編寫說明

區塊鏈起源於[比特幣](https://baike.baidu.com/item/%E6%AF%94%E7%89%B9%E5%B8%81/4143690" \t "/Users/apple/Documents\x/_blank)，2008年11月1日，一位自稱[中本聰](https://baike.baidu.com/item/%E4%B8%AD%E6%9C%AC%E8%81%AA/5740822" \t "/Users/apple/Documents\x/_blank)(Satoshi Nakamoto)的人發表了《比特幣:一種點對點的電子現金系統》一文，闡述了基於[P2P](https://baike.baidu.com/item/P2P/139810" \t "/Users/apple/Documents\x/_blank)網路技術、加密技術、[時間戳](https://baike.baidu.com/item/%E6%97%B6%E9%97%B4%E6%88%B3/6439235" \t "/Users/apple/Documents\x/_blank)技術、區塊鏈技術等的電子現金系統的構架理念，這標誌著比特幣的誕生。兩個月後理論步入實踐，2009年1月3日第一個序號為0的[創世區塊](https://baike.baidu.com/item/%E5%88%9B%E4%B8%96%E5%8C%BA%E5%9D%97/22448241" \t "/Users/apple/Documents\x/_blank)誕生。2009年1月9日出現序號為1的區塊，並與序號為0的創世區塊相連接形成了鏈，標誌著區塊鏈的誕生。

區塊鏈是一個[資訊技術](https://baike.baidu.com/item/%E4%BF%A1%E6%81%AF%E6%8A%80%E6%9C%AF/138928" \t "/Users/apple/Documents\x/_blank)領域的術語。從本質上講，它是一個共用資料庫，存儲於其中的數據或資訊，具有“不可偽造”“全程留痕”“可以追溯”“公開透明”“集體維護”等特徵。基於這些特徵，[區塊鏈技術](https://baike.baidu.com/item/%E5%8C%BA%E5%9D%97%E9%93%BE%E6%8A%80%E6%9C%AF/23686191" \t "/Users/apple/Documents\x/_blank)奠定了堅實的“信任”基礎，創造了可靠的“合作”機制，具有廣闊的運用前景。隨著時代的進步，“區塊鏈”已走進大眾視野，成為社會的關注焦點。

目錄

1. 行業分析

1.1區塊鏈的概念

1.2區塊鏈的發展趨勢及投資前景

1.3中心化與去中心化

1.4智能合約

2、Hash Ahead平臺

2.1Hash Ahead簡介

2.2任務及願景

2.3Hash Ahead的優勢特點

3、Hash Ahead的技術架構

3.1網路層

3.2共識機制

3.3區塊結構

3.4區塊節點

3.4.1Hash Ahead節點

3.4.2節點驗證

3.4.3節點獎勵

3.4.4惡意節點行為及懲罰

3.5安全主鏈

3.6去中心化系統

1. Hash Ahead應用

4.1智能合約庫

4.1.1Hash Ahead智能合約庫簡介

4.1.2智能合約審核

4.2分層確定性錢包

4.3Hash Ahead去中心化交易所

5、HAH發行機制

5.1HAH發行計畫

5.2發行週期

5.3收益說明

5.4使用計畫

6、發展戰略

7、風險提示

8、免責說明

1、行業分析

1.1區塊鏈的概念

區塊鏈是一個[資訊技術](https://baike.baidu.com/item/%E4%BF%A1%E6%81%AF%E6%8A%80%E6%9C%AF/138928" \t "/Users/apple/Documents\x/_blank)領域的綜合術語。自2008年發展至今，集當今多種技術於一體，包括但不限於分佈式帳本、共識機制、智能合約、P2P網路、非對稱加密等。在每個區塊鏈中，區塊即資訊塊，資訊以區塊的形式進行集成、打包，並按照實際產生時間的先後順序進行連接。

1.2區塊鏈的發展趨勢及投資前景

自2009年比特幣網路運行以來，區塊鏈各類技術進入了飛速發展的階段，尤其是底層技術，自2017年以來發展勢頭明顯。基於底層技術，金融領域、公共服務領域、公益慈善領域、供應鏈領域、物聯網領域等不斷進行B端、C端的場景落地嘗試，DApp應用也不斷湧現。區塊鏈正式走進大眾視野，成為社會的關注焦點，影響將不僅僅體現在經濟上，還體現在文化和政治上。在未來，區塊鏈的場景應用將不可估量。

1.3中心化與去中心化

對於去中心化，很多人認為去中心化就是不要中心。去中心化，而是由節點來自由選擇多個出塊節點、自由決定出塊節點。

中心化是中心決定節點。節點必須依賴中心，節點離開了中心就無法生存。在去中心化中，任何人都有可能成為出塊節點，任何人也都可以成為其中一個中心點。任何一個中心都不是永久的，而是階段性的，任何一個中心對節點都不具有強制性。

1.4智能合約

智能合約程式不只是一個可以自動執行的電腦程式：它自己就是一個系統參與者。它對接收到的資訊進行回應，它可以接收和儲存價值，也可以向外發送資訊和價值。這個程式就像一個可以被信任的人，可以臨時保管資產，總是按照事先的規則執行操作。

智能合約模型：它是運行在可複製、共用的帳本上的電腦程式，可以處理資訊，接收、儲存和發送價值。

1. Hash Ahead平臺

2.1Hash Ahead簡介

2.2任務及願景

區塊鏈概念自2008年底由匿名者中本聰提出後不斷發展，由比特幣到以太坊，智能合約的出現大量的應用開始浮現，可是這跟傳統技術距離還是差天共地…

編程語言 - Go Language 2009年由Google 推出，至今佔有率已達全球十大之一，箇中原因和代碼庫有很大關系，當程式員編程時每次也需要由零開始而不是從前人所作調用，一個複雜的程式何年何月才會出現？更莫說操作系統了！

Hash Ahead除了在智能合約庫為程式員提供方便，更提供誘因讓更多開發人員為智能合約發展打好基礎，每當智能合約被調用時，使用者需付出（Force），而該智能合約的作者能得到部份獎勵，吸引更多人開發出更實用更複雜的智能合約庫供開發者調用，再複雜的應用甚至操作系統即將誕生，真正的區塊鏈操作系統大門從此開啟。

2.3Hash Ahead的優勢特點

在區塊鏈飛速發展的時代，無論是比特幣還是以太坊，這些都是區塊鏈技術中的佼佼者，但人們始終離打開區塊鏈應用的大門還差一點。

在此之前，智能合約只是一種特殊協議，旨在提供、驗證及執行合約。智能合約的執行效率低、開發人員的收益低、編寫智能合約的成本過高，這已然成為智能合約的痛點，而Hash Ahead的智能合約庫將打破現一觀點。

3、Hash Ahead的技術架構

3.1網路層

Hash Ahead網路由運行Hash Ahead軟體的節點構成 P2P 網路。整體網路架構由節點網路層作為核心構成，分為共識傳輸層、區塊傳輸層、交易傳輸層，共識數據不會因區塊和交易擁堵而影響傳輸效率，每層可以為獨立的傳輸方案，層與層之間互不影響。

採用動態組合驗證者和領導者節點的P2P網路，讓領導者節點或驗證者節點能最快速度接收區塊等數據，傳輸效率高於非功能節點。

節點網路層由運行Hash Ahead核心節點程式的節點構成，節點之間同步校驗區塊和交易數據，並進行共識組織區塊數據。其中共識層包含了共識機制，出塊層包含出塊機制，而交易層則負責交易數據。

3.2共識機制

共識機制是區塊鏈必不可少的一部分。在共識機制方面，Hash Ahead為提高區塊生產結束消息準確性和及時性，則由獨立P2P網路傳輸該消息，提高領導者接收區塊生產結束消息的及時性。同時子鏈每秒的交易筆數(TPS, Transaction Per Second)能夠高達百萬，並且一筆交易最快500ms即可完成鏈上確認，足以滿足當今數據交易頻繁延遲低的應用場景。

3.3區塊結構

主鏈和子鏈的主塊之間有直接關聯，即一個主塊頭中包含有上一個主塊的塊HASH，該關聯可用於塊的快速較驗，只需要同步主塊就可以完成較驗。每天的邊界區塊頭關聯，只需下載每天的邊界區塊頭，即可較驗全鏈區塊頭的正確性，有利於輕節點等客戶端快速全鏈較驗。

主鏈和子鏈的主塊關聯前一天的主塊HASH，只有一天邊界的主塊才有前一天的邊界主塊的塊HASH，其他主塊沒有該參數，主要用於全鏈掃描較驗使用，用於輕節點、輕錢包、數據裁剪等功能使用。

全鏈所有歷史區塊，不需要節點全部存儲，由存儲節點分佈式存儲歷史區塊，一個存儲節點只存儲部分區塊，並提供查詢功能，存儲節點提供存儲和查詢功能，可獲取相應的收益，收益由區塊獎勵和查詢費用組成，區塊分佈式存儲功能解決了歷史區塊龐大的問題，功能節點（如輕節點、驗證節點等）無須存儲歷史區塊，降低節點的存儲要求。

3.4區塊節點

3.4.1Hash Ahead節點

節點指的是區塊鏈網路中的電腦，包含手機，礦機和服務器等等。節點可分為“全節點”和“輕節點”，全節點就是擁有全網所有的交易數據的節點，輕節點則是只擁有和自己相關的交易數據節點。

Hash Ahead節點，在無交易時不生產區塊，少同步，提高效率，減少空區塊佔用資源，同時出塊獎勵固定，選舉後保障節點主能獲取獎勵。在交易量達到最大區塊大小時，可立即生產區塊，不受時間限制，交易上鏈速度更快，減小交易池壓力。

Hash Ahead中驗證節點和提案節點需要投票鎖定後才能參與共識。投票後有初始鎖定期（鎖定期在10至30天），鎖定期內TOKEN不能流動，鎖定期後可以流動，鎖定期後需要轉出TOKEN，需要一段時間的等待期（一般為一天），防止作惡後立即逃跑問題。

同時節點自我投票有最小數量要求，超過最小數量才能成為一個驗證者節點或領導者節點，系統有最小節點自我投票數量，但節點可以多自我投票，高自我投票的節點，擁有更高的侯選節點權重，可獲得更高收益（即節點擔保費用越高，則收益越高，並更值得投票人信任）

3.4.2節點驗證

Hash Ahead節點結合現有公鏈節點的優勢上進一步創新。

輕量化驗證節點，驗證者節點無需全鏈同步區塊，只需要同步最高確認區塊的狀態數據，即可以驗證新區塊，驗證者節點不需要存儲歷史區塊數據，減小驗證者節點存儲要求，普通伺服器也可以作為驗證者節點工作，降低驗證者節點基本要求。

節點選擇性驗證，驗證者節點或領導者節點根據節點伺服器處理能力，選擇處理子鏈數量，以及選擇處理那些子鏈，節點程式可評估伺服器處理能力，節點主可根據評估數據選擇需要處理的子鏈。

低門檻驗證者節點要求，增強去中心化程度：一個驗證者節點可由多臺伺服器組成，伺服器分工合作，共同完成驗證工作；能力較弱的參與者要參與驗證工作，可多個參與者的伺服器合作組成一個驗證節點，參與驗證工作，獲得的收益按參與者的能力以及投票數量分成，該功能有效降低參與者的門檻，增強去中心化程度。

領導者生產區塊時，不需要等待上一區塊被確認後才生產，可以連續生產區塊，而未確認的區塊按最長鏈機制選擇，驗證者可連續確認區塊，並可跳區塊投票（即投票後區塊可證明前區塊，減少驗證投票數量，提高效率）。

3.4.3節點收益

普通用戶由於無法建立節點伺服器，或沒有足夠的TOKEN達到最小自我投票，則可以選擇投票其他節點獲得收益。在選舉驗證者和領導者時，每個侯選節點的權重都相同，即被選中的概率相同。節點獲得的獎勵，按節點各投票人的投票TOKEN數占比來分配獎勵。被選中為侯選節點後，每個節點的收益是相同的，與投票TOKEN數量無關。

節點主會收取節點擁金，即節點主建立伺服器有成本開銷，需要向投票人收取擁金來支持成本開銷，節點主在創建節點時，需要設置擁金比例（0%~100%），節點地址設置了擁金比例，就不能更改，如需更改，則需要另建節點地址，該功能防止節點主隨意更改擁金比例，損害投票人的利益。

Hash Ahead中獎勵利率與投票抵押率和通貨膨脹率相關，即塊獎勵數量週期性變動（一個週期內是固定的），塊獎勵數根據投票抵押率和通貨膨脹率等相關數據計算而得。

3.4.4惡意節點行為及懲罰：

屬於一條鏈的驗證者，卻不為該鏈的區塊提供合法性驗證，驗證中簽名了該鏈一個不合法的區塊，不應答共識消息或不發送共識消息（不遵循共識機制的規則處理節點的消息），驗證者在鏈兩個競爭性的分叉上同時簽名，在該生產區塊時未生產區塊，生產區塊後不廣播生產區塊結束消息，在惡意分叉上生產區塊，不在上一領導者的末尾區塊後生產區塊，或在兩個競爭性的分叉上同時生產區塊等等一系列的行為，在Hash Ahead中都將受到懲罰。

對惡意節點懲罰，Hash Ahead將鎖定惡意節點自已的投票TOKEN，以及投票該惡意節點的投票人的TOKEN，鎖定期為三個月（驗證者和領導者節點有最小自已投票要求），並永久不能獲取驗證者資格，在鎖定期結束後，將惡意節點自已的投票全部TOKEN轉入黑洞地址，並將投票人的TOKEN的10%轉入黑洞地址。

3.5高效安全主鏈

安全主鏈為Hash Ahead區塊鏈的共識鏈，承載驗證者和領導者的質押TOKEN交易，以及子鏈的共識憑證、社區自治投票等數據。所有的支鏈均為其“後代”，其被用於支撐全區塊系統的安全和共識，在 P2P 網路中主鏈的同步廣播消息轉發優先順序高於應用支鏈。廣播數據採用瀑布模型，相比於傳統P2P網路傳輸模型，傳輸路徑和時間更短。

安全主鏈以區塊系統創世區塊為起點，安全主鏈被用於支撐全區塊系統的安全和共識，所有應用分支節點都需要同步和校驗主鏈區塊頭資訊。新節點接入網絡後，首先完成主鏈同步，才開始進行對應應用分支同步。共識主鏈+功能子鏈組成多鏈結構，可無限擴展功能子鏈，鏈與鏈之間可跨鏈交易。最佳環境單鏈可達100萬TPS，最小區塊間隔1毫秒，交易確認時間500毫秒，同時去中心化交易所資產交易確認時間也為500毫秒。

3.6去中心化系統

作為一個去中心化性質的平臺，Hash Ahead由完全透明的去中心化自治體系支撐其管理架構。這結構讓每個通證持有者清晰瞭解公鏈基礎內的全部技術構建和價值流轉、充分體現區塊鏈的公信價值。Hash Ahead內的所有決策均以通證持有方的公投決策為依據，所有技術更新均由社區公示。這完全去中心化的管理體系將完全避免了傳統機構的中心化管理弊端。為中心化管理層專權，篡改資料和獨自決策集團走向等問題提供了優良及無信任風險的解決方案。

4、Hash Ahead應用

4.1智能合約庫

4.1.1Hash Ahead智能合約庫簡介

智能合約庫雖然在以太坊生態中已經被很早的應用，但很多合約庫的作者付出了聰明才智，實際並沒有獲得收益。調用合約產生的GAS費用歸礦工所有，而合約的作者在整個生態中默默的做貢獻。

Hash Ahead生態的模型確保可以讓合約的作者與出塊者共同獲利，為了提高合約的安全性增加了合約的審核機制，在DAO的管理機制下，提交的合約被社區所審核，才能被系統所調用. 因此也要求合約的作者提交合約的時候需要支付一筆審核費用。

Hash Ahead採用wasm的技術，智能合約運行代碼和源碼存儲在鏈上，相同的代碼只存儲一份，直接使用代碼HASH創建合約，無須上傳代碼，並且同一區塊中的多個智能合約可同時執行，提高智能合約運行效率，保證高效率的執行力。

而智能合約虛擬機採用WebAssembly技術，可運行WASM二進位代碼的虛擬機，WASM虛擬機性能比EVM虛擬機更高，同時支持多種編程語言，包括Solidity、C++、RUST等語言，增加開發人員的編程體驗。

4.1.2智能合約審核

以太坊中的ERC20來說，系統中有太多個相同的合約在跑，他們的代碼相同，只是初始化的參數不同，給鏈也帶來很大的數據重複，降低了鏈的存儲效率。

在Hash Ahead系統中，相同的合約只會審核一份，極大的減輕了系統的負擔， 當合約被調用的時候花費的GAS 費用按照一定的比例給到合約作者的帳戶。智能合約代碼上鏈後，需要鏈上去中心化審核後才能被使用，審核代碼安全性，審核是否抄襲他人代碼等等。審核通過的智能合約代碼可用於創建合約，合約被調用而產生的GAS費，部分會獎勵給合約代碼創作者，其他獎勵給礦工，這也為更好的區塊鏈應用打下基礎，從而促使更多的程式員願意往區塊鏈發展。

4.2分層確定性錢包

在區塊鏈網路中，每個用戶都擁有一個甚至多個區塊鏈帳戶即地址。普通的確定性錢包將為用戶私鑰的管理上帶來不便，因為Hash Ahead採用分層確定性錢包。

Hash Ahead錢包採用去中心化、輕量化和多元化的設計，其中輕量化的設計，使用戶能在不同的場景中隨時隨地的使用，而多元化的設計，能保證用戶不用頻繁的更換錢包進行貨幣兌換，從而降低時間上的成本。同時，Hash Ahead錢包能有效保證用戶的匿名性跟相關隱私，增加用戶的信任。

4.3Hash Ahead去中心化交易所

中心化交易所給投資者帶來了重大風險，每年有數十億美元主要來自比特幣和以太坊的資金在複雜的駭客攻擊和詐騙中損失，這引起監管機構的憤怒，他們現在越來越多地對其進行監管，並在此過程中影響用戶隱私。

Hash Ahead打造的完全去中心化鏈上交易所，用戶將完全保管他們的資金，並可以隨心所欲地使用它們。平臺以開放式生態接入智能式合約，鏈上自動運行，沒有任何的中心。背靠全球最快公鏈，強大技術支撐，領先全行業。上幣去中心化，可輕鬆創建虛擬代幣，並與原生鏈主幣有相同功能，利用智能合約綁定和管理虛擬代幣，同時可參與去中心化交易所交易，即時掛單，即時撮合，安全確認，無限接近中心化交易所的用戶體驗。

在最佳環境下，Hash Ahead可在500毫秒以內完成交易確認，支持大併發量掛單和撮合，支持訂單刪除和修改功能。通過具有去中心化子鏈實現跨鏈橋功能，橋接BTC、ETH等公鏈的資產，提供安全轉移資產功能，同時通過去中心化交易所，可提供多種資產的高效交易能力，能夠實現完整、安全的資產去中心化跨鏈流通兌換，支持多種公鏈自由流通兌換。

5、HAH發行機制

5.1HAH發行計畫

5.2發行週期

5.3收益說明

5.4使用計畫

6、發展戰略

7、風險提示

在Hash Ahead的開發、維護和運營過程中存在著風險，這其中很多都會超出開發團隊的控制。

7.1市場風險

Hash Ahead的價格與整個數字貨幣市場形勢密不可分，如市場行情整體低迷或存在其他不可控因素的影響，則可能造成 Hash Ahead本身即使具備良好的前景，但價格依然長期處於被低估的狀態。

7.2監管風險

由於區塊鏈的發展尚處早期，在全球沒有有關募集過程中的前置要求、交易要求、資訊披露要求、鎖定要求等相關的法規檔。

7.3競爭風險

當前區塊鏈領域專案眾多，競爭十分激烈，存在較強的市場競爭和專案運營壓力。並且隨著資訊技術和移動互聯網的發展，其他應用平臺的層出不窮和不斷擴張，Hash Ahead將面臨持續的運營壓力和一定的市場競爭風險。

7.4人才流失風險

Hash Ahead聚集了一批在各自專業領域具有領先優勢和豐富經驗的技術團隊和顧問專家，其中不乏長期從事區塊鏈行業的專業人員以及有豐富互聯網產品開發和運營經驗的核心團隊。核心團隊的穩定和顧問資源對Hash Ahead保持業內核心競爭力具有重要意義。在今後的發展中，不排除有核心人員離開，核心人員或顧問團隊的流失，可能會影響平臺的穩定運營或對未來

發展帶來一定的不利影響。

7.5駭客或盜竊風險

駭客或其他組織或國家均有以任何方法打斷Hash Ahead應用或功能的可能性，包括但不限於拒絕服務攻擊、女巫攻擊、遊襲、惡意軟體攻擊或一致性攻擊等。

7.6核心協議風險

Hash Ahead目前基於某個特定的鏈開發，儘管團隊會挑選目前最安全穩定的區塊鏈作為基礎設施，但該鏈發生的任何故障，不可預期的功能問題或遭受攻擊都有可能導致Hash Ahead以難以預料的方式停止工作或功能缺失。

7.7系統性風險

軟體中被忽視的致命缺陷或全球網路基礎設施大規模故障造成的風險。雖然其中部分風險將隨著時間的推移大幅度減輕，比如修復漏洞和突破計算瓶頸，但其他部分風險依然不可預測，比如可能導致部分或全球互聯網中斷的政治因素或自然災害。

7.8無法預料的風險

基於密碼學的數字金幣是一種全新的技術，除了本白皮書內提及的風險外，還存在著一些創始團隊尚未提及或尚未預料到的風險。此外，其他風險也有可能突然出現，或者以多種已經提及的風險的組合的方式出現。

1. 免責說明

本網站的宗旨是在不違反國際相關法律法規的前提下，盡可能地為全球廣大數字資產愛好者及投資者提供一個平臺。禁止使用本網站從事洗錢、走私、商業賄賂等一切非法交易活動，若發現此類事件，本站將凍結帳戶，立即報送有權機關。

當有權機關出示相應的調查檔要求本站配合對指定用戶進行調查時，或對用戶帳戶採取查封、凍結或者劃轉等措施時，本站將按照有權機關的要求協助提供相應的用戶數據，或進行相應的操作。

本網站使用者因為違反本聲明的規定而觸犯國際相關法律的，本站作為服務的提供方，有義務對平臺的規則及服務進行完善，但本網站並無觸犯國際相關法律的動機和事實，對使用者的行為不承擔任何連帶作用。

凡以任何方式登錄本網站或直接、間接使用本網站服務者，視為自願接受本網站聲明的約束。