AI Bug 白皮書

引言

隨著科技的飛速發展，人工智慧（AI）和區塊鏈技術已經逐漸滲透到我們生活的各個領域。在這個數位化時代，軟體已經成為我們日常生活的重要組成部分，而漏洞的存在則給駭客和惡意攻擊者提供了可乘之機。為了解決這一問題，我們推出了AI Bug賞金獵人專案。

AI Bug賞金獵人的目標是創建一個充滿活力和可持續性的社區，讓所有人都可以參與其中，共同查找和修復軟體漏洞。我們相信，通過眾人的力量，我們可以及時發現並修復軟體中的漏洞，提高軟體的安全性和可靠性。

在過去的幾年中，我們已經見證了駭客攻擊事件的頻繁發生，這些攻擊給企業和個人帶來了巨大的損失。儘管傳統的安全防禦方法在一定程度上可以緩解這些問題，但它們往往無法及時發現和修復所有漏洞。因此，我們需要一個更加高效和創新的解決方案來應對這個挑戰。

AI Bug賞金獵人的出現正是為了解決這一問題。我們的平臺將利用人工智慧技術來自動化漏洞查找和報告過程，同時通過智能合約和加密貨幣來提高賞金的透明度和效率。我們希望通過這種方式，幫助軟體開發商及時發現和修復漏洞，提高軟體的安全性和可靠性。

在接下來的章節中，我們將詳細介紹AI Bug賞金獵人的功能特點、發行代幣及分配、技術實現與架構、以及風險評估等方面的內容。我們還將探討未來規劃與發展戰略，以及我們對社區建設和治理的看法。

我們相信，通過引入人工智慧和區塊鏈技術，AI Bug賞金獵人將開創一個新的時代，讓更多的人能夠參與並貢獻於軟體安全事業。我們期待著與全球的開發者、安全專家和社區成員一起努力，共同打造一個更加安全、透明和高效的軟體生態環境。

在閱讀本白皮書的過程中，我們希望您能夠感受到我們對這個專案的熱情和決心。我們相信，通過眾人的力量，我們可以共同創造一個更加美好的未來。謝謝您的關注和支持！

目 錄

目 錄

一、互聯網大環境存在大量BUG

1.1 軟體複雜性與漏洞增長

隨著軟體在各個領域的廣泛應用，軟體安全性問題也日益凸顯。軟體是由人類編寫的，其複雜性和規模使得漏洞難以避免。

1.1.1 軟體複雜性增加的原因

功能增加：為了滿足用戶多樣化的需求，軟體開發商不斷在軟體中增加新功能。功能的增加使得軟體變得更加複雜，從而增加了漏洞存在的可能性。

技術更新：隨著互聯網和移動設備的普及，軟體技術也在不斷更新。新技術引入增加了軟體複雜性，同時新技術也可能帶來新的漏洞。

分佈式系統：現代軟體系統越來越多地採用分佈式架構，使得系統變得更加複雜。分佈式系統中的通信和數據交換環節可能成為駭客攻擊的目標。

1.1.2 漏洞增長的原因

代碼量增加：隨著軟體複雜性的增加，代碼量也在不斷增長。更多的代碼意味著更多的可能產生錯誤的代碼行，從而增加了漏洞的數量。

編程錯誤：人類在編程過程中容易犯錯，如邏輯錯誤、輸入驗證不足等。這些錯誤可能成為駭客攻擊的突破口，導致漏洞的產生。

第三方組件：現代軟體系統中第三方組件的使用越來越普遍。這些組件可能存在已知的安全漏洞，而開發人員可能無法及時跟蹤和修復這些漏洞，從而增加了軟體中的漏洞數量。

1.2 駭客攻擊與惡意軟體

隨著互聯網的普及，網路安全問題也日益嚴重。駭客攻擊和惡意軟體是互聯網安全領域的重要威脅。

1.2.1 駭客攻擊

駭客攻擊的定義：駭客攻擊是指利用互聯網安全漏洞，通過非法手段獲取對目標系統的訪問許可權，進而竊取數據、破壞系統或進行其他惡意行為的過程。

駭客攻擊的分類：根據攻擊目標和手法，駭客攻擊可分為多種類型，如釣魚攻擊、勒索軟體、DDoS攻擊等。

駭客攻擊的危害：駭客攻擊不僅可能導致數據洩露、系統崩潰等安全問題，還可能影響企業的正常運營和聲譽。此外，駭客攻擊還可能涉及刑事犯罪，對個人和社會造成嚴重危害。

1.2.2惡意軟體

惡意軟體的定義：惡意軟體是指通過互聯網傳播、感染目標系統的軟體，其目的是進行惡意行為，如竊取數據、破壞系統、監控用戶等。

惡意軟體的分類：根據功能和傳播方式，惡意軟體可分為多種類型，如病毒、木馬、蠕蟲、間諜軟體等。

惡意軟體的傳播途徑：惡意軟體通常通過各種途徑進行傳播，如插件、廣告彈窗、下載站、社交媒體等。此外，惡意軟體還可能通過電子郵件、即時通訊工具等途徑進行傳播。

1.3 漏洞賞金與安全防禦

隨著互聯網的普及，網路安全問題也日益嚴重。為了解決網路安全問題，許多企業和組織推出了漏洞賞金計畫。

1.3.1 漏洞賞金計畫

漏洞賞金計畫的定義：漏洞賞金計畫是指企業或組織為發現和報告其產品或系統中的安全漏洞而提供的獎勵計畫。

漏洞賞金計畫的分類：根據獎勵方式和參與方式，漏洞賞金計畫可分為多種類型，如現金獎勵、積分獎勵、禮品獎勵等。

漏洞賞金計畫的意義：漏洞賞金計畫可以提高企業和組織的安全防禦能力，促進社區參與和合作，提高安全專家的參與度，發現和修復安全漏洞，降低駭客攻擊的風險。

1.3.2 安全防禦措施

安全防禦的定義：安全防禦是指通過各種技術和手段來保護企業或組織的網路和系統免受攻擊和破壞的行為。

安全防禦的分類：根據保護對象和防禦手段，安全防禦可分為多種類型，如防火牆、入侵檢測/防禦系統、加密技術、身份驗證等。

安全防禦的重要性：安全防禦可以減少或防止駭客攻擊和惡意軟體的入侵，保護企業的核心資產和業務運營，提高企業的競爭力和聲譽。

1.3.3 漏洞賞金計畫與安全防禦的關係

提高安全意識：漏洞賞金計畫可以激勵更多的人參與安全防禦，提高公眾對網路安全問題的認識和安全意識。

發現和修復漏洞：漏洞賞金計畫可以促進安全專家和開發者發現和報告安全漏洞，進而幫助企業和組織及時發現和修復漏洞。

增強安全防禦能力：通過漏洞賞金計畫，企業和組織可以獲取更多的安全資訊和建議，進而加強安全防禦措施，提高安全防禦能力。

二、AI Bug專案概述

2.1 專案簡介

AI Bug專案是一個基於人工智慧技術的安全漏洞賞金獵人平臺。該專案旨在利用人工智慧技術自動化漏洞查找和報告過程，同時通過智能合約和加密貨幣提高賞金的透明度和效率。AI Bug旨在創建一個充滿活力和可持續性的社區，讓更多的人可以參與其中，共同查找和修復軟體漏洞，提高軟體的安全性和可靠性。

2.2 專案背景

技術支持：AI Bug專案得到了穀歌子公司DeepMind的支持，使用了其先進的AI技術，包括AlphaCode系統，可以自動化漏洞查找和報告過程。

社區參與：AI Bug專案已經吸引了來自全球的開發者、安全專家和用戶的參與，形成了一個充滿活力的社區。社區成員可以通過平臺提交漏洞報告，獲得相應的獎勵。

合作夥伴：AI Bug專案已經與多家知名企業和組織建立了合作夥伴關係，共同推動安全漏洞賞金獵人的發展。這些合作夥伴的支持和認可也為AI Bug專案的可信度和可持續性提供了保障。

法律保障：AI Bug專案已經與法律機構合作，確保平臺的合法性和合規性。用戶在使用平臺提交漏洞報告時也需遵守相關法律法規，保障合法合規的運作。

2.3 專案目標

AI Bug專案的目標是實現以下目標：

自動化漏洞查找和報告過程：通過利用人工智慧技術，AI Bug希望能夠自動化漏洞的查找和報告過程，減少人工干預，提高效率。

提高賞金的透明度和效率：通過智能合約和加密貨幣，AI Bug希望能夠提高賞金的透明度和效率，讓更多的人願意參與並獲得相應的獎勵。

創建充滿活力的社區：AI Bug希望創建一個充滿活力和可持續性的社區，鼓勵更多的人參與安全防禦，共同查找和修復軟體漏洞。

提高軟體的安全性和可靠性：通過眾包的方式，AI Bug希望能夠提高軟體的安全性和可靠性，減少駭客攻擊和惡意軟體的影響。

三、AI Bug功能特點

3.1協作漏洞查找的定義

協作漏洞查找是指多個安全專家、開發者或用戶共同參與漏洞查找的過程。通過團隊協作，可以共用資源、經驗和知識，提高漏洞查找的效率和準確性。

3.1.1 協作漏洞查找的優勢

提高效率：多人同時參與漏洞查找，可以更快地發現和報告漏洞。

增加準確性：多人的視角和經驗可以互相補充，減少漏報和誤報的可能性。

知識共用：團隊協作過程中，成員可以相互學習和分享經驗，提高整體的安全意識和技能。

降低成本：通過協作，可以共用資源、時間和成本，提高整體的效益。

3.1.2協作漏洞查找的實踐方法

分工合作：根據團隊成員的技能和經驗，進行合理的分工和任務分配。

資訊共用：建立共用平臺或管道，及時分享漏洞資訊、研究成果和經驗教訓。

討論交流：定期舉行團隊會議或線上討論，交流進展、討論問題和分享經驗。

激勵措施：設立獎勵機制，激勵團隊成員積極參與和貢獻。

3.2參數漏洞報告

AI Bug的參數漏洞報告是一種基於人工智慧技術的自動化漏洞報告方法。該方法通過分析軟體系統的參數輸入和輸出，檢測並報告潛在的安全漏洞。

3.2.1 參數漏洞報告的定義

參數漏洞報告是指針對軟體系統中的參數輸入和輸出進行安全漏洞檢測和報告的過程。參數漏洞通常涉及輸入驗證、參數傳遞和輸出處理等方面的安全問題，如緩衝區溢出、注入攻擊等。

3.2.2 AI Bug參數漏洞報告的原理

AI Bug參數漏洞報告基於人工智慧技術，通過分析軟體系統的參數輸入和輸出，構建模型來識別潛在的安全漏洞。該過程包括以下步驟：

數據收集：收集軟體系統的參數輸入和輸出數據，包括正常情況和異常情況下的數據。

特徵提取：從收集的數據中提取特徵，包括輸入驗證、參數類型、參數長度、輸出格式等方面的特徵。

模型訓練：利用提取的特徵訓練機器學習模型，學習正常情況和異常情況下的參數輸入和輸出模式。

漏洞檢測：將訓練好的模型應用於實際軟體系統的參數輸入和輸出數據，檢測潛在的安全漏洞。

報告生成：根據檢測結果生成詳細的漏洞報告，包括漏洞類型、嚴重程度、建議的修復措施等資訊。

3.2.3 AI Bug參數漏洞報告的優勢

自動化程度高：AI Bug參數漏洞報告利用人工智慧技術自動化進行漏洞檢測和報告生成，減少了人工干預和審核工作量。

高效率：通過自動化檢測，可以快速發現和報告潛在的安全漏洞，提高了漏洞報告的效率。

準確性高：AI Bug參數漏洞報告基於機器學習模型進行檢測，能夠提高檢測的準確性和可靠性。

靈活性好：AI Bug參數漏洞報告適用於各種類型的軟體系統，可以靈活地適應不同的系統和環境。

3.3共用加密貨幣支付

AI Bug共用加密貨幣支付是一種創新的賞金支付方式，它使用加密貨幣來獎勵漏洞查找和報告的參與者。通過這種方式，AI Bug旨在提高漏洞賞金的透明度和效率，同時鼓勵更多的人參與安全防禦。

3.3.1 AI Bug共用加密貨幣支付的原理

AI Bug共用加密貨幣支付基於區塊鏈技術和智能合約，實現了自動化、透明化和不可篡改的賞金支付。具體而言，AI Bug使用區塊鏈技術作為底層技術支撐，通過智能合約分配賞金和任務，並使用加密貨幣進行支付。當參與者提交有效的漏洞報告並經過審核確認後，智能合約會自動將賞金發放給參與者。

3.3.2 AI Bug共用加密貨幣支付的優勢

提高透明度：加密貨幣的交易記錄是公開透明的，因此賞金的分配和支付過程也是透明的，減少了不公平和欺詐行為的可能性。

提高效率：通過智能合約和自動化交易，AI Bug可以快速處理賞金支付和交易確認，提高了支付的效率和可靠性。

降低成本：使用加密貨幣支付可以減少傳統支付方式的成本和手續費，降低了整個賞金計畫的運營成本。

全球化：加密貨幣是全球化的數字貨幣，不受地域限制，可以吸引來自全球的參與者參與安全防禦。

3.4 即時交易級安全斷路器

AI Bug即時交易級安全斷路器是一種基於人工智慧技術的安全機制，旨在在即時交易環境中快速識別和阻斷潛在的安全威脅。這種斷路器結合了AI的高級分析能力和即時回應的特點，以確保交易系統的安全和穩定。

3.4.1 即時交易級安全斷路器的定義

即時交易級安全斷路器是一種安全機制，用於在即時交易環境中監視、識別和阻斷潛在的安全威脅。該斷路器利用人工智慧技術，對交易數據進行即時分析，以發現異常模式和可疑行為，並在必要時迅速切斷交易，以防止潛在的安全風險。

3.4.2 AI Bug即時交易級安全斷路器的原理

數據收集：收集交易系統的即時數據，包括交易資訊、用戶行為、系統日誌等。

特徵提取：利用AI演算法從收集的數據中提取與安全相關的特徵，如異常交易模式、用戶行為的偏差等。

即時分析：通過機器學習模型對提取的特徵進行即時分析，以識別潛在的安全威脅。

風險評分：為每個交易或行為分配風險評分，表示其潛在的安全風險級別。

決策與阻斷：根據風險評分，當超過預定閾值時，斷路器會迅速切斷相關交易或行為，以防止安全風險。

回饋機制：提供即時回饋和警報，通知相關人員已阻斷的安全事件，以便進一步調查和處理。

3.4.3 AI Bug即時交易級安全斷路器的優勢

即時性：通過即時監測和分析交易數據，能夠在安全事件發生時迅速作出回應，減少潛在損失。

精確性：利用先進的AI演算法和機器學習模型，能夠精確地識別和區分正常交易與可疑交易。

靈活性：可以根據不同的交易系統和業務需求進行定制和優化，以適應各種複雜環境。

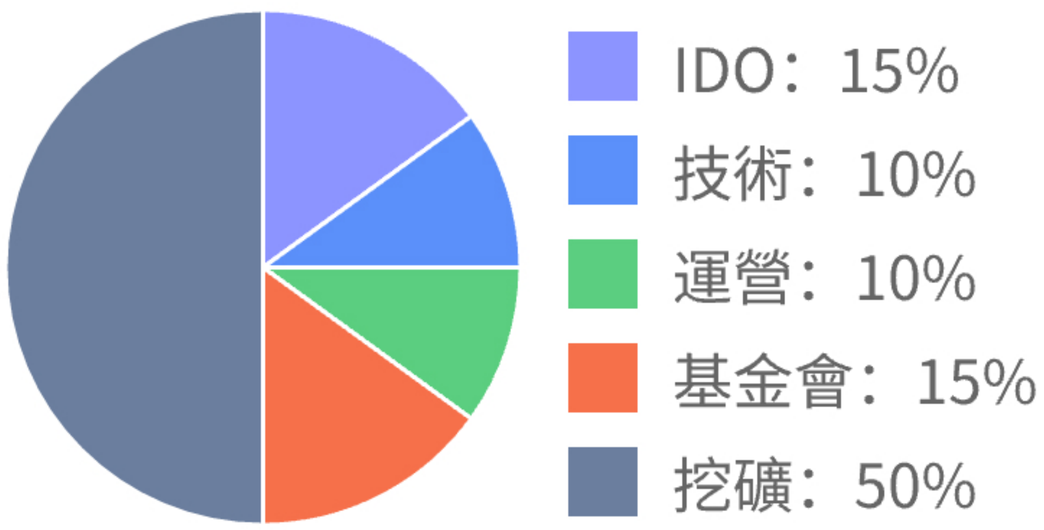
可擴展性：隨著業務量的增長和新的安全威脅的出現，可以輕鬆地擴展和更新斷路器的功能和演算法。

四、代幣經濟模型

4.1 代幣分配模式

代幣名稱：IBUG

代幣總量：1億



4.2 IBUG的主要作用

平臺交互：為了使用特定專案平臺的一些功能，用戶需要持有或購買相應的IBUG。

價值存儲：IBUG被設計為存儲價值，類似於黃金或其他傳統資產。這

交換媒介：IBUG可以作為交換媒介，用於在不同的市場或經濟體中進行交易。

交易手續費：在AI Bug網路平臺，IBUG可作為交易手續費。

服務費用：AI Bug可以提供各種服務，並收取相應的IBUG服務費用。

挖礦收入：允許參與者通過參與挖礦活動來賺取IBUG獎勵。

生態系統發展：AI Bug常構建一個完整的生態系統，包括開發者社區、合作夥伴和其他利益相關者。通過促進生態系統的發展和參與者的互動，IBUG可以吸引更多的用戶和資金，從而助力生態系統發展。

五、技術實現與架構

5.1 技術架構

數據層：這一層主要負責數據的收集、存儲和處理。數據可以來自多種來源，包括用戶輸入、感測器數據、外部API等。數據層會對數據進行清洗、預處理和轉換，以便於上層模型使用。

模型層：這一層包含各種機器學習和深度學習模型，例如神經網路、決策樹、支持向量機等。模型層的主要任務是接收來自數據層的輸入，進行計算和推斷，然後輸出結果。

控制層：這一層主要負責控制整個系統的流程和邏輯。它接收來自用戶或其他層的輸入，然後根據這些輸入和系統的狀態，控制模型層和數據層的操作。

用戶介面層：這一層負責與用戶進行交互。它提供了一個可視化介面，讓用戶可以直觀地看到系統的狀態和結果，同時也可以輸入指令和數據。

5.2 人工智慧技術在漏洞查找中的應用

自動化掃描：AI Bug可以利用自動化掃描工具，對目標系統進行全面的漏洞掃描。與傳統掃描工具相比，AI Bug能夠更準確地識別漏洞，並降低誤報率。這是因為AI Bug基於深度學習演算法，能夠自動學習和改進模型，提高掃描準確度。

威脅情報分析：AI Bug可以通過分析威脅情報，獲取有關漏洞利用和攻擊者的相關資訊。這有助於發現潛在的漏洞，並為防禦者提供寶貴的預警資訊。通過結合威脅情報和系統環境資訊，AI Bug能夠更準確地定位和修復漏洞。

代碼審計：AI Bug可以通過代碼審計技術，對源代碼進行自動審查，發現潛在的安全漏洞。該技術基於機器學習演算法，能夠自動識別代碼中的安全缺陷和錯誤模式。通過與開發人員合作，AI Bug可以幫助企業提高代碼品質和安全性。

即時監控：AI Bug可以通過即時監控技術，對運行中的系統進行即時監測和預警。當發現異常行為或潛在威脅時，AI Bug能夠及時發出警報，通知管理員採取應對措施。即時監控有助於及時發現和修復漏洞，降低安全風險。

滲透測試：AI Bug可以模擬駭客攻擊過程，對目標系統進行滲透測試。通過模擬各種攻擊手段和漏洞利用方式，AI Bug能夠發現潛在的安全隱患，並為防禦者提供詳細的測試報告和建議。這有助於提高系統的安全性，減少被攻擊的風險。

5.3 智能合約在漏洞報告與賞金支付中的應用

5.3.1 AI Bug智能合約在漏洞報告中的應用

定義與觸發條件：AI Bug智能合約首先定義了一組規則和條件，當滿足這些條件時，合約將自動觸發漏洞報告流程。例如，當檢測到異常交易行為、系統性能下降或安全事件時，智能合約可以自動啟動漏洞報告流程。

漏洞報告：一旦觸發條件滿足，AI Bug智能合約將自動將漏洞詳細資訊（包括漏洞類型、位置和嚴重程度等）打包成安全可傳輸的數據包，並通過加密通道發送給組織方。

審核與修復：組織方收到漏洞報告後，經過專業人員審核確認後，將通知相關人員修復漏洞。修復後，智能合約將再次進行驗證以確保漏洞已被妥善修復。

賞金支付：如果漏洞確實存在且被成功修復，組織方將根據漏洞的嚴重性和報告者的貢獻程度，通過智能合約自動發放賞金給報告者。

5.3.2 AI Bug智能合約在賞金支付中的應用

設定支付規則：在AI Bug智能合約中，可以定義一套詳細的支付規則，包括支付標準、支付方式、支付時間等。這些規則將確保賞金支付的透明度和公平性。

安全審計與驗證：為了確保賞金支付的安全性，AI Bug智能合約採用了多重安全審計和驗證機制。這包括對報告者的身份驗證、漏洞有效性的驗證以及賞金支付的審批流程等。

自動化支付：一旦審核通過並確認漏洞已被修復，AI Bug智能合約將自動執行賞金支付流程。這避免了人為操作失誤和提高了支付效率。同時，智能合約的透明性和不可篡改性也確保了支付過程的安全性和公正性。

持續優化：通過收集和分析賞金支付的數據，AI Bug智能合約可以不斷優化自身的功能和性能。例如，它可以學習識別更多的漏洞類型、提高檢測準確性以及改進賞金支付策略等。

5.4 安全斷路器技術與實現

5.4.1 AI Bug安全斷路器實現方法

數據收集與處理：為了實現AI Bug安全斷路器技術，首先需要收集系統和應用程式的流量數據以及用戶行為數據。這些數據包括網路請求、回應時間、錯誤率等。通過對這些數據進行預處理和清洗，可以提取出有用的特徵用於後續的分析和檢測。

模型訓練與優化：基於收集的數據，可以使用機器學習演算法訓練一個異常檢測模型。這個模型可以根據系統和應用程式的正常行為模式進行學習，並能夠識別出偏離正常模式的可疑活動。為了提高模型的準確性和效率，可以使用深度學習技術進行優化和改進。

即時監測與回應：將訓練好的模型部署到系統中，對系統和應用程式進行即時監測。當模型檢測到可疑活動時，會觸發安全斷路器的回應機制。這個機制可以立即切斷系統與外部網路的連接，並通知管理員進行進一步的處理和調查。

回饋與持續改進：為了不斷提高AI Bug安全斷路器的準確性和性能，需要建立一個回饋機制。這個機制可以根據實際應用的效果和用戶回饋，對模型進行持續的改進和優化。通過不斷地學習和調整參數，可以提高模型的檢測精度和回應速度。

5.4.2 AI Bug安全斷路器在提高系統安全性方面的作用

防止惡意攻擊：AI Bug安全斷路器可以檢測並識別出潛在的惡意活動和異常行為，從而防止惡意攻擊者對系統進行攻擊和破壞。通過及時切斷系統與外部網路的連接，可以降低攻擊成功的風險。

保護敏感數據：通過監測系統和應用程式的流量和行為模式，AI Bug安全斷路器可以識別出對敏感數據的非法訪問和操作。這有助於保護敏感數據不被洩露和濫用。

提高系統穩定性：當系統面臨潛在的安全風險時，AI Bug安全斷路器可以及時切斷連接，從而避免系統崩潰或受到損害。這有助於保持系統的穩定性和可用性。

降低運營成本：通過自動化地檢測和處理安全威脅，AI Bug安全斷路器可以降低運營成本並提高工作效率。這減少了手動監控和回應安全事件的需求，節省了人力資源和時間成本。

六、團隊介紹

AI Bug團隊是一支專注於人工智慧和機器學習領域的創新團隊，致力於為全球用戶提供先進、高效的人工智慧解決方案。團隊成員由一批經驗豐富的工程師、科學家和行業專家組成，他們擁有深厚的學術背景和豐富的實踐經驗，在人工智慧、機器學習、網路安全等領域有著卓越的表現。

Adrian：是AI BUG的CEO，曾在一家全球領先的人工智慧企業擔任高級研究員，負責機器學習演算法的研發和應用。他成功開發出多款高效、穩定的人工智慧模型，廣泛應用於圖像識別、自然語言處理等領域。他還參與了多項重要專案，為企業提供了先進的解決方案，得到了客戶的高度評價。

Stanford：是AI BUG的CTO，具備深厚的技術實力和豐富的實踐經驗。他的研究方向主要包括機器學習、深度學習、強化學習等領域，致力於推動人工智慧技術的不斷創新和進步。他還關注人工智慧技術在自然語言處理、圖像識別、推薦系統等領域的實際應用，努力將最新的人工智慧技術應用於產品開發和優化中。

Bradley：曾在一家全球領先的人工智慧企業擔任市場行銷總監，負責企業的市場拓展和品牌推廣。他成功策劃並實施了多個市場行銷專案，為企業打開了新的市場空間，得到了客戶的高度評價。他還參與了企業的戰略規劃和運營管理，為企業的長遠發展提供了重要支持。

七、專案發展路線

研發階段（已完成）：

a. 建立研發團隊，包括人工智慧和機器學習領域的專家、軟體工程師等。

b. 開發AlphaCode系統的基礎架構和核心功能。

c. 實現AlphaCode系統的自動化代碼生成演算法。

d. 設計和開發用戶介面，提高系統的易用性。

測試階段（已完成）：

a. 在Codeforces平臺上進行編程競賽測試。

b. 分析測試結果，評估AlphaCode系統的性能和效果。

c. 根據測試結果和用戶回饋，優化AlphaCode系統的性能和功能。

應用階段（進行中）：

a. 將AlphaCode系統應用於實際場景中，例如軟體開發、數據分析和預測等。

b. 與合作夥伴和客戶合作，拓展AlphaCode系統的應用領域和市場。

拓展階段（計畫中）：

a. 根據市場需求和技術發展趨勢，持續改進和擴展AlphaCode系統的功能。

b. 拓展更多的應用領域和市場，滿足不同用戶的需求。

c. 加強與全球合作夥伴的交流與合作，共同推動人工智慧技術的進步和發展。

8.免責聲明

本白皮書內任何內容均不構成法律、財務、商業或稅務建議，您應在參與任何與此有關的活動之前諮詢自己的法律、財務、商業或其他專業顧問。平臺的工作人員、專案研發團隊成員、第三方研發組織以及服務商都無需對因使用本白皮書所可能導致的直接或者間接的損害和損失承擔責任。

本白皮書僅供一般資訊參考之用，並不構成招股說明書、要約檔、證券要約、招攬投資或出售任何產品、物品或資產（不論是數字資產還是其他資產）的任何要約。以下資訊可能並非詳盡無遺，也不意味著具有合約相關的任何要素。白皮書無法保證資訊的準確性或完整性，不保證也不承諾提供資訊的準確性和完整性說明。在本白皮書包含從第三方獲得的資訊的情況下，平臺和團隊尚未獨立驗證此類資訊的準確性和完整性。此外，您需要瞭解的是，周圍環境和情況可能會隨時發生變化，因此本白皮書可能因此而過時，平臺沒有義務更新或更正與此相關的內容和文件。

本白皮書的任何部分不構成也將不會構成平臺、分銷商以及任何銷售團隊（如本協議中所定義的）的任何要約，也不可以將白皮書所陳述的內容作為任何合同和投資決策所依賴的基礎。本白皮書中所包含的任何內容都不能作為對未來業績的陳述、承諾或保證。通過訪問和使用該白皮書或其中任何內容時，您將向本平臺、其附屬機構和您的團隊提供如下保證：

◎ 在任何購買資產（IBUG代幣）的決定中，您並未依賴本白皮書中的任何聲明內容;

◎ 您將自願承擔費用並確保遵守適用於您的所有法律、監管要求和限制（視情況而定);

◎ 您承認、理解並同意資產可能沒有任何價值，不保證也不代表有任何價值和流通屬性，並不可以用來做投機相關的投資;

◎ 平臺及其附屬機構以及團隊成員均不對資產的價值、可轉讓性、流通性以及通過第三方或其他方式提供AI BUG 專案的任何市場負責或承擔責任;

◎ 您承認、理解並同意，如果您是滿足以下條件的某個地理區域或國家的公民、國民、居民（稅務或其他相關的）、居住地或國家的綠卡持有人，您將不具備購買任何資產的資格：

・ 出售資產可能會被定義或解釋成為出售證券（無論如何命名）或投資產品;

・ 法律禁止接觸和參與資產的銷售或者資產被法律、政策、條例、條約或行政法規所禁止的國家和地區。

平臺和團隊不會也不打算向任何實體或個人作出任何陳述、保證和承諾，並在此聲明不承擔任何責任（包括但不限於本白皮書的內容以及任何平臺發佈的其他材料內容的準確性、完整性、及時性和可靠性）。在法律允許的最大範圍內，平臺、相關實體和服務提供商不承擔任何因使用了白皮書內容、平臺發佈的相關材料以及通過其他形式展現的相關內容（包括但不限於任何錯誤或遺漏的內容）所產生的侵權、合同糾紛或其他形式導致的非直接的、特殊的、偶然的、間接的或其他形式的損失的責任（包括但不限於任何由此產生的違約或疏忽引起的責任、任何收入和利潤的損失以及使用方面和數據的損失）。潛在購買者應仔細考慮、評估與銷售，平臺、分銷商和團隊相關的所有風險和不確定性（包括財務、法律和不確定性的風險）。

本白皮書中提供的資訊僅供社區討論，並不具有法律約束力。任何人均無義務就收購AI BUG訂立任何合約和具約束力的法律承諾，除此之外，本白皮書不會接納任何虛擬貨幣或其他形式的付款。資產的買賣協議和長期持續持有資產須遵守一套獨立條款或一個包含有相關條款和條件的購買協議（視情況而定），這些條款和條件會單獨提供給您或可以從網站上獲取。如果本條款與條件與本白皮書之間有任何不一致之處，請以本條款與條件為准。監管機構並沒有審查或批准本白皮書中列出的任何資訊，而且在任何司法管轄區的法律、法規要求和規則中，都沒有規定需要或將要求這樣做。本白皮書的發佈，分發或傳播並不意味著適用的法律、法規的要求或規則已得到履行和遵守。

這只是一個概念白皮書，用來描述將要研發的AI BUG專案的遠景發展目標。本白皮書可能會不時修改或更換。這裏並沒有更新白皮書和向受眾提供超出本白皮書內容範圍之外的其他資訊的義務。白皮書中包含的所有聲明、新聞稿和公眾可訪問的聲明以及平臺和AI BUG專案團隊可能做出的口頭聲明均可構成前瞻性聲明（包括相關的意向聲明以及對當前市場狀況、經營戰略和計畫、財務狀況、具體規定和風險管理決策的信心和預期等方面）。

請注意，不要過分依賴這些前瞻性聲明，因為這些聲明涉及已知和未知的風險、不確定性風險以及其他多方因素，這可能會導致未來實際結果與這些前瞻性聲明所描述的內容大不相同，同時，需要說明的是，並沒有獨立的第三方審查和判斷這些陳述和假設的合理性。這些前瞻性陳述僅適用於本白皮書所示的日期，平臺和AI BUG專案團隊明確表示對該日期之後因對這些前瞻性聲明進行修訂所引起和產生的後果或事件不承擔任何責任（無論明示還是默示）。

在此使用的任何公司或平臺的名稱或商標（除了與平臺或其關聯公司相關的內容）並不意味著與這些第三方平臺和公司有任何關聯或得到了其背書。本白皮書中提及的特定公司和平臺僅供參考和說明之用。