Assignment A
https://docs.google.com/forms/d/e/1FAIpQLSfh1JuWwFQYdSwSKmw5dNJS_xkTLFCvAY7Nd3AKTsHqbBMAfA/viewform

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. If you analyzed data wrongly and lost money in this current market, whom should you blame?

Ans : Yourself

2. As of 2024/3/12, BTC's price reached more than $72k. MSTR just completed the purchase of 12000 BTC at the price of $68k. That is, MSTR poured ~US$820m into the 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 till now.

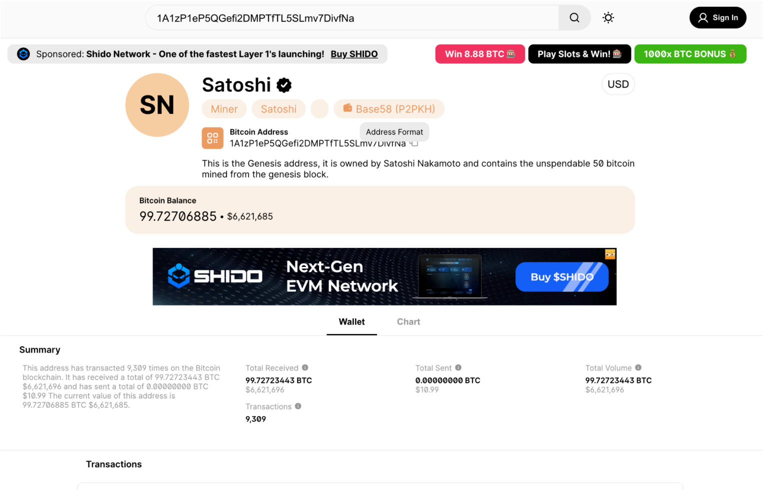
Ans : Reason 4: MSTR in NASDAQ gives investors to trade BTC with leverage (買現股自帶融資槓桿又不會被margin call)

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.

Ans : January 3, 2009 18:15 UTC, 1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa



1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa

Satoshi

Bitcoin Address
1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa

This is the Genesis address, it is owned by Satoshi Nakamoto and contains the unspendable 50 bitcoin mined from the genesis block.

Bitcoin Balance
99.72706885 • $6,621,685

Summary

This address has transacted 9,309 times on the Bitcoin blockchain. It has received a total of 99.72723443 BTC $6,621,696 and has sent a total of 0.00000000 BTC $10.99 The current value of this address is 99.72706885 BTC $6,621,685.

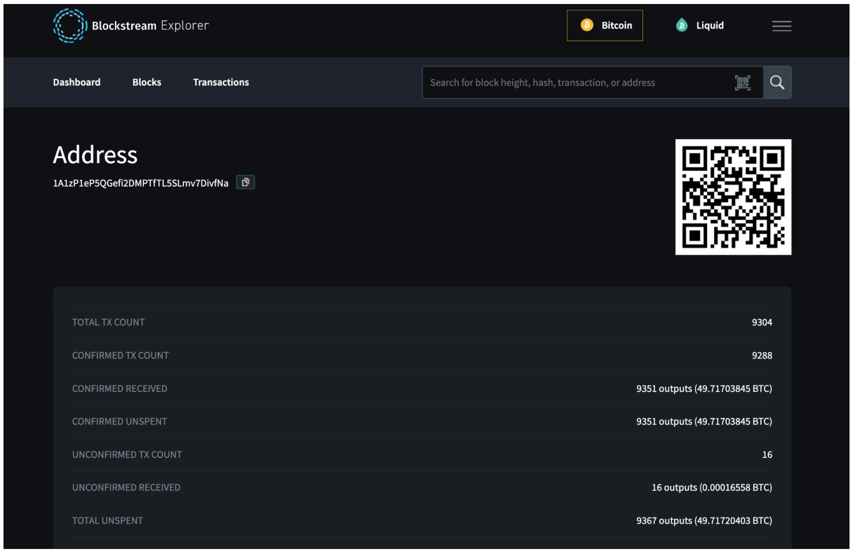
Total Received
99.72723443 BTC
$6,621,696

Total Sent
0.00000000 BTC
$10.99

Total Volume
99.72723443 BTC
$6,621,696

Transactions
9,309

Transactions



Address

1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa

TOTAL TX COUNT	9304
CONFIRMED TX COUNT	9288
CONFIRMED RECEIVED	9351 outputs (49.71703845 BTC)
CONFIRMED UNSPENT	9351 outputs (49.71703845 BTC)
UNCONFIRMED TX COUNT	16
UNCONFIRMED RECEIVED	16 outputs (0.00016558 BTC)
TOTAL UNSPENT	9367 outputs (49.71720403 BTC)

🚩 4. In 2024 "halving" is a hot topic. In the context of Bitcoin's blockchain, what does the term "halving" refer to?

Ans : The reduction of Bitcoin mining rewards by half approximately every four years

🚩 5. Considering the volatile nature of Bitcoin's price, analysts often apply various statistical models to predict future movements. Which of the following statistical approaches is most appropriate for capturing the heavy tails and skewness often observed in the distribution of Bitcoin returns, and why?

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

🚩 6. Which of the following statements is true regarding Bitcoin's blockchain technology?

Ans : Each block in the blockchain contains a unique set of transactions with no two blocks being exactly the same

7. How does the Bitcoin network adjust the difficulty of the Proof of Work (PoW) puzzle?

Ans : By adjusting the target hash value based on the total computational power of the network.

8. Please search this keyword : "Strange Block 74638", 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/).

Ans : [What happened] The incident involving "Strange Block 74638" in the Bitcoin blockchain occurred on August 15, 2010, and is known as the "Value Overflow Incident." It was discovered that this block contained a transaction that anonymously created 184,467,440,737.09551616 bitcoins, distributed across three different addresses. Two of these addresses received an overwhelming amount of 92.2 billion bitcoins each, due to an integer overflow error. This bug essentially allowed for a massive creation of bitcoins far beyond the intended total supply cap of 21 million BTC, due to the failure of the system to check for overflow in the combined transaction output values.
[How to fix the problem]
The Bitcoin Core Development team swiftly responded by releasing a new version of the Bitcoin client within five hours of the incident's discovery. This update included a soft fork change in the consensus rules to reject transactions with output value overflows, as well as any transaction outputting more than 21 million bitcoins for any reason. The blockchain was then forked to a "good" chain that did not include the overflow transaction.

🚩9. In the context of Bitcoin's underlying technology, which of the following statements best describes the role and primary function of a Merkle Tree?

Ans : It is utilized to efficiently summarize and verify the integrity of large sets of transactions included in a block, enhancing the security and scalability of the blockchain.

🚩10. What is involved in the process of Bitcoin mining?

Ans : Building blocks

🚩11. In the Bitcoin network, what role do nodes play?

Ans : Nodes validate and propagate transactions and blocks, maintaining the integrity of the network.

🚩12. Which encryption technique does Bitcoin use?

Ans : SHA-256

🚩13. What is the primary purpose of the cryptographic process known as "hashing" in the Bitcoin protocol?

Ans : To secure transactions and ensure the integrity of the blockchain data.

🚩14. What kind of digital signature is required for Bitcoin transactions?

Ans : ECC (Elliptic Curve Cryptography)

🚩15. Which of the following is NOT a difference between Ethereum 1.0 and Bitcoin?

Ans : Proof of Work

Assignment C

1. Software is eating the world. 能吃掉全世界的軟體為 ABCD. What does NOT belong to ABCD, according to Deloitte'17?

Ans : Dark pool

2. AI is very hot these days. NVIDIA stock price soared to US$950 on 2024/3/20. Which of the following is wrong?

Ans :

As Moore's law continues, 1 NVidia's H100 machine with standard 8 GPU cards is cheaper than $10m Taiwan dollars today.

—-----

This statement seems to be incorrect without needing further specific data on the current price. Moore's Law traditionally refers to the doubling of transistors on integrated circuits approximately every two years, leading to performance improvements. While Moore's Law has faced challenges at the cutting edge of chip manufacturing, it does not directly correlate to the pricing of GPUs. However, stating that an H100 machine with 8 GPU cards is cheaper than 10 million Taiwan dollars (approximately 330,000 USD) today might not align with reality. High-end computing systems, especially those equipped with several state-of-the-art GPUs like Nvidia's H100, can be expensive, but it is unlikely they would cost as much as 10 million Taiwan dollars unless there are specific circumstances or configurations that drive up the price unusually.

這個說法似乎無需具體的當前價格數據就顯得不正確。摩爾定律傳統上指的是集成電路上的晶體管數量大約每兩年翻倍，從而帶來性能的提升。雖然摩爾定律在晶片製造的前沿面臨挑戰，但它並不直接與GPU的定價相關。然而，聲稱目前一台配備8塊GPU卡的Nvidia H100機器售價低於1000萬新台幣（大約330,000美元）可能與實際情況不符。尤其是裝備了幾塊最先進的GPU，如Nvidia的H100的高端計算系統，可能會非常昂貴，除非存在特殊情況或配置異常地推高了價格。

—-----

3. 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. If you analyzed data wrongly and lost money in this current market, whom should you blame?

Ans : Yourself

4. [Smart contract] Which is not using smart contract?

Ans : Ubuntu

5. [Smart contract security] Smart contract programmers may transform Listing 1 below to Listing 2 by algebraic identities. However, most of them will not optimize the program in Listing 3, which changed the type of “val” from int to float. Why is it NOT a good idea to perform the same optimization on floating-point programs?

Ans : Floating point's precision problem

6. What will be the output after running the following code?

Ans : 22 20 18 16

7. [Underwriting: Rule checking] To establish whether a formula G is a logical consequence of formula from F1 to Fn, which of the following methods can be applied?

Ans : Check that ˥ F1 V ... V ˥ Fn V G is valid

8. [Underwriting: Rule checking speed] Which of the following problems have a bigger time complexity compared with O(n*logn) complexity?

Ans : Given a list L of n integers, find 3 numbers x,y,z in L (if x,y,z exist) such that x+y=z.

9. [Underwriting: Rule checking] Let P, Q, R be propositional variables. Which of the following propositional formulas corresponds to the boolean function with 3 arguments returning TRUE when its inputs represent a binary encoding of a prime number?

Ans : (˥ P ∧ Q) V (P ∧ ˥ Q) V (P ∧ Q)

10. [Claims Management] Unlike underwriting, claims management is more of a space problem than a speed problem. Suppose you have the following hash table, implemented using linear probing. For the hash function we are using the identity function modulo the length of the list, h(x) = x mod 9. In which order could NOT be the elements added to the hash table?

Ans : 9 18 12 3 4 14 21

11. [Claims Management] Given the following “character” and its corresponding frequency, draw the optimal Huffman Code tree structure. Given the data is [A : 3, B : 2, C : 5, D : 4, E : 1, F : 6]. Please draw a tree of optimal Huffman Codes and explain why it's optimal.

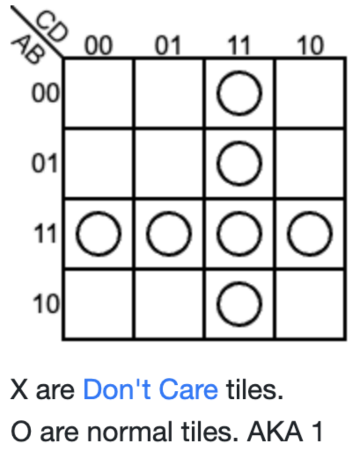
Ans :

12. [IoT system] A 16-bit von Neumann architecture has a page size of 4096 bytes and 12 KB of RAM. Access to the pages of the system happen as follows: 5,15,15,5,10. Which of the following is true?

Ans : The FIFO algorithm causes 2 page faults to be issued.

13. [IoT system] Please simplify:

Ans : AB + CD



AB\CD	00	01	11	10
00			○	
01			○	
11	○	○	○	○
10			○	

X are Don't Care tiles.
O are normal tiles. AKA 1

14. [IoT system security] Meltdown is a hardware vulnerability affecting a wide range of processors. It uses a cache timing attack to read kernel space data by observing the results of speculative operations conditioned on data fetched with invalid privileges. Which processor below is NOT affected by Meltdown?

Ans : Intel Itanium, a Very-Long-Instruction-Word processor

🚩15. [BTC's price on 2024/3/29 is $70k!] 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.

Ans : Reason 2: MSTR in NASDAQ gives investors to trade BTC with leverage (買現股自帶融資槓桿又不會被margin call)