



Bit Asset Chain


# 去中心化高性能數字資產管理公鏈

V 3.0.0

2020.08.01

# 目 錄

Bit Asset Chain.....	1
去中心化高性能數字資產管理公鏈.....	1
第一章、摘要.....	4
第二章、現狀與改進.....	5
2.1 穩定的性能與可靠性.....	5
2.2 被社區認可的經濟系統.....	5
2.3 完善的配套生態.....	6
2.4 監管配套機制.....	6
2.5 升級空間.....	7
第三章、BAC Chain.....	8
3.1 共識機制.....	8
3.2 智能合約與內置合約.....	10
3.3 存儲網.....	11
3.4 跨鏈.....	12
第四章、去中心金融(DeFi)應用.....	13
4.1 發行 Token.....	13
4.2 穩定幣.....	14
4.3 去中心交易協議 DEX.....	15
4.4 去中心化借貸.....	17
4.5 征信系統.....	23
4.6 基金專戶.....	23
第五章、其他區塊鏈應用.....	25
5.1 物流追溯.....	25
5.2 數字版權.....	25
5.3 支付.....	25
第六章、BAC Chain 技術詳情.....	26
6.1 經濟系統.....	26
6.2 總體模組.....	27
6.3 POS+BFT 共識.....	29
6.4 費用模型和激勵體制.....	32
6.5 智能合約.....	34
6.6 預言機.....	34
6.7 治理.....	35
6.8 數據存儲.....	36
6.9 安全多方計算 (MPC).....	37
6.10 監管.....	38
6.11 安全.....	39
6.12 擴展.....	40
6.13 BAC 的配套生態.....	41
第七章、技術路線圖.....	43
7.1 2020 年 4 月主網上線.....	43
7.2 2020 年 7 月存儲網上線.....	43



7.3 2020 年 8 月推進開源，開啟應用.....	43
7.4 2020 年 11 月實現去中心化交易協議.....	43
7.5 2021 年 1 月內置合約實現 DeFi 業務模型.....	43
7.6 2021 年 6 月合約上線.....	44
第八章、參考資料.....	45

## 第一章、摘要

自從 2009 年 1 月 3 日第一個比特幣被挖出以來，區塊鏈技術已經走過了 10 個年頭。在過去的十年中，區塊鏈行業在質疑聲中穩步發展，並逐漸被大眾所認可和接受。如今各國的央行已經在研究發行基於區塊鏈技術的數字法幣，而像 Facebook 這樣的跨國企業也發佈了基於區塊鏈技術的 Libra 專案，高盛，彭博社等老牌金融機構也開始涉足區塊鏈業務。

數字資產源於比特幣，是一套以密碼學為基礎，基於公鑰和私鑰的分佈式帳本系統，數字資產的誕生，使金融服務的去中心化成為了可能。與傳統金融以銀行為中心的帳戶系統相比，去中心化的金融服務具有更高的效率，更低的成本，並且運行機制更加的公開，公正，透明。預計在不遠的將來，會有更多的用戶和機構參與到去中心化的金融世界中，從而誕生出很多與數字資產管理相關的新型服務。這些服務有可能是現有金融服務類型的延續，比如轉賬，衍生品交易，理財基金，資產託管，抵押貸款，供應鏈金融等，也有可能是嶄新的金融服務類型，比如，數字資產錢包，去中心化交易所，DeFi，穩定幣等。而使用區塊鏈技術特性的溯源，征信等功能早已進入各大企業的供應鏈系統之中，未來將會獲得更多的應用場景。

幣威鏈旨在為去中心化金融服務專門設計一條高效的公鏈，並以公鏈為底層基礎設施，內置強大的數字資產管理能力，結合錢包應用前端等實現完善的 DeFi 支撐體系，真正達成有價值的應用落地。在具體實現上，幣威鏈以 BCV、BAC 雙幣制的經濟系統保證公鏈基礎服務與抵押挖礦的平衡，用 ZI-POS 共識在安全、通縮的經濟模型下，保證公鏈的效率，並使用 tendermint 共識引擎和跨鏈交互協議 IBC，構建側鏈和中繼鏈體系，達成跨鏈目標，實現跨鏈資產流通，滿足多源數字資產管理的設計。幣威鏈在支持智能合約，保證通用功能服務擴展的同時，以內置的形式實現 DEX 協議、借貸、基金等典型的業務，並重視用戶體驗與產品周邊設施建設，結合數字資產錢包等，為用戶提供良好體驗的 DeFi 生態。

## 第二章、現狀與改進

在數字資產的世界，一定需要一條公鏈，可以專門為新型的去中心化的金融環境來服務。我們認為，一條能夠滿足數字資產管理應用需求的公鏈，需要具備以下條件：

### 2.1 穩定的性能與可靠性

在電腦世界中，如果操作系統性能不好，或者不穩定，電腦上的所有軟體都無法正常運行，就更別提使用電腦有效率的完成工作了。公鏈的性能與穩定性對於區塊鏈系統來講就像操作系統對於電腦一樣重要。首先一條可以被廣泛使用的公鏈，必須具有合理的性能。我們知道去中心化的系統性能很難與中心化的系統性能匹敵，這是享受去中心帶來的安全性等優點所需要付出的代價，但是我們依然可以努力的尋求改變和升級，設計出可以滿足當下主流 DApp 性能需要的公鏈。比如以 TRX 和 EOS 為代表的公鏈，轉賬基本上可以在數秒內完成，用戶不需要像比特幣一樣等待 10 分鐘以上的時間，現在這些公鏈上已經有成千上萬的 DApp 在運行，每天有數以百萬的用戶使用，流量已經超過了很多中心化的應用。

無論是 ETH 還是 EOS 等主流的公鏈，都出現過穩定性問題，比如智能合約出現漏洞，主網升級時出現問題等等，這些問題都對公鏈的生態造成了打擊，也對用戶的資產造成了損失。我們也應該吸取前人的教訓，同專業安全團隊合作，在安全和穩定性上竭盡全力，主動和被動的避免，防止公鏈出現問題，特別是在智能合約和主網升級等層面，並在系統的核心機制層面進行防範，一旦出現問題，也可以將損失降到最低。

### 2.2 被社區認可的經濟系統

在 POS 共識的區塊鏈系統中，經濟模型是站在滿足公鏈的功能和安全性的角度來設計的。節點通過抵押代幣可以獲得驗證節點的身份，用戶通過使用代幣投票給支持的節點獲取收益。如果節點作惡，其收益將受到影響，用戶也會將投票轉移到更加可信的節點從而杜絕節點作惡的情況。這套被廣泛採納的 staking 機制雖然在功能性和安全性上滿

足了 POS 共識，但是卻缺乏經濟角度的考慮。用戶可以一次性購買代幣抵押後，持續永久的獲得投票的收益獎勵。如果新增的抵押數量減少，而產出的代幣數量持續增加，代幣的價值將無法被支撐，整個公鏈生態的投資者都會蒙受損失，這對公鏈生態的長期發展是不利的。

而市場上被驗證過的比特幣 POW 共識的數學模型具有一定程度的通縮性，總量恒定，並且產量會定期減半，只要專案用戶的活躍度持續增長，代幣價值就會得到支撐。這套經濟系統設計雖然很合理，但是性能上無法達到 POS 公鏈的標準。

因此區塊鏈行業需要一套新的共識體系，既在性能上可以滿足大規模應用的需求，在經濟系統上，對通證的價值可以有支撐，這樣會更好的激勵社群戶更加深度的參與和推廣，也可以給公鏈生態創造更加長遠發展的土壤。

## 2.3 完善的配套生態

一個受歡迎的公鏈，離不開開發者和使用公鏈的發起方。要吸引用戶參與到公鏈的生態中來，一定要為開發者創造簡單易用的研發環境。比如節點搭建的教程，錢包的組件，智能合約開發所需的 IDE 工具，以及完善的文檔教程、框架，類庫，範本等都可以大大降低使用者的進入門檻和研發的時間成本。公鏈的開發越是便捷，就會有越多的開發者選擇這條公鏈，這條公鏈的生態就會發展的越好。除了對開發者開發環節友好之外，公鏈生態中的用戶對於開發者也不可或缺，因為只有用戶的參與，開發的應用才有人使用，才能真正創造價值。

## 2.4 監管配套機制

區塊鏈雖然具有去中心化的高可信度，但同時也具有一定的匿名性和不可逆性。如果這些特性被錯誤的使用，很有可能使公鏈成為犯罪的溫床。為了公鏈的健康發展，我們認為公鏈系統也必須進行一定的監管，這種監管不能太過嚴苛，這樣會與區塊鏈去中心化，人人平等的哲學邏輯相違背，阻礙公鏈發展。但是同樣的，也不能夠完全沒有監管，否則會任憑惡意的人濫用公鏈。我們認為公鏈系統也必須符合各國的監管機制。雖然當前並沒有明確的法律法規監管公鏈，但是我們相信隨著區塊鏈技術越發的普及，相

關的政策一定會被制定出來，為了公鏈可以長遠，穩定的發展，一定要對監管政策進行配合和進行相關的開發。

## 2.5 升級空間

當前的區塊鏈技術雖然比剛誕生的時候進步了很多，但還有許多不完善的地方。

比如當下的公鏈都是串行運行的，也就是同一時間只能處理單筆交易，一條全球性的可以支持大規模應用的公鏈，必須能夠併發性的同時處理多筆運算。目前公鏈的併發技術還沒有取得突破，所以公鏈的性能受到了很大的限制。

另外去中心化的存儲也是一個很大的挑戰，如比特幣和以太坊等主流公鏈，只能存儲簡單的轉賬記錄，這遠遠不能滿足大規模應用的需求。幾個備受期待的分佈式存儲專案，如 IPFS 等都還沒有上線，需要等待市場的驗證。

這些技術上不完善的因素都限制了區塊鏈應用的普及，我們相信這些問題終將得到解決，並在不遠的未來迎來區塊鏈應用的集體大爆發。而我們的公鏈也需要緊隨技術的潮流，不斷升級改進，才能不被淘汰。

## 第三章、BAC Chain

### 3.1 共識機制

#### 3.1.1 當下主流共識機制間的矛盾

目前流行的公鏈共識機制主要有以BTC為代表的POW工作量證明機制和以EOS和TRX等3.0公鏈為代表的POS權益證明機制兩種。

其中POW的經濟系統，具有總量恒定，產量週期性減半的特性，這種類通縮的經濟系統，為token的價值提供了一定的保證，BTC多年來價格不斷地上漲就是歸功於這套經濟系統，是一套被市場驗證過，並且取得了成功的經濟系統，但是POW共識由於出塊速度慢，帳本需要同步的節點過多，在性能上已經很難滿足新時代的公鏈應用需求。

如果說POW是一種全民投票機制的話，POS共識就像人民代表大會機制，POS在眾多參與者中選出驗證節點，代表用戶負責區塊鏈的出塊，使網路中需要同步的節點由幾十萬個下降到幾十個，這樣大大提高了公鏈的性能，但是POS共識機制的經濟系統，是一套通脹的經濟系統，需要超發token為節點和給節點投票的用戶發放獎勵，在這種通脹的模式之下，token的價值很難得到支撐。

#### 3.1.2 ZI-POS 共識機制

為了解決經濟系統和性能之間的矛盾，BAC Chain發明了ZI-POS(Zero Inflation Proof of Stake)共識機制，在傳統POS共識機制的基礎上，建立了一種雙幣雙通縮的經濟模型，使得幣威鏈既擁有POS共識機制的性能，同時還具備BTC一樣被市場認可的經濟模型，保證公鏈生態穩定與良性發展，為生態節點和參與投票的社群用戶創造更多收益。



### 3.1.3 雙幣種

BCV: BAC Chain 的權益通證, 持有 BCV 代表享受 BAC Chain 的權益。因此作為 BAC Chain 核心的主網節點, 需要持有並抵押至少 10 萬枚 BCV 才可以參與競選。而為節點投票的用戶, 需要銷毀 BCV 方可獲得投票權。

BAC: BAC Chain 的功能通證, BAC Chain 的鏈上業務, 如轉賬手續費, 智能合約執行, 分佈式存儲等業務都需要消耗 BAC。BAC 的經濟模型參考 BTC 的總量恒定, 產量減半機制, 由 0 流通量開始挖礦產出, 發起方 0 預留。

### 3.1.4 通縮銷毀機制

BCV: BCV 總量 12 億枚, 永不增發。用戶抵押或者銷毀 BCV 購買 BAC 投票礦機挖礦是獲得 BAC 的唯一方法。另外每臺 BAC 投票礦機還需要充值能量值方可繼續挖礦。銷毀 BCV 也是獲得能量值的唯一途徑。

BAC: BAC 總量 43,695,126 枚, 初始時 BAC Chain 每產出一個區塊, 賦予出塊節點 10 枚 BAC 作為獎勵。之後每半年獎勵數量減半, 並向下取整, 直到大約兩年半後所有 BAC 被挖出。

在所有 BAC 被挖出前, 用戶使用 BAC Chain 轉賬的手續費, 運行智能合約的費用, 以及存儲網的存貯費用都將使用 BAC 支付, 而在挖礦完成之前, 所支付的所有 BAC 都將被銷毀。

	總量	銷毀機制	獲得方式
BCV	12 億	購買 BAC 礦機	交易所
BAC	43,695,126	轉賬手續費	抵押或者銷毀 BCV 挖礦

時間	每塊獎勵個數	每天獎勵總數
第一年前半年	10	144,000
第一年後半年	5	72,000
第二年前半年	2	28,800
第二年後半年	1	14,400
第三年	0	0

### 3.1.5 驗證節點與投票礦機

與傳統 POS 機制一樣，ZI-POS 需要驗證節點作為出塊節點構建區塊鏈網路。在傳統 POS 共識機制中，驗證節點抵押的幣與獲得的出塊獎勵是同一種通證，而在 BAC Chain 的 ZI-POS 共識機制下，節點抵押的通證是作為權益通證的 BCV，然而獲得的出塊獎勵是作為功能性通證的 BAC。這樣不僅可以將兩個不同的通證按照功能的不同分開，還可以避免通證的超發，避免通脹。

而作為社群用戶，需要給節點投票，表示對社群的參與以及對節點的支持。用戶需要銷毀 BCV 獲得投票權。而節點會將自己的出塊獎勵，分給支持自己的用戶。我們為了用戶更好的理解這套機制，我們將投票權虛擬成為投票礦機，用戶的投票行為也可以等同於一種挖礦行為，從而節點也可以等價為礦池。

而節點抵押和獲得的票數越多，代表該節點過得社群的信任和 support 越大，該節點獲得出塊機會的概率也就越高，收益也就越大。相反，若該節點做惡，或者不作為，將會受到 slash 的懲罰，用戶會將投票轉投給其他節點。

## 3.2 智能合約與內置合約

### 3.2.1 智能合約

智能合約對金融資管公鏈必不可少，BAC Chain 智能合約不僅具有圖靈完備，使用靈活，安全可靠等智能合約等基本特點，還提供了生態友好的合約引擎 BVM。BVM 通過 webAssembly 和預言機技術等為合約提供了執行安全，性能，多語言等支持智能合約執行。

### 3.2.2 BVM 虛擬機

BVM 是在 webAssembly 是在基礎上改進而成，webAssembly 是一種高效加載，可移植，平臺無關的位元組碼格式，可以在平臺上接近原生的速度執行程式，這是一項全新的 web 標準，由谷歌，蘋果，微軟，mozilla 等幾大公司同時支持和制定。webAssembly 是被 EOS 驗證過的技術，EOS 智能合約伴隨 EOS 上線一直穩定執行。另外 BVM 也考慮到 webAssembly 的生態很好，很多高級語言都可編寫的程式都可以編程成 wasm 位元組碼的程式，wasm 位元組碼既可以編譯成機器碼後執行，又可以使用解釋器直接執行，這樣就降低了開發人員的學習成本。

安全問題對智能合約至關重要，在執行的時候可能會出現安全問題，比如計算和存儲資源的過度使用，節點執行效果不一致等。BVM從設計層面非常重視合約的安全性和正確性，使用gas機制防止資源被過度使用，BVM對執行深度和執行耗費時間的做了很多安全限制。BVM在代碼層面明確了介面之間的許可權，智能合約的入口函數需要進行許可權限制，防止開發者在入口函數調用未經授權的函數，破壞合約執行內容。

### 3.2.3 內置合約

BAC Chain將協議層和通用性較強的功能需求，寫成了內置合約。這些合約都是硬編碼在鏈上的，開發者可以按照合約的介面參數進行調用，對於不符合介面要求的請求會直接拒絕調用，這樣的合約既給開發者提供了便捷，又提升了安全性和穩定性。

目前BAC Chain 規劃的內置合約功能如下：

[發行 Token](#)

[去中心交易協議](#)

[帳戶信用審查](#)

[去中心化借貸](#)

[基金機構專用帳戶](#)

## 3.3 存儲網

Bac Chain 實現存儲網功能，在設計過程中考慮了以下因素：

- 1、存儲數據需要以交易的形式發送，要以狀態的形式存儲。這樣硬升級的時候，交易數據會存在升級前的主網上，狀態數據始終和帳戶綁定，仍然可以在升級後的主網上查詢到。幣威鏈把需要存儲的數據當作資產處理；
- 2、考慮商業數據具有多樣性，用戶在實現存儲的時候可以自定義數據格式存儲，確保用戶的使用便利性；
- 3、幣威鏈承載了存儲數據的摘要或者數據的簽名，真實的數據可以選擇存儲在其他分佈式系統上，這樣可以減少鏈本身的數量，又實現了數據一致性和防止篡改，目前使用 FastDFS 集群作為後端檔系統；
- 4、用戶存儲的時候可以選擇是否加密存儲，確保數據安全性；

5、存儲本身需要消耗資源，在幣威鏈存儲需要消耗相應的 BAC 作為費用，存儲的數據量越大，消耗的存儲費用越大，這部分費用可以通過社區投票方式選擇是消耗還是以收益的方式分給挖礦用戶，目前是直接消耗；

6、存儲數據都有 location 字段，可以方便的檢索到在主網版本，高度和交易首碼。

BAC Chain 目前已經初步實現了存儲網的功能，正在探索在商業領域的應用。

### 3.4 跨鏈

目前主流的區塊鏈跨鏈技術方案按照其具體的實現方式主要分為三大類，分別是公證人機制，哈希鎖定，側鏈和中繼鏈。

公證人機制安全性保障依賴於公證人系統，參與跨鏈的相關方需要對給予公證人機制較大的信任。哈希鎖定目前較適合偏資產或者關鍵數據的交換，使用場景受限較多。幣威鏈底層使用 tendermint 共識引擎和跨鏈交互協議 IBC，構建側鏈和中繼鏈體系，達成跨鏈目標。對於早期的數字資產鏈，比如 BTC/ETH，使用跨鏈技術將 BTC/ETH 價值轉移到幣威鏈上來。對於已經支持了 IBC 資產鏈，使用 IBC 協議達成跨鏈目標。

## 第四章、去中心金融(DeFi)應用

區塊鏈技術的誕生，在以銀行為中心的中心化價值存儲機制以外，給我們提供了一個去中心化的存儲和傳遞資產價值的新選擇。區塊鏈作為一種價值存儲媒介，鏈上存儲的數字資產，可以賦能很多金融類的服務，完全鏈上的服務也都是去中心化的。所有傳統金融領域中存在的服務，都應該可以在區塊鏈上以去中心化的形式重新設計實現。

一個合理的去中心金融公鏈，需要以下基礎功能才可以滿足應用的需要：

1. 可以發行 Token
2. 有穩定幣
3. 有去中心交易協議（DEX）

因為目前的智能合約安全性較差，並且不易升級，對於這些典型業務，我們將使用內置合約的方式實現 DeFi 功能，既保證更好的安全性，也可以使交易運行的更加高效，也為未來升級提供更便利的空間。當然，如果我們提供的功能無法滿足專案方或者用戶的需求，將來用戶也可以使用智能合約來實現額外的功能。

### 4.1 發行 Token

BAC Chain 以內置合約的形式支持發行 Token 的功能，用戶只需要運行簡單的幾行代碼，就可以在鏈上發行自己的 Token，用戶可以自定義 Token 的名稱，小數點精度，發行總量等參數，還可以以 BAC 作為自己發行 Token 的背後擔保資產，增加 Token 的信用。

所有 BAC Chain 上發行的 Token 都可以自由的在鏈上轉賬，用戶只需要支付 BAC 手續費。如果該 Token 出現信譽問題，用戶可以將持有的 Token 按等比例兌換成背後擔保的 BAC 資產，減低自己的損失，兌換後的 Token 會被直接銷毀。

為了進一步降低用戶的操作門檻，幣威錢包也發佈了通證寶產品，作為支持幣威鏈發行 Token 的應用前端，一鍵發行幣威鏈上的 Token。

幣威鏈目前已經上線主網發行數字資產功能,具體字段如下:

字段	類型	描述
outer_name	string	發行時指定的名稱,例如 ABC;用戶指定
inner_name	string	發行時候生成的新名稱, outer_name 加上尾碼
supply_num	bigInt	發行總量;用戶指定
margin	string	保證金;用戶指定
website	string	通證網址;用戶指定
description	string	通證簡介: 用戶指定
precision	uint8	精度: 用戶指定
exchange_rate	string	兌換比例 $exchange\_rate = deposit / supply$
owner_address	string	用戶地址;用戶指定

## 4.2 穩定幣

### 4.2.1 基於資質背書的中心化穩定幣方案

USDT 使用這種方案實現, Tether 公司為其背書,每發行 1USDT,就有 1 美元作為兌換。USDT 是目前使用最廣泛的穩定幣方案,但這種方案本身也存在一些問題,USDT 的儲備金並不透明,其增發可能會導致信任危機,面臨不確定的監管政策等等。

### 4.2.2 基於 DCEP 和 Libra 去中心化穩定幣方案

這類穩定幣基於國家或者主要銀行做背書,運營會收到高度監管,貨幣政策由各個國家控制,它本身也是基於區塊鏈技術實現,有一定的匿名性,這類穩定幣需要考慮的因素更多,也更複雜。目前還處理討論或者實驗階段,並沒有進入主流市場。

### 4.2.3 完全去中心化穩定幣方案

DAI 是 makerDAO 創建併發行的一種錨定美元 USD 1:1 的穩定幣,是基於以太鏈發行

的。和 BTC、ETH、EOS 以及一般的 Token 不同，Dai 不是通過挖礦產生的，而是必須由 Dai 的需求者質押一定量的 ETH，然後由智能合約作用向 ETH 的質押者發行一定數量的 DAI。目前 DAI 的活躍度還遠不及 USDT。

在 DeFi 的各類業務實施中，穩定幣是必不可少的媒介。專案方可以使用 BAC Chain 的內置發行 Token 機制發行自己的有資質背書的穩定幣，該穩定幣還可以使用 BCV 作為背後擔保資產，或者以其他方式來錨定穩定幣資產的價值。

另外其他主網如 ETH/TRX 等上發行的穩定幣，也可以通過通過 BAC Chain 的跨鏈機制在 BAC Chain 上被使用，提供如 USDT/USDC 等主流穩定幣的支持。

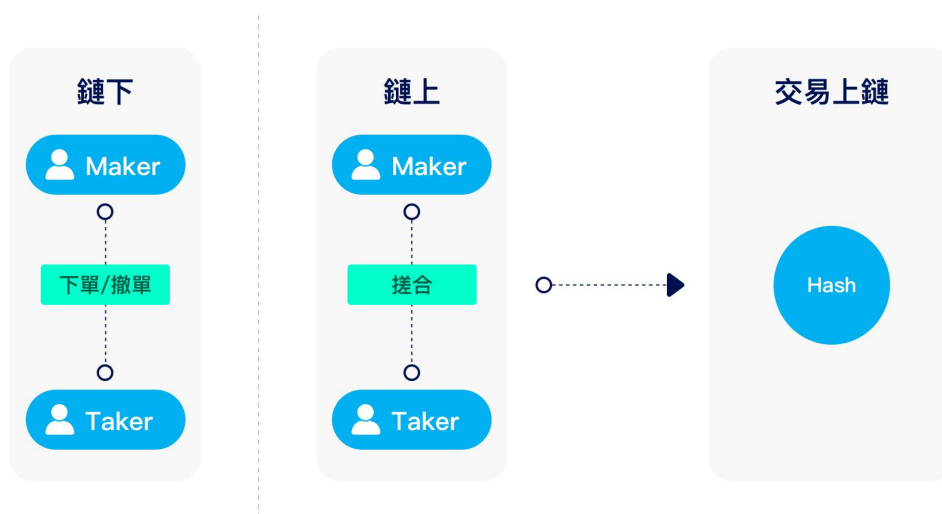
## 4.3 去中心交易協議 DEX

現在主流交易所都是以中心化形式運作，用戶只有在充幣和提幣的時候才可以在鏈上查到自己資產的流向，但是交易記錄並沒有記錄在區塊鏈上，並且每個交易所都有自己獨立的帳戶系統，這些帳戶資訊也都是中心化存儲的。目前主流交易所的這種中心化交易機制，與 DeFi 的去中心體系並不匹配，也無法真正去中心化地實現稍微複雜 DeFi 業務流程。我們需要去中心化交易協議對 DeFi 業務的支持，用戶的地址就是交易標識，用戶只需要持有私鑰就可以進行交易，與 DeFi 應用相相容，並且交易記錄直接鏈上可查，更加的透明公開。

### 4.3.1 鏈上鏈下的混合機制

鑒於當下區塊鏈技術還不成熟的限制，鏈上性能還無法滿足用戶下單撤單的毫秒級回應需求。另外用戶掛單和撤單的操作，如果沒有成交，全部記錄在鏈上的話，不單只耗費鏈上存儲空間，沒有好的委託體驗，也會消耗用戶不必要的手續費。所以 BAC DEX 採用了鏈上，鏈下相結合的混合機制，用戶的下單簽名只是在鏈下的系統中記錄，當有成交撮合的時候，用戶的交易才會成交並上鏈。





#### 4.3.2 BAC DEX 的基本數據結構

變數名	功能
makerAddress	吃單方地址
takerAddress	掛單方地址
makerData	吃單方相詳細資訊，比如價格，成交數量，下單時間，委託類型等
takerData	掛單方相詳細資訊，比如價格，成交數量，下單時間，委託類型等
makerAmount	吃單總量
takerAmount	掛單總量
makerFee	吃單方的手續費
takerFee	掛單方的手續費
commitID	該筆交易的唯一識別字

#### 4.3.3 交易簽名機制

用戶的每一筆交易，都需要數字簽名驗證以確保該交易的真實性和完整性，保證該筆交易是來自該地址的真實控制人，並且在資訊傳遞過程中，下單資訊沒有被篡改。

BAC DEX 的每一筆交易都使用了數字簽名，並且對訂單進行加密。這讓下單者可以放



心，除了他們授權的訂單外，沒有其他人可以與他們的地址進行未授權的交易。同時潛在的交易方也可以驗證該訂單是否是一個安全有效的訂單。



#### 4.3.4 多平臺共用深度

因為BAC DEX的交易邏輯使用BAC Chain的內置合約功能完成，用戶可以基於BAC Chain的公開協議構建多家去中心交易所，而這些交易所共用相同的數據結構，並在同一條公鏈上撮合，所以多家交易所可以共用交易的深度，不同交易所之間的用戶也可以互相成交彼此的訂單。

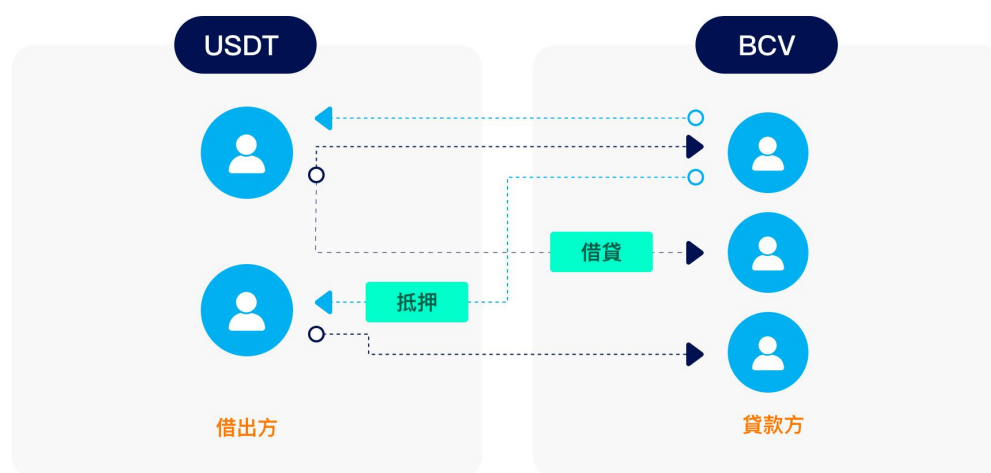
### 4.4 去中心化借貸

借貸是金融領域的基本應用，一方面可以滿足借貸人的資金需求，另一方面也可以為出借人提供利息收益。去中心化的借貸系統與傳統借貸系統相比，具有操作便捷，風險低，放款快等優點，將會是DeFi在未來的主要應用場景之一。

BAC鏈結合了當下主流的DeFi借貸技術和傳統金融的借貸機制，在內置合約中提供了借貸功能的支持。該系統可以支持多點對點借貸模型和代幣交換兩種不同的借貸機制，以及分期還款和單次付清等多種抵押借貸機制，用戶可以很方便的放貸或者借款，專案方也可以使用內置合約介面，快速開發出一套功能完備的借貸平臺，如果內置合約的功能無法滿足需求，專案方還可以使用結合智能合約在內置合約的基礎上進行二次開發。

#### 4.4.1 點對點借貸模型

點對點借貸是一種地址對地址的借貸機制，出借方可以在鏈上發起出借請求，並設定期望收取的利率和還款時間和抵押率等資訊，貸款人也可以在鏈上發起貸款請求，並設定期望貸款的額度和抵押資產的類型。如果出借方或者貸款人雙方有匹配的意向，BAC Chain 的鏈上借貸模型將會將匹配雙方的帳戶，並將借貸交易匹配上鏈，貸款方可以馬上獲得貸款，同時出借方也會馬上獲得抵押代幣的鎖定權。如果貸款方違約或者爆倉，借款方也可以馬上獲得貸款方的抵押物，從而將風險降到最低。



#### 4.4.2 計息方式

在 BAC Chain 的借貸模型中，因為已經有鎖定的代幣作為抵押物，風險較低，所以可以有多种不同的還款方式。從傳統還款方式來分類，支持等額本息和等額本金的還款形式，等額本息還款是指借款人每月以相等的金額償還貸款本息。等額本金還款是借款人每月等額償還本金，貸款利息隨本金逐月遞減，還款額也逐月遞減。另外如果出借方同意，也可以支持在借貸到期日到期時，一次過還清本息的方式。另外，用戶也可以選擇還款的利息是和貸款幣種為不同的幣種，比如用戶貸款 USDT，但是每月還款時的利息，可以用 BCV 支付，支付的數量按照預言機的即時價格進行折算。在貸款完全還清前，貸款方無法贖回抵押物。

#### 基礎數據結構

出借資產	USDT, BUSD, BCV, BAC 等
利率	年化利率百分比
利息資產	USDT, BUSD, BCV, BAC 等
出借日期	出借的當日時間
還款週期	如 30 天
到期日期	150 天
還款類型	等額本息, 等額本金
抵押率	50%
出借人地址	BAC Chain 地址
貸款人地址	BAC Chain 地址
抵押資產	BCV 500,000
出借資產	10000 USDT
已還金額	1000 USDT
已還利息	2000 BCV

#### 4.4.3 清算

如果貸款人抵押的資產價值觸及爆倉線，或者貸款人違約，系統將會自動將貸款人的抵押物所有權轉移給出借人。出借人全權擁有抵押物的處置權。出借人可以選擇將抵押物轉至交易所出售，如果交易所的流動性較差，出借人還可以選擇將抵押物在 BAC 借貸平臺的拍賣系統中進行拍賣。

#### 4.4.4 點對點借貸挖礦機制

由於點對點借貸具有一定的流動性問題，比如當貸款人遠大於借款人或者借款人遠大於貸款人時，人們的借貸需求無法被馬上滿足，這大大的影響了用戶的借貸體驗。Bac Chain

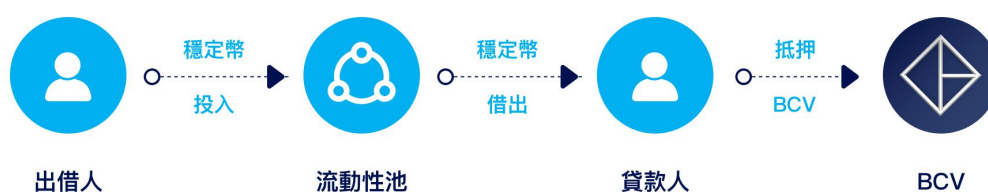
的內置點對點借貸模組，還設計了挖礦機制，借貸平臺可以存入一定的 BAC 作為挖礦獎勵，借貸訂單在一定時間內沒有被滿足，將會觸發挖礦機制，用戶完成該筆借貸需求，將會獲得 BAC 獎勵，同時該借貸需求等待的時間越長，滿足該需求時獲得的 BAC 就越多。

#### 4.4.5 流動性池借貸系統

點對點的借貸系統是一個一對一的借貸系統，該應用適合比較小規模的借貸平臺或者債券雙方或多方是相識的個體的借貸行為。

流動性池借貸系統則更加像是一個銀行。用戶可以將資金存入銀行獲得利息，貸款人也可以從資金池中抵押代幣，支付利息，貸出資金。借貸雙方都在流動性池子中互相支取，並沒有綁定相互的關係。它首先將資產全部彙集一起，然後當收到借款需求時再進行借貸分配，再將利息返回給儲戶。

由於流動性池是將大家的資產彙集在一起，所以特定儲戶的資產並沒有鎖定在某個特定的貸款中。這意味著，儲戶如有需要，可以隨時取出其資產，這比點對點借貸更加方便靈活。但是，這只有在流動性池的資產並沒有全部借貸出去的情況下才可能。



#### 4.4.6 利率的計算

在當今的現實世界，利率和流動性儲備是由國家的央行決定的。然而，DeFi 的世界中，

利率將由市場決定，這樣可以更自然的平衡貸款需求和代幣供應。貸款的需求越大，利率就越高。反之亦然。

一般情況下，並非所有存入流動性池中的資產都會被借出。用戶所提供的資產被借出的越多，資產利用率就越高，同時回報就越大，但同時這也意味著用戶擁有較低的流動性，不是所有的資產都可以隨時取出。

#### 4.4.7 存款利率

當出借人將穩定幣存入流動性池的時候，會獲得投入資產的憑證 ALT，穩定幣與 ALT 的兌換比例公式如下：

**totalCash** = 放入流動性池，但還沒有被借走的穩定幣的數量

**totalBorrows** = 所有借款人應償還穩定幣的總數量，包括本息

**totalReserves** = 總保留金數量

**totalSupply** = 所有兌換 ALT 的總數量

兌換比例 =  $(\text{totalCash} + \text{totalBorrows} - \text{totalReserves}) / \text{totalSupply}$

可見，隨著借款的數量增加，兌換比例也會相應的增加，如用戶在存入穩定幣的時候兌換比例是 1:1，一年後取出穩定幣的時候，兌換比例是 1.11，用戶就獲得了 10% 的存款年利率。



#### 4.4.8 借款利率

借款的利率應當根據當前市場的供需關係自由浮動，一般來說，借款需求越大，利率就會上漲，從而吸引更多的人提供借貸，最終將利率維持在一個動態平衡的系統中。

借款年利率由以下三個因素影響

1. **基礎利率：**基礎利率為全網基礎利率，有專案方或者專案社群決定
2. **使用率：**使用率就是當前流動性池中，被借出的使用比例，表現出市場當前的供需關係

$$\text{使用率 UtilRate} = \text{totalBorrows} / (\text{totalCash} + \text{totalBorrows})$$

3. **加給率：**用於調整使用率對利率的影響

$$\text{使用率 UtilRate} = \text{totalBorrows} / (\text{totalCash} + \text{totalBorrows})$$

$$\text{借款年利率} = \text{基礎利率} + \text{使用率} * \text{加給率}$$

#### 4.4.9 放貸利率

放貸利率由以下三個因素影響

1. 借款年利率
2. 使用率
3. **保留利率：**保留利率為全網基礎利率，有專案方或者專案社群決定

$$\text{放貸利率} = \text{借款年利率} * (1 - \text{保留利率}) * \text{使用率}$$

由於流動性池是一個開放自由的資金池，用戶可以隨意的存入資產和取出資產，貸款人也可以隨時支付利息歸還借貸本金，並贖回抵押的資產。該流動性池中可以有不同類型的穩定幣，根據市場的供需關係，不同的穩定幣也擁有不同的借貸利率。但是整體的借貸流程和還款方式比較單一，我們認為流動性池與點對點借貸是兩種互相互補的借貸機制，用戶可以根據自己的需求，選擇合適自己的服務。

## 4.5 征信系統

雖然區塊鏈具有一定的匿名性，但是 Bac Chain 仍然具有一套機制來評估每個地址的信用等級。影響信用等級的因素有帳戶流水，帳戶借貸記錄，帳戶違約記錄，帳戶資產價值，帳戶交易記錄等，Defi 應用可以根據帳戶的信用評級，選擇僅對某些地址開放服務。

## 4.6 基金專戶

數字資產開放交易以來，越來越多的資產管理服務團隊 Token Fund 成立數字資產基金。但是這些基金大多在中心化交易所操作，由於數字貨幣市場缺乏管理措施，基金的資產安全性很難保證。

隨著去中心化交易所的技術越來越成熟，也越來越普及，使用去中心化的帳戶系統進行基金資產管理成為了可能。

BAC Chain 針對基金理財機構，專門設計了由內置合約控制的機構帳戶，該機構帳戶的入金和出金受到一系列的參數所限制，可以保證投資人的資產安全。

### 4.6.1 基金專戶帳戶結構

**募資額度：**總募資額度

**清盤規則：**當帳戶觸發清盤線時，合約將會自動講帳戶資產按投資比例返還至投資人地址中

**募資人數上限：**最多募資人數


**分紅模式：**基金的分紅模式會在合約上寫好，系統會根據分紅模式，在分紅日自動分紅。

**結算日期：**基金的結算日子。

機構需要成立一支基金募資的時，可以開設一個 BAC Chain 的基金專戶地址，並設置相關的募資額度，分紅模式和清盤規則等。設置完畢後，儘管基金管理人持有該帳號的私鑰，但是無法通過分紅模式和清盤規則外的手段提幣。

基金經理可以管理該帳戶的資產通過去中心交易所交易獲得利潤。智能合約會根據利潤情況和分紅模式設定自動在分紅日進行分紅，將收益轉入投資人地址。





基金經理也可以借助去中心借貸功能，存入穩定幣獲得固定收益，分散配置資產，也可以質押小幣，獲得穩定幣，在小幣種價格下跌後買回來做空市場。

基金專戶不僅可以簡化基金的募資和分紅等管理流程，還可以增加基金的透明度和可信度。

BAC Chain 使用內置合約的形式，給用戶提供了完備的去中心化金融應用，可以滿足絕大多數的應用需求，其中包括，交易，借貸，理財，存款，征信等。



## 第五章、其他區塊鏈應用

### 5.1 物流追溯

區塊鏈在物流追溯應用上有很大的優勢，特別是在食品安全以及原產地證明和綠色有機產品溯源等領域，區塊鏈不可篡改的特性，可以賦予溯源更大的可信度和更低的成本。特別是當區塊鏈技術和物聯網技術相結合的時候，可以發揮出極大的效能。

用戶可以利用物聯網溫度數據，氧氣含量和地理位置等感測器，採集整個物流關鍵環節中的相關數據，並記錄在 BAC Chain 區塊鏈上，並啟用預警，並即時監控數據；基於區塊鏈的不可篡改特性，可以保證數據的安全有效性，並制定出一整套物流溯源系統。基於數據的分析和監控，系統可以保證物流流程的整體安全性，並在出現問題的時候，準確召回有缺陷的產品。另外，物流數據也可以與保險公司和有關部門共用，幫助其提供更加全面的保險和監管。

### 5.2 數字版權

在互聯網，數字資訊很容易被複製和傳播。如果數字資訊的分發通過 BAC Chain 的解決方案，可以將版權登記、內容分發、版權轉讓等相關數據存儲在區塊鏈上，相關非結構化數據可以存儲在存儲網，並且保證同時只有一個副本被傳播，實現知識產權可追溯。該解決方案立足區塊鏈技術的不可篡改性、公開性、透明性等特點，可以減少內容提供方對版權登記、內容分發、版權交易的成本，實現點對點分發，使內容流通和交易更加快捷、透明。

### 5.3 支付

BAC Chain 的 POS+PBFT 混合共識機制，可以保證單筆轉賬基本上可以在 5 秒內在鏈上被確認，用戶的鏈上轉賬確認時間和當下中心化的線上支付系統的確證時間相差無幾，可以給用戶提供與現在支付寶和微信支付等系統相近的支付體驗。配合幣威錢包的應用層功能，可以以去中心化的形式完成，掃碼支付，刷臉支付等功能。

## 第六章、BAC Chain 技術詳情

幣威鏈 Bit Asset Chain(BAC Chain)，是由幣威資產管理平臺研發的去中心化的高性能數字資產管理公鏈。幣威鏈的設計理念以先進的高可靠性，高性能技術為核心，搭配成熟的經濟系統和經過長期實踐積累的社區治理機制，並一系列的以用戶體驗為重的配套應用和開發工具，力圖打造全球性的高效的、可靠的、易用的、並能夠滿足全方位應用場景的數字資產公鏈。

### 6.1 經濟系統

BCV Chain 是一條基於 POS 共識體系的面向資產管理服務並支持企業級應用的高併發公鏈。為了解決傳統 POS 共識機制無法避免通貨膨脹的缺點，BCV Chain 改良了現有的 POS 經濟系統，設計出了 ZI-POS (Zero Inflation Prove of Stake) 經濟模型，該模型將傳統 POS 系統與經典的比特幣數學模型相結合，建立了一套具有通縮屬性的 POS 經濟系統，可以為生態節點和參與投票的社群用戶創造更多收益。

#### 6.1.1 獨創 ZI-POS 共識機制 (Zero Inflation Prove of Stake)

傳統 POS 共識機制有以下缺點：

通貨膨脹：儘管不同的 POS 專案都擁有自己的增發機制和不同的獎勵額度，但是總的來說，傳統 POS 共識機制給驗證節點的獎勵是通過通脹機制增發代幣而產生的。

傳統 POS+比特幣數學模型比較

	ZI-POS	POS	POW
幣種	雙幣種	單幣種	單幣種
性能	高	高	低
去中心化程度	低	低	高
通縮/通脹	雙幣雙通縮	通脹	滿足一定條件通縮
挖礦	銷毀	抵押	實體礦機

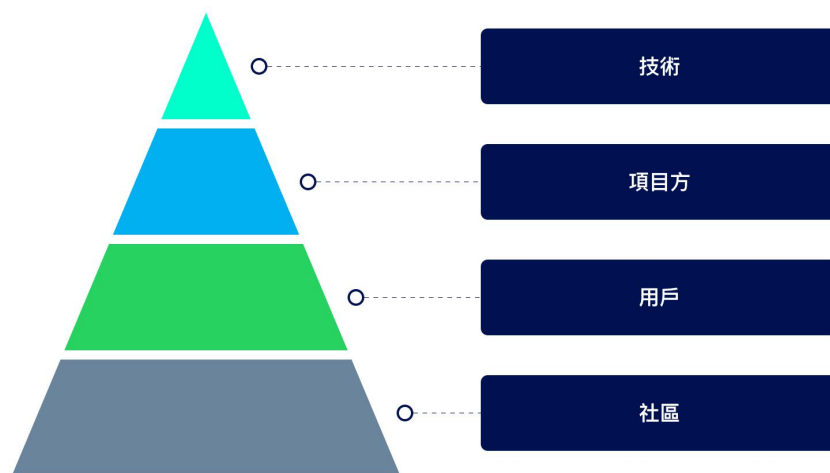
### 6.1.2 雙幣制

#### 為什麼雙幣？

在一個經濟系統中，資產按照用戶的持有意圖，可以分為兩種。第一種是可以升值的資產，這類資產人們願意長期持有，而把它花掉的意願比較低。另一種是高流通性的資產，這種資產或許升值潛力不如第一種，但是有很高的認可度，可以很輕易的流通起來，人們願意對這類資產進行轉移和交換。這兩種資產存在一定的矛盾性，如果經濟系統中只有一種資產，人們會在花掉它，還是存起來之間產生糾結。為了解決這個問題，我們採用了雙幣制度，將期望長期持有的權益通證與用來支持主網流轉的礦工手續費通證分開，以更好的滿足用戶的需求，降低人們的困擾。

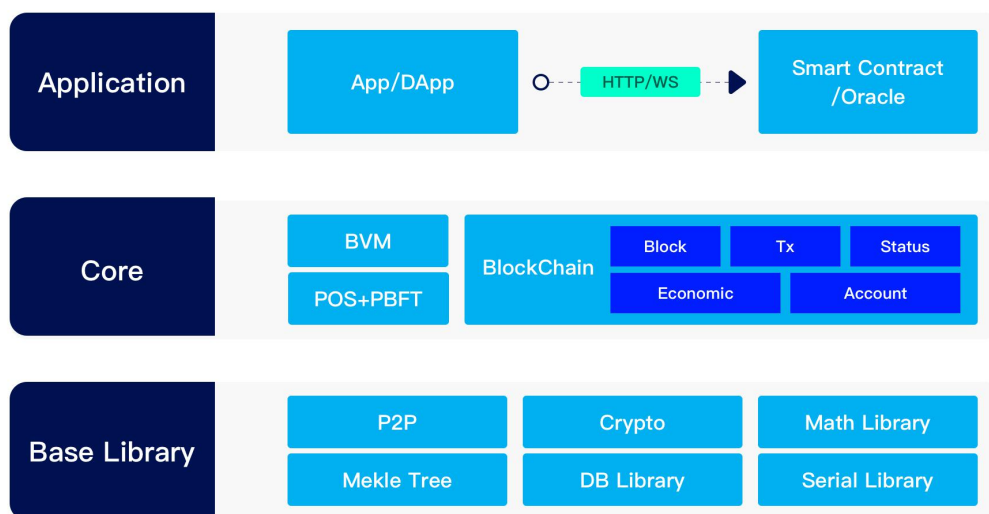
**權益通證：**BCV 用於公鏈驗證節點的權益抵押

**挖礦通證：**BAC（BCV for Circulation）用於驗證節點的挖礦獎勵，以及支付使用公鏈的轉賬手續費等。



## 6.2 總體模組

BAC Chain是一條致力於數字資產服務的可監管的，高性能的，完全去中心化的資管公鏈。主要分為如下模組：



#### Base Library : 為BAC Chain提供基礎庫服務

P2p 提供節點之間的消息傳輸提供服務

Crypto 提供了公鏈所需要的密碼學功能

Math Library 計算庫:提供精度計算服務

Merkel 提供消息摘要，壓縮等功能

DB Library 提供公鏈所需要的存儲服務

Serrial Library 提供消息數據的序列化服務

#### Core:BAC Chain的主要組件

BVM 為智能合約提供執行環境

Block 提供區塊的存儲檢索區塊服務

Tx 提供交易的存儲檢索服務

Status 提供公鏈對象當下或者以前某版本的數據狀態

Economic 公鏈的經濟模型

Account Model 帳號模型，管理帳號資產

#### Application 應用層:

App/Dapp 為用戶提供服務

Smart Contract 智能合約

Oracle 預言機

## 6.3 POS+BFT 共識

隨著區塊鏈的不斷發展，區塊鏈用戶的數和各種運算元的增加，對共識演算法的安全性可靠性和性能要求也越來越高，目前pow協議非常耗費資源，交易確認慢，DPOS比較中性化，BAC Chain使用POS+BFT的共識模式，實現共識的快速達成。

### 6.3.1 POS 模型

在BAC 中，POS模型包括以下三個步驟：

#### 6.3.1.1 創建驗證人

成為驗證人需要初始化如下參數：

- A、節點公鑰：該公鑰對應的私鑰會對區塊和共識狀態做簽名，該公鑰會被各節點作為區塊驗證和hash狀態。
- B、節點名稱：該節點名稱會在主網上展示，作為標識
- C、抵押數量：節點自身抵押BCV獲取的投票權數量，數量越大會，越能被礦工認可。
- D、最小抵押比例：節點自身抵押數量占總該節點總抵押量的比例。

#### 6.3.1.2 礦工投票

礦工想獲取收益，可以銷毀BCV獲取投票權，然後將投票權投給驗證節點。驗證節點承擔驗證區塊，打包交易，產生區塊的功能，經濟模型會對驗證節點作出獎勵，驗證節點根據礦工的票數把收益分給礦工。因為驗證節點需要有穩定的網路，硬體設備或者雲服務。如果驗證節點不能穩定的出塊，系統將消滅節點和節點下礦工的權益，這有助於礦工選擇更優秀的節點進行投票。

#### 6.3.1.3 分配模型的簡化

每個區塊產生之後，驗證人都會分到獎勵，然後將這些獎勵分配給他的礦工，如果每次出塊都做這樣的迭代會消耗大量的資源，甚至將會影響系統的整體運行。BAC Chain使用如下模型進行簡化處理

一個礦工在高度 $h$ 給驗證節點抵押了 $x$  bcvstake 驗證節點在區塊 $i$ 的總抵押數量為 $s_i$ ，分到的總獎勵為 $f_i$  礦機在區塊 $n$ 處提現，則可以提現的獎勵為

$$\sum_{i=h}^n \frac{x}{s_i} f_i = x \sum_{i=h}^n \frac{f_i}{s_i}$$

在一段時間內，如果沒有新的礦機或者節點抵押， $s_i$ 會保持不變，稱這樣保持不變的一段區間為 $p$ ，在這一段區間內，驗證節點 $v$  收到的獎勵為 $T_p$ ，抵押的資產為 $N_p$ ；如上礦工在高度 $h$ 開始挖礦，開始的區間為 $p_{init}$ ，結束的區間為 $p_{final}$ 則上式可以表述為

$$x \sum_{i=h}^n \frac{f_i}{s_i} = x \sum_{p_{init}}^{p_{final}} \frac{T_p}{N_p}$$

$p_0$ 為驗證人第一次抵押的區間

礦機需要抵押挖礦的時候會創建一個數據結構 $entry_f$  定義 $entry_f$ 為

$$entry_f = \sum_{i=0}^f \frac{T_i}{N_i} = \sum_{i=0}^{f-1} \frac{T_i}{N_i} + \frac{T_f}{N_f} = entry_{f-1} + \frac{T_f}{N_f}$$

針對每次驗證節點抵押數量變化都會創建一個 $entry_f$ 。則礦機在區間 $k$ 成創建礦機，在區間 $f$  從提交收益，他應該提取的收益為

$$x \sum_{i=k+1}^f \frac{F_i}{N_i} = x \left( \sum_{i=0}^f \frac{F_i}{N_i} - \sum_{i=0}^k \frac{F_i}{N_i} \right) = x(entry_f - entry_k)$$

BAC Chain會存儲從區間 0 到區間 $k$ 每個區間 $i$ 單位抵押量對應的累積獎勵為 $entry_f$ 。這樣在處理每個礦機獎勵的時候，就不需要迭代每個區塊，減少計算複雜度。

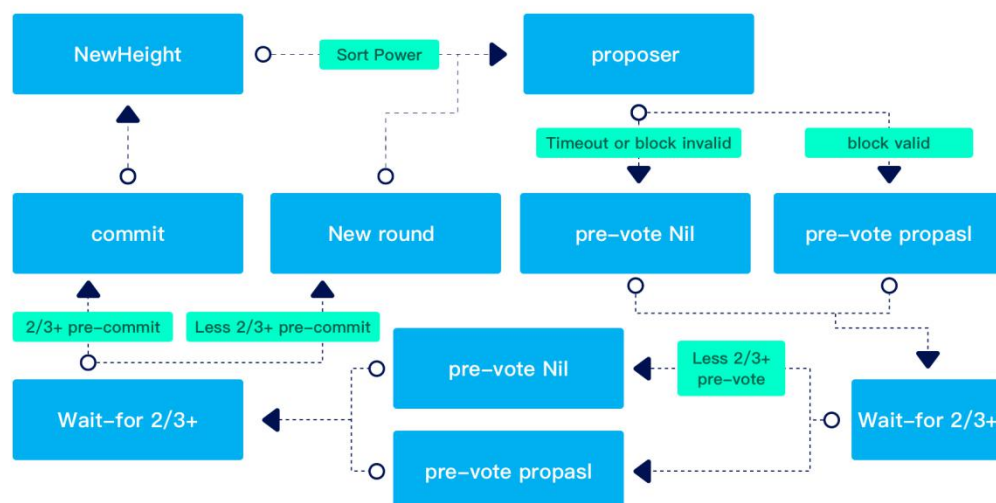
### 6.3.2 BFT 共識過程

協議中有兩個角色：

- A、 驗證人:不同的驗證者在投票過程中具備不同的權力（power），power來自自身抵押和礦機委託
- B、 提議人：由驗證人輪流產生。

驗證人輪流對交易的區塊提議並對提議的區塊投票。區塊被提交到鏈上，且每個區塊就是一個區塊高度。但區塊也有可能提交失敗，這種情況下協議將選擇下一個驗證人在相同高度上提議一個新塊，重新開始投票。

驗證人按照power比重，選出proposer，proposer針對當前高度提出出塊提案(Block Proposal)，每個區塊就對應一個高度，所有驗證人收到Block Proposal之後會發起pre-vote投票，當節點收到超過 2/3 的驗證人在同一輪提議中對同一個塊進行了pre-vote投票之後會進入pre-commit階段，當節點收到超過 2/3 的驗證人在同一輪提議中對同一個塊進行了pre-commit投票之後認定該區塊已經被超過 2/3 的人認可，會commit該區塊



#### 6.3.2.1 Block Proposal 過程

節點根據上一輪狀態選擇出當前power最大的節點作為出塊節點，該節點會搜集本地交



易池的交易，封裝成block，然後把該block包含在proposal中廣播出去。由於離線或者網路延遲等原因，可能造成提議人提議區塊失敗。這種情況在共識中也是允許的，因為驗證人會在進入下一輪提議之前等待一定時間，用於接收提議人提議的區塊，該過程相當於pBFT的pre-prepare階段。

### 6.3.2.2 Pre-Vote 過程

一個節點收集到一個完整的提案，它會校驗該提案中的區塊的正確性，然後對該區塊進行pre-vote投票，如果該節點在提案時間之內沒有收到提案，他會投遞一個空票。節點在pre-vote時間段收集其他節點的pre-vote投票，在當該節點獲取超過  $2/3$  的pre-vote會進入pre-commit階段。進入該過程相當於pBFT的prepare階段，目標是防止出現prosoal節點是BFT節點。

### 6.3.3.3 Pre-Commit 過程

當節點獲取超過  $2/3$  的pre-vote投票後會進入pre-commit階段，該節點會投pre-commit票，如果該節點在pre-vote沒有收到超過超過  $2/3$  的投票，則在在pre-commit階段投遞Nil票。在該階段節點會收集其他節點的pre-commit的票，如果收集到超過  $2/3$  的投票，節點會commit該區塊，同時修改驗證點power值。該過程相對於pBFT的commit階段，目標是當收到超過  $2/3$  的節點都同意commit該區塊的時候則commit該區塊。

## 6.4 費用模型和激勵體制

費用模型和激勵機制是激發整個參與生態的重要保障，對主網的安全穩定的運行至關重要。

### 6.4.1 出塊獎勵

BAC Chain使用類似比特幣獎勵模型，初始每塊獎勵 10 BAC，每半年減半一次，詳細



獎勵如下：

時間	每塊獎勵個數	每天獎勵數	截止發放獎勵總數	減半高度
第一年前半年	10	132920	24275070	2427508
第一年後半年	5	66460	36412605	4844015
第二年前半年	2	26584	41267619	7282522
第二年後半年	1	13292	43695126	9710029
第三年前半年	0	0	43695126	

#### 6.4.2 鏈上交易 gas 消耗

鏈上交易 gas 也可以根據公鏈驗證節點治理需求進行調整，現在設置如下：

迭代操作	1000nbac
寫操作每byte	30nbac
寫操作	2000nbac
寫操作每byte	3nbac
讀操作	1000nbac
刪除	1000nbac
存在判斷	1000nbac

#### 6.4.3 交易 hash gas 消耗

每執行一筆交易都需要消耗gas，這次交易消耗的gas等於本次交易所用操作執行的總和。

#### 6.4.4 驗證人委託

驗證人在創建的時候需要抵押bcv兌換成bcvstake，這些bcvstake可以兌換回來，重新兌換成bcv。

#### 6.4.5 礦機挖礦銷毀

礦機在創建的時候需要銷毀bcv換成bcvstake，此bcvstake將不能贖回。

#### 6.4.6 挖礦能量銷毀

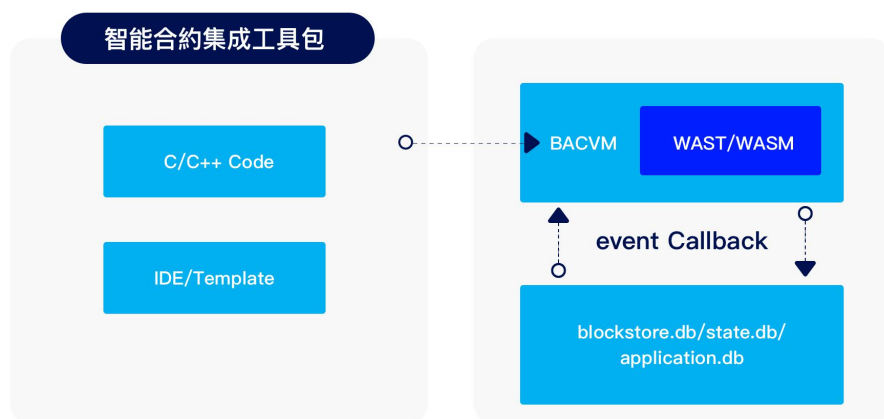
挖礦需要消耗電量(energy)，礦機在挖礦過程中需要消耗電量，1bcv stake 1 個高度消耗 1 個energy，用戶可以銷毀bcv兌換energy。

### 6.5 智能合約

智能合約對金融資管公鏈必不可少，BAC Chain智能合約不僅具有圖靈完備，使用靈活，安全可靠等智能合約等基本特點，還提供了生態友好的合約引擎BVM。BVM通過webAssembly和預言機技術等為合約提供了執行安全，性能，多語言等支持。智能合約執行如下圖

### 6.6 預言機

BAC ORACLE模組是預言機的實現，主要分為內部預言機和外部預言機，預言機建立了智能合約和數據的可讀通道。BAC ORACLE通過預定義的可配置預言機，智能合約可以確保只有在智能合約驗證條件滿足後才會真正發生價值轉移，同時讓智能合約可以同外部數據進行交互。同時，根據約定的合約規則履行情況可以避免糾紛。預言機智能合約可以持任何的JSON API類型。



## 6.7 治理

BAC Chain 允許任何持有 bcvstake 的用戶參與到公鏈的共同治理共同治理區塊鏈。Bcvstake 可以通過 bcv 抵押或者銷毀得到，Bcvstake 的持有者可以通過簽署特殊類型的交易來提交提案或者表明他們是否支持（或不支持）提交給區塊鏈網路的提案。治理主要分如下步驟

### 6.7.1 存款階段

任何 bcv 代幣持有人都可以發起提案，對於想要進入到投票階段的提案，需要在提交該提案之後的兩周時間記憶體入至少 1000 bcv 代幣，這是進入到投票階段的最低存款金額要求。除提案發起人之外，其他人也可以只發送一筆存款的交易為該提案提供存款。提案被創建之後可以被查詢，用戶可以通過瀏覽器查詢提案進展。當提案在規定時間達到存款要求，提案會被通過，如果在規定時間內不能達到要求，提案會被否決。

### 6.7.2 投票階段

一旦提案滿足了最低存款限額要求，提案會進入一定時間的投票階段。在此期間，所有抵押礦機，即 bcvstake 的持有者可以對該提案進行投票，目前有四個投票選項，分別是“是”、“否”、“行使否決權的否定（No with Veto）”、“棄權”。

bcvstake的持有數量決定了對提案決策的影響力。礦機可以繼承驗證人的投票，如果礦機沒有投票，驗證人的投票會覆蓋驗證人的決定。

### 6.7.3 投票結果

在提案投票階段接受後，投票至少需要滿足以下幾個條件都滿足才會被接受。

超過 40% 的bcvstake 參與投票

需要超過 50% 的bcvstake 支持該提案（即選擇的投票結果是 “是”）；

低於 33.4% 的 bcvstake 行使 “否決權（No with Veto）”。

如果在投票階段結束時上述要求中有任何一項沒有滿足，比如法定人數沒有達到，那麼該提案就不能被通過。如果提案沒有通過，提案的存款不會被退還，會被納入到社區池中，如果通過了則退換存款。

BAC Chain治理仍處於早期階段，會隨著生態社群意見逐步改進。

## 6.8 數據存儲

區塊鏈的分佈式帳本僅限於存儲簡單的交易數據，而不能存儲過大的文檔，如事務歷史記錄，歷史數據等繁雜的數據流需要專門的存儲空間，尤其是非結構化文檔，更是無法在區塊鏈上直接存儲，而非結構化文檔，比如合同電子檔備份，存證圖片，跟區塊鏈上的數據在業務上緊密關聯。為了支持關聯鏈上數據和相關的非結構化文檔，實現數據的快速存儲和查詢，我們引入了傳統分佈式檔系統跟區塊鏈系統關聯，形成了一個“可擴展性”和“去中心化”的開放存儲協議。

針對一個區塊鏈上的交易，如果交易存在相關的文檔，則將文檔的 MD5 Hash 值放在該交易記錄中，用一個專門的字段存儲。

在讀取該記錄的時候，先讀取鏈上數據，再根據該交易記錄中的 Hash 值定位到分佈式檔系統中，讀取文檔內容，在讀取的同時校驗該文檔的一致性，在確保 Hash 值匹配的情況下，表示該檔是正確的檔，而且本身安全可靠。

使用分佈式檔系統是第一步，第二步也可以進一步將檔存儲於去中心化的檔存儲專案中，比如 IPFS 以及 Lambda 等專案提供的服務中。

### 6.8.1 隱私數據保護

數據是未來最重要的生產資源，也是個人和企業未來最重要的隱性資產。如何讓這樣的隱性資產高效、合理、安全地存儲和流通起來，也是BAC Chain公鏈重點要解決的問題之一。BAC Chain會持續的探索隱私數據的存儲和流通中遇到的隱私洩露的問題

#### 6.8.1.1 數據加密存儲

BAC Chain把用戶數據在鏈外用私鑰加密後存儲在ipfs或者hdfs等多副本的檔系統中，然後用密碼學方式生成檔hash，加入到BAC Chain主鏈中，這樣能減少主鏈存儲資源的使用，也能讓數據在隱私存儲和公開訪問上有所選擇。

#### 6.8.1.2 數據授權訪問

非對稱加解密技術保證了數據在傳輸過程中，只有持有私鑰的雙方才能對內容進行解密，從而保證第三方無法對內容進行截取和爆破。BAC Chain 使用ECDH可以計算兩對公私鑰之間共用密鑰，從而實現帳號可以被授權訪問。

#### 6.8.1.3 隱私數據交換

BAC Chain可以在不同場景下考慮以下方案：

## 6.9 安全多方計算 (MPC)

由姚期智在 1982 年正式提出。它主要探討的是， $n$ 個參與方各自輸入資訊去計算一個既定的函數，在保證計算的正確性的同時，不洩露參與方輸入數據的隱私。具體來說，對於 $n$

個參與方，每個參與方*i*均知道自己的輸入 $x_i$ ，他們想協同計算一個既定函數  $f(x_1, \dots, x_n) = y$ ，使得所有參與方都能獲得最終的結果  $y$ ，但 無法獲知其他參與方的輸入數據。

### 6.9.1 同態加密 (HE):

同態加密是一種允許在密文上進行計算的加密方式。除了傳統加密方案的原始組件之外，還有另一種計算演算法，它將目標函數 $F$ 和加密數據作為輸入。同態加密會生成一個加密的結果，當解密此結果時，獲得的消息就像是在加密數據的明文上執行 $F$ 。支持 密文上的任意計算的密碼系統稱為全同態加密 (FHE)。

## 6.10 監管

### 6.10.1 社區監管

BAC Chain 通過投票選舉到方式，篩選出一類監管節點，監管節點會監管整個主網的運行情況，以及危機處理。例如發生盜幣的情況下，被盜者可以向監管節點申報暫時封鎖盜幣帳號，監管帳戶發送特定的交易，暫停盜幣帳號的轉賬功能，驗證節點收到這個交易後會執行該交易，盜幣帳戶會被臨時凍結。監管節點主要用於緊急處理危機情況。

### 6.10.2 政策監管

區塊鏈的去中心化是區塊鏈的優點，也是局限。在目前情況下，區塊鏈的使用者並不關心業務的安全性是由去中心化的區塊鏈提供背書的還是由政策權利提供背書的，區塊鏈也是需要接受行業和政策的監管的，BAC Chain通過隱私授權訪問的方法接受政策監管。

## 6.11 安全

### 6.11.1 中間人攻擊

中間人攻擊是一種由來已久的網路入侵手段，如 SMB 會話劫持、DNS 欺騙等攻擊都是典型的 MITM 攻擊。其原理是通過攔截正常的網路通信數據，並進行數據篡改和嗅探，而通信的雙方無法知曉。BAC Chain 使用類似 Station-to-Station (STS) 協議，在節點之間建立通信的時候建立共用密鑰，消息的傳播都會使用該密鑰加密，可以有效的避免中間人攻擊。

### 6.11.2 雙花攻擊

雙花攻擊是指當一個交易被發出後已經經過了  $z$  個區塊時，攻擊者又在極短的時間內重新產生了一條新的區塊鏈，使新鏈比之前的區塊鏈更快，這樣攻擊者就可以把以前的交易中的花費的虛擬貨幣取回來並用於二次交易。因為在區塊鏈中，系統會自動承認最長的那條鏈為有效鏈。BAC Chain 使用類似 pbft 的共識協議，一旦共識被達成，即不可更改，可以有效的避免這個問題。

### 6.11.3 女巫攻擊

Sybil 攻擊是指利用社交網路中的少數節點控制多個虛假身份，從而利用這些身份控制或影響網路的大量正常節點的攻擊方式。BAC Chain 使用 bcvstake 作為權利幣，持有幣才能獲取相應的收益和執行相關交易，所以雙花攻擊不會對 BAC Chain 造威脅。

### 6.11.4 分叉攻擊

分叉攻擊是指攻擊者直接或者間接獲得算力，讓他們幫助自己分叉出另外一條最長的區塊鏈。BAC Chain 在處理抵押關係的時候，如果某個驗證人的抵押量過大，礦機的抵押會被拒絕，這樣可以有效避免某個驗證人擁有過大的權利。



### 6.11.5 DDos 攻擊

拒絕服務攻擊（DDOS）亦稱洪水攻擊，是攻擊者使用網路上被攻陷的電腦作為“僵屍”向特定的目標發動“拒絕服務”式攻擊時其目的在於使目標電腦的網路或系統資源耗盡，使服務暫時中斷或停止，導致其正常用戶無法訪問。BAC Chain 可以哨兵模式，遮罩後端節點伺服器，有效地保護出塊機器，避免或者減少 DDos 的攻擊。

### 6.11.6 量子攻擊

目前區塊鏈系統上普遍使用的非對稱加密簽名演算法，比如基於整數因子分解難題的RSA演算法和基於橢圓曲線上離散對數計算難題的ECC演算法，可以被量子Shor演算法將NP問題變成P問題，從容易被破解。BAC Chain 體系會根據項目進度和量子電腦實用化的發展適時引入抗量子計算暴力破解的加密演算法，比如基於格的密碼系統（Lattice-based cryptography），基於編碼的密碼系統（code based cryptosystems）和多元密碼（multivariate cryptography）等；其中基於格密碼可以設計加密、簽名、密鑰交換等各種密碼系統，是後量子密碼學演算法的一個重要向。同時，我們也會對抗量子密碼系統的前沿研究向進行跟進。

## 6.12 擴展

隨著業務的發展，想要公鏈真正做到更深度化的應用和普及，公鏈最終會遇到一個關鍵的問題和瓶頸，就是解決交易的吞吐量和交易的速度問題，這在區塊鏈中也被稱作可擴展性，BAC Chain會持續探索公鏈以下各種可擴展性方案的實現。

### 6.12.1 單鏈可擴展性

假設每筆交易為 200Byte，在 10Mbps的傳輸寬頻下，吞吐量可以達到 6000Tps，普通硬碟的Tps可以達到 10000Tps以上，普通CPU可以達到 8000Tps，目前主流公鏈的Tps還遠遠沒有達到，使用優化的數據結構和演算法有可能進一步挖掘單鏈的性能，提高公鏈的Tps。



### 6.12.2 側鏈技術

側鏈（SideChains）是針對比特幣提出，所以這個概念後期也更多的是在描述比特幣相關的擴容，它的定義是：可以讓比特幣安全地從比特幣主鏈轉移到其他區塊鏈，又可以從其他區塊鏈安全地返回比特幣主鏈的一種協議。側鏈是一個獨立的系統，是一個隔離環境，即使內部出現問題，也不會影響到原有的系統。

### 6.12.3 分片

分片就是將區塊鏈網路劃分成若干能夠處理交易的較小的網路，每個小網路可以並行的處理未建立連接的交易，以提高網路的併發量，這樣隨著節點數名。

## 6.13 BAC 的配套生態

當下的區塊鏈技術，並不缺乏各種改進想法，反而最為缺少的是應用。沒有應用場景的技術，沒有未來。很多公鏈只考慮技術實現，在主網運行之後，沒有應用場景，沒有用戶，從使用上也根本無法發揮和創造價值，從而缺乏價值支撐，無法激勵參與者長久參與。

作為公鏈的生態，節點、礦工本身得到激勵，維護整個公鏈的基本運行，而在應用上的生態，我們主要從下麵 3 個角色分開說：

### 6.13.1 開發者

公鏈主網運行之後，依託公鏈底層開發公鏈應用，需要公鏈和開發者雙向構建開發者生態。公鏈開發團隊需要將公鏈代碼開源、提供主網服務調用API，各種語言與服務的SDK，配套開發測試工具，當然也包括所有這些技術工具的文檔。這些內容也可以由開發者社群完成。而開發者則基於公鏈的基本功能，基於面向最終用戶的業務需要，開發各式各類應用，包括工具、遊戲、金融、存證場景應用等。BAC Chain 將基於錢包提供開發所需要完善文檔、工具、SDK等，為開發者提供便利。

### 6.13.2 用戶

開發者所開發的應用要面向用戶提供服務，開發者以自己的服務價值獲得用戶增長，但是如果公鏈生態本身存在大量用戶和應用場景，則為開發者基於公鏈開發應用提供了重要動力和實驗場景，所以用戶也是公鏈生態非常重要的組成部分。

BAC Chain 生態與幣威錢包都是幣威生態成員，幣威錢包以百萬級用戶，為幣威生態提供用戶與流量支持，開發者開發的 BAC Chain應用，可以優先供給給幣威錢包用戶使用，公鏈為幣威錢包豐富了用戶的應用，幣威錢包又為開發者提供了低成本的實驗環境和便利的流通獲得管道。

## 第七章、技術路線圖

### 7.1 2020 年 4 月主網上線

主網穩定上線，實現持有BCV的用戶可以挖礦得到BAC。BAC作為支付手續費可以支持主網的流通。

### 7.2 2020 年 7 月存儲網上線

存儲網以及其他配套存儲設施上線，結合主網考慮存儲經濟模型，支持用戶持久的存儲數據。

### 7.3 2020 年 8 月推進開源，開啟應用

實現多種語言開發包的支持，並開放公鏈源代碼。對現有錢包和交易所業務開始挖掘，比如像帳戶資產驗證等上鏈，實現透明化運營進行探索。

### 7.4 2020 年 11 月實現去中心化交易協議

去中心化交易協議是資產管理和借貸業務上鏈的基礎，

### 7.5 2021 年 1 月內置合約實現 DeFi 業務模型

實現內置合約功能，以內置合約形式實現借貸、基金等模型，以實現對純鏈上DeFi業務的支持。

## 7.6 2021 年 6 月合約上線

智能合約開發完成，對適合智能合約的業務做一些遷移探索。

## 7.7 2021 年之後主網的擴展

加強已經在主網上運行業務的體驗，考慮對主網進行分片，分層，側鏈，跨鏈等擴容，使用成熟的技術手段達成業務目標。

## 第八章、參考資料

- [1] NAKAMOTO, S. Bitcoin: A peer-to-peer electronic cash system, 2008.  
<http://bitcoin.org/bitcoin.pdf>.
- [2] L. Lamport, R. Shostak, and M. Pease. The Byzantine Generals Problem. ACM Transactions on Programming Languages and Systems, 4(3), 1982.
- [3] A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER  
<https://ethereum.github.io/yellowpaper/paper.pdf>
- [4] Vitalik Buterin. Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform. 2013a. <http://ethereum.org/ethereum.html>
- [5] CRYPTOKITTIES. Cryptokitties, 2017. [https:// www.cryptokitties.co](https://www.cryptokitties.co).
- [6] cosmos white paper <https://cosmos.network/resources/whitepaper/zh-CN>
- [7]Slasher:  
<https://blog.ethereum.org/2014/01/15/slasher-a-punitive-proof-of-stake-algorithm/>
- [8] PBFT: <http://pmg.csail.mit.edu/papers/osdi99.pdf>
- [9] TheDAO: <https://download.slock.it/public/DAO/WhitePaper.pdf>
- [10] 0x protocol: <https://0x.org/docs>
- [11] uniswap:<https://uniswap.org/docs/v2>