TimesPay: 將區塊鏈上的美元穩定幣帶到普羅大眾手機裏作日常生活使用

01/31/2020
Rick H
timespayhk@gmail.com

摘要：金錢的概念已經發展了數千年，由銀器、紙幣到手機錢包。在2008年 Satoshi Nakamoto 介紹了另一種更廣泛的工作量證明安全價值代幣。這個項目的成果就是比特幣，比特幣成為了第一個被全球廣泛認可的去中心化交易賬本。在2019年中美國紐約州金融服務廳承認以太坊區塊鏈技術上的美元穩定幣地位後[1]，我們相信未來去中心化區塊鏈技術和穩定幣將會在全球金融體系中扮演著重要角色。使用美元穩定幣的國家或獨立地區將會大大提升地區競爭力與世界金融接軌。本白皮書將初步介紹我們為美國政府監管的美元穩定幣帶入現實生活面對的問題與解決方法。

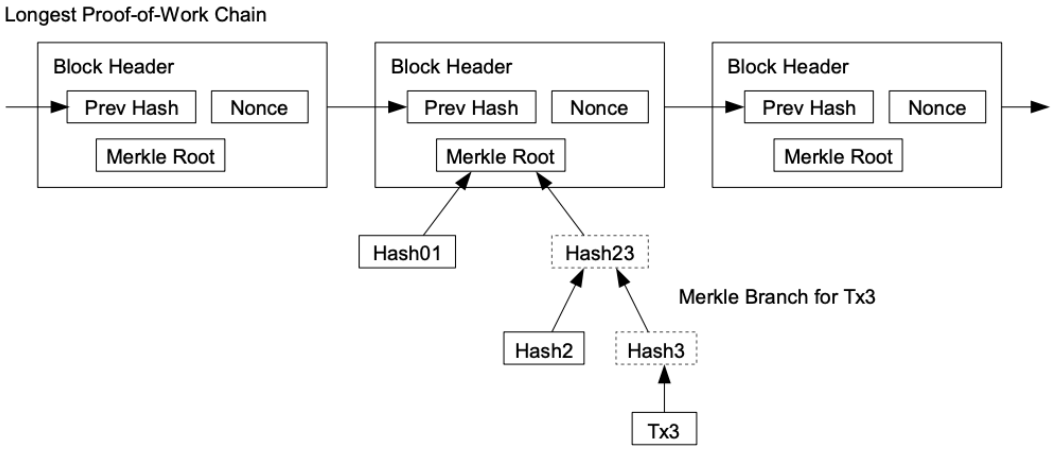
1. 簡介

「區塊鏈數字貨幣是一種完全的點對點電子貨幣能夠提供在線支付從一方直接發送到另一方而不需要通過一個金融機構。它是由通過將交易哈希進一條持續增長的基於哈希的工作量證明鏈來給交易打上最大化，形成一條除非重做工作量證明否則不能更改的記錄。最大的鏈兩端是被見證事件序列的證據，而且也是它本身是由最大CPU算力池產生的證據。只要多數的CPU算力被不打算術聯合攻擊網絡的異步控制，這些匯總就將生成最長的鏈而超過攻擊者。」這種Proof of Work 網絡本身只是極簡的架構，亦是美國政府機構已承認的網絡，建立在PoW網絡上的穩定幣被交易時需要等候主網絡確認，時間較長並且用戶需要對 Gas 有認知，完全不實用於普羅大眾現實生活日常所使用。

我們需要打造一個為了現實生活日常所使用的簡單去中心化區塊鏈手機錢包。建立在PoW上層的和智慧錢包互動的場外確認的網絡。此精心打造的錢包有效解決交易速度，負荷，降低網絡成本費用和匯率各種繁瑣的問題。為普羅大眾帶進去中心化的世界裏。

2. 節點與伺服器 - 交易速度

交易速度是貨幣支付日常生活不可缺少的一部份，Timespay 將分為兩個快捷確認通道與錢包連接。一層為一個不運行完整的網絡例程節點，一層為場外進行的簡化交易伺服器。Timespay 節點不運行一個完整的網絡例程。通過向其他網絡例程查詢以確認他擁有了最長的鏈，並獲取鏈接交易到給交易打區塊鏈的Merkle Tree分支。進行互動優先確認並且由其後追加的區塊進一步確認。在接受其他網絡節點發現一個無效區塊時會向收款人錢包發出的警告。



如果快捷驗證節點網絡被攻擊者控制會變得比較脆弱，所以我們另外需要一台獨立伺服器取出一部份的以太坊主網絡記憶體中狀態轉換函優先計算出交易後的狀態 σ'，函數為 $\sigma' = \Upsilon(\sigma, T)$ （T 表示交易，σ 表示狀態, 而狀態轉移函數為 Υ）[2]。所有交易在執行簡化驗證時，必須先通過有效性測試，這些包含：(1) 交易是 RLP 格式數據，沒有多餘的後綴字節；(2) 交易的簽名是有效的；(3) 交易的隨機數是有效的（等於發送者賬戶的當前隨機數）;(4) 燃料上限不小於實際交易過程中用的燃料 $g0$;(5) 發送者賬戶的餘額至少大於費用 $v0$, 需要提前支付。可以簡化主要提取的項目為 Transaction Hash, Block, Timestamp, Address “From, To”, Value, Gas fee, Gas Limit, Gas Used, Gas Price, Nonce, InputData (Stablecoin Function: Transfer address _to, uint256 _value)。伺服器提取確認傳送格式優先計算出結果。不單只令穩定幣達到光速支付交易，還包括合約創建，信息調回，利用及訪問帳戶存儲，在虛擬機上執行操作等都可以根據函數規則，達到同樣光速場外認證效果。

3. 安全性與負荷

安全性與負荷為我們最注重的一部份，用戶仍須保管好自己的記憶助詞如同現金一樣。我們將可被攻擊的網絡可以分為兩部份，對場外網絡或對以太坊網絡進行攻擊。

假若攻擊者持續攻擊場外網絡並且成功控制伺服器，節點也不會接受這個交易。假若攻擊者成功控制我們所有網絡，那麼收款人可能被攻擊者的偽造交易欺騙。我們會在接受其他網絡節點發現一個無效區塊時會向收款人錢包發出的警告。我們可以為快捷驗證節點加入一些條件：只為實體商舖錢包提供並加入上限金額和網絡未確認總數等等，將會最少化攻擊者攻擊場外網絡的收穫，令攻擊者使用假鈔犯罪無利可圖。

假若一個攻擊者在主網絡試圖生成一條比誠實鏈更快的替代鏈的情況。攻擊者從一定虧損開始，進行可能無限次的算力攻擊試圖趕上誠實鏈達到盈虧平衡。試圖改變他自己的某筆交易來拿回他不久前已經支出的錢[3]。即使這個目標達到了，我們也可通過部署智能合約凍結、增加和燒毀方案解決令其無法提取任何金錢。過程或會被理解為中心化，但為了打擊犯罪活動、截斷恐怖主義，我們必須跟隨美國紐約州金融服務廳對中心化的穩定幣的指引和守則。

如處理着Visa級負荷的每秒2000項交易。Timespay 可以提升服務器數量而解決此類問題。相反，以太坊主網絡處理着這一困境的折磨下，對用戶唯一的影響可能是要支付比較昂貴的Gas Price。

4. 網絡成本 - Gas Refill 技術

以太坊為了避免網絡濫用及迴避Turing Complete 而帶來的一些惡化的問題，在以太坊中所有的程序執行都需要費用。各種操作費用以gas為單位計算。由於ETH本身並不符合自己的 ERC-20標準，所以在錢包上需要不單只有穩定幣的存在，還需要有少部份額的 ETH (gas) 同時存在。由於場外網絡不需與其他以太坊用戶爭奪網絡確認速度，所以用戶大部份時間都可以在便宜安全的網絡成本 (safe price) 進行交易。處理去中心化用戶 gas 為 Timespay 錢包最複雜的一部份。我們可以把Gas refill交易技術分為四個部份，

交易環境一：傳送人和收款人也有足夠gas作未來交易費用。在此環境下的光速交易將會直接完成此項交易確認。

交易環境二：傳送人有足夠gas作未來交易費用，但收款人沒有或剩下的gas不足夠執行去中心化交易所兌換程序。此環境下收款人大多數為新地址用戶，此時Server會向傳送人提出要求打散穩定幣傳送。傳送人接受這項要求後，發送的穩定幣將會有少部份被轉換成ETH一同發送到收款人錢包。額外的網絡傳送成本會在發送的穩定幣裏面扣除由收款人承擔。

交易環境三：傳送人即將沒有足夠gas作未來交易費用。此環境下傳送人為經常使用用戶。傳送人的將會被要求執行去中心化交易所兌換程序，兌換相同價值ETH。

交易環境四：傳送人持有穩定幣但完全沒有gas，須向友人/網站/便利店/ATM 等地方買入 Gas。去中心化使用者可透過智能合約上鎖定ether等避免進入此環境等而得到長時間使用改善。

5. 匯率問題 - 去中心化交易所

匯率問題是在地區上使用跨國貨幣必然會面對的主要問題，我們可以採用兩種方法解決此問題。一：由銀行匯率結算；二：固定地區匯率機制貨幣 (Pegged to local currnecy) 並且在去中心化的交易所上由用戶與用戶之間自行兌換。

去中心化的交易所 (DEX) 為本白皮書最簡單的一部分，可以部署簡單的智能合約DEX或透過前人工作 DEX 聚合器上的API。

6. 總結

我們提出了去中心化區塊鏈技術的方案，這簡易使用的錢包應用程式將會解決穩定幣交易速度，安全性，網絡成本和匯率複雜的問題。這個錢包不單只令美國紐約州金融服務廳監管的穩定幣帶到普羅大眾手機上與世界金融接軌，還可為以太坊極其大量的金融和非金融協議帶到普羅大眾手機上進一步應用作日常使用。大大提升地區競爭力，發展去中心化無限可能。

參考文獻

[1] (n.d.). *DFS Authorize Paxos to Offer "BUSD" Stablecoin. (N.d.).* Retrieved from https://www.dfs.ny.gov/reports_and_publications/press_releases/pr1909051

[2] Wood, G. (n.d.). Ethereum: A secure decentralised generalised transaction ledger.

[3] Nakamoto, S. (2009). Bitcoin: A peer-to-peer electronic cash system.