MCC項目白皮書

MainstreamCodeWhitePaper

2018/09 V1.1.2

創新的多元化數字資產交易平台
下代數字資產交易開拓者

目 錄

1. 背景

自比特幣誕生以來，以區塊鏈技術為基礎的數字資產蓬勃發展。如今，數字資產的種類和影響力與日俱增。數字資產的公允價格形成、不同數字資產間的兌換交易，以及相關的客戶服務、監管合規，甚至是衍生品交易都是基礎的需求。當前，承載這部分需求的是各種各樣的數字資產交易平台。在數字資產不長的歷史中，這些平台發揮了極大作用，同時也發生過嚴重的事故。這些問題，與其歸咎於交易平台自身，不如說是傳統模式的交易平台已經不能適應新的數字資產時代的要求。

基於區塊鏈技術的數字資產的誕生，使得資產和交易的全透明、可自證成為可能。這將推動未來公司及監管治理結構的變革。我們認為這個變革的方向是，公司向社區進化，監管向技術靠攏。而數字資產交易平臺本身，擁有引領此變革的能力和責任。於是，我們發起了MCC。

2. MCC全球首家自治型數字資產交易平台

MCC交易平台

MCC致力於創建一個自治的、高效的、透明的數字資產交易平台，讓交易員和投資者可以放心地進行任何規模的交易，而無需擔憂平台的公正性和透明性、數據安全隱私保護的可靠性、或其訂單管理系統的完整性和穩健性。

同時，MCC不是傳統意義的公司，它邁出了數字資產交易平台向社區進化的關鍵一步。 MCC社區是一個公開透明的、Token化的組織，MainstreamCode currency Token代表MCC交易平台的所有權益。 MCC採用“交易即挖礦”模式，超過一半的MCC將通過手續費挖礦的形式獎勵給社區用戶。更加特別的是，MCC社區會將50%的收入分配給MCC的持有者。我們會依照收入的組成，等比例的將這部分收入進行分配。

3. 交易平台優勢

MCC的使命是為投資者投資、交易及管理數字資產營造公平理想的環境。因此，平台設計的目標就是全面的保證訂單的公正性和透明性。並可以以最安全和最有效的方式滿足安全、審計、報告、分析等監管合規方面的需求。

公開透明

MCC將是世界範圍內首個實時公開透明的交易社區。傳統類型的交易所無法做到

資產的公開透明，最主要的原因是受到了技術的製約。而區塊鏈技術的誕生使這一目標在技術上變得可行。 MCC的使命就是把這種可行性轉化為真正的實踐。 MCC將建立實時的資產與交易數據查詢驗證機制，並面向公眾公開。

社區型自治組織

MCC不使用傳統中心化的公司架構，不設CEO和董事會。 MCC依托區塊鏈技術和通證經濟理念，將是世界範圍內首個自治的社區型交易平台。 MCC通過“交易即挖礦”的模式，將60%的MCC獎勵給社區。同時，MCC將50%的收入分配給MCC的持有者，並由全體MCC持有者通過智能合約投票完成社區治理。

金融級交易系統

MCC的交易系統可以實現金融級別的快速和穩定，使交易高效有保障。 MCC提供證券級先進算法，支持GTT、GTC、FOK、IOC等多種專業交易指令，為交易者提供專業量化支持，撮合借鑒了LMAXExchange的相關經驗，能夠每秒處理200萬筆交易。

安全防護

對數字資產交易來說，安全是重中之重。 MCC採用基於多重簽名、離線簽名、分層架構等安全設計，將95%數字資產存儲在冷錢包中。無偏性零知識訂單加密通過CertEurope6的PKI-on-blockchain服務提供的密鑰完成。我們將進行定期的外部審計。

4. 數字資產篩選標準

區塊鏈的現實意義是把技術創新和金融創新融為一體，利用基於數學算法構造的一整套全新的激勵體系，通過重構協作關係來進一步解放生產力。在這個背景下，大量真實的創新會脫穎而出，同時也會不可避免的伴隨出現大量圈錢及欺詐行為。

我們會結合數字資產的特點和世界頂級交易平台、相關監管機構的經驗，形成一套篩選數字資產的標準與機制，通過這套標準和機制的不斷迭代完善，MCC將與市場投資者共同發掘數字資產價值。我們的核心理念是，不代替市場做價值判斷，而強調對項目的透明度和治理結構的要求，保證社區的權力與利益。

5. MCC(MainstreamCode currency Token)

什麼是MCC?

MCC是MainstreamCode currency Token的簡稱，前期是以太坊ERC20標準代幣（目前團隊已將主鏈完善成熟，已经推出上線自主研發的MCC主鏈，可1:1兌換主流貨幣）。MCC通過“交易即挖礦”的方式產生，總量50億，永不增發。其中60%由礦工挖出，其餘40%為預先發行且凍結，凍結部分也隨著礦工挖礦而按日解凍。

交易所權益+公鏈，挖礦激活後每天分紅交易所當日手續費，公鏈的礦工每次挖礦流通湮滅10%.全網總共湮滅99.49%，最終剩餘2100萬枚。

MCC會將大部分收入及時分配給MCC的持有者。同時，MCC持有者共同享有社區的治理各類權利。

挖礦詳細規則

在MainstreamCode currency進行交易即被視作挖礦，交易用戶即被視為“礦工”，挖礦產出物為平台幣MCC，MCC引入智能調節機制，挖礦產出依據交易所交易量智能調節。

您僅需在MainstreamCode currency交易，產生的交易手續費會折算為MCC，每六個小時發放一次，統一返還至您賬戶。

MCC使用場景

1. 交易分紅

擁有MCC就像擁有了MCC交易所的分紅憑證，可以享受交易所的每天收益的分紅。

2. 發布側鏈

可以使用MCC支付礦工費用用於開通屬於自己的數字資產，就像在以太坊上發行數字資產一樣。

3. 投票上市

發行的數字資產在MCC全球交易所上市時，可以使用MCC抵扣上市需要的手續費等費用，也可以使用MCC對要上市的數字資產競選進行投票。

4. 費用抵扣

在需要往主鏈上存儲信息向整個網絡宣告時，可以使用MCC給礦工抵用存儲費用。

5. 超級節點表決權

用MCC表決公鏈超級節點的挖礦權。

MCC權利

Token作為可流通的加密數字權益證明，將成為未來數字經濟時代的基本要素。MCC作為MainstreamCode currency社區權益的代表，是MainstreamCode currency社區治理的基石。

權利	說明
收入分配	MCC交易平台的收入，第一個月：50%分配給MCC持有者，50%用於回購市場上流通的MCC;一個月後：50%分配給MCC持有者，35%用於回購市場上流通的MCC，15%用於中冶開發及運營費用。
參與決策	MCC社區通過發起智能合約投票，讓MCC持有者參與重大經營事務的決策。
選舉和監督	MCC社區委員會成員定期換屆，MCC持有者可以參與委員會成員的選舉，也可以對平台的透明程度和委員會成員的盡職程度進行監督。

6. MCC臨時章程

什麼是臨時章程？

本章程是基於應用區塊鏈優勢的多方所簽訂而成。這部章程是臨時的，直至正式

章程公民投票的形式製訂和批准之前，它都具有有效性。

什麼是全民公投？

全民公投，即全民公決，在重大事項的確定、涉及事項產生分歧無法解決時，MCC採取全體公民投票的方式來解決。

修改章程的發起條件？

公投發起條件：1000萬個MCC擁有發起權，抵押發起投票，投票期間MCC進行凍結，凍結期不享受收益，投票結束釋放。

第一節　章程修改

本章程及其附屬文件不得修改，除非發起全民公投，並且有超過51%的token持有者投票贊成；

第二節　MCC公鏈

交易所權益+公鏈，挖礦激活後每天分紅交易所當日手續費，公鏈的礦工每次挖礦流通湮滅10%.全網總共湮滅99.49%，最終剩餘2100萬枚。

礦工費用

轉賬	1個MCC(其中礦工收0.9个MCC，湮滅0.1个MCC)
發行側鏈	1000個MCC(通過公投表決是否增加動態計費，礦工收取900個MCC，湮滅100個MCC)
SDK調用API (支持Java Go語言)	收費標準後期推出
智能合約	收費標準後期推出
IPFS	收費標準後期推出

第三節　MCC交易所

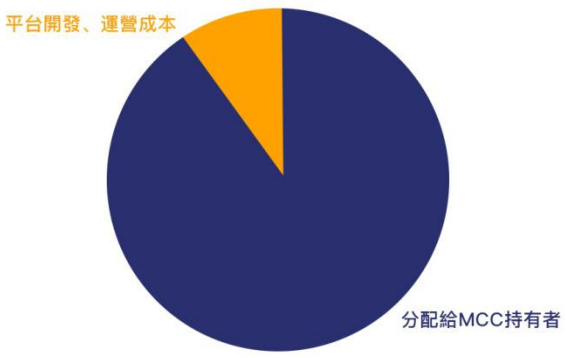
MCC是擁有主鏈的去中心化交易所，本次發行的MainstreamCode currency Token 後續會升級為全球連鎖交易所公認的主鏈（目前主鏈已經自主開發完成，可1:1兌換主鏈貨幣。）另外，每個MCC持有者都有權利參與社區的業務決策、團隊選舉等社區活動。MCC是一個所有持有者共有、共治、共享的社區型組織。

交易所章程

（DPOS機制）

手續費	不同的交易對收費不等		
上市(数字资产)	抵押1000萬MCC 1個月(or 3個月，公投決定)		
分紅機制			
15%			85%
5% MCC基金	5% 公投 全球四大節點服務客服	5% 公投 開發團隊獎勵	持有MCC的大眾

MainstreamCode currency開放交易第一個月會會平台總收益50％獎勵給持有MCC的用戶，50％用於回購市場上流通的MCC。後期會將平台總收益的50％作為分紅獎勵，獎勵給 持有MCC的用戶；35％用於回購市場上流通的MCC；5％作為四大節點（美國，韓國，馬來西亞，加拿大）運營成本; 5％作為平台開發費用）（按照代碼貢獻分配）;5％作為MCC基金。全天24小時，每留个小時對持MCC賬戶進行快照，統計每賬戶應得分紅額度，每六個小時會將分紅獎勵發放至MCC持有者賬戶。



分紅規則：

1.分紅機制為MCC持有者權益，僅MCC持有者可得分紅

2.每六個小時為一個分紅週期，平台按週期發放分紅

3.每留个小時快照一次，計算應發分紅，累計六個小時發放一次

4.分紅所得幣種以平台實際獲得手續費為準

*僅限流通的MCC方可參與分紅，未解鎖部分不參與

計算公式：

每百萬份MCC分紅=（平台當日總收益*50%/MCC總流通量）*1,000,000

礦工當日分紅收入=MCC持有量/MCC總流通量*平台當日總收益*50%

回购MCC规则：

平台第一個月會將平台總收益50%（一個月後改為35%）用於回購市場上流通的MCC，回購地址將在交易所網站進行公示，回購所得MCC屬於所有MCC持有者，使用需要在MCC社區中發起投票並獲得超過一半的投票支持。

第四節　MCC發行機制

我們使用“挖礦同步釋放”的機制來完成MCC的發行。

社區獎勵部分：60%比例的MCC通過“交易即挖礦”的方式，逐步分配給交易用戶，每日發放。（挖完即止）

預先發行部分：40%比例的MCC通過預先發行的方式被基金、團隊所持有（伴隨挖礦解凍）

預先發行部分解凍規則：

為了保障所有人獲得平等的收益權，將“預先發行部分”全部凍結，並按照如下公式按日等比解凍：

每日解凍數量=預先發行MCC總量*（前一日挖礦的總產出量/挖礦總量）

第五節　MCC聯盟交易所

MCC開放共贏計劃首期將開放100個名額，開放交易所將支持多種費率模式，首期100家將採用平台幣的運作模式，細則如下:MCC開放共贏計劃將支持每家交易所運營方發行平台幣，每家交易所平台幣的60%“挖礦部分”，40%為“發行部分”。挖礦部分:每家交易所的挖礦部分通過“交易即挖礦”的模式獎勵給交易用戶，每日發放。交易平台每六个小時都會將用戶在該交易所產生的交易手續費，100%折算成平台幣進行

累積，折算價格按該小時平台幣的均價計算(均價計算方式為總成交金額/總成交量)。我們將每间隔六个小时将累積的平台幣返還。交易平台手續費部分:收入以50%將作為鼓勵金分配給本交易所平台幣持有者(只有挖礦產出的部分及已經解凍的“發行部分”參與分配)。發行部分:該交易所發行部分預先全部凍結，根據挖礦部分已挖出的比例同步解凍，每日發放。

申請條件（需要滿足以下條件）：

1.需要抵押1000萬MCC 10年，並且支付100萬MCC開通交易所費用給四大節點用於矿工宣告。

2.請開通交易所。

3.所在國家合法手續。

4.與MCC交易所機制一樣。

5.同意交易所管理條例。

交易所收益：

1.交易所手續費。

2. 平台資產發行。

3.資產上市權。

4. MCC節點支持、技術社群支持、基金優先投資支持。

7. 交易平台路線圖

8. MCC主鏈核心概念與組件

MCC首創全球連鎖交易所理念，未來將在全球開通100家連鎖交易所。 MCC主鏈

將用於解決用戶從主鏈發行數字資產到上市融資流通一系列需求。本次發行的MCC主鏈為全球連鎖交易所公認的主鏈。

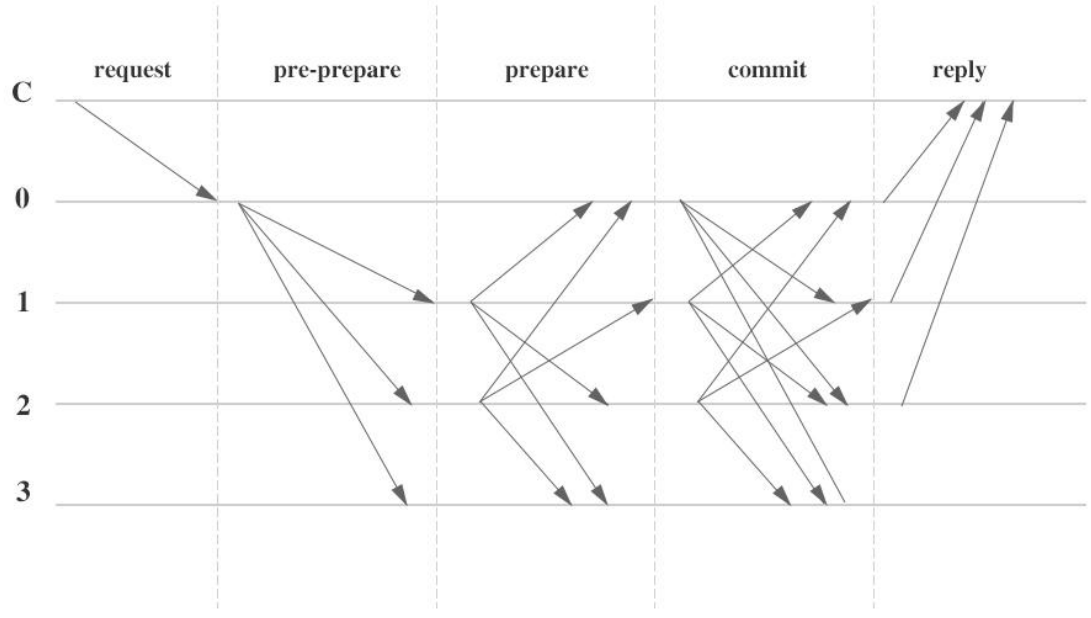
MCC主鏈核心組件

1. 共識算法(PBFT)

MCC鏈採用了目前最優的去中心化共識算法—實用拜占庭容錯算法PracticalByzantineFaultTolerance(PBFT)。這是一種基於消息傳遞的一致性算法，算法經過三個階段達成一致性，這些階段可能因為失敗而重複進行。

假設節點總數為3f+1，f為拜贊庭錯誤節點：

1) 當節點發現leader作惡時，通過算法選舉其他的replica為leader。
2) leader通過pre-prepare消息把它選擇的value廣播給其他replica節點，其他的replica節點如果接受則發送prepare，如果失敗則不發送。
3) 一旦2f個節點接受prepare消息，則節點發送commit消息。
4) 當2f+1個節點接受commit消息後，代表該value值被確定。如下圖表示了4個節點，0為leader，同時節點3為fault節點，該節點不響應和發出任何消息。最終節點狀態達到commited時，表示該輪共識成功達成。



優點：上述共識算法都脫離不了幣的存在，系統的正常運轉必須有幣的獎勵機制，系統的安全性實際上是由系統幣的持有者維護保證。當我們區塊鏈系統實際

運用到商業應用時，由其承載的資產價值可能遠遠超出系統發行的幣的價值，如果由幣的持有者保證系統的安全及穩定性將是不可靠的。

a) 系統運轉可以脫離幣的存在，pbft算法共識各節點由業務的參與方或者監管方組成，安全性與穩定性由業務相關方保證。

b) 共識的時延大約在0.1~0.2秒鐘，達到商用實時處理的要求。

c) 共識效率高，可滿足高頻交易量的需求。

根據這一算法，在使用MCC鏈構建的區塊鏈上持有通證的人，可以通過一個持續進行的投票系統來選擇區塊生產者。任何人都可以選擇參加區塊生產，只要能夠說服通證持有人為其投票，就會有機會參與區塊生產。

MCC鏈可以讓區塊每0.1s生成一個。任何時刻，只有一個生產者被授權產生區塊。如果在計劃的某個時間內沒有成功出塊，則跳過該塊。如果有一個或更多的區塊被跳過，則在區塊鏈上會有0.1s或者更久的空白。

使用MCC链，区块的产生是以30个区块(每个出块者六个区块，乘以5个出块者)为一个周期。在每个出块周期开始时，会根据通证持有人所投票数选出5个区块生产者。被选中的区块生产者的顺序会根据5个区块生产者的同意，制定出块顺序的安排。

如果出塊者錯過了一個塊，並且在最近24小時內沒有產生任何塊，則這個出塊者將被剔除在考慮範圍之外，直到他們通知區塊鏈可以重新開始產生區塊。這確保了網絡的順利運行，把被證明為不可靠的區塊生產者排除在出塊排程之外，通過這一方式使得錯過區塊的數量最小化。

在正常情況下，PBFT塊鏈不會經歷任何分叉，因為區塊生產者並非競爭關係，他們合作產生區塊。如果有區塊分叉，共識將自動切換到最長鏈。這一方式之所以有效，是因為區塊鏈分叉上增加區塊的速度，與具有相同共識的區塊生產者的比例直接相關。換句話說，具有更多生產者的區塊鍊長度將比具有較少生產者的區塊鏈增長速度更快，因為，有更多生產者的區塊鏈分叉上，丟塊更少。

此外，沒有塊生產者可以同時在兩個區塊鏈分叉上生產塊。如果一個塊生產者發現這麼做了，就可能被投票出局。這類雙重生產的密碼學證據，也可能會被用來自動移除作惡者。

與傳統的POS/POW算法相比較，mcc採用拜占庭容錯算法(PracticalByzantineFaultTolerance)，所有的出塊者都要對所有區塊簽名，以此來確保在同一時間戳或者同一區塊高度上，沒有區塊生產者能夠同時在兩個區塊上簽名。一個區塊有了5個區塊生產者的簽名，該區塊就被認為是不可逆的。任一拜占庭區塊生產者如果想在同一時間戳或者同一區塊高度的兩個區塊上簽名，就不得不留下密碼學證據。在這一模式下，0.1秒之內就可以達成不可逆的共識。

2. Gossip數據傳輸協議

MCC鍊網絡中的節點之間通過Gossip協議來進行狀態同步和數據分發。Gossip協議是P2P領域的常見協議，用於進行網絡內多個節點之間的數據分發或信息交換。由於其設計簡單，容易實現，同時容錯性比較高，而被廣泛應用到了許多分佈式系統，例如Cassandra採用它來實現集群失敗檢測和負載均衡。 Gossip協議的基本思想十分簡單，數據發送方從網絡中隨機選取若干節點，將數據發送過去；接收方重複這一過程（往往只選擇發送方之外節點進行傳播）。這一過程持續下去，網絡中所有節點最終（時間複雜度為節點總個數的對數）都會達到一致。數據傳輸的方向可以是發送方發送或獲取方拉取。

3. Gossip協議

Peer利用gossip以可擴展的方式廣播分類帳和channel數據。 Gossip消息是連續的，channel上的每個peer都在不斷接收來自多個peer的當前和一致的分類帳數據。每個gossip消息被簽名，從而拜占庭人員發送偽造的消息會容易地識別出來，並且將消息分發到不想要的目標以被阻止。受延遲，網絡分區或導致丟失的塊的其他因素影響，peer最終將通過聯繫擁有這些丟失塊的peer將同步到當前分類帳狀態。

基於Gossip-based數據傳播協議在MCC網絡上執行三個主要功能：管理peer發現和通道成員資格，通過不斷識別可用成員peer，並最終檢測已脫機的peer。在channel上的所有peer上傳播分類帳數據。任何與channel其他部分不同步的數據都可以通過複製正確的數據來識別缺失的塊和同步自身。通過允許對賬本數據的點對點狀態傳輸更新，使新連接的peer達到速度要求。 Gossip-based的廣播通過peer

接收來自該channel上的其他peer的消息，然後將這些消息轉發到channel上的多個隨機選擇的peer，其中該數量是可配置的常數。 Peer也可以執行pull機制，而不是等待發送消息。該帶有channel成員資格循環重複，分類帳和狀態信息不斷保持實時性和同步。為了傳播新區塊，該channel的leaderpeer從ordering服務中提取數據，並向peer中發起gossip傳輸。

4. Gossip消息

在線peer通過不斷地廣播“alive”消息來指示它們的可用性，每個消息包含公鑰基礎設施（PKI）ID和消息中發送者的簽名。 Peer通過收集這些alive的消息來維持渠道成員資格;如果沒有peer從特定對等體接收到活動消息，則該“死”對等體最終從信道成員資格中清除。由於“活著”消息是加密簽名的，所以惡意peer不能偽造其他peer，因為它們缺少根證書頒發機構（CA）授權的簽名密鑰。

除了接收到的消息的自動轉發之外，狀態協調進程通過channel上的peer同步全局狀態。每個peer不斷地從channel上的其他peer中提取塊，以便在識別出差異時修復自己的狀態。由於不需要固定連接來維護基於gossip的數據傳播，因此該流程可以可靠地為共享分類帳提供數據一致性和完整性，包括對崩潰節點的容錯。

由於channel被隔離，一個channel上的peer不能在其他channel上發送消息或共享信息。雖然任何peer可以屬於多個channel，但是分區消息通過基於peer的channel訂閱應用消息路由策略來防止塊被傳播到不在channel中的peer。在MCC.IO網絡中，節點會定期地利用Gossip協議發送它看到的賬本的最新的數據，並對發送消息進行簽名認證。通過使用該協議，主要實現如下功能：

- 通道內成員的探測：新加入通道的節點可以獲知其他節點的信息，並發送Alive信息宣佈在線；離線節點經過一段時間後可以被其他節點感知。
- 節點之間同步數據：多個節點之間彼此同步數據，保持一致性。另外，Leader節點從Orderer拉取區塊數據後，也可以通過Gossip傳播給通道內其他、節點。

5. 企業級區塊鏈應用系統

MCC主鏈在區塊鏈基礎支撐系統的基礎上進行研發，實現交易量峰值達

到每秒十萬次，延遲不超過0.03秒，完全符合企業級區塊鏈系統的應用。

區塊鏈基礎支撐系統支持面向多種不同應用需求的二次開發，實現高效數據交換，提高區塊鏈應用的開發效率，降低開發成本。為區塊鏈應用的產業鏈發展提供技術和平台支撐。

1） 豐富的參數配置和快速部署

通過不同的參數配置，改變區塊鏈的功能和性能，以適應不同企業的需求，達到完全定制化的要求。

網絡部署和維護方便，只需要2-3步就可以快速部署一條區塊鍊或者加入一個已有的區塊鏈。

2） 完備的開發接口

MCC主鏈提供完備的API開發接口，基於安全的RPC通信模式，支持GOLANG、JAVA、PHP等主流開發語言調用。

官方提供標準的開發和測試工具，包括Web區塊瀏覽器、APP區塊鏈瀏覽器，並且全部開源。

3） 企業成本支出低

挖礦是保證區塊鍊網絡和數據安全的基礎。 MCC主鏈改進挖礦算法，礦機可以採用CPU挖礦模式，避免大量電力資源浪費，減低了企業建設和運營的費用。

經行業評測，MCC主鏈整體的設備投資和運維成本遠遠低於其他區塊鏈平台，並且滿足節能環保的要求。

版本

2018年9月V1.2