HW 2- HES CS 118 BLOCKCHAIN
Max Bildner
3/1/21

1 Bitcoin vs "Bitcoin Core"

- Bitcoin was the first implementation by Satoshi Nakamoto. It is an open source project (anyone can freely use and volunteer to contribute)
- Bitcoin Core came after Bitcoin and can be thought of as a reference implementation or guide on how to implement the Bitcoin project. Bitcoin core includes wallets, transaction and block validation as well as the peer-to-peer network

https://github.com/bitcoinbook/bitcoinbook/blob/develop/ch03.asciidoc#bitcoin-core-the-reference-implementation

2 UTXO Model vs an Account Model?

- UTXO Model (Unspent Transaction Output) is a type of record keeping model used by Bitcoin. There is no notion of accounts with balances like a traditional bank account. UTXO is an output of a Bitcoin transaction. The following is a high level abstracted example of how UTXO works- if I have a $5 note in my wallet and want to buy milk for $1. When I give my $5 note to the cashier, it gets incinerated and two notes appear, where $1 goes to the cashier, $3.90 goes to me, and 10 cents goes to the miner who just performed/verified this operation. A person's bitcoin balance (usually created by a wallet) aggregates all the UTXOs registered to that person's address by scanning the entire blockchain
- The Account Model is a type of record keeping model used by Ethereum. This model represents the more traditional view of record keeping where each account is associated with a certain balance (like bank accounts)

https://academy.santiment.net/metrics/details/stack-coin-age-model/
https://medium.com/@sunflora98/utxo-vs-account-balance-model-5e6470f4e0cf
https://river.com/learn/bitcoins-utxo-model/
https://academy.horizen.io/technology/expert/utxo-vs-account-model/

3 What is the UTXO set? How/Where is it stored in Bitcoin Core?

- UTXO set includes all existing UTXOs at a given point in time. This set can be thought of as a global database that tracks all the spendable outputs. When a transaction is created, it uses an unspent output from the UTXO set (set will shrink), then when a new unspent output is created the UTXO set will grow.
- The set is scattered throughout the blockchain. The Active Chain (longest valid chain of blocks) is stored in $DATADIR/blocks (a LevelDB database that has key-value storage)

https://bitcoin.stackexchange.com/questions/37397/where-is-the-utxo-data-stored
https://www.mycryptopedia.com/bitcoin-utxo-unspent-transaction-output-set-explained/
https://eprint.iacr.org/2017/1095.pdf

4 What is bitcoin dust?

- Bitcoin Dust are tiny pieces of Bitcoin. Coins generated from transaction outputs and are so small they require more fees to verify than they're worth. A transaction output is dust when its value is lower than the cost of spending it

https://www.coindesk.com/bitcoin-dust-tell-get-rid
https://www.investopedia.com/terms/b/bitcoin-dust.asp#:~:text=Due%20to%20the%20working%20mechanism,for%20the%20transaction%20to%20occur.
https://bitcoin.stackexchange.com/questions/10986/what-is-meant-by-bitcoin-dust

5 Describe what a blockchain fork is. What is the difference between a soft and hard fork?

- A blockchain fork is an alternate version of a blockchain that represents disagreements between miners/users on which blockchain to use
- Soft Fork = change in software protocol where only previously valid transaction blocks are made invalid. This requires only a majority of the minors enforcing the new rules/software opposed to a hard fork (requires all nodes to upgrade)
- Hard Fork = radical change to the protocol of a network (ex. 2017 Bitcoin Cash forked from Bitcoin)

https://www.cmcmarkets.com/en/learn-cryptocurrencies/what-is-a-blockchain-fork
https://www.investopedia.com/terms/h/hard-fork.asp
https://www.investopedia.com/terms/s/soft-fork.asp

6 What is a testnet?

- A testnet is a different blockchain used for testing (allows developers to experiment without having to use real bitcoins)

https://en.bitcoin.it/wiki/Testnet#:~:text=The%20testnet%20is%20an%20alternative,to%20be%20used%20for%20testing.&text=This%20allows%20application%20developers%20or,breaking%20the%20main%20bitcoin%20chain
https://github.com/bitcoinbook/bitcoinbook/blob/develop/ch09.asciidoc#bitcoins-test-blockchains

7 What is SPV? (Simplified Payment Verification)

- A way to verify payments/transactions without downloading the entire blockchain (often used for light wallet apps)

https://github.com/bitcoinbook/bitcoinbook/blob/develop/ch08.asciidoc#node-types-and-roles

8 What are bloom filters used for in Bitcoin?

- A “probabilistic” data structure that can determine whether or not an element is in a set by an extremely high speed operation. Probabilistic meaning, that it can only give results that are not in the set or maybe in the set, but not “definitely in the set”. These filters are used by SPV nodes to help quickly verify a transaction

https://github.com/bitcoinbook/bitcoinbook/blob/develop/ch08.asciidoc#bloom-filters
https://bitflyer.com/en-us/glossary/bloomfilter#:~:text=A%20bloom%20filter%20is%20a,an%20extremely%20high%20speed%20operation

9 There are four functions of a Bitcoin Node: routing, full blockchain database, mining, and wallet services. Describe each of these functions. Which of these functions must a Full Node implement? Which must a solo miner implement? Which must a lightweight (Simplified Payment Verification) wallet implement?

- **Routing** (Network Routing Node)- all nodes have this function. This function allows the node to participate in the network. This function allows the node to discover, connect to other nodes, and validate transactions/blocks
- **Full Blockchain Database**- contains the full blockchain database
- **Mining**- verify transactions by competing to create new blocks
- **Wallet Services**- Can be desktop, mobile, web, hardware. Used for storing private keys and a corresponding Wallet address

- **Full Blockchain Node**- contains the Full Blockchain Database, and the network routing function
- **Solo Miner**- Contains the mining function, the Full Blockchain Database, and the network routing function
- **SPV Wallet**- contains a wallet and the network routing function

https://github.com/bitcoinbook/bitcoinbook/blob/develop/ch08.asciidoc#node-types-and-roles
https://medium.com/coinmonks/the-bitcoin-network-6713cb8713d

10 Describe what a mining pool is

- A group of miners who combine their computational resources to increase their chances of finding a nonce to verify transactions/blocks. Mining reward is shared among miners in the pool. AntPool, Huobi, and F2Pool are some of the biggest mining pools.

https://github.com/bitcoinbook/bitcoinbook/blob/develop/ch10.asciidoc#mining-pools
https://www.investopedia.com/terms/m/mining-pool.asp

11 What is segwit? (Segregated Witness)

- SegWit helps segregate the digital signature from the transaction data
- SegWit helps increase the block size limit (the amount of data if all the bitcoin transactions since 2009 would not be sustainable if they were all in each block)

https://github.com/bitcoinbook/bitcoinbook/blob/develop/ch07.asciidoc#segregated-witness
https://www.investopedia.com/terms/s/segwit-segregated-witness.asp

12 What is a transaction pool? (Mempool)

- place where all unconfirmed/unverified transactions go

https://github.com/bitcoinbook/bitcoinbook/blob/develop/ch08.asciidoc#transaction-pools

13 Describe a coinbase transaction

- The first transaction in a new block (created by the miner). This transaction has no inputs except for a coinbase, and there is only one created with each new block that's mined. This coinbase transaction rewards the miner for verifying the transaction.

https://github.com/bitcoinbook/bitcoinbook/blob/develop/ch10.asciidoc#the-coinbase-transaction