

Assignment 1

DYOR!

1. **Read all chapters of “[21 Lessons](#)” and the [Bitcoin whitepaper](#).**
 - a. Summarize your key learnings from each chapter of “21 lessons.”
 - b. Summarize your key learnings from the Bitcoin whitepaper in your own words.
2. **Practical: Bitcoin transaction**
 - a. Obtain a Bitcoin address and send there some fractions of a Bitcoin.
 - b. Observe the transactions on the block explorer.
 - c. Also observe the mempool.

Present your observations

- d. Work and record your findings in a Google Slides presentation for your presentation in the next session.
- e. Create high-quality slides.
- f. Include references and hints for the other participants.

REMINDER: In order to participate in the program, you need to fill out this [FORM](#). We need your confirmation on this form for GDPR reasons. Please note **that you cannot participate in the program** without filling out the survey.

Assignment:1.Read all chapters of “[21 Lessons](#)” and the [Bitcoin whitepaper](#).

1a.Summarize your key learnings from each chapter of “21 lessons.”



Lesson 1 : Immutability and Change

While it's technically possible to make changes to the Bitcoin network, the process is intentionally challenging and requires a broad consensus among network participants. This design is pivotal in maintaining the network's integrity, security, and trustworthiness.

Assignment:1.Read all chapters of “[21 Lessons](#)” and the [Bitcoin whitepaper](#).

1a.Summarize your key learnings from each chapter of “21 lessons.”

Lesson 3 : Replication and Locality

The network doesn't track balances of addresses; instead, it tracks all transactions. Each transaction has inputs (which are spent UTXOs) and outputs (which create new UTXOs).

Transaction Fee=(Total Input Value)–(Total Output Value)

A **coinbase transaction** is how new bitcoins are introduced into circulation. The miner who successfully mines a block creates a **coinbase transaction** as part of the block, awarding themselves a certain number of bitcoins as a reward. This reward is composed of the block subsidy (newly created bitcoins) and transaction fees from other transactions included in the block.

Lesson 2 : The Scarcity of Scarcity

- **Genesis of Bitcoin (January 3, 2009)**
 - The reward for mining a block started at 50 bitcoins.
 - This initial reward lasted until the first halving.
- **1st Halving (November 28, 2012, at block 210,000)**
 - The mining reward halved from 50 to 25 bitcoins.
 - By this point, 50% of the total supply (10.5 million BTC) was already in circulation.
- **2nd Halving (July 9, 2016, at block 420,000)**
 - The mining reward reduced from 25 to 12.5 bitcoins.
 - A total of 75% of the Bitcoin supply (15.75 million BTC) was in circulation after this halving.
- **3rd Halving (May 11, 2020, at block 630,000)**
 - The mining reward dropped from 12.5 to 6.25 bitcoins.
 - After this event, 87.5% of the total supply (18.375 million BTC) was in circulation.
- **4th Halving (Expected in 2024, at block 840,000)**
 - The mining reward is expected to decrease from 6.25 to 3.125 bitcoins.
 - This event will see 93.75% of the total supply (19.6875 million BTC) in circulation.
- **Future Halvings**
 - Halvings will continue approximately every four years until the maximum supply of 21 million bitcoins is reached, which is expected to be around the year 2140.
 - As the reward decreases, the proportion of miner revenue from transaction fees is expected to increase.

Fixed total supply; deflation

Assignment:1.Read all chapters of “[21 Lessons](#)” and the [Bitcoin whitepaper](#).

1a.Summarize your key learnings from each chapter of “21 lessons.”

Lesson 4 : The Problem of Identity

Bitcoin taught me that decentralization contradicts identity.

Bitcoin's Split on August 1, 2017 (Bitcoin Cash Hard Fork):

- This split resulted from a disagreement within the Bitcoin community over how to scale the network. One camp wanted to increase the block size to allow more transactions per block, leading to the creation of Bitcoin Cash (BCH) with a larger block size.
- The other camp wanted to implement a different scaling solution called Segregated Witness (SegWit), which would later facilitate the development of the Lightning Network.
- The market and most of the original developers continued to support the unaltered chain (BTC), which implemented SegWit, viewing it as the original Bitcoin. This decision was likely influenced by factors such as the support of the majority of the mining power, the continuity of the existing ledger, and adherence to the original philosophical and technical vision of Bitcoin.

Assignment:1.Read all chapters of “[21 Lessons](#)” and the [Bitcoin whitepaper](#).

1a.Summarize your key learnings from each chapter of “21 lessons.”

Ethereum's Split on October 25, 2016 (Ethereum Classic Hard Fork):

- Ethereum's split was triggered by a different kind of debate, following the exploitation of a vulnerability in a smart contract known as The DAO. The debate was over whether to effectively "rollback" the blockchain to reverse the effects of the exploitation.
- The altered chain, which chose to revert the DAO hack through a hard fork, continued as [Ethereum](#) (ETH). It was supported by the majority of the community, including Ethereum's founders and most developers, who believed that taking action to reverse the hack was necessary to preserve the ecosystem's integrity and investor confidence.
- The unaltered chain, which insisted on the principle of "code is law" and the immutability of the blockchain, continued as [Ethereum](#) Classic (ETC). This camp believed that the blockchain should not be altered, regardless of the circumstances.

Assignment:1.Read all chapters of “[21 Lessons](#)” and the [Bitcoin whitepaper](#).

1a.Summarize your key learnings from each chapter of “21 lessons.”

 Lesson **5**: An Immaculate Conception

Bitcoin taught me that narratives are important

The Mysterious Founder - Satoshi Nakamoto:

Begin by discussing the enigmatic figure of Satoshi Nakamoto, the pseudonymous person or group of people who published the Bitcoin whitepaper in 2008 and released the first software in 2009. The ~~.....~~ anonymity and eventual disappearance of Nakamoto add a layer of intrigue and purity to Bitcoin's inception, as the absence of a known founder removes potential biases or ~~centralized~~ control from the equation.

Assignment:1.Read all chapters of “[21 Lessons](#)” and the [Bitcoin whitepaper](#).

1a.Summarize your key learnings from each chapter of “21 lessons.”

The Genesis Block and Its Significance:

Discuss the creation of the first block in the Bitcoin blockchain, known as the Genesis Block or Block 0. Highlight its symbolic significance, especially the embedded message in the [coinbase transaction](#) of the Genesis Block, which reads: "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks." This message is widely interpreted as a critique of the fragility of the traditional financial system and positions Bitcoin as a revolutionary alternative.



Assignment:1.Read all chapters of “[21 Lessons](#)” and the [Bitcoin whitepaper](#).

1a.Summarize your key learnings from each chapter of “21 lessons.”

🔥 Lesson [6](#) :The Power of Free Speech

“Bitcoin taught me that in a free society, free speech and free software are unstoppable.”

Not quite understand this chapter

🔥 Lesson [7](#) :The Limits of Knowledge

“Bitcoin taught me that I know very little about almost anything. It taught me that this rabbit hole is bottomless.”

Lesson7 for me is more like the feeling of the author.

🔥 Lesson [8](#) :Financial Ignorance

“Bitcoin taught me to look behind the curtain and face my financial ignorance.”

Lesson8 more like author's personal experience.

Assignment:1.Read all chapters of “[21 Lessons](#)” and the [Bitcoin whitepaper](#).

1a.Summarize your key learnings from each chapter of “21 lessons.”



“Bitcoin taught me about the hidden tax of inflation and the catastrophe of hyperinflation.”

💡 Hard Money:

- **Definition:** Hard money refers to currency that has intrinsic value or is backed by a physical commodity, typically gold or another precious metal. Historically, currencies were often based on physical commodities (like the gold standard).
 - **Characteristics:**
 - **Intrinsic Value:** Hard money has inherent value; for example, gold has value due to its rarity, industrial applications, and desirability for jewelry.
 - **Resistance to Inflation:** Hard money tends to be resistant to inflation because it's not easy to increase its supply. The supply of gold, for example, can only increase through mining, which is a slow and costly process.
 - **Historical Significance:** Historically, hard money was seen as a stable and reliable form of currency. However, most modern economies have moved away from hard money due to its limitations in expanding the money supply during economic downturns.
- **Bitcoin as Hard Money?**: Some proponents of Bitcoin argue that it shares characteristics with hard money due to its fixed supply and the cost (in terms of energy and hardware) required to mine new bitcoins. This perspective views Bitcoin as "digital gold."

💡 Soft Money:

- **Definition:** Soft money refers to currency that is not backed by a physical commodity. Instead, its value comes from the trust and confidence that individuals and institutions have in the issuing government or financial authority.
 - **Characteristics:**
 - **No Intrinsic Value:** Soft money does not have intrinsic value; its worth is derived from the stability and creditworthiness of the issuer, usually a country's government or central bank.
 - **Susceptible to Inflation:** Soft money is more susceptible to inflation because the issuing authority can decide to increase the money supply, for instance, by printing more money. This can lead to devaluation of the currency if not managed properly.
 - **Flexibility:** One advantage of soft money is that it gives governments and central banks more tools to manage the economy, such as adjusting interest rates, conducting monetary policy, and responding to financial crises.
- **Current Dominance:** Most modern economies use soft money. The value of currencies like the US dollar, the euro, or the Japanese yen is based on trust in the respective governments and the performance of their economies, not on a physical commodity.

💡 Mild Inflation is good? Should we all use bitcoin?

Assignment:1.Read all chapters of “[21 Lessons](#)” and the [Bitcoin whitepaper](#).

1a.Summarize your key learnings from each chapter of “21 lessons.”

Lesson **10** :Value

Bitcoin taught me that value is subjective but not arbitrary.

Value = Scarcity + Utility

Scarcity:

- 1** it is extremely rare (21 million)
- 2** increasingly hard to produce (reward halvening)
- 3** can't be replaced (a lost private key is lost forever)

Utility:

- 1** It is arguably the best tool for value transfer across borders virtually resistant to censorship and confiscation in the process
- 3** it is a self-sovereign store of value, allowing individuals to store their wealth independent of banks and governments

Assignment:1.Read all chapters of “[21 Lessons](#)” and the [Bitcoin whitepaper](#).

1a.Summarize your key learnings from each chapter of “21 lessons.”

 Lesson   :Money

Bitcoin taught me what money is.

This Lesson more like a preparation of next few lessons, mention about what's money? History of money Disadvantage of nowadays money. Sound money.

Assignment:1.Read all chapters of “[21 Lessons](#)” and the [Bitcoin whitepaper](#).

1a.Summarize your key learnings from each chapter of “21 lessons.”

🔥 Lesson [1](#) [2](#):The History and Downfall of Money

“Bitcoin taught me about the history of money and the greatest sleight of hand in the history of economics: fiat currency”

I partially agree.

📍 Commodity money:

- 1 One of the downsides of using precious metal coins is that they can be clipped
- 2 They are bulky and not very convenient to transport

📍 Representative money:

The introduction of representative money heralded the downfall of hard money

📍 Fiat money

gold and silver were used as money for millennia. Over time, coins made from gold and silver were replaced by paper. Paper slowly became accepted as payment. This acceptance created an illusion — the illusion that the paper itself has value. The final move was to completely sever the link between the representation and the actual: abolishing the gold standard and convincing everyone that the paper in itself is precious.

Assignment:1.Read all chapters of “[21 Lessons](#)” and the [Bitcoin whitepaper](#).

1a.Summarize your key learnings from each chapter of “21 lessons.”

🔥 Lesson [1](#) [3](#) : Fractional Reserve Insanity

“Bitcoin taught me that fractional reserve banking is pure insanity.”

Actually I don't see any problems with Fractional Reserve has doing anything wrong here.

🔥 Lesson [1](#) [4](#) :Sound Money

“Bitcoin taught me that sound money is essential.”

Stock-to-flow ratio

Bitcoin's difficulty ~~adjsutment~~

🔥 Lesson [1](#) [5](#) : Strength in Numbers

“Bitcoin taught me that there is strength in numbers.”

SHA-256

Assignment:1.Read all chapters of “[21 Lessons](#)” and the [Bitcoin whitepaper](#).

1a.Summarize your key learnings from each chapter of “21 lessons.”



Lesson **1** **6** :Reflections on “Don’t Trust, Verify”

“Bitcoin taught me not to trust, but to verify.”

Chain-of-trust

Dive into how Bitcoin introduces a system where trust is replaced by cryptographic verification. Explain how the blockchain's transparency allows anyone to verify transactions, how mining ensures the integrity and chronological order of the blockchain, and how users can have full control over their funds without needing to trust a third party.

Assignment:1.Read all chapters of “[21 Lessons](#)” and the [Bitcoin whitepaper](#).

1a.Summarize your key learnings from each chapter of “21 lessons.”

Lesson 1 7 :Telling Time Takes Work

“Bitcoin taught me that telling the time is tricky, especially if you are decentralized.”

Mining as a Timestamp Mechanism:

- One of the primary functions of mining, as outlined in the [Bitcoin whitepaper](#), is to act as a distributed timestamp server. Each block in the blockchain contains a timestamp, a reference to the previous block (hence creating a chain), and a record of some or all recent transactions.

Assignment:1.Read all chapters of “[21 Lessons](#)” and the [Bitcoin whitepaper](#).

1a.Summarize your key learnings from each chapter of “21 lessons.”

 Lesson 1 8:Move Slowly and Don't Break Things

“Bitcoin taught me that moving slowly is one of its features, not a bug.”

This lesson mainly talking about decentralisation of bitcoin which make it moving slowly.

 Lesson 1 9:Privacy is Not Dead

“Bitcoin taught me that privacy is not dead.”

This lesson mainly about Satoshi successfully hide himself.

 Lesson 2 0:Cypherpunks Write Code

Bitcoin taught me that cypherpunks write code.

It seems like advocate the spirit of cypherpunks.

 Lesson 2 1:Metaphors for Bitcoin's Future

“Bitcoin taught me that understanding the past is essential to understanding its future. A future which is just beginning...”

Using metaphor like electricity and internet, later bitcoin will be taken as granted.

Assignment:1.Read all chapters of “[21 Lessons](#)” and the [Bitcoin whitepaper](#).

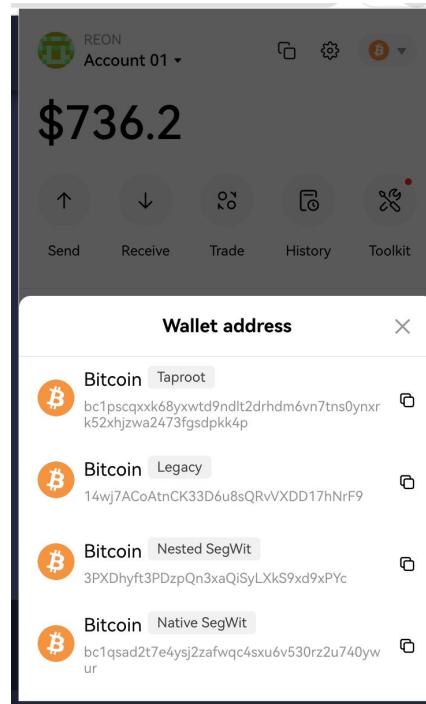
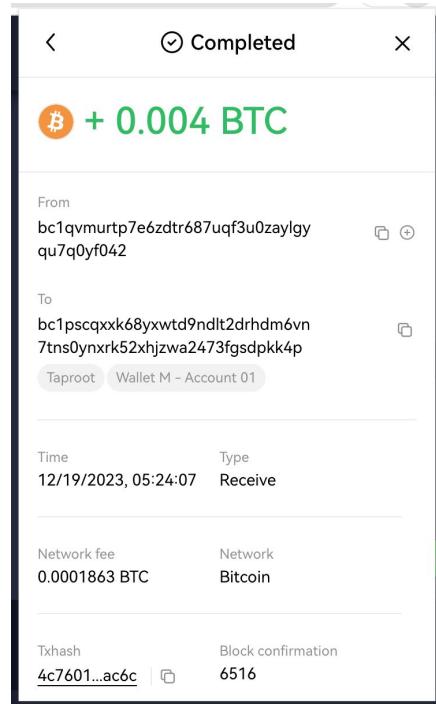
1b.Summarize your key learnings from the Bitcoin whitepaper in your own words.

I read the white paper, it seem like not much excite me.

Bitcoin, ~~blockchian~~, decentralised,50%

Assignment 2.Practical: Bitcoin transaction

2a. Obtain a Bitcoin address and send there some fractions of a Bitcoin.



Assignment 2.Practical: Bitcoin transaction

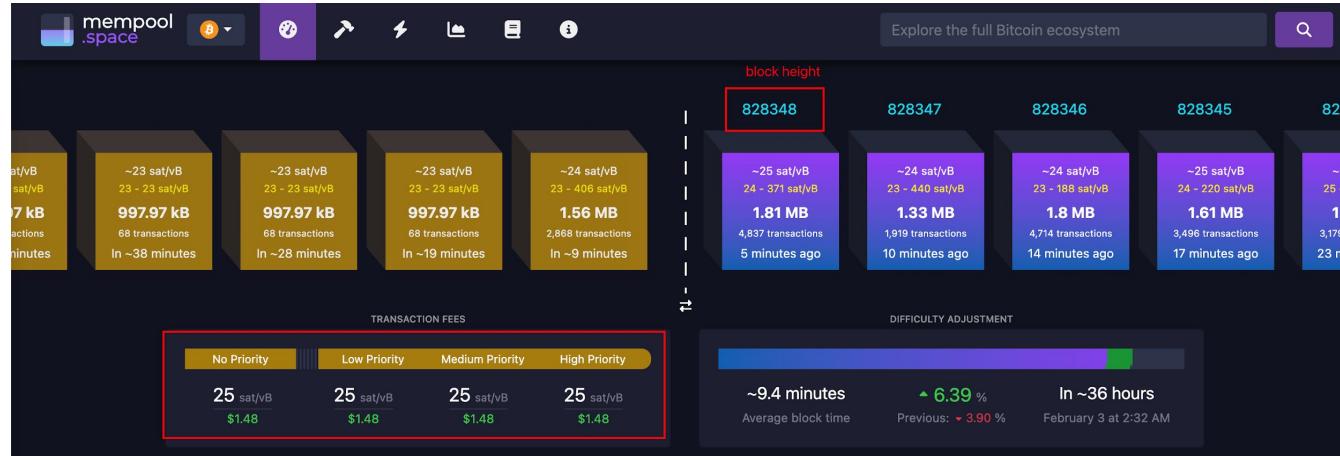
2b.Observe the transactions on the block explorer.

Transaction details

Txn hash: 4c7601d2a7865724d06e9eca2ed2e3bc06e32bc124b911e6c9d31ee04bbbac6c 🔗			
Block height	821829	Fee rate	121.79 sat/vB
Confirmations	6,518	Txn fee	0.00018634 BTC
Timestamp	12/19/2023, 05:24:07	Weight	609
Size	234 bytes	Input amount	0.00447141 BTC
Virtual size	153 bytes	Output amount	0.00428507 BTC
BTC transfers			
Input (1) ◀ bc1qvmurtp7e6zdtr687uqf3u0zaylgqu7q0yf042 payer's UTXO	0.00447141 BTC (\$189.64)	Output (2) payee's UTXO bc1pscqxxk68yxwtd9ndlt2drhdm6vr7tns0ynxrk52xhjzwa2473fgs... payer's new UTXO	0.00428507 BTC (\$181.74) 0.004 ► 0.00028507 Confirmed 6518
Input - Output = transcation fee -> 0.00447141 - 0.00428507 = 0.00018634			

Assignment 2.Practical: Bitcoin transaction

2c. Also observe the mempool.



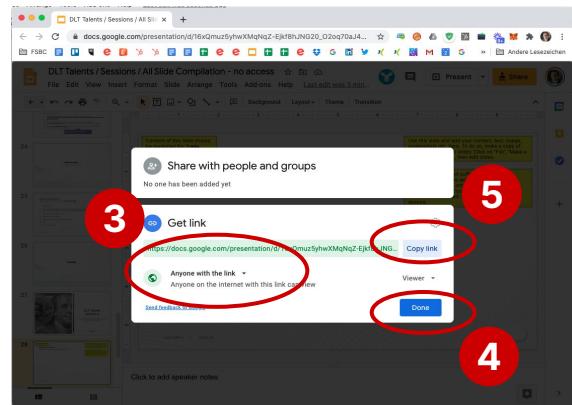
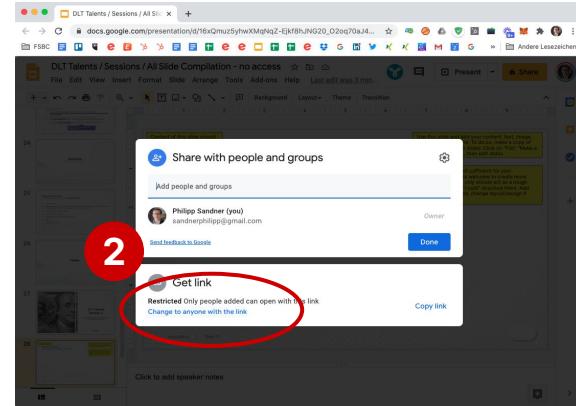
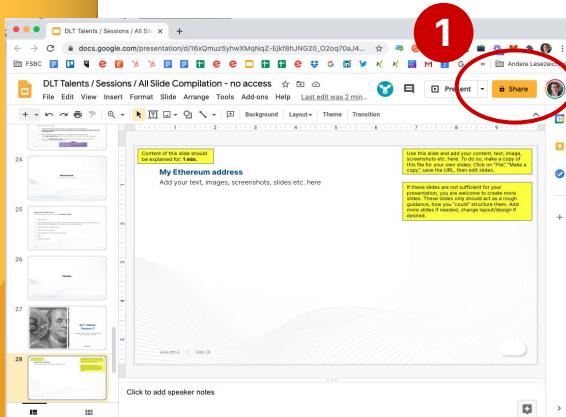
Submit Assignment



<https://forms.gle/iRNjCf8TCHi8My7v5>

How can you share a Google Slides presentation?

With a few click within Google Slides you can generate an internet link so that others can view your slides. You can also allow or prevent editing as you wish.





Bitcoin Talents

Next: Session 2

February 7, 2024

Supported by

