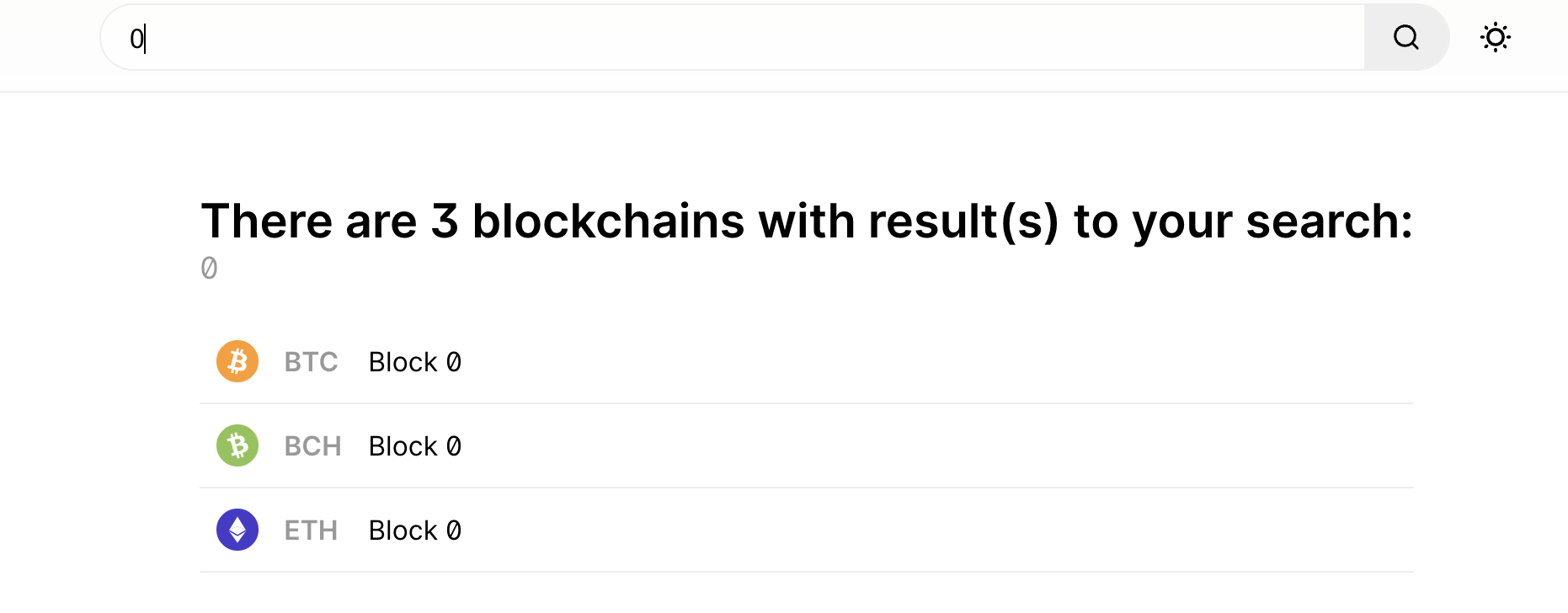
1. In June 2023, SEC charged CZ, Binance' CEO at that time, for violating US securities rules. In November 2023, CZ pled guilty to violating the American [Bank Secrecy Act](https://en.wikipedia.org/wiki/Bank_Secrecy_Act). If you analyzed data wrongly and lost money in this current market, whom should you blame?
2. As of 2024/3/12, BTC's price reaches higher than $72k. MSTR just completed the purchase of 12000 BTC at the price of $68k. That is, MSTR poured in ~US$820m to BTC market. MSTR used convertible debt (again!) to close this deal. The fact that MSTR's main business is in BTC nowadays begs the question: Why has MSTR gone up much more than BTC? You can see below that MSTR has gone up $142.01 in 24 hours and has gone up 129% from 2024/1/1 til now.
3. Bitcoin trackers not only help us detect abnormal transactions but also provide interesting historical information about Bitcoin. The first block in Bitcoin, called the Genesis Block, led the world into the cryptocurrency era. (3pts) Please help me use the Bitcoin tracker to find when the first block in Bitcoin was created (include the time zone after your answer). Additionally, (4pts) help me find the address that mined this block (this address belongs to Satoshi Nakamoto).

Congratulations! You used a simple way to track the address belonging to. Satoshi Nakamoto, who created the BTC protocol.

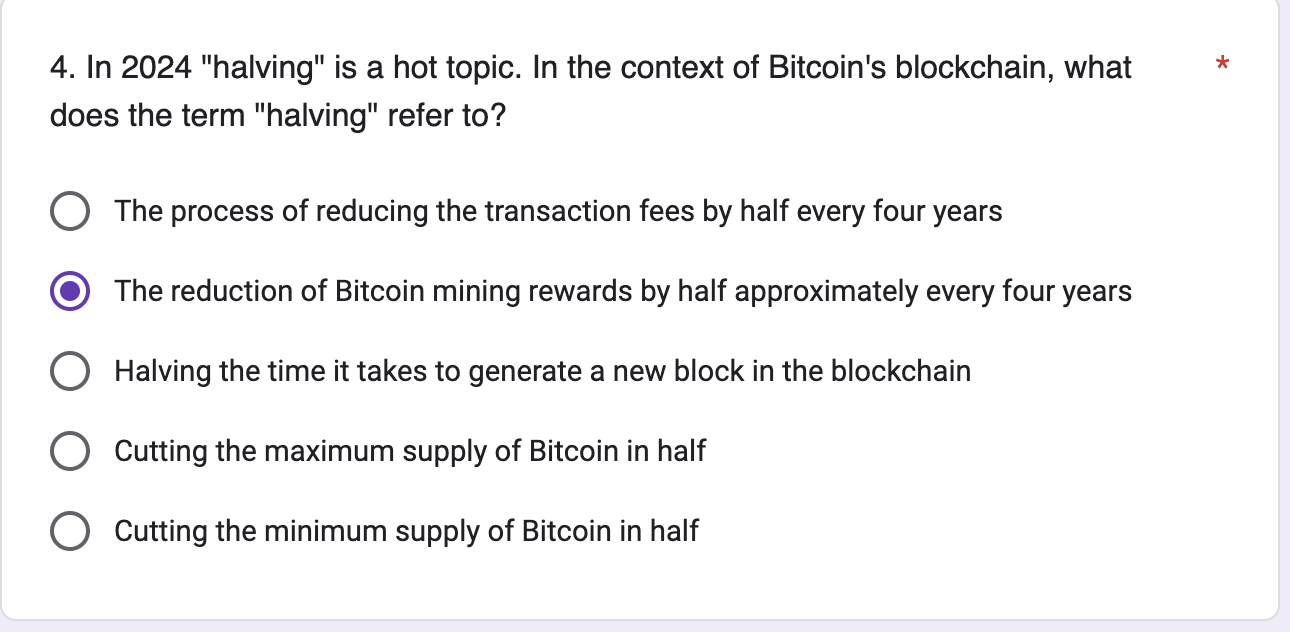
You can. use <https://www.blockchain.com/explorer> or <https://blockstream.info/> to gather all the necessary information.



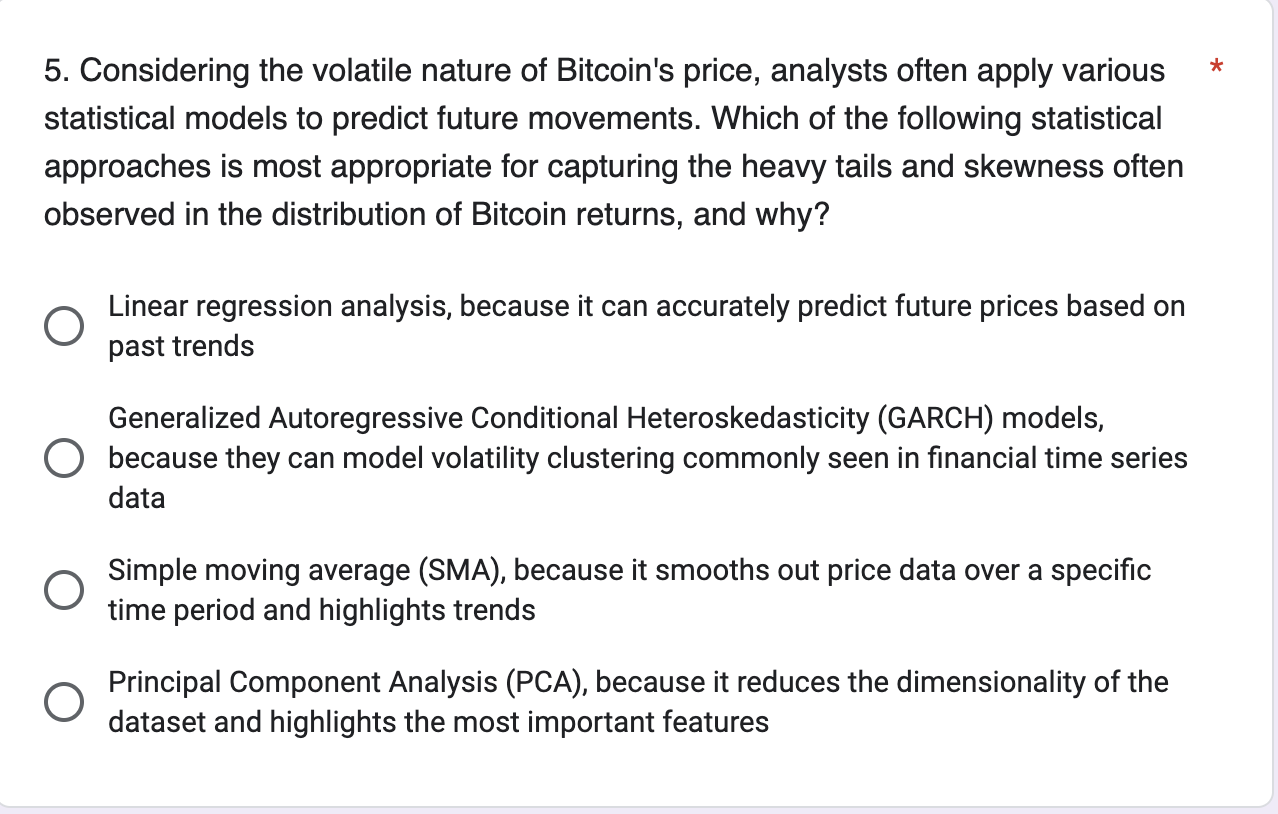
在網址中輸入的是他的height or hash, 因為是genesis, 所以height = 0  
2009年1月4日 上午2:15:05" (January 4, 2009, at 2:15:05 AM ＧＭＰ+8 （看browser時區）

用第二個網址可以找到block 0 address

000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f

1. 

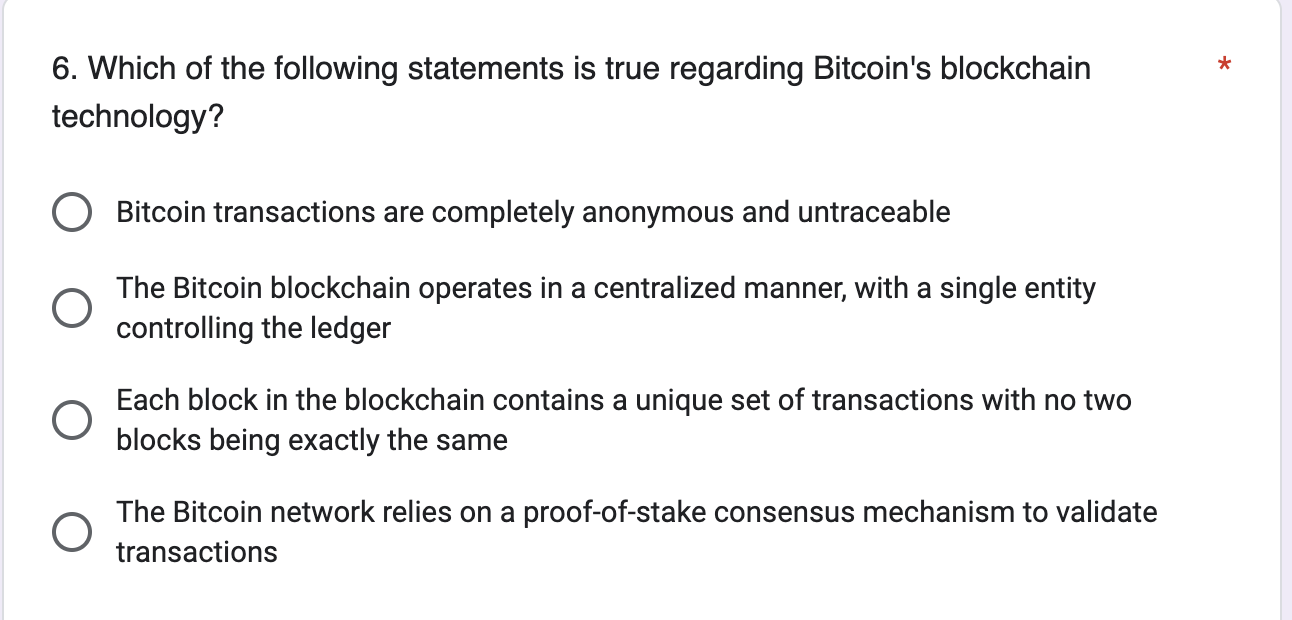
在比特幣區塊鏈的背景下，術語「減半」是指比特幣挖礦獎勵大約每四年減少一半。該事件被編程到比特幣的程式碼中，並用於逐漸降低新比特幣的創建速度，從而在總供應量接近 2,100 萬比特幣的最大上限時強制實施一定程度的稀缺性。減半會影響礦工的積極性，並可能對比特幣市場產生影響。



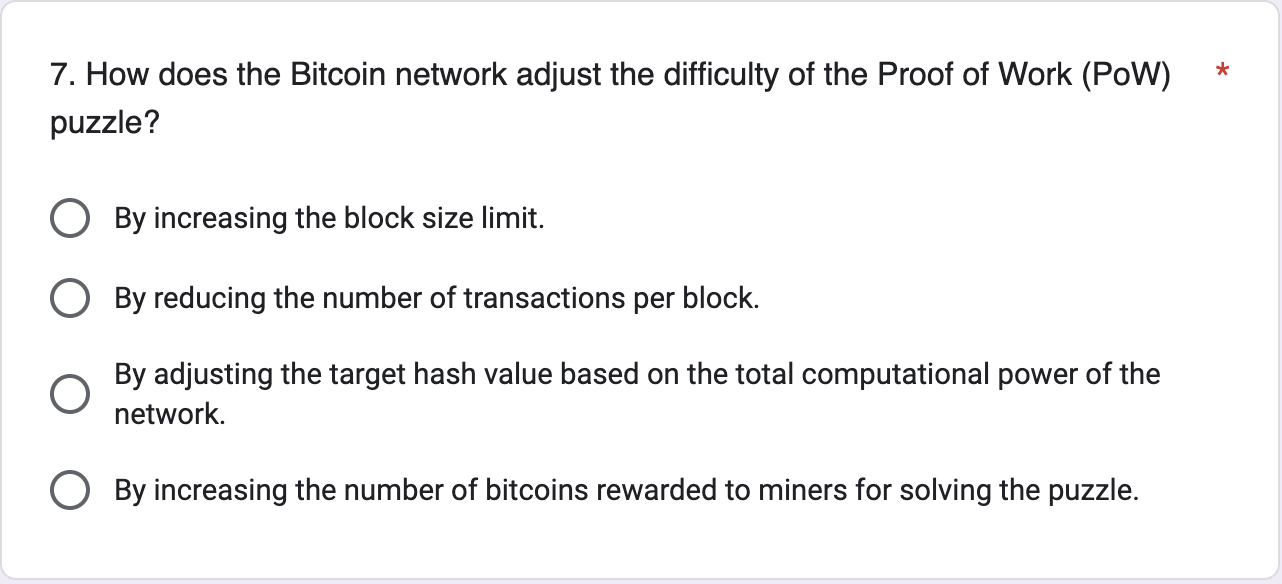
Generalized Autoregressive Conditional Heteroskedasticity (GARCH) models, because they can model volatility clustering commonly seen in financial time series dat

廣義自迴歸條件異方差 (GARCH) 模型的第二個選項是正確的答案。這些模型是專門為處理比特幣價格變動中觀察到的波動而設計的

1. **線性迴歸分析**：這是用來建立一個因變數與一個或多個自變數之間關係的模型。它假設變量之間有線性關係，但由於比特幣價格的波動具有非線性特性，此模型不適用於比特幣。
2. **簡單移動平均（SMA）**：通過計算一定時期內的收盤價總和後再除以時間段數來獲得的算術平均值。由於它無法捕捉到價格的波動性，也不適合預測未來價格，因此不適用於如比特幣這般波動的市場。
3. **主成分分析（PCA）**：一種統計技術，通過轉換成一組新的變量（主成分）來減少數據的維度，這些主成分概括了數據的特點。它主要用於探索性數據分析和模式識別，而不是預測未來價格，特別是在比特幣這樣的波動市場中。



1. **比特幣交易完全匿名且無法追踪**：這是錯誤的。比特幣交易是偽匿名的，每筆交易都會記錄在公共的區塊鏈上，並且可以通過交易地址追踪。
2. **比特幣區塊鏈以集中式的方式運作，由單一實體控制賬本**：這也是錯誤的。比特幣是去中心化的區塊鏈，沒有單一實體控制賬本。
3. **區塊鏈中的每個區塊包含一組獨特的交易記錄，沒有兩個區塊是完全相同的**：這是正確的。每個區塊都有一組獨特的交易，且每個區塊的哈希值是基於它包含的交易而獨一無二的。
4. **比特幣網絡依賴於證明權益（Proof of Stake）共識機制來驗證交易**：這是錯誤的。比特幣使用的是證明工作（Proof of Work）共識機制。



比特幣網路調整工作證明（Proof of Work, PoW）難度的方式是：

* **通過調整目標哈希值來基於網絡的總計算能力**。

這項調整大約每兩周進行一次，以確保平均每十分鐘能夠產生一個區塊。當網絡的計算能力增加時，解決PoW難題的速度會加快，因此網絡會提高難度，反之亦然。

其他選項的錯誤原因：

* 增加區塊大小限制、減少每個區塊的交易數量、增加礦工解決難題後得到的比特幣數量，這些方法與調整挖礦難度無關。

8. Please search this keyword : "[Strange Block 74638](https://bitcointalk.org/index.php?topic=822.0)", then describe what. happened(5pts) and how to fix the problem(2pts).

Here are some useful tools and information:(<https://www.blockchain.com/explorer>),

([https://github.com/bitcoin/bitcoin/commit/](https://github.com/bitcoin/bitcoin/commit/d4c6b90ca3f9b47adb1b2724a0c3514f80635c84#diff-118fcbaaba162ba17933c7893247df3aR1013)).

Hack 想利用integer overflow的錯誤，將overflow隱藏為費用，這起事件包含了兩筆92233720368.54(7ffffffffff85ee0).

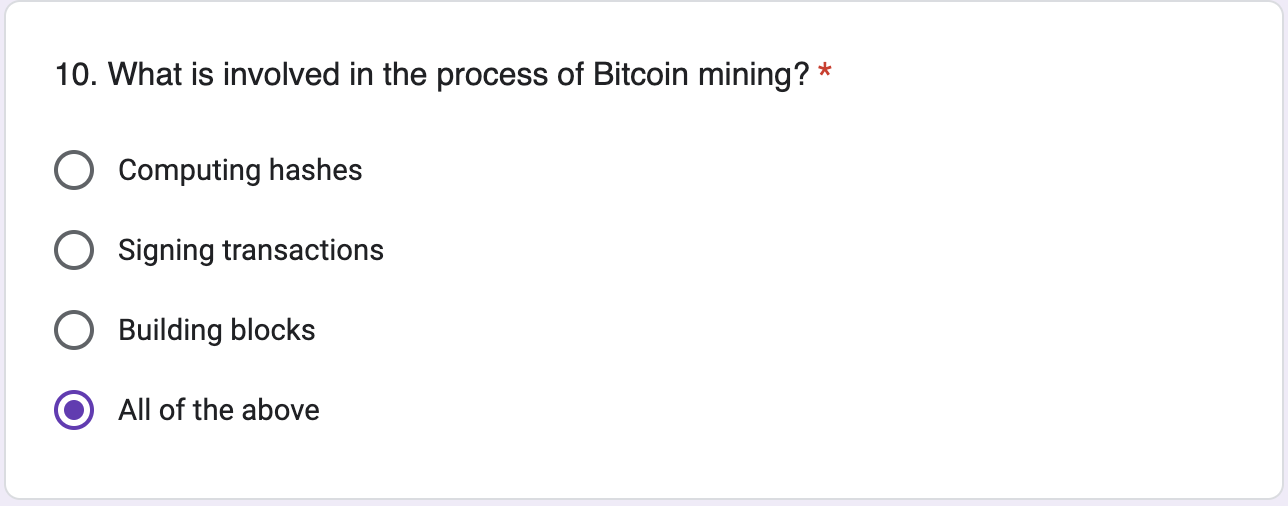
解決方式： 在code中新增check overflow or negative input, output value.

All nodes had to immediately upgrade to the new client version of 0.3.10, which patched the overflow bug from block 74638.

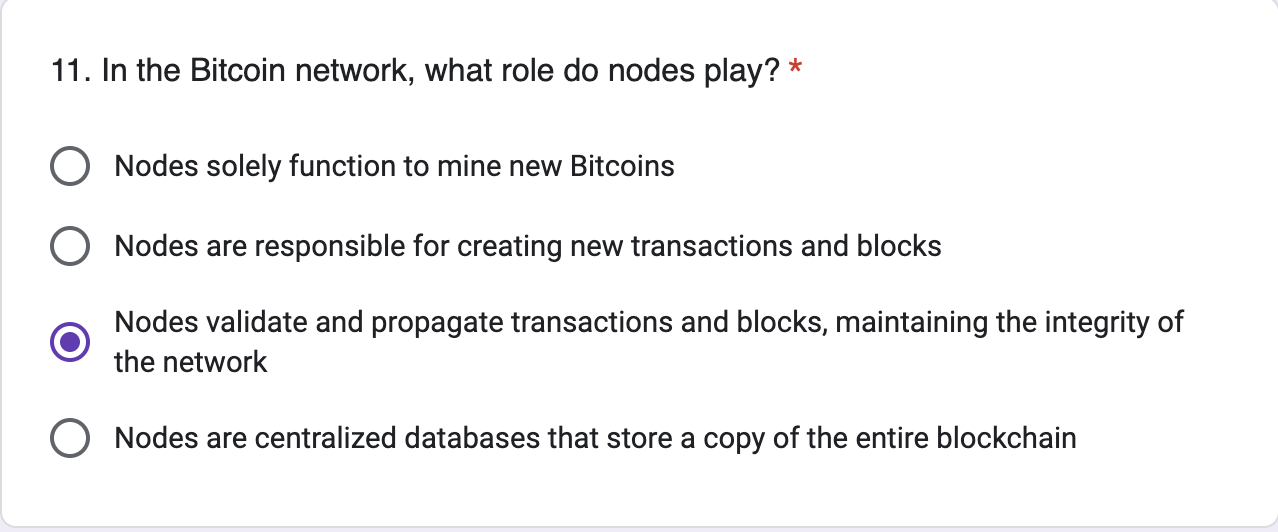
As of 2:16 AM on August 16, Satoshi had announced that over half of the nodes had upgraded to the new client meaning that they had successfully got more power than the bad chain, effectively rolling back the transaction itself.



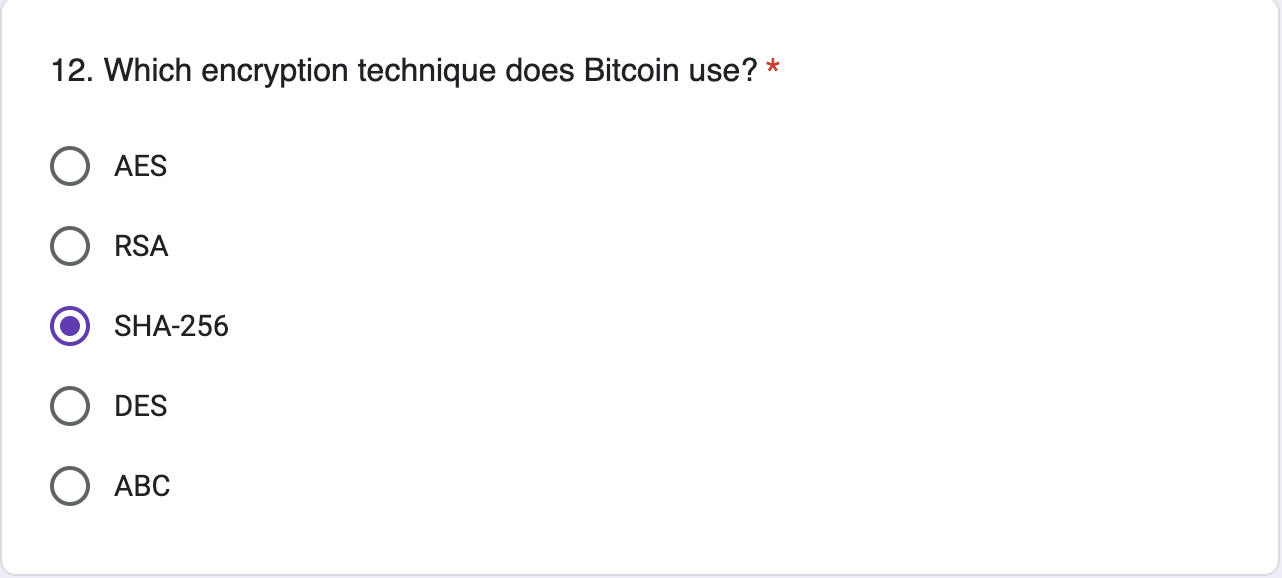
在比特幣的區塊鏈技術中，默克爾樹的主要角色和基本功能是高效地總結和驗證一個區塊中包含的大量交易的完整性。這有助於增強區塊鏈的安全性和可擴展性，因為它提供了一種方法來確認交易數據的準確性，而不需要檢查每筆個別交易的完整數據。這是因為默克爾樹允許網絡參與者快速且有效地證明交易是否包含在一個區塊中，而無需下載全部交易數據。



在比特幣挖礦過程中涉及到的主要活動包括計算哈希值、簽署交易以及構建區塊。計算哈希值是為了找到一個符合特定難度目標的數值，簽署交易是確保交易的有效性和安全性，而構建區塊則是將有效的交易打包進區塊鏈中。因此，這些步驟是挖礦過程不可或缺的部分。



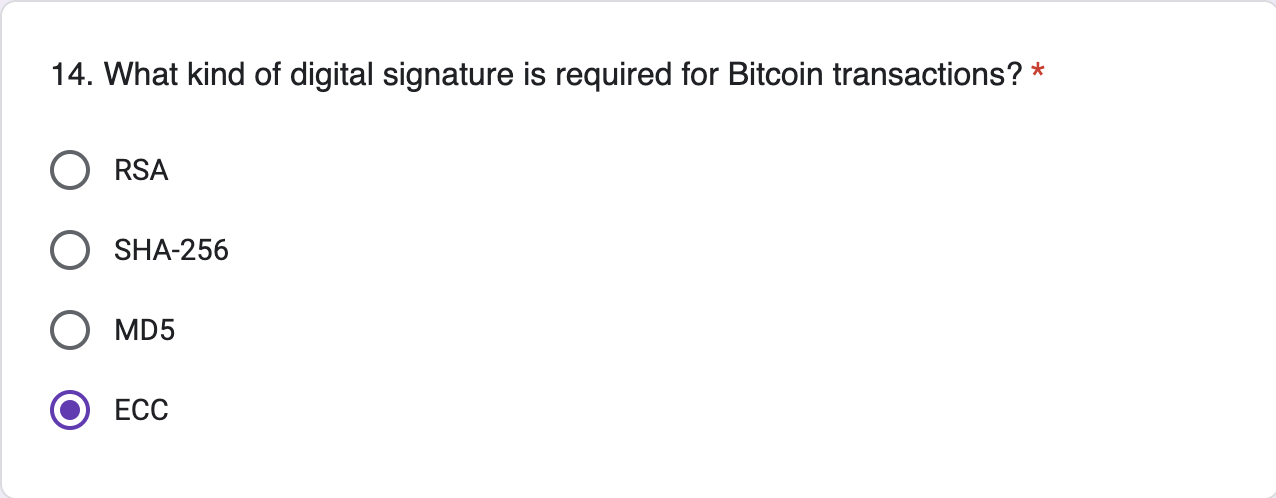
在比特幣網絡中，節點（nodes）的角色是驗證和傳播交易與區塊，同時維持網絡的完整性。節點不僅僅只是挖掘新比特幣；它們還確保所有交易和區塊的正確性，幫助防止雙重支出和其他詐騙行為。節點之間的這種去中心化共識機制是比特幣區塊鏈安全性的關鍵



比特幣使用的是SHA-256這種加密技術。SHA代表安全哈希演算法（Secure Hash Algorithm），而256位指的是這種演算法產生的哈希值長度。SHA-256是比特幣區塊鏈中用來創建比特幣地址、挖礦過程中計算工作量證明的一部分，以及確保交易不可逆和安全的關鍵技術。其他選項，如AES和RSA，是其他類型的加密技術，並不是比特幣區塊鏈的核心部分。DES是較舊的加密標準，已在很多現代系統中被更先進的加密方法取代。ABC則不是一種公認的加密技術。

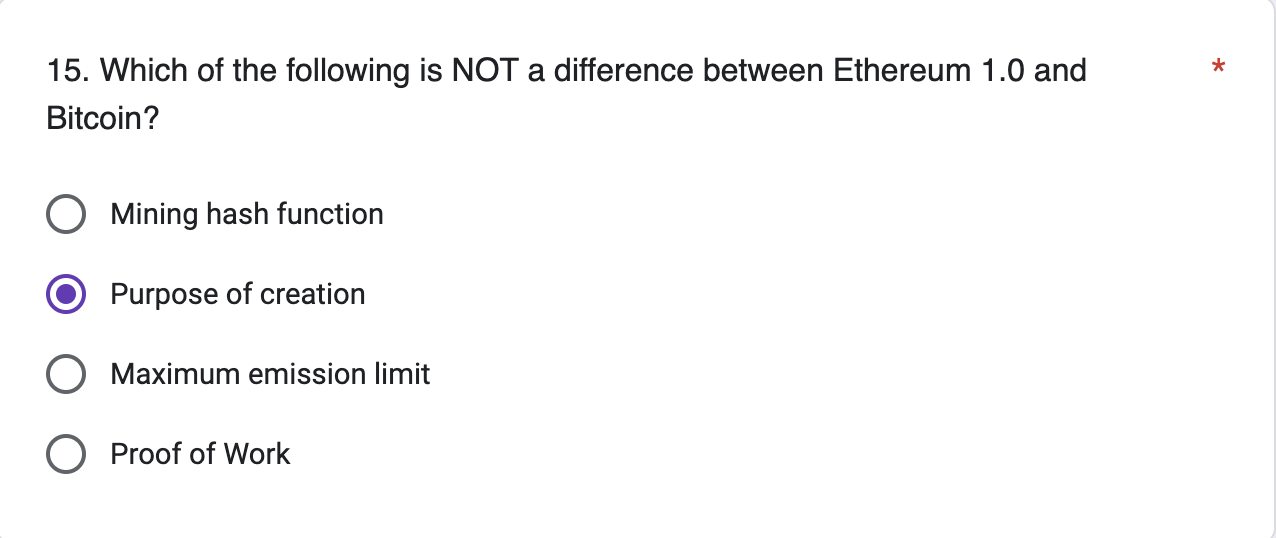


在比特幣協議中，"hashing"（哈希運算）的主要目的是為了確保交易和區塊數據的完整性和安全。透過對數據進行哈希運算，每個交易和區塊都會有一個獨特的哈希值，這可以用來驗證數據的未被篡改和保護區塊鏈的整體安全性。



Bitcoin transactions require Elliptic Curve Digital Signature Algorithm (ECDSA) for digital signatures. Therefore, the correct answer is:

ECC (Elliptic Curve Cryptography)



以太坊的創建目的是成為智慧合約和去中心化應用程式（DApp）的去中心化平台，而比特幣主要是作為點對點電子現金系統創建的