IOTA/ Blockchain

IOTA Introduction

- IOTA 新型數字加密貨幣
- 專注於解決 M2M 的交易問題
- 實現機器與機器間無交易費支付，建構機器經濟(Machine Economy)
- 高效、安全、輕便，實時的微交易, 並且不產生交易費用
- 專為IOT而設計，
- 基於非區塊技術加密貨幣
- IOTA 是基於 Tangle, 而非區塊鏈技術。

IOTA Introduction

- 官網: https://iota.org/
- 論譚: https://forum.iota.org/
- 新型的交易結算和Data專移層.
- 新型的分佈賬本– Tangle.
  - 克服區塊鏈設計中的低效性,
  - 去中心化 P2P 系統的共識創造了一種新方法
  - 透過 IOTA 轉不需要支付手續費。

Tangle V.S. 區塊鏈

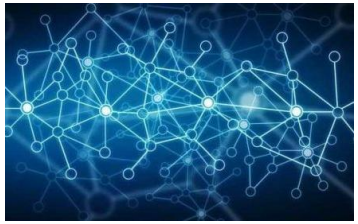
- 完全獨主的架構, But 同一規則之上。
- Tangle 是基於定向非循圖的 TAG. 不是連續的鏈式架構.
- 通過 DAG, IOTA能夠實現較高的交易吞吐(平行驗證). 不收手續費.
  - 隨著Tangle的不斷發展，越來越多的參與者都將發起交易，整個系統也會變得越來越安全和快速，確認時間會縮短，交易也完成的越來越快。
- 區塊鏈中添加下壹個區塊需要多方進行競爭，並獲取區塊獎勵或交易手續費
- 在IOTA系統中，網絡中的每位參與者都能進行交易並且積極參與共識。更具體點說，妳直接定位了兩筆交易(主交易和分支交易)，且間接在子tangle中定位其它交易。通過這種方式，驗證就能同步進行，網絡能夠保持完全去中心化，不需要礦工傳遞信任，也不需要支付交易手續費。

Tangle V.S. 區塊鏈

- 區塊鏈是壹種分布式分類帳，它存儲通過其網絡發送的所有交易的歷史記錄。驗證和處理這些交易產生了分布式共識，這是壹種奇怪的方式沒有壹組專門處理交易的礦工或驗證人，發送交易的每個人都負責處理糾紛中的其他交易。，即網絡同意所有收到的交易。

- 礦工負責處理構建這些塊的交易。確保每筆交易都是合法的.

- 礦工的區塊鏈網絡使用稱為工作證明（Proof of Work）的機制來處理交易，這意味著礦工必須積極地利用他們的計算機工作（並相互競爭）來驗證交易。



Tangle V.S. 區塊鏈

- 沒有壹組專門處理交易的礦工或驗證人，發送交易的每個人都負責處理糾紛中的其他交易。這意味著無需任何人運行加密核心軟件並連接到網絡節點來驗證事務
- IOTA使用直接非循環圖（Directed acyclic Graph, DAG）算法來管理其分布式分類帳。這允許網絡達到分布式共識，而不使用區塊鏈技術或以塊存儲交易。網絡上的每個交易都必須確認兩個以前的交易，然後才能進行驗證。
- 分散式保護：由於每個使用網絡的人都負責維護，因此不需要礦工; (ASIC 採礦集中. Not needed..)
- 量子抗性：IOTA團隊已經制定了Tangle如何為加密貨幣提供針對量子計算的安全緩沖，這可能會威脅到區塊鏈技術的安全性。
- 可擴展性和小額支付：
- IOTA專為物聯網而建，智能設備的生態系統以某種方式使用互聯網來實現功能（例如，Google Home，智能電視，也可以告訴您天氣的那些奇特的冰箱）

IOTA 量子安全與手續費

- IOTA使用哈希簽名而不是橢圓曲線密碼學(ECC)。哈希簽名不僅僅在速度上勝過ECC，還能大大簡化整個協議(簽名和驗證)。

- IOTA能夠實現量子安全是因為我們采用了文格尼茨簽名。IOTA的三進制哈希函數稱為Curl(編程語言)。

- IOTA系統中不存在礦工或驗證者(來完成這項工作，因此不需要支付手續費)。IOTA的共識是完全去中心化的，每位網絡成員都能發起交易，直接或間接地確認過去的交易。

能用 IOTA 做什麼

- 交易結算(尤其是微支付)和數據完整性。通過這兩個功能衍生出的大部分用例都是很有意義的，而且大多數情況下只能通過IOTA來實現。更多功能(比如說Oracles和智能合約等)已經在我們的發展計劃中，不久將會正式添加進來。

- IOTA主要致力於物聯網，通過機器支付資源、服務或者許可，包括智能城市、智能電網、基礎設施、供應鏈等在內的用例都是IOTA可能實現的目標。

- IOTA總供應量為(3 ^ 33-1)/ 2 或2,779,530,283,277,761個。所有IOTA都是在初始塊創建的，