可對抗偽冒、竊盜、洗錢之 PoR 共識演算法

(Hsiao-Chun Han. Proof of Work Blockchain Technology and Byzantine Fault Tolerance Consensus Algorithm in Cryptocurrency, along with Proof of Relation (SOC Laboratory). (n.d.). Research report. National Chung Hsing University, Taiwan.

Hsiao-Chun Han
SOC Laboratory
National Chung Hsing University
2023.08.30

1.研究動機

51%攻擊證明目前加密貨幣使用的共識演算法 PoW 無法防止篡改，對加密貨幣的威脅不斷升高。為此本研究舉實例反證「主帥 v.s. 副官」模式下即使 n>3m 仍無法達成拜占庭容錯，接著舉實例證明若能事先辨識叛徒的行為再加以屏蔽，可提升決策品質。本研究也提出新的共識演算法 PoR(Proof of Relation)，這是全世界第四個共識演算法，主張：從各將領過去的選擇記錄裡找出模式或規則，以此來判斷是否有將領的選擇出現異常，將之剔除後再採多數決，如此可達成拜占庭容錯。本研究以企業財務報表品質問題為例，以台灣 869 家公司 1995~2022 年的財報資料進行實證研究，得到證據證明 PoR 是可行的，即使面臨少數劣質財報威脅，依然可確保整體決策品質。最後本研究將 PoR 應用在加密貨幣上，提出可對抗篡改、竊盜、洗錢等等的區塊鏈技術；除了可解決 51%攻擊問題，還可以大幅減少挖礦行為的鉅額耗電量，有助於加密貨幣長遠的健全發展。

2 拜占庭將軍問題與容錯

2.2.1 分散式對等網路的通信問題

Lamport, Shostak, and Pease [1982]提出拜占庭將軍問題是為了解決分

散式對等網路通信問題。這是指部份的節點可能故障或進行惡意行為，如何確保整體網路的一致性、正確性或可信度。Lamport, Shostak, and Pease [1982]以一群拜占庭將軍聯手圍攻一個城鎮的通信與決策，來模擬這個問題。

2.2.2 拜占庭將軍問題

一群拜占庭將領分別各率領一支軍隊共同圍攻一座城市，每個將領皆各自決定作戰方式，而不是由一名主帥下達指令給所有將領。 將領可以選擇的決策只有兩種，進攻或是撤退。

此次圍城必須行動一致才能獲得勝利，若部份將領率隊進攻時其他將領卻撤退，將導致戰敗及災難性後果。

為了確保所有將領的行動一致，Lamport, Shostak, and Pease [1982]提出共識演算法，即由每一位將領投票決定隔天要進攻或撤退，再看那一項決定獲得的票數較多，所有將領皆會服從投票表決的多數結果。此外，為了執行共識演算法，每位將領皆須將自己的選擇告訴其他所有將領，但只能透過信使傳達口頭訊息。拜占庭將軍問題是指，將領裡面可能有叛徒，故意傳遞假信息來破壞彼此行動的一致性。

2.2.3 叛徒搞破壞

例如這次一共有 7 位將領聯手進攻城鎮，但其中潛藏 1 名叛徒。在投票過程中 6 名正常的將領中有 3 人選擇進攻，3 選擇撤離退。此時叛徒可對 3 名選擇進攻的將領派信使表示自己支持進攻，並對 3 名選擇撤退的將領表示自己支持撤退。如此將導致前 3 位將領看到有 4 票投進攻，從而服從共識於隔日發起進攻，同時另外 3 名將領軍看到有 4 票投撤退而服從共識於隔日率隊撤退。這樣整個拜占庭部隊的一致性就被破壞了。

2.2.4 拜占庭容錯

Lamport, Shostak, and Pease [1982]同時提出拜占庭容錯，這是指當從事惡意行為的節點為少數時，分散式對等網路仍可確保整體通信的一致性、正確性、可信度，並提出「主帥-副官模式」及「簽章模式」，來達成拜占庭容錯。

「主帥-副官模式」是指拜占庭將領裡有一人擔任主帥(C)的角色，由主帥向所有人發號施令，其他為副官(V)，只能遵守命令。但副官不知誰是叛徒，而主帥可能是叛徒，因而副官還是依照共識演算法，須向他人詢問收到什麼指令，再服從所有人回答的多數指令。

Lamport, Shostak, and Pease [1982]令叛徒人數為 m，全部將領人數為 n，並主張當 n>3m 時能達成拜店庭容錯，例如：

(1)其中一名副官為叛徒，提供錯誤訊息，但其他兩名副官收到的指令中，進攻指令有 2 個，撤退指令為 1 個，故依共識決執行進攻，得到正確結果。

(2)主師為叛徒，分別給三位副官不同的指令,但三名副官收到的指令中，進攻指令有 2 個，撤退指令為 1 個，故依共識決執行進攻，得到正確結果。

然而當 n<=3m 時，無法達成拜店庭容錯，例如：

(1)其中一名副官為叛徒，提供錯誤訊息，導致另一名副官收到的進攻指令數 1 個，等於撤退指令數 1 個，無法決策，無法達成一致行動。

(2)主帥為叛徒，分別給兩位副官不同的指令，導致兩名副官收到的進攻指令數 1 個，等於撤退指令數 1 個，無法決策，無法達成一致行動。

2.2.5 拜占庭容錯的反證

本研究檢視 Lamport, Shostak, and Pease [1982]發現，其證明並非直接

證明，而是透過主張 1 個 lemma 及 1 個 theorem 成立的方式來間接證明，這樣的證明效果似乎不足，因而本研究舉出一個實例來反證即使在 n>3m 時，「主帥-副官模式」仍無法達成拜店庭容錯：

(1)假設一共有 5 位將領，n=5，一位叛徒，m=1，此時 n>3m，而叛徒為主帥。

(2)主師為叛徒，分別給四位副官不同的指令，給 2 名副官下達進攻指令，給另外 2 名副官下達撤退指令

(3)這 4 名副官向其他人確認，每人都是收到 2 個進攻指令，2 個撤退指令。出現跟前面一樣無法決策，無法達成一致行動的結果。

本研究認為需要找出新的共識演算法來證明拜占庭容錯是可以達成的，除了加密貨幣需要新的共識演算法來解決 51%攻擊以及耗電過巨的問題，還牽涉到另一個很重要的問題，到底網路世界對人類文明是好是壞？是福是禍？

Web 1.0 為中心伺服器架構，是由一群專業人士製作內容，建立網站伺服器供大眾查詢使用，網站為中心化的監督與管理角色，個別網路節點只能接受其提供的內容。

2.3 PoR(Proof of Relation)共識演算法

在思考如何能達成拜占庭容錯之前，本研究先以情境模擬的方法針對拜占庭將軍問題進行分析。

2.3.3 情境模擬步驟二：初步結論

依據前面兩個情境假設，可推論，叛徒會等到收齊所有將領的選擇後，才會依據當時共識結果來決定是否要作弊。在這裡本研究提出初步結論：

情境模擬分析初步結論：如果將領裡有叛徒作弊，則所有正常將領

收到的最後一個信息，將會是叛徒發出來的。

依據這個結論，本研究將 Lamport, Shostak, and Pease [1982]所提出的共識演算法進行修改，稱為「共識改進演算法」：

當每個將領發現，自己所收到的最後一個信息，將會改變或決定投票表決的多數決結果時，先將最後一個信息剔除不予採納，再服從之前的投票表決結果。

接著本研究以前面的「7 將領情境案例」來驗證「共識改進演算法」。經過實例驗證，在前面的「7 將領情境案例」下，「共識改進演算法」雖然尚無法達成拜占庭容錯，但至少免去了戰敗陣亡的悲劇，因而依據此項驗證，本研究提出第一個定理，稱為「拜占庭容錯改進第一定理 The First Theorem of Enhanced Byzantine Fault Toleran」：

雖然給定將領無法辨識叛徒，但若改進共識演算法來偵測叛徒行為再加以屏蔽，則可為整體帶來效益。**(P28)**。

2.3.4 情境模擬步驟三：兩個問題

2.3.5 情境模擬步驟四：PoR(Proof of Relation)共識演算法

由於拜占庭過去曾有很多次作戰經驗及記錄，而將領在做選擇時會受人際關係影響，依據此推論，本研究提出新的共識演算法，PoR(Proof of Relation)：

(1)從各將領過去的選擇記錄裡找出其決策的模式或規則。

(2)以此模式或規則來判斷是否這次圍攻時，某些將領的選擇出現異常。

(3)將異常的投票剔除後再採共識。

(2)步驟二：將關係繪成圖形來分析

本研究先模擬產業供應鏈上下游銷售進貨的關係，假設整個供應鏈有 12 家公司，以英文字母 A~L 表示，其銷售與進貨之關係為：

本研究使用「拓璞抽象思考-先線後點法」將企業間銷售與進貨的關係，以線條來呈現，而由此關係連結的企業財報數字，則以點來表達，畫出以下圖形：

(3)步驟三：圖形分析

本研究所繪製的線點圖，是假設整個供應鏈有 12 家公司，以圓點 A~L 表示，H 為供應鏈的終點，其對象為一般消費者。點跟點之間的線為企業間的銷售與進貨關係：

- 消費者消費金額是下游廠商 H 的銷貨收入，
- H 公司的銷貨成本 一部份來自進貨成本，
- H 進貨成本則為上游 B 公司對其銷售商品的銷貨收入，以此類推。

(4)步驟四：數學函數關係

本研究依據「拓璞抽象思考-數圖轉換法」將圖形分析的邏輯關係，以數學函數來表達：

即企業間的銷貨成長率的關聯應該會具備一定程度的穩定性」。

基於此分析結論，本研究依據 PoR(Proof of Relation)共識演算法主張

此關係可用來辨識企業財報數字是否異常。

3.研究方法與實驗設計

3.1 理論模式之推論

本研究對原始的拜占庭將軍問題進行四個步驟的情境分析，並於 2.3.5 提出 PoR(Proof of Relation)共識演算法，主張：「可以從各將領過去參與作戰時的選擇記錄裡找出其決策的模式或規則，然後以此來判斷這次圍攻時是否某些將領的選擇出現異常，若有則將之剔除後再採共識決。」如此將可以確保分散式對等網路在發生少數節點惡意行為時，仍可確保

整體通信的品質或可信賴度，即有助達成拜占庭容錯。

接著本研究於 2.4.1 說明為何企業財報品質符合分散式對等網路通信問題，並主張可以將 PoR(Proof of Relation)共識演算法應用在這個問題並驗證是否可行。為了達成這個目標，本研究提出假說：「若能找出企業財報數字間的關聯性，則當企業的財報數字明顯偏離此關聯性時，可視為品質較差或有詐欺嫌疑，可將之剔除後再以剩餘的財報進行投資決策。」

若有企業的比率的排名在不同年度出現亂跳，依據混亂性，應該是少數，會被判定為異常。

3.2 實驗程序

為了呈現企業間財報數字的關聯性，並以此辨識財報資訊品質之良窳，本研究建立以下實驗程序：

本研究以盈餘成長率與股價報酬率的相關係數大小來代表會計資訊品質之高低。

4.資料與實證結果

4.1 實證資料

本研究從 TEJ 資料庫的一般產業選取了 869 家公司 1995 至 2022 年的財務報表資料。TEJ 資料庫裡可查詢的報表一共 23 種，合計 745 個科目。本研究最後選取了 88 個會計科目，將其他報表及科目刪除的理由如下：

- 財務比率為使用會計科目數字計算而得，為重覆性資訊，故全部刪除，包含：「獲利能力指標、成本費用率指標、每股比率指標、成長率指標、償債能力指標、經營能力指標、法定比率」。
- 與當年度營運成效無關的全部刪除，包含：「盈餘分配表、補充項目-其他、關係人交易、退休金項目、認股權及用人費用、停止維護、其他」。

- 與當年度營運成效關係較低且單次金額較大者，以及明顯重複者刪除，包含：「存貨明細、不動產廠房設備明細」。
- 無資料或空值較多者皆刪除。

4.2 實證結果

4.2.1 企業間財報數字的關聯性

本研究將選取的企業財報資料依據 3.2 實驗設計執行程序(a)到(g)，最後將每家公司的 STD 值的平均值 mean 由大到小排序成果如下圖。

在 869 家公司裡有 828 家公司的 STD 的平均值小於 0.1，從圖形來看這 828 家公司的 mean 值由低到高的增加幅度十分平緩，大約從第 829 家公司開始忽然大幅上升，轉變十分劇烈。增幅平緩的 828 家公司占全體的 95.3%，剩餘劇烈變化的 41 家公司占 4.7%。

STD 數字的大小代表某公司某會計科目在 869 家公司裡的排名順序在 28 年的期間裡的變化幅度，數值愈小意味著變化愈小，數值大代表某公司的財報數字一下子排行第 20%，下個年度跳到 80%，再下個年度又跳回 20%，本研究認為排序順序的大幅度變化是因為會計科目的數字脫離了企業間財報數字的函數關係，此符合本研究 2.4.4 混沌現象裡的混亂性，而混亂性發生的機率為低。從上圖可看出，只有少數 4.7%企業的 STD 平均值偏高，這跟本研究的推論是相符的。

此外本研究於 2.4.4 得出結論為：「企業間財報數字會存在某種關聯，且具備相當的穩定性」。從上圖可看出，95.3%的企業的 STD 的平均值小於 0.1，代表財務報表數字的跨年度變化比較小，企業間財報數字的關聯性相當穩定，這跟本研究的推論是相符的。

4.2.2 會計資訊品質差異

4.1.1 的結果顯示企業間財報數字確實存在某種關聯性，而且台灣 869 家

公司裡 95.3%的企業的跨年度財務報表數字的變化，未偏離此關聯性。這個關聯性是產業供應鏈上下游公司互相從事的銷售與採購行為，造成企業間的銷貨收入存在函數關係。一家公司的年度經營表現如果與產業概況一致，就會符合此關聯性。相反的，但有少數 4.7%的企業偏離了這個關聯性，這意味著其財報數字偏離了產業況，未能允當表達其年度營運成果，依據財務會計理論，代表會計資訊品質比較差，而原因就是這些公司進行不適當的人為調帳。

盈餘是最能代表企業營運成果的單一會計數字，因而 Ball & Brown [1968 是以盈餘成長與股價報酬的關係來代表會計資訊的品質及有用性，因而本研究依據 3.2 實驗設計的(h)來執行以下兩個程序，成果如下圖：

- 從 869 家公司的 STD 的平均值由低到高排序資料裡，取最高的 41 家公司為大群(上圖的紅框)，最低的 41 家公司為小群(上圖的藍框)。
- (J)分別計算大群及小群的 1995 年至 2022 年的盈餘成長率及股價成長率，並以 Python 語言程式計算皮爾森相關係數。

檢視結果，小群的盈餘成長率與股價成長率的皮爾森相關係數值為 0.115，與過去會計實證研究成果大致相符。然而大群的相關係數為 0.109，差了十倍，這代表大群 41 家公司的財報數字變化較大，脫離供應鏈上下游的企業間關聯性，意味著曾經對財務報表進行不當的人工會計調帳，導致資訊品質較差，並造成盈餘與股價的相關係數偏低。

這個研究結果告訴我們，由於企業公司財報及會計師簽證屬於分散式對等網路通信問題，如果依照本研究提出的共識演算法 PoR，找出企業財報數字間的關聯性，以此辨識出經過不當的人工會計調帳的財務報表並加以屏蔽，確實能提升整體投資決策品質，確保整體企業財報的可信賴度。

這個結果也意味者，儘管出現少數節點惡意行為(4.7%的企業對財務報表進行不當的人工會計調帳)，只要能找到有效的共識演算法如 PoR，仍然可以確保分散式對等網路通信的可信賴度，即 Lamport，Shostak， and Pease [1982]所提出的拜占庭容錯確實是可以達成的，網路不會成為整體社會做出不利決策的原因。