Assignment 2

DYOR!

1.Update Profile Slide Information **(Deadline: Friday, February 23, 2024, 12:00 PM [CET/CEST])**

2.Bitcoin technical deep dive

Get a copy of “Mastering Bitcoin, 2nd Edition” by Andreas Antonopoulos for reference.

Free (non-.pdf version) at https://github.com/bitcoinbook/bitcoinbook. At least cursory read chapters 4 & 5.

a. Describe the steps to create a public (legacy) address, from private key to Base58 address type.
b. What other address types are there? Create a short description for each.
c. What is a HD wallet? What advantage does it have over non-deterministic wallets?
d. What information is contained in the Block header?
e. What is the current difficulty (Block 828904)? How many hashes does it take to mine a block?

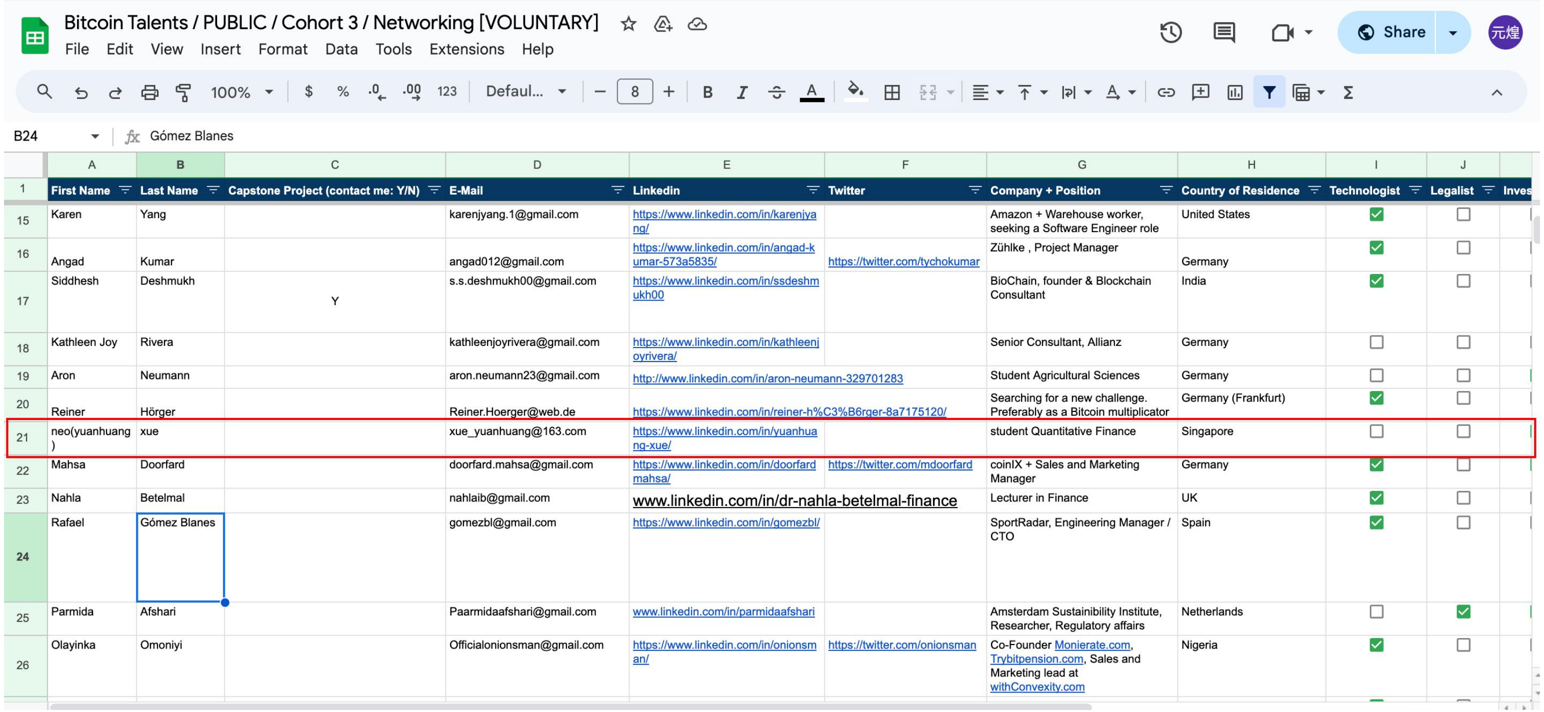
3.Energy consumption and CO2 footprint

a. Research the current and historical power consumption of Bitcoin.
b. What are possible ways to reduce the CO2 footprint?

4.Practical: Connect with other Talents on Twitter, join the #twitter slack channel, follow the Bitcoin Talents Twitter list, participate in a Twitter Space. You can also introduce yourself to the whole cohort using **THIS TABLE**.

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.Update Profile Slide Information (Deadline: Friday, February 23, 2024, 12:00 PM [CET/CEST])



	First Name	Last Name	Capstone Project (contact me: Y/N)	E-Mail	Linkedin	Twitter	Company + Position	Country of Residence	Technologist	Legalist	Inves
15	Karen	Yang		karenjyang.1@gmail.com	https://www.linkedin.com/in/karenjyang/		Amazon + Warehouse worker, seeking a Software Engineer role	United States	☑	☐	
16	Angad	Kumar		angad012@gmail.com	https://www.linkedin.com/in/angad-kumar-573a5835/	https://twitter.com/tychokumar	Zühlke , Project Manager	Germany	☑	☐	
17	Siddhesh	Deshmukh	Y	s.s.deshmukh00@gmail.com	https://www.linkedin.com/in/ssdeshmukh00		BioChain, founder & Blockchain Consultant	India	☑	☐	
18	Kathleen Joy	Rivera		kathleenjoyrivera@gmail.com	https://www.linkedin.com/in/kathleenjoyrivera/		Senior Consultant, Allianz	Germany	☐	☐	
19	Aron	Neumann		aron.neumann23@gmail.com	http://www.linkedin.com/in/aron-neumann-329701283		Student Agricultural Sciences	Germany	☐	☐	
20	Reiner	Hörger		Reiner.Hoerger@web.de	https://www.linkedin.com/in/reiner-h%C3%B6rger-8a7175120/		Searching for a new challenge. Preferably as a Bitcoin multiplicator	Germany (Frankfurt)	☑	☐	
21	neo(yuanhuang)	xue		xue_yuanhuang@163.com	https://www.linkedin.com/in/yuanhuang-xue/		student Quantitative Finance	Singapore	☐	☐	
22	Mahsa	Doorfard		doorfard.mahsa@gmail.com	https://www.linkedin.com/in/doorfardmahsa/	https://twitter.com/mdoorfard	coinIX + Sales and Marketing Manager	Germany	☑	☐	
23	Nahla	Betelmal		nahlaib@gmail.com	www.linkedin.com/in/dr-nahla-betelmal-finance		Lecturer in Finance	UK	☑	☐	
24	Rafael	Gómez Blanes		gomezbl@gmail.com	https://www.linkedin.com/in/gomezbl/		SportRadar, Engineering Manager / CTO	Spain	☑	☐	
25	Parmida	Afshari		Paarmidaafshari@gmail.com	www.linkedin.com/in/parmidaafshari		Amsterdam Sustainibility Institute, Researcher, Regulatory affairs	Netherlands	☐	☑	
26	Olayinka	Omoniyi		Officialonionsman@gmail.com	https://www.linkedin.com/in/onionsman/	https://twitter.com/onionsman	Co-Founder Monierate.com, Trybitpension.com, Sales and Marketing lead at withConvexity.com	Nigeria	☑	☐	

Assignment:2.Bitcoin technical deep dive

2a.Describe the steps to create a public (legacy) address, from private key to Base58 address type.

How to get public key from private key:

The public key is calculated from the private key using elliptic curve multiplication, which is irreversible: K = k × G, where k is the private key, G is a constant point called the generator point, and K is the resulting public key.

Public key K is defined as a point K = (x, y)

Example:

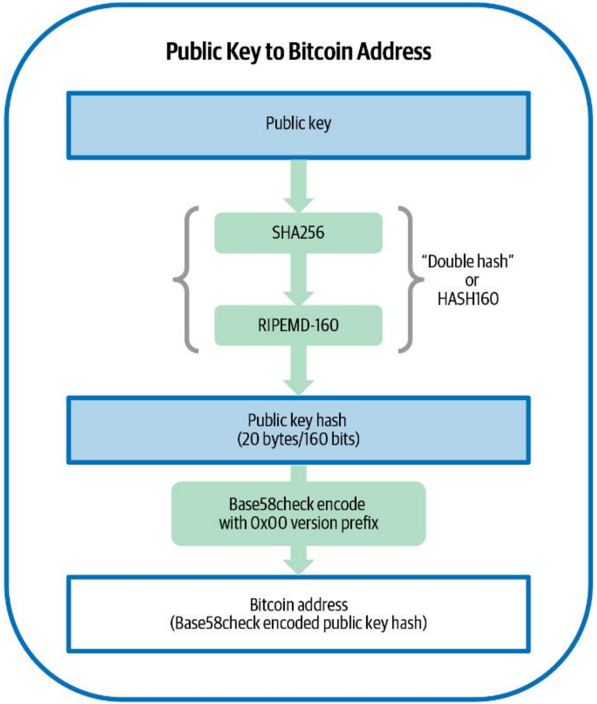
K = 1E99423A4ED27608A15A2616A2B0E9E52CED330AC530EDCC32C8FFC6A526AEDD

x = F028892BAD7ED57D2FB57BF33081D5CFCF6F9ED3D3D7F159C2E2FFF579DC341A

y = 07CF33DA18BD734C600B96A72BBC4749D5141C90EC8AC328AE52DDFE2E505BDB

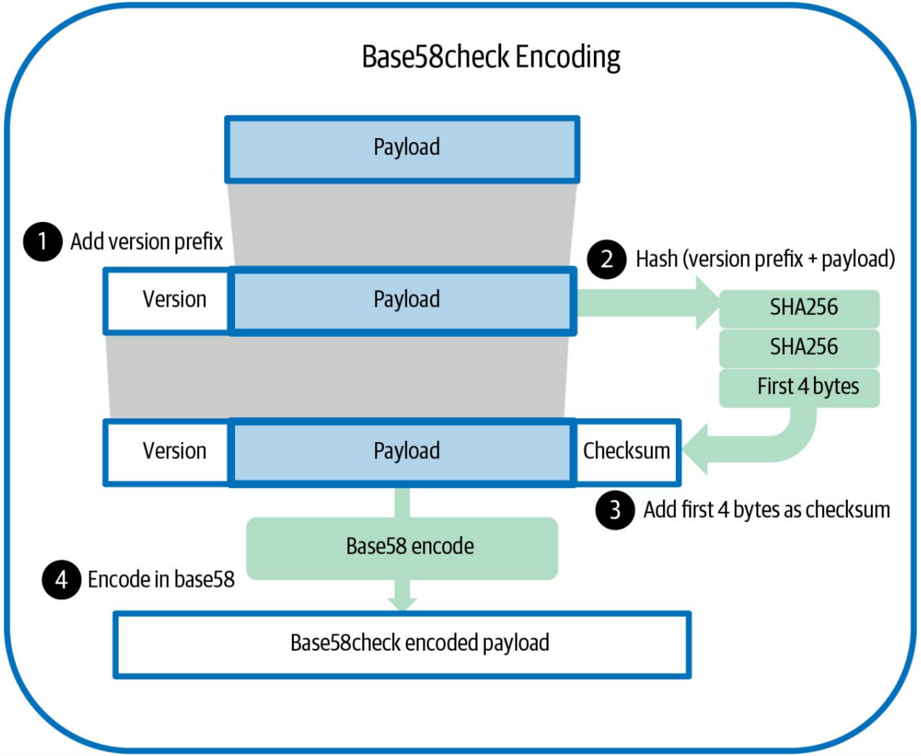
Assignment:2.Bitcoin technical deep dive

2a.Describe the steps to create a public (legacy) address, from private key to Base58 address type.



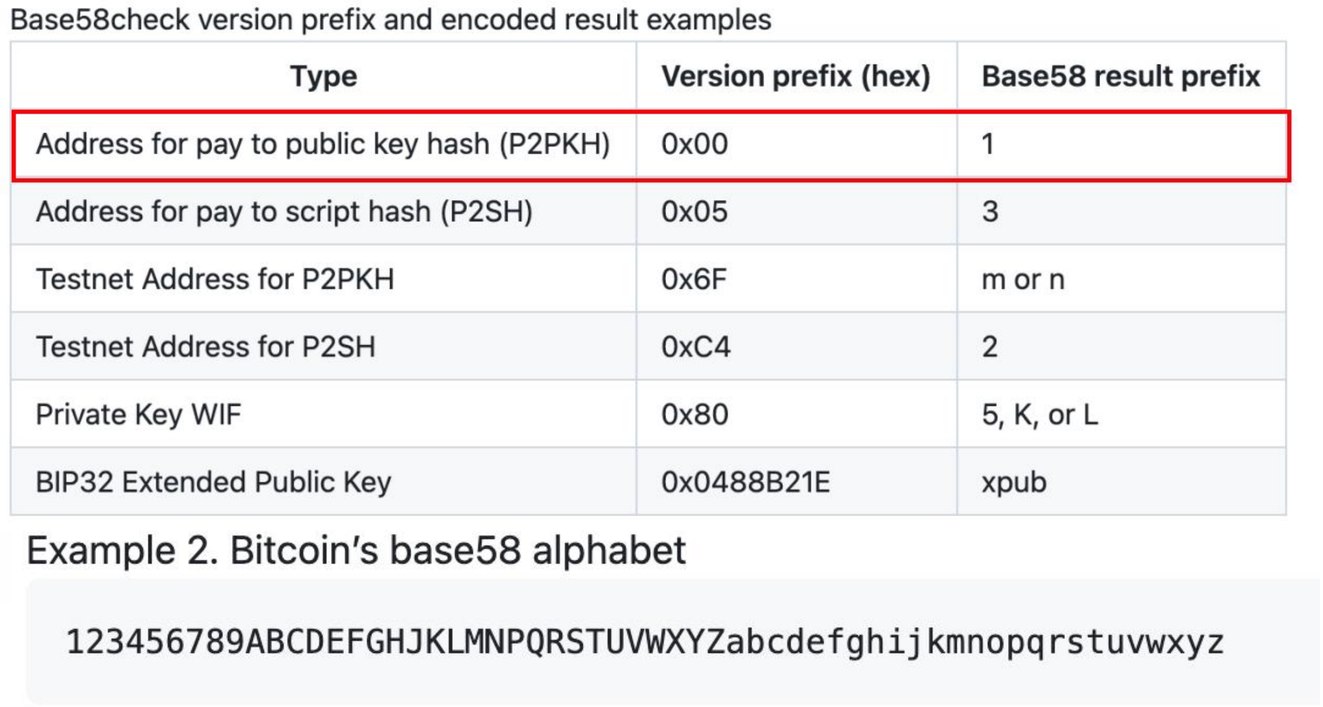
Assignment:2.Bitcoin technical deep dive

2a.Describe the steps to create a public (legacy) address, from private key to Base58 address type.



Assignment:2.Bitcoin technical deep dive

2a.Describe the steps to create a public (legacy) address, from private key to Base58 address type.



Base58check version prefix and encoded result examples

Type	Version prefix (hex)	Base58 result prefix
Address for pay to public key hash (P2PKH)	0x00	1
Address for pay to script hash (P2SH)	0x05	3
Testnet Address for P2PKH	0x6F	m or n
Testnet Address for P2SH	0xC4	2
Private Key WIF	0x80	5, K, or L
BIP32 Extended Public Key	0x0488B21E	xpub

Example 2. Bitcoin’s base58 alphabet

```
123456789ABCDEFGHJKLMNPQRSTUVWXYZabcdefghijkmnopqrstuvwxyz
```

Assignment:2.Bitcoin technical deep dive

2b.What other address types are there? Create a short description for each.

P2PK:using ip address to pay, every time given different public key, so transcations will not being connected.

P2PKH:using hash function RIPEMD160(SHA256(K)) to shorter public key from 65 bytes to 20 bytes.

Besh32:Bech32 uses only numbers and a single case of letters (preferably rendered in lowercase)

Bech32m:The version of bech32 with a single different constant is known as bech32 modified (bech32m)

Assignment:2.Bitcoin technical deep dive

2c.What is a HD wallet? What advantage does it have over non-deterministic wallets?

HD wallet:A tree of keys generated from a single seed

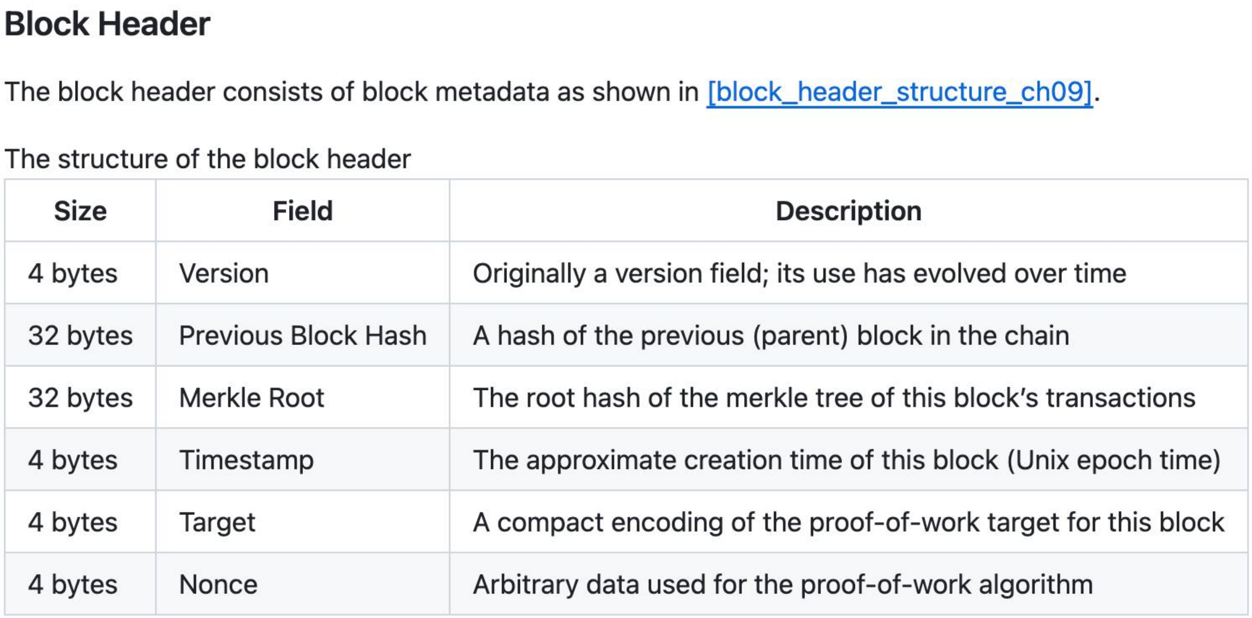
Disadvantage:

1.it required users to back up the wallet database each time they generated and distributed new keys, which could be as often as each time they generated a new address to receive a new payment. Failure to back up the wallet database on time would lead to the user losing access to any funds received to keys that had not been backed up.

2.For each independently generated key, the user would need to back up about 32 bytes, plus overhead.

Assignment:2.Bitcoin technical deep dive

2d.What information is contained in the Block header?



Block Header

The block header consists of block metadata as shown in [block_header_structure_ch09].

The structure of the block header

Size	Field	Description
4 bytes	Version	Originally a version field; its use has evolved over time
32 bytes	Previous Block Hash	A hash of the previous (parent) block in the chain
32 bytes	Merkle Root	The root hash of the merkle tree of this block’s transactions
4 bytes	Timestamp	The approximate creation time of this block (Unix epoch time)
4 bytes	Target	A compact encoding of the proof-of-work target for this block
4 bytes	Nonce	Arbitrary data used for the proof-of-work algorithm

Assignment:2.Bitcoin technical deep dive

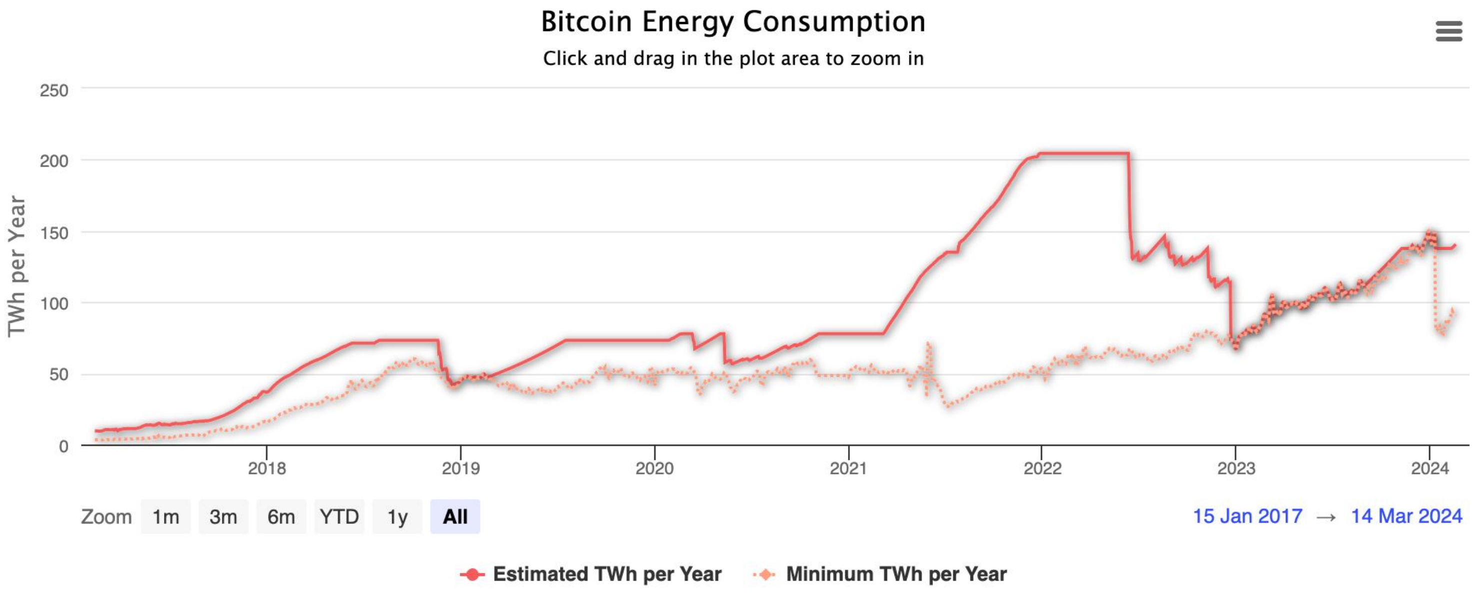
2e.What is the current difficulty (Block 828904)? How many hashes does it take to mine a block?

200.32T

200.32 trillion

Assignment:3.Energy consumption and CO2 footprint

One TWh is enough to continuously power about 114,000 average American homes for an entire year.



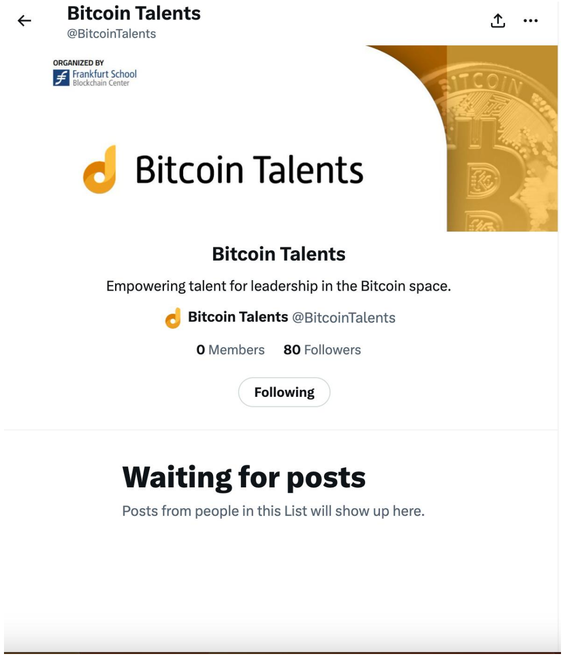
Assignment:3.Energy consumption and CO2 footprint

3b.What are possible ways to reduce the CO2 footprint?

Mining Process Reforms: Changing the fundamental approach to Bitcoin mining, like shifting from "proof of work" to "proof of stake", could significantly reduce energy consumption. This method would eliminate the need for miners to solve complex calculations, instead of allowing the system to validate transactions based on the stake of network participants.

However, I don’t think POS is a good way.

Assignment:4.Practical: Connect with other Talents on Twitter, join the #twitter slack channel, follow the Bitcoin Talents Twitter list, participate in a Twitter Space. You can also introduce yourself to the whole cohort using THIS TABLE.



Bitcoin Talents
@BitcoinTalents

Bitcoin Talents

Empowering talent for leadership in the Bitcoin space.

Bitcoin Talents @BitcoinTalents

0 Members 80 Followers

Waiting for posts

Posts from people in this List will show up here.

Submit Assignment

https://forms.gle/iRNjCf8TCHi8My7v5

You can use the Content Questionnaire to submit content, e.g., articles, studies, projects relevant to Bitcoin (needs to have relevant Bitcoin insights/content)