授信等功能，及穩定幣所需的發行、銷毀和管理功能。

1個系統管理器

負責合約實體的更新升級與管理授權等功能。

代理合約-Proxy

代理合約爲永久合約，一次部署永不更替，如此設計是爲了讓請求代幣資料的位址始終一致，在合約集升級之後，協力廠商開發者不必變更調用代幣資料的方式和參數。代理合約是BICA向使用者提供的唯一介面合約，以向系統使用者提供所有ERC20標準介面。

存儲合約-Ledger

存儲合約提供BICA帳本核心資料的存儲功能，以及對帳本資料的操作介面(業務型操作)，並且讀寫介面只開放給邏輯合約實體，只接受邏輯合約的調用。存儲合約的部署也是一次性的，永不更替。

邏輯合約-Logic

邏輯合約實現BICA的核心邏輯，連接代理合約與存儲合約。在發行與銷毀時，邏輯合約只接受管理合約的委託操作，發行代幣並將代幣發送至申請人位址上，或者執行銷毀操作；在執行ERC20標準邏輯時，邏輯合約只接受代理合約發送的委託操作，並委託給存儲合約進行核心帳本的直接操作。

BITCAPITAL COIN

管理器

當邏輯合約需要更新時，創建新的邏輯合約實體，並首先單方面關聯邏輯合約與代理合約、邏輯合約與存儲合約，再關聯代理合約與邏輯合約、存儲合約與邏輯合約，最終實現邏輯合約與代理合約、存儲合約的雙向關聯。

上述關聯操作都必須授權於管理器實體，且由不同的管理器實體實現。管理器實體可爲乙太坊外部位址實體，亦可爲乙太坊合約實體。

此外，系統的管理器實體亦支援更新，當管理器實體更新時，管理器需要取消自身的管理許可權並授權給新的管理器實體，實現管理許可權的傳遞。

BITCAPITAL COIN

安全-多簽合約

管理合約集的升級與代幣發行、銷毀等操作都是BICA系統中風險較高的操作

例如管理人員誤操作、惡意操作等

此外金鑰保存也是高風險的事件

例如管理人員所保管的金鑰丟失、不可控的災難性事件導致的金鑰不可恢復等

因此需要採取必要的措施分散金鑰個體所控制的這些權力

多簽合約可以從技術上在鏈上實現這一功能

N/M的多簽合約(N<M)將操作許可權均分於M個不同的位址，由這些位址中的N個聯合可成功發起某些定義的操作。

根據的BICA的組織架構，BICA系統利用3/5多簽合約來管理合約集的升級、代幣發行、代幣銷毀等功能。

多簽協商過程全程明文存在於鏈上，而非處於鏈下的錢包內，

使得這些操作一切皆可查詢、可審計，實現系統技術和業務操作的完全透明。

BITCAPITAL COIN

安全-密鑰管理

多簽合約實際控制者本質上也是多個乙太坊外部位元址控制者的集合，
使用過程將會成爲系統風險暴露點，這將挑戰多簽金鑰的全生命週期管理

為了強化生態資產的安全管理

BICA對於最末端管理者的外部位址金鑰將採取嚴格的金鑰管理方案，
其生成、使用、保存、更替、銷毀都將使用包括離線阻隔、
門限切分等在內的多種高級別管理與操作標準。

發行方提交資料 供管理方審查

發行公司

公司設立登記文件

負責人身份證明文件(身份證件/駕照/護照 擇其二)

申請表單一、發行公司徵信資料表

申請表單二、公司徵信授權表(同意管理方對發行方進行全球徵信)

發行之目標

目標相關產權資料

申請表單三、資產目標簡介資料表

申請表單四、資產標的鑒定估價授權表(同意管理方對資產進行調查)

BITCAPITAL COIN

穩定幣發行流程

資料審查

- 發行方填寫
  相關書表檔
- 管理方對發行方
  KYC及資料審查
- 確認目標現況
  並查明產權狀況
- 由管理方指定之
  持牌估價師進行估價
- 由管理方及律師
  審查估價師報告

發行試算

- 管理方試算
  發行量及利息
- 發行方確認
  發行條件是否OK
- 管理方與發行方
  簽定發行合約
- 移轉目標相關權利
  發行方->管理方

公告發行

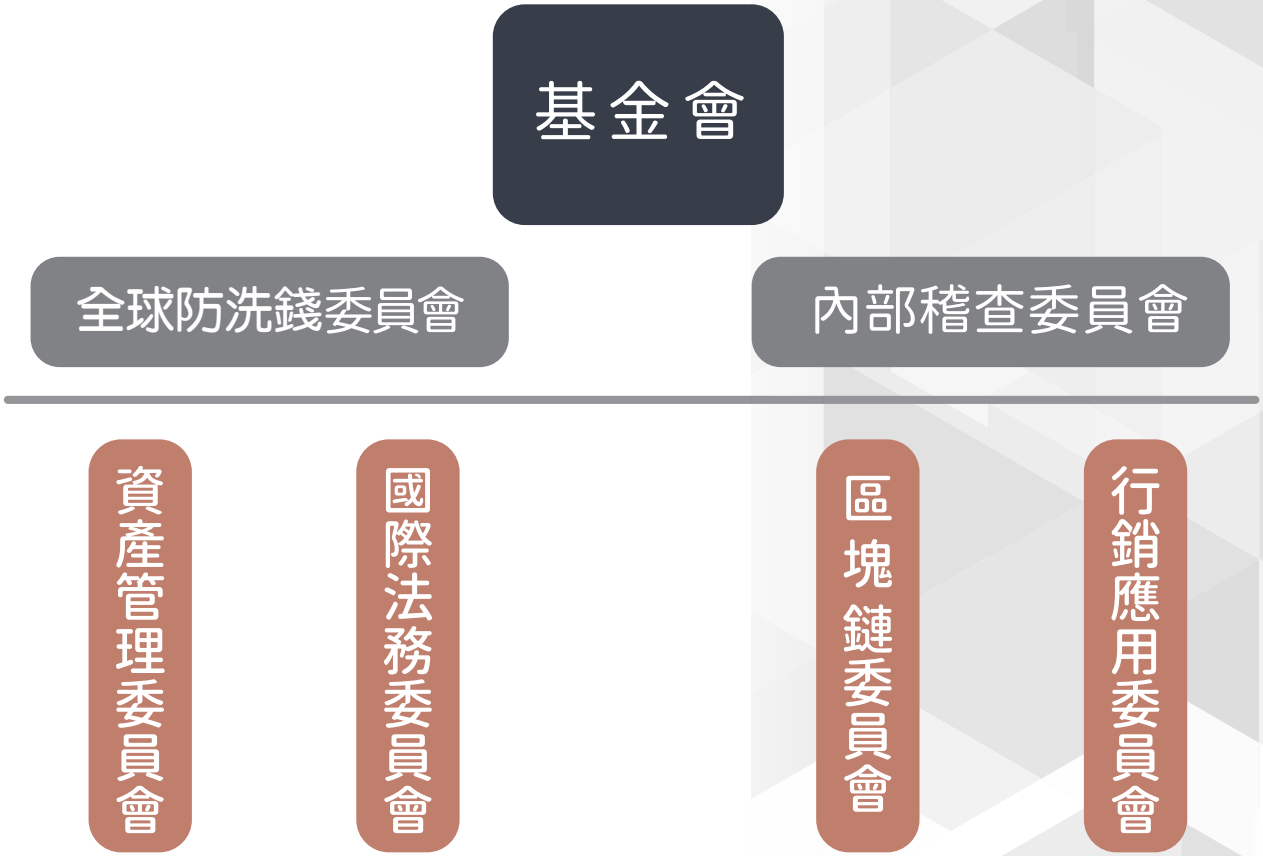
- 管理方網站
  公告發行報告書
- 啓動智能合約
  增發其數量
- 核算發行方徵信費用、
  資產鑒定估價費用及
  基金會相關業務費用
- 將預計發行的BICA
  扣除首期利息及相關費用

正式發行

- 確認發行方資產
  已移轉至協力廠商管理機構
- 確認發行方與管理方合同
  已完成簽約程式
- 基金會主席做最後確認
- 依據基金會主席確認文件
  及多簽錢包私密金鑰後
  將其BICA提領到熱錢包
- 依據發行合約時間
  打入發行方指定錢包地址

BITCAPITAL COIN

基金會組織



基金會設立四個業務委員會及兩個獨立監察委員會

一名基金會主席、二位獨立副主席、四位業務委員

BITCAPITAL COIN

基金會組織 - 1

資產管理委員會

負責所有發行方之資產鑒定.估價及管理

國際法務委員會

集合全球菁英律師，研究各國地區相關法律

區塊鏈委員會

負責所有區塊鏈估技術業務 ，例如：穩定幣的增發及消毀

行銷及應用委員會

負責穩定幣的行銷公關相關業務， 並負責增加穩定幣的應用使用場景

BITCAPITAL COIN

基金會組織 - 2

兩個獨立委會

全球防洗錢委員會

對於基金會各項業務進行督察，落實全球防洗錢法之相關規定

內部稽查委員會

對於基金會各項業務進行督察，以建全保障持幣者權力

BITCAPITAL COIN

結論

目前BICA處於初級階段，BICA選擇金融工具最爲齊全的美元作爲價值錨定物，

這是可操作性與市場認可度最高的方案。

在BICA發展的高級階段，價值錨定物將會多元化，會涵蓋歐元、人民幣、日元等主流法幣，

更近一步可以是具備高流動性的有價證券，以及有形資產。

當BICA錨定的價值抵押物類型越多時，BICA會成爲靠更可靠的穩定資產。

區塊鏈技術也在經歷革新與進步，乙太坊目前是最友好的智慧合約平臺，

但未來的數位世界會是多鏈、多層、多維的，BICA亦將支持在更多主流區塊鏈生態中的流通，

並開放和擁抱這些先進的技術。

BITCAPITAL COIN

免責聲明與風險提示

- 本白皮書並非提供您是否應購買任BICA幣的建議，亦非您進行任何契約或購買行爲應參考的文件。
- 本白皮書不構成任何買賣行爲之要約，亦不構成任何形式的合約或承諾。
- BICA幣並未計畫在任何國家或司法管轄區構成證券或其他任何應受管制的產品。
- 本白皮書非募集說明書或其他任何證券發行文件的基礎，亦不擬作爲在任何國家或司法管轄區發行或募資證券或其他任何應受管制的產品。
- 本白皮書未被任何國家或司法管轄區的任一監管機構審核。
- BICA茲此聲明免責於所有您因使用任何本服務所產生或與之相關的任何損失或損害(包括但不限於: 有關任何具體區塊鏈網路的運作，因交易或因無法控制因素導致的損失風險)。
- BICA亦免責於所有與網路攻擊或與之相關的任何損失或損害(包括但不限於: 您的個人資訊遭竊)、交易量前所未有的遽增或遽減、服務的任何中斷或終止、或有關本服務的其他技術困難。
- 您認知並同意， BICA 幣不具備下列功能：
    1. 代表BICA或任何司法管轄區之任何其他機構之股權、控制權或義務，或參與、控制前述機構應用決策之權利。
    2. 代表任何類型之投資。
    3. 代表任何擁有內在價值或市場價格的有價證券。
    4. 代表任何人有義務贖回或購買的商品或資產。

BITCAPITAL COIN

免責聲明與風險提示

非有價證券之發行

使用及購買BICA發售的代幣，須承擔高度的財務風險。
BICA交易在任何司法管轄地法例下，皆不構成有價證券之發行。
BICA上發布的任何文件，皆不構成投資資金之募集。

非開放予所有人

BICA幣不開放予所有的人。
持幣人應了解風險因素，並且白皮書中的任何聲明都不應被解釋爲本團隊對當前或未來幾年盈利的暗示。
欲參與該相關交易，必須經過一系列的步驟，包括應提供特定的資訊及文件。

無聲明與保證

本白皮書無任何聲明或保證確保其中所描述或所傳達與本計畫有關的資訊、陳述、意見或其他事項爲正確或完整，未對任何具前瞻性或概念性陳述的成果或合理性做出任何聲明或保證，且無聲明與保證之事項不限於前述事項。
本白皮書中任一處皆不應構成或被視爲對未來所作之任何承諾或聲明。
在適用法律充分允許的範圍內，任何人按照本白皮書行動而因此產生或有相關的任何損失或損害時，不論其是否係屬疏忽、默認或注意不足，我們不會對該等損失或損害賠償或負任何責任。

精複技術

代幣多被形容是非常高深的技術語言，要理解其風險本質，須具備對應用密碼學及電腦科學有很完整的瞭解。
爲使用本服務，您聲明並保證您有足夠的知識、對市場的高熟悉度、經驗及/或專業建議，以對您依本服務事之所有交易的優點及風險進行審慎的評估，且您同意獨自承擔前述評估的責任。