ORGANIZED BY

Frankfurt School
Blockchain Center

Follow us on

Bitcoin Talents

Sid Jain | Session 2 | Assignment 2

February 19, 2025

Mastering Bitcoin, 2nd Edition by Andreas Antonopoulos

Steps to create a Legacy Bitcoin Address

1) **Generate a Private Key** - a randomly generated 256-bit number
   Example: *18e14a7b6a307f426a94f8114701e7c8e774e7f9a47e2c2035db29a206321725*
2) **Generate a Public Key** - Elliptic Curve Digital Signature Algorithm (ECDSA) with the secp256k1 curve to derive the public key from the private key. The public key is typically compressed or uncompressed
3) **Hash the Public Key** - SHA256(Public Key) and RIPEMD160(SHA256(Public Key))
   Result: Public Key Hash (20 bytes)
4) **Add the Version Byte** - a version byte to indicate the network and address type, for Legacy P2PKH addresses on mainnet, use ‘0x00’
   Example for mainnet: 00 + Public Key Hash
5) **Compute the checksum** - 1) Perform double SHA-256 hashing on the extended hash (version byte + public key hash) - SHA256(SHA256(Version Byte Public Key Hash)), 2) first 4 bytes of this result as the checksum
6) **Create the Binary Bitcoin Address** - Concatenate the version byte, public key hash, and checksum (Version Byte)+(Public Key Hash)+(Checksum)
7) **Encode in Base58Check** - 1) Convert the binary Bitcoin address into Base58Check format for human readability. 2) Leading zero bytes in binary are encoded as "1" in Base58.
   Result: Base58Check string is the legacy Bitcoin address, starting with "1" for mainnet P2PKH addresses.
   1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa

Other Bitcoin Address Types

1) **Pay-to-Script-Hash Address (P2SH)**

   Prefix: Starts with 3.

   Description: Encodes a script hash instead of a public key hash, enabling advanced features like multi-signature wallets and SegWit compatibility.

   Characteristics: Allows more complex spending conditions while maintaining backward compatibility with older wallets.

   Example: 3J98t1WpEZ73CNmQviecrnyiWrnqRhWNLy.

2) **Bech32 Address (Native SegWit - P2WPKH/P2WSH**

   Prefix: Starts with bc1.

   Description: A newer address format introduced with SegWit (Segregated Witness). It directly encodes witness data in a more efficient format.

   Characteristics: Reduces transaction size and fees, improves scalability, and eliminates ambiguity in character encoding. However, it may not be supported by some older wallets or exchanges.

   Example: bc1qar0srrr7xfkvy5l643lydnw9re59gtzzwf5mdq.

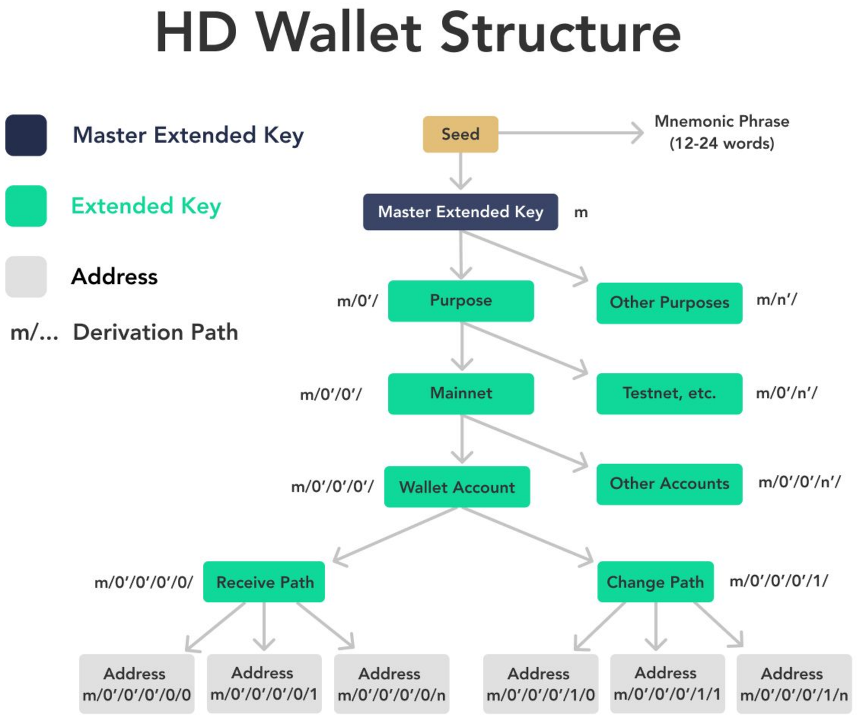
Other Bitcoin Address Types

3) Taproot Address (P2TR) -
Prefix: Starts with bc1p.
Description: The most advanced address type, introduced with Bitcoin's Taproot upgrade in 2021.
Characteristics: Enhances privacy, scalability, and flexibility by enabling Schnorr signatures and more complex scripting capabilities. Not all platforms support it yet.
Example: bc1puaz84y65g0jh7zlhwv9vwhuu3se8ldf82lk5ca6zru6kdny2zvws69x6jd

HD wallets

HD wallets as defined in BIP 32 (Bitcoin Improvement Proposal 32) are cryptocurrency wallets that generate a hierarchical tree-like structure of private/public key pairs from a single master seed.

The "hierarchical" aspect refers to the ability to organize keys into a tree structure, while "deterministic" means that the same keys are generated in the same way each time.



https://river.com/learn/terms/h/hd-wallet/

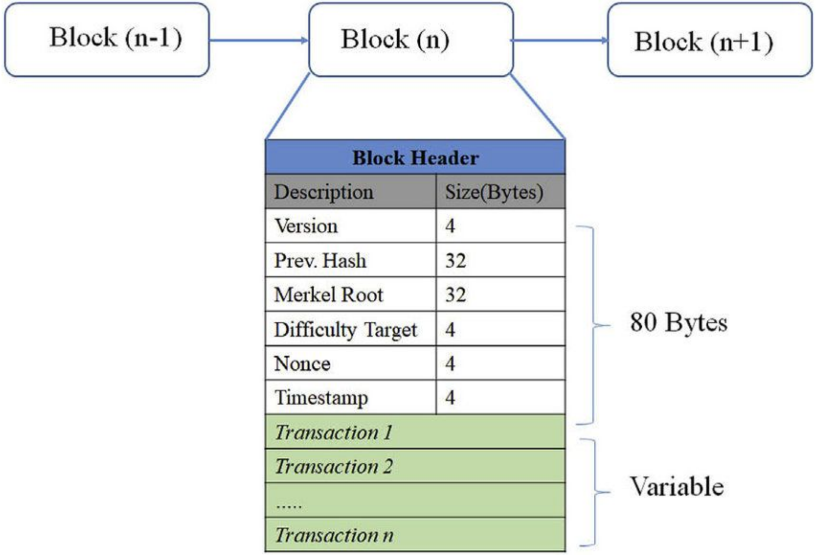
Advantages of HD Wallets over non-deterministic wallets

1. **Simplified Backup and Recovery**
   Only the master seed needs to be backed up, rather than individual private keys.
   The entire wallet can be restored from this single seed phrase.
2. **Enhanced Privacy**
   HD wallets can generate a new public address for each transaction, making it harder to link multiple transactions to a single user.
3. **Improved Key Management**
   The hierarchical structure allows for logical organization of keys, such as different branches for various purposes or departments within an organization.
4. **Public Key Generation Without Private Keys**
   Users can create a sequence of public keys without access to the corresponding private keys.
   This feature enables the use of HD wallets on insecure servers or in receive-only scenarios, enhancing security.
5. **Simplified Multi-Account Management**
   Multiple accounts can be managed from a single interface, with the ability to track balances across the entire hierarchy.
6. **Interoperability**
   The standardized approach allows for easier migration between different wallet implementations that support the HD wallet standard.

Block Header

Information inside Block Header

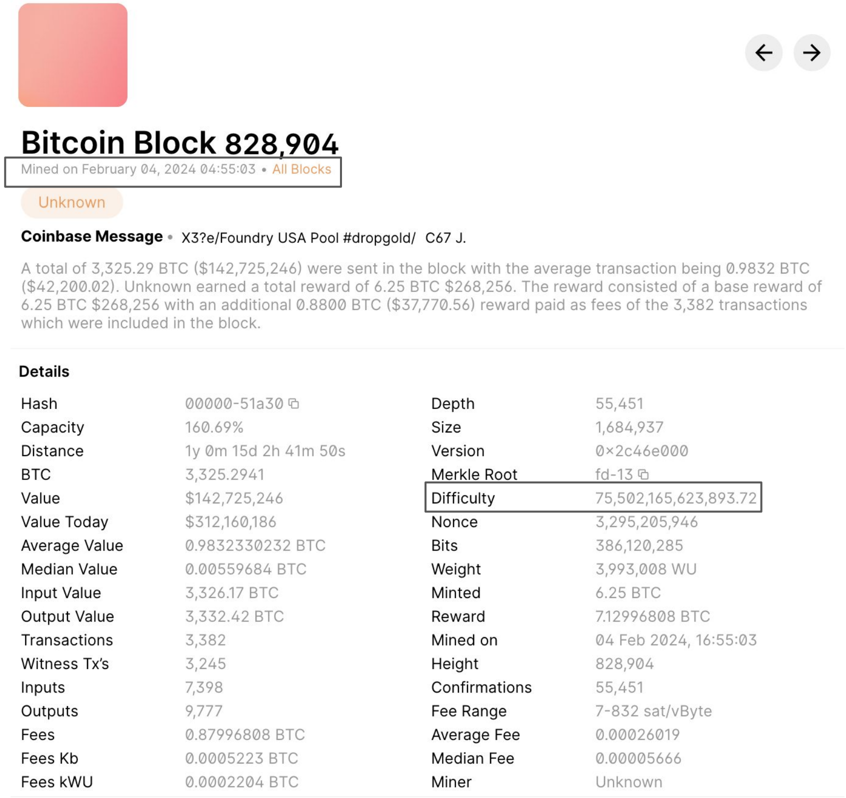
1. **Version:** A 4-byte field indicating the block version number, which helps track changes in the Bitcoin protocol.
2. **Previous Block Hash:** A 32-byte hash of the previous block's header, linking this block to the blockchain.
3. **Merkle Root:** A 32-byte hash representing the root of the Merkle tree of all transactions in the block.
4. **Timestamp:** A 4-byte field showing when the block was mined, recorded in seconds since the Unix epoch.
5. **Difficulty Target:** A 4-byte field (also known as "Bits") that indicates the mining difficulty for the block.
6. **Nonce:** A 4-byte field that miners adjust to find a valid block hash, used in the Proof of Work process.



Block Header	
Description	Size(Bytes)
Version	4
Prev. Hash	32
Merkel Root	32
Difficulty Target	4
Nonce	4
Timestamp	4
Transaction 1	
Transaction 2	
.....	
Transaction n	

https://www.researchgate.net/publication/332692835_A_new-type_of_blockchain_for_secure_message_exchange_in_VANET

Information inside Block Header



Bitcoin Block 828,904

Mined on February 04, 2024 04:55:03 • All Blocks

Unknown

Coinbase Message • X3?e/Foundry USA Pool #dropgold/ C67 J.

A total of 3,325.29 BTC ($142,725,246) were sent in the block with the average transaction being 0.9832 BTC ($42,200.02). Unknown earned a total reward of 6.25 BTC $268,256. The reward consisted of a base reward of 6.25 BTC $268,256 with an additional 0.8800 BTC ($37,770.56) reward paid as fees of the 3,382 transactions which were included in the block.

Details

Hash	00000-51a30	Depth	55,451
Capacity	160.69%	Size	1,684,937
Distance	1y 0m 15d 2h 41m 50s	Version	0×2c46e000
BTC	3,325.2941	Merkle Root	fd-13
Value	$142,725,246	Difficulty	75,502,165,623,893.72
Value Today	$312,160,186	Nonce	3,295,205,946
Average Value	0.9832330232 BTC	Bits	386,120,285
Median Value	0.00559684 BTC	Weight	3,993,008 WU
Input Value	3,326.17 BTC	Minted	6.25 BTC
Output Value	3,332.42 BTC	Reward	7.12996808 BTC
Transactions	3,382	Mined on	04 Feb 2024, 16:55:03
Witness Tx's	3,245	Height	828,904
Inputs	7,398	Confirmations	55,451
Outputs	9,777	Fee Range	7-832 sat/vByte
Fees	0.87996808 BTC	Average Fee	0.00026019
Fees Kb	0.0005223 BTC	Median Fee	0.00005666
Fees kWU	0.0002204 BTC	Miner	Unknown

https://www.blockchain.com/explorer/blocks/btc/828904

Current Difficulty: at Block 884,356
114.17 T

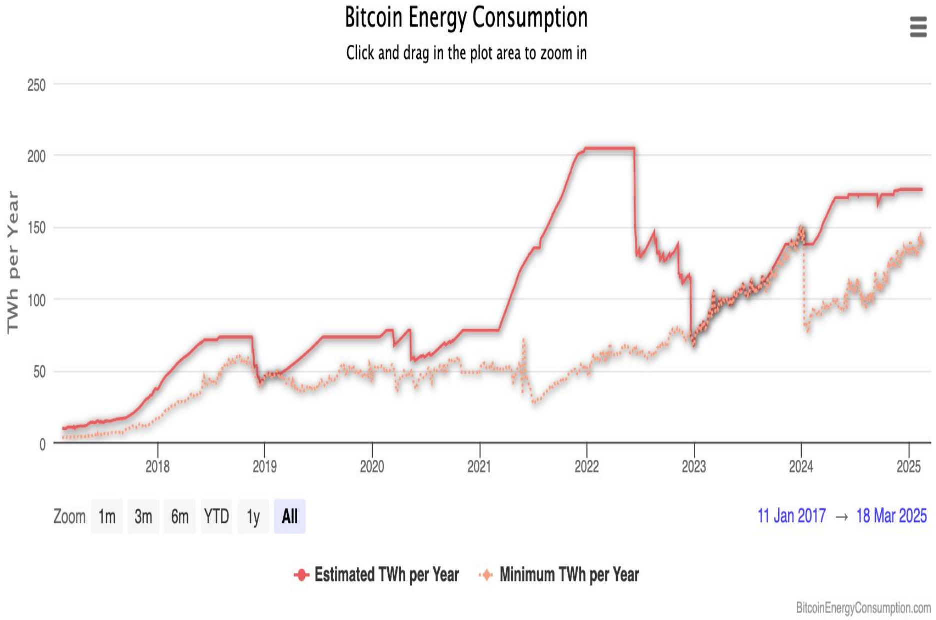
How many hashes does it take to mine a block? (https://bitcoin.stackexchange.com/questions/4565/calculating-average-number-of-hashes-tried-before-hitting-a-valid-block)

Number of hashes ≈ Difficulty * 2^32

14.17 trillion (114.17 * 10^12), it takes approximately 490,356,416,184,320,000,000,000 hashes on average to mine a single Bitcoin block. This is equivalent to about **490 quintillion (4.9 x 10^20) hashes.**

Energy consumption and CO2 footprint

Current and historical power consumption of Bitcoin.



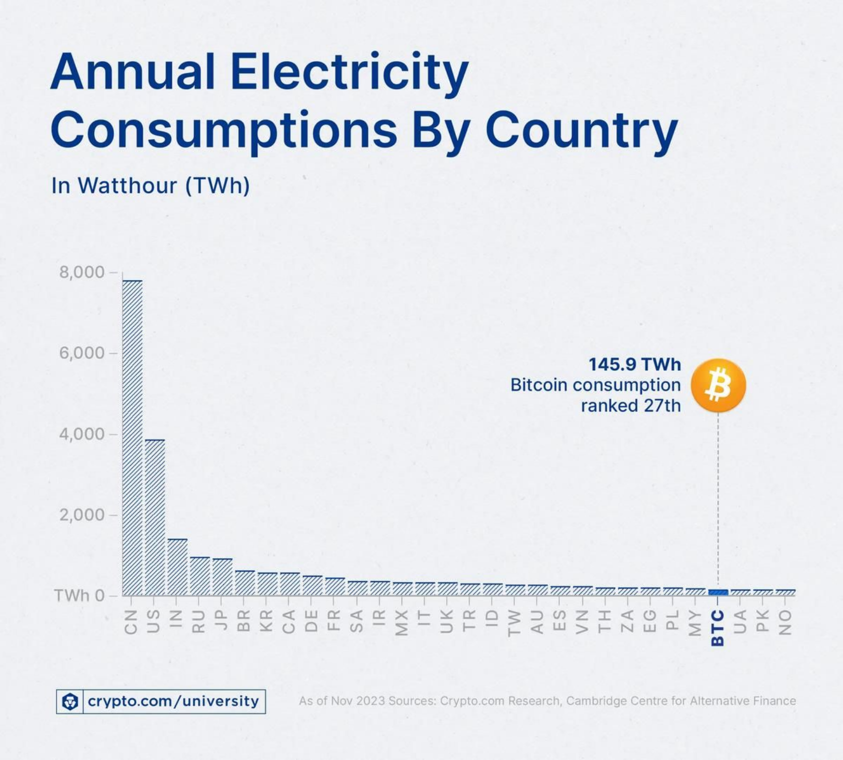
As of February 2025, Bitcoin's annual electricity consumption is estimated to be around 160 terawatt-hours (TWh), which represents approximately 0.5% of global energy consumption.

The Bitcoin Energy Consumption Index peaked at 1,312.07 MWh per BTC mined in February 2025

https://www.ainvest.com/news/bitcoin-energy-consumption-plummets-global-mining-boom-2502/

https://digiconomist.net/bitcoin-energy-consumption

Current and historical power consumption of Bitcoin.



Annual Electricity Consumptions By Country

In Watthour (TWh)

145.9 TWh
Bitcoin consumption
ranked 27th

As of Nov 2023 Sources: Crypto.com Research, Cambridge Centre for Alternative Finance

https://crypto.com/bitcoin/bitcoin-energy-consumption

Possible ways to reduce the CO2 footprint

1. **Transition to Renewable Energy Sources**
   Encourage mining operations to use solar, wind, and hydroelectric power.
   As of 2024, over 50% of Bitcoin's energy mix is already coming from renewables.
2. **Improve Energy Efficiency**
   Upgrade to more energy-efficient ASIC (Application-Specific Integrated Circuit) mining rigs.
   Optimize cooling systems for mining hardware.
3. **Grid Stabilization and Energy Waste Reduction**
   Locate mining operations near renewable energy sources to reduce transmission costs.
   Use excess capacity during off-peak times to help stabilize energy grids.
   Consume excess renewable energy that would otherwise be curtailed.
4. **Carbon Offsetting**
   Implement carbon credit systems and sequestration methods to offset emissions.
   Use carbon offsets to make Bitcoin mining carbon neutral.
5. **Utilize Stranded Energy Sources**
   Use vented methane from oil production to power mining operations, reducing overall greenhouse gas emissions.
6. **Regulatory Measures**
   Implement policies that incentivize the use of renewable energy for mining operations.

References

1. https://www.forbes.com/sites/digital-assets/2024/09/09/new-research-shows-bitcoin-mining-cuts-carbon-emissions/
2. https://www.summit.io/blog-posts/reducing-the-carbon-footprint-of-bitcoin-mining
3. https://carboncredits.com/the-energy-debate-how-bitcoin-mining-blockchain-and-cryptocurrency-shape-our-carbon-future/
4. https://www.baltictimes.com/environmental_impact_of_cryptocurrency_mining_and_sustainable_solutions/
5. https://river.com/learn/terms/h/hd-wallet/
6. https://www.researchgate.net/publication/332692835_A_new-type_of_blockchain_for_secure_message_exchange_in_VANET
7. https://www.ainvest.com/news/bitcoin-energy-consumption-plummets-global-mining-boom-2502/
8. https://bitcoin.stackexchange.com/questions/4565/calculating-average-number-of-hashes-tried-before-hitting-a-valid-block
9. https://crypto.com/bitcoin/bitcoin-energy-consumption