Lalita Sharkey
01063704

CS 764/864: Blockchains and Cryptocurrencies: Fundamentals, Technologies, and Economics

Spring 2020

Module 9: Homework 8

Q1. [5 points] If two data miners have identical transaction pool, they have identical computing resources, will they come up with identical hashes, in identical times? Please look at different scenarios and explain. This is not a one line answer.

In my opinion, I do not think that two miners can have the same hash values even if they both have the identical transaction pool and computing resources. Especially when consider bitcoin nature. The first transaction in a block is called the "generation" or "coinbase" transaction. It has no real inputs and spends no coins. Instead, it pays out the subsidy and fees to the miner that generated the block. I believe any two miners will have a different address they want their payout to. Therefore, their coinbase transactions will be different. According to my understanding, if the coinbase transactions are different, the Merkle trees will be different too. The purpose of mining is ordering transactions, to choose one of multiple valid transactions that spend the same coins. However, miners are incentivized to only include valid transactions, because if they didn't, the network wouldn't accept their blocks. However, there is no guarantee that even ignoring the coinbase transaction, two miners are going to be working on the exact same set of transactions. In fact, if we had technology to guarantee that, we wouldn't need a blockchain or mining at all.

Q2. [5 points] Pick any one online wallet for bitcoins and describe its features. In particular, explain how it stores the information, what it stores, how it facilitates transacting with bitcoins for purchases, etc. Make sure to state the URLs where you found the information.

Coin Space Wallet

URLs https://coin.space/?network=bitcoin and https://github.com/CoinSpace/CoinSpace

1. Privacy

   According their website, Coin Space coins are encrypted on the device using AES-256 encryption. Coin enforces a BIP 39 passphrase encryption on wallet creation, hardening the security of user's wallet right out of the gate. Private keys are created and stored on the user device and are never communicated with any server or anyone. They mentioned that they will never reuse address or leaking any metadata about user's purchasing habits by parsing all previous transactions before building a new transaction. They also support Tor and VPN. They also mentioned that they store zero personal data to keep the transactions completely secure and anonymous.

2. Sending coins

   Coin Space wallet supports Bitcoin, Litecoin, Bitcoin Cash, Ripple, Ethereum, ERC223 and all ERC20 tokens. Their website states that they include a built-in exchange service. This service is provided by "ShapeShift". The ShapeShift platform provides the power to quickly swap between assets in a seamless, safe, and secure environment (https://shapeshift.io/#/coins).

3. Seamless payment

   The Coin Space has integrated payments via credit card, Google Pay, and Apple Pay. Their users can purchase Bitcoin and other cryptocurrencies with the payment methods that they have been using.

4. Security

   The Coin Space claims that they use bank-level security to prevent hacking and application-level authentication to protect unauthorized logins. They ensure that only users know their passwords by not storing it in any database. They keep the users' device fully localized by maintaining a server-free environment.

Q3 [5 points] Given the bitcoin difficulty information in https://www.coinwarz.com/mining/bitcoin/difficulty-chart, determine the bitcoin difficulty on March 1, 2020 and March 1, 2021. State any assumptions made in this determination.

The bitcoin difficulty on March 1, 2020 is 15,486,913,440,293.00000000. My assumption for the difficulty on March 1, 2021 would be around 6.96892E+41.

Next difficulty = (previous difficulty*20160)/(time in minutes to mine last 2016 blocks)
The mining difficulty is changed once every 2016 blocks or approximately once in 2016*10 minutes or 20160/1440 days or 14 days or TWO WEEKS.

Date	Estimate Next difficulty (Next 2 weeks)
March 1, 2020	2.16817E+14
March 14, 2020	3.03544E+15
April 1, 2020	4.24961E+16
April 14, 2020	5.94945E+17
May 1, 2020	8.32923E+18
May 14, 2020	1.16609E+20
Jun 1, 2020	1.63253E+21
Jun 14, 2020	2.28554E+22
Jul 1, 2020	3.19976E+23
Jul 14, 2020	4.47966E+24
Aug 1, 2020	6.27153E+25
Aug 14, 2020	8.78014E+26
Sep 1, 2020	1.22922E+28
Sep 14, 2020	1.72091E+29
Oct 1, 2020	2.40927E+30
Oct 14, 2020	3.37298E+31
Nov 1, 2020	4.72217E+32

Nov 14, 2020	6.61104E+33
Dec 1, 2020	9.25545E+34
Dec 14, 2020	1.29576E+36
Jan 1, 2021	1.81407E+37
Jan 14, 2021	2.5397E+38
Feb 1, 2021	3.55557E+39
Feb 14, 2021	4.9778E+40
Mar 1, 2021	6.96892E+41

Q4 [5 points] Write a summary of the forks that occurred on Bitcoin network since its inception until now. Make sure to state whether a fork was a hard fork or a soft fork.

A "fork" is the term used to describe a single blockchain diverging into two paths. Generally, this occurs as the result of a significant change in the network's protocol that effectively splits the blockchain into an old way of doing things and a new way of doing things.

Date	Software Version	Type	Description
28 July 2010	0.3.5	Softfork	OP_RETURN disabled, fixing a critical bug which enabled anyone to spend any Bitcoin.
31 July 2010	0.3.6	Hardfork	The addition of the OP_NOP functions.
		Softfork	OP_VER and OP_VERIF disabled.
1 Aug 2010	0.3.7	non-deterministic hardfork	Separation of the evaluation of the scriptSig and scriptPubKey. Fixing a critical bug which enabled anyone to spend any Bitcoin
15 Aug 2010	0.3.10	Softfork	- Output-value-overflow bug fix following a 184.5-billion Bitcoin spend incident. The 0.5 BTC that was the input to the transaction remains unspent to this day. - Disabling OP_CAT, which removed a DoS vector, along with the disabling of 14 other functions.
7 Sept 2010	0.3.12	Softfork	Adding the 20,000-signature operation limit in an incorrect way. This incorrect limit still exists.
12 Sept 2010	n/a	Softfork	Adding the 1MB blocksize limit. The "MAX_BLOCK_SIZE = 1000000" commit occurred on 15 July 2010, which was released in the 0.3.1 rc1 version of the software on 19 July 2010. The commit enforcing the 1MB rule occurred on 7 September 2010, activating at block 79,400. On 20 September 2010, Satoshi removed this activation logic, but kept the 1MB limit.
15 March 2012	BIP30	Softfork	Disallow transactions with the same TXID, unless the older one was fully spent. In September 2012, the rule was applied to all blocks, apart from 91,842 and 91,880, which violate the rule.

1 April 2012	BIP16	Softfork	Pay-to-script hash (P2SH) allows transactions to be sent to a script hash (address starting with 3) instead of a public-key hash (addresses starting with 1).
24 Mar 2013	BIP34	Softfork	Requires the coinbase transaction to include the block height.
18 Mar 2013	0.8.1	Softfork	This was a temporary softfork, introducing a new rule requiring that no more than 4,500 TXIDs are referenced by inputs in a block. This rule is stricter than the 10,000-BDB lock limit. The rule expired on 15 May 2013, a flag-day hardfork.
15 May 2013 or 16 Aug 2013	BIP50	Hardfork	In August 2013, a block may have been produced that violated the original 10,000-BDB lock limit rule, which was relaxed on 15 May 2013.
4 July 2015	BIP66	Softfork	Strict DER signature upgrade means Bitcoin is no longer dependent on OpenSSL's signature parsing.
14 Dec 2015	BIP65	Softfork	Check Lock Time Verify enables funds to be locked until a specific time in the future. This is Bitcoin's first new function.
4 July 2016	BIP68 BIP112 BIP113	Softfork	Relative lock-time enables a transaction output to be banned for a relative amount of time after the transaction. CheckSequenceVerify. Median time-past removes the incentive for a miner to use a future block timestamp to grab more transaction fees.
23 July 2017	BIP91	Softfork	This temporary softfork makes signaling for the SegWit upgrade mandatory.
01 Aug 2017	BIP148	Softfork	This temporary softfork makes signaling for the SegWit upgrade mandatory for a two week period following 1 August 2017.
24 Aug 2017	BIP141 BIP143 BIP147	Softfork	The segregated-witness (SegWit) upgrade.
24 Oct 2017	Bitcoin Gold	Hard forks	Splitting the cryptocurrency
15 Nov 2018	Bitcoin SV	Hard forks	Splitting the cryptocurrency