x) Read and summarize (with some bullet points)

Nakamoto 2008: Bitcoin: A Peer-to-Peer Electronic Cash System, chapters

- The abstract presents the idea that a purely peer-to-peer version of electronic cash will allow payments to be sent straight to the receiver excluding the need for a financial institute such as bank in the process.
- The records of these transactions are hashed into an ongoing chain called as proof-of-work of the events that have occurred.

1 Introduction

- Digital transactions that rely on financial institutions suffer from weaknesses such as lack of completely non-reversible transactions which creates a need for trust on merchant's part.
- The system that would solve these problems and make a direct transactions between two different partiers is based on cryptographic proof.
- System is secure as long as the CPU used by adversaries is smaller than the CPU of honest nodes in the peer-to-peer network.

2 Transactions

- Electronic coin as a digital signature is transferred to next owner "by digitally signing a hash of the previous transaction and the public key of the next owner" (Nakamoto 2006, p. 22).
- To make sure that the owners don't double spend their coin a trusted third party such as mint is needed in the verification process.
- To achieve a trust without this trusted third party the transactions must be publicly announced and agreed by majority of the nodes.

3 Timestamp Server

- By adding a timestamp we can proof that the data have existed at the time.
- Timestamp consists of previous timestamp in its hash, forming a chain, with each additional timestamp reinforcing the ones before it.

4 Proof-of-Work

- The "distributed time stamp server" on "peer-to-peer basis" implementation is based on proof-of-work system.
- The CPU usage that is needed to produce hash with required zeros is the proof-of-work.
- If honest nodes produce more hashes and use more CPU than the bad ones, the chain will remain uncorrupted.

5 Network

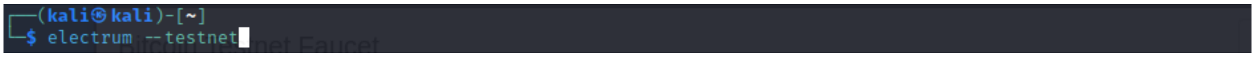
  - To put it shortly the network works in a way that the transactions are broadcasted to all nodes.
  - The longest chain is always considered to be the correct one.
  - New transactions don't have to reach all nodes, but as long as they reach many ones, they will become part of the chain eventually.

6 Incentive

- The first transaction block starts a new coin owned by the creator of the block - this gives incentive for nodes to support the network and to give more coins into circulation.
- Also the CPU based proof-of-work system is less appealing as you get rewards much easier by playing by the rules.

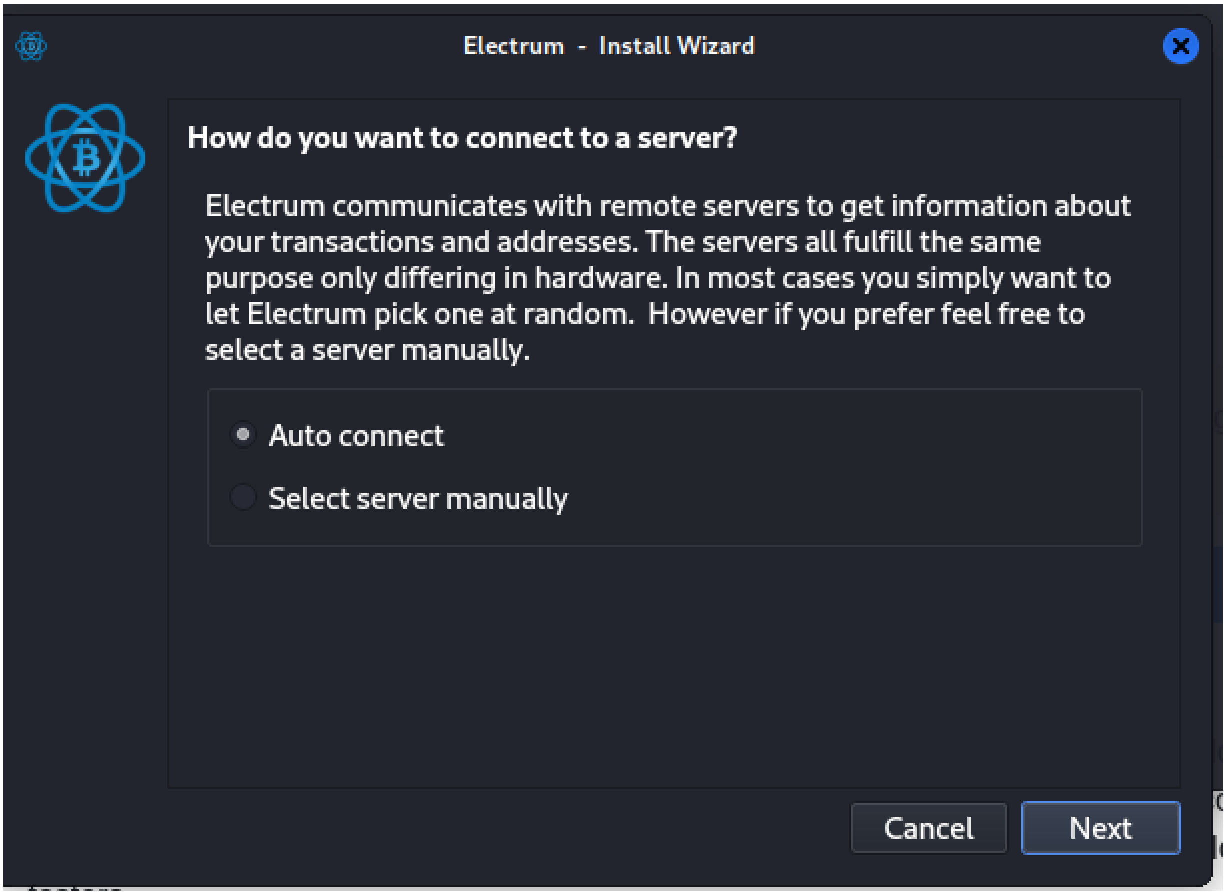
a) Wallet. Create a BitCoin testnet wallet.

I created a BitCoin testnet wallet with electrum. This command launches the test wallet:



```
┌──(kali㉿kali)-[~]
└─$ electrum --testnet
```

The install wizard prompts for different options during the creation process, I will go with default options such as ‘auto connect’:



Electrum - Install Wizard

How do you want to connect to a server?

Electrum communicates with remote servers to get information about your transactions and addresses. The servers all fulfill the same purpose only differing in hardware. In most cases you simply want to let Electrum pick one at random. However if you prefer feel free to select a server manually.

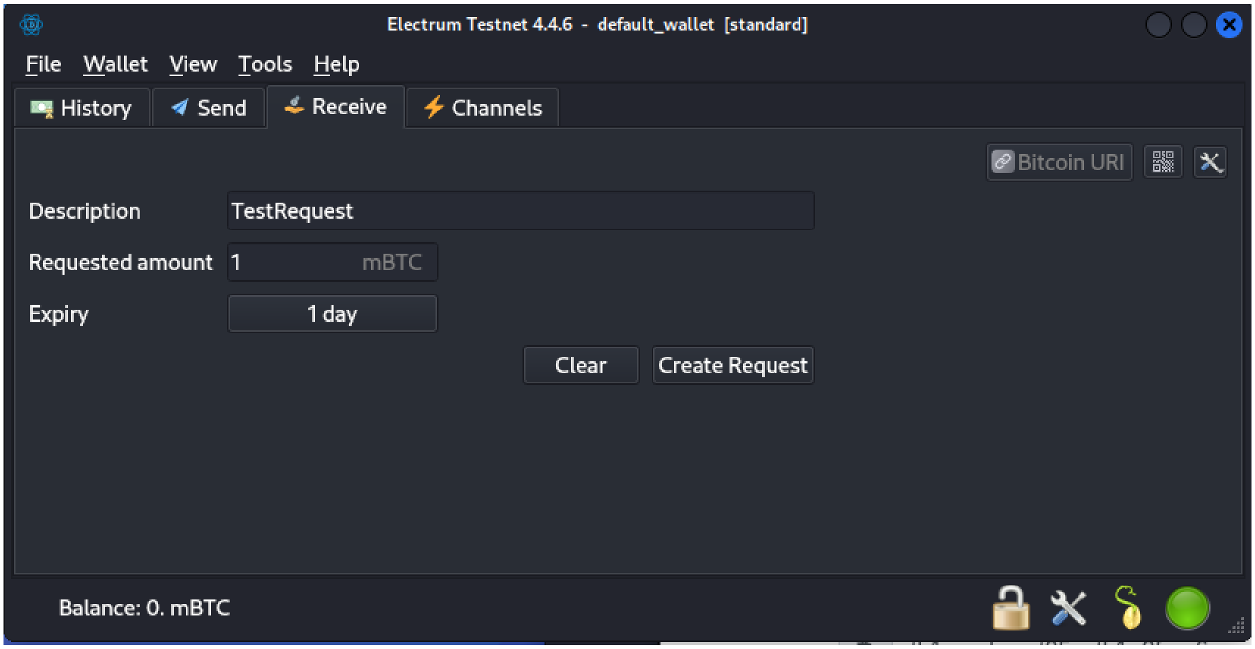
● Auto connect

○ Select server manually

My wallet generation seed is *garment wild cement antique say usual noodle radar increase glance picture rebel*.

b) Faucet. Get worthless fake money from a testnet Bitcoin faucet.

First I create a request in Electrum:



Description: TestRequest

Requested amount: 1 mBTC

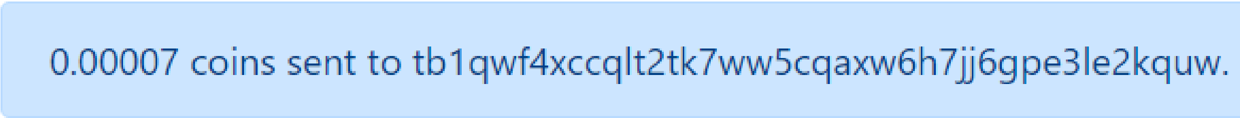
Expiry: 1 day

Balance: 0. mBTC

I have now a test BitCoin wallet which address is:

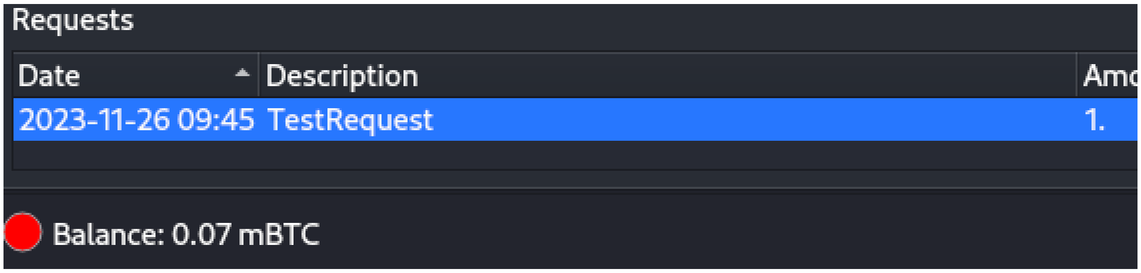
tb1qwf4xccqlt2tk7ww5cqaxw6h7jj6gpe3le2kquw

I sent fake BitCoins from https://bitcoinfaucet.uo1.net/ service:



0.00007 coins sent to tb1qwf4xccqlt2tk7ww5cqaxw6h7jj6gpe3le2kquw.

The balance is now changed and fake money is received:



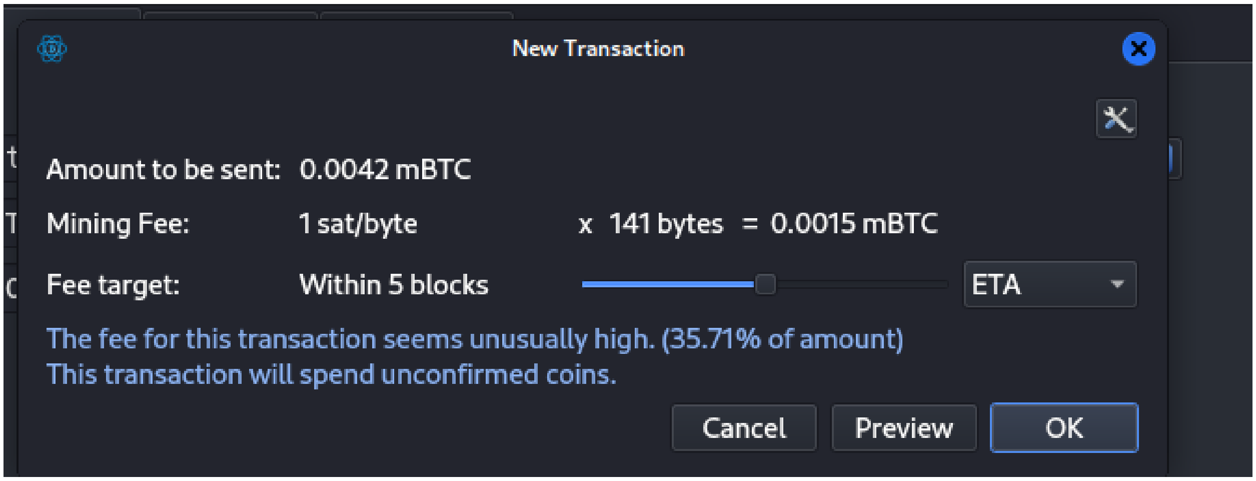
Requests

Date	Description	Amo
2023-11-26 09:45	TestRequest	1.

Balance: 0.07 mBTC

c) Giveway. Move money to another Bitcoin wallet. Choose an amount where the last two digists are 42.

Sending money to a test address ‘tb1q6dlta43hxj0tsp9m2l8ayr0fuwlhgnaedue4pz’:



New Transaction

Amount to be sent: 0.0042 mBTC

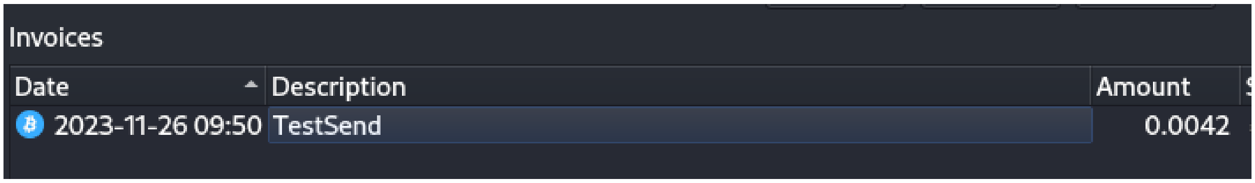
Mining Fee: 1 sat/byte x 141 bytes = 0.0015 mBTC

Fee target: Within 5 blocks

ETA

The fee for this transaction seems unusually high. (35.71% of amount)
This transaction will spend unconfirmed coins.

Sent:



Invoices

Date	Description	Amount
2023-11-26 09:50	TestSend	0.0042

d) Explorer. Use a block explorer to analyze a block on the real Bitcoin blockchain. Explain what each value and field means. You only need to analyze the block information and one sample transaction, as a block can contain many transactions.

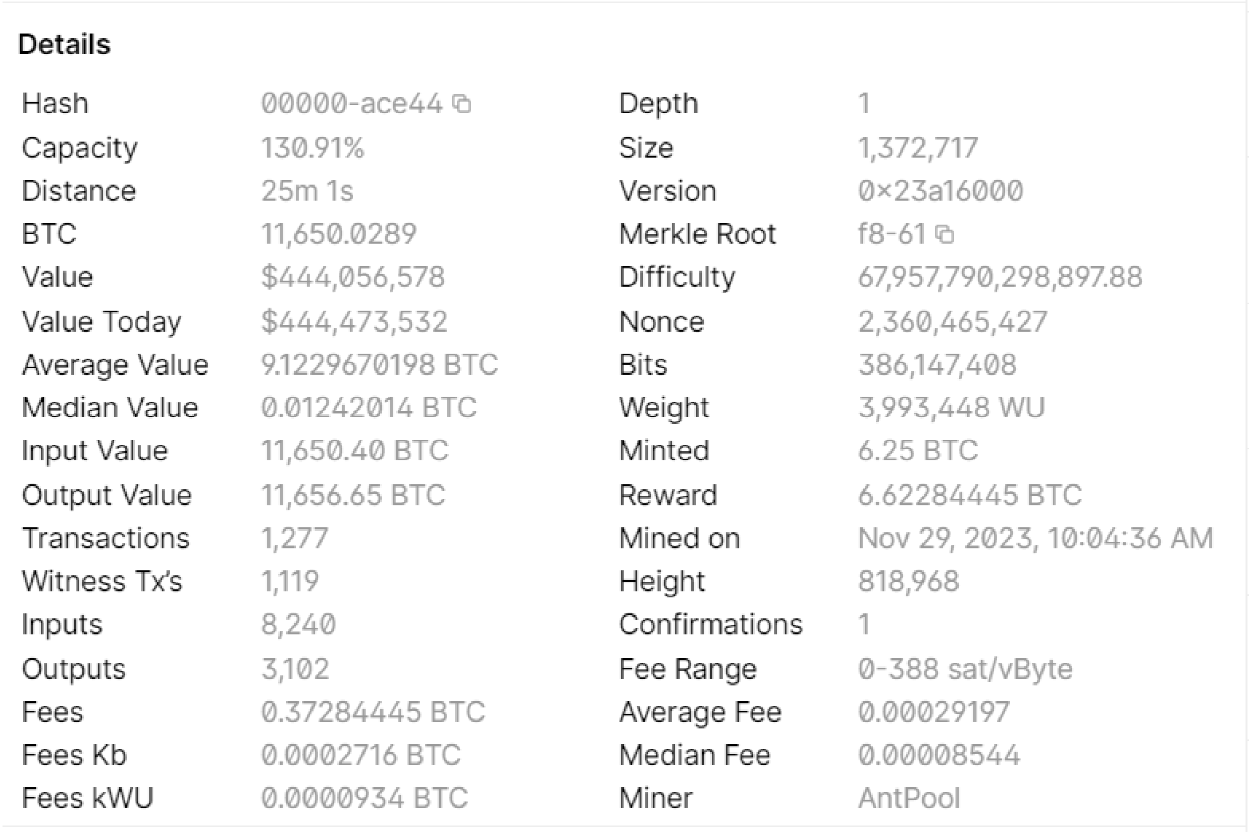
Bitcoin Block 818,968

Mined on November 29, 2023 10:04:36 • All Blocks

The Bitcoin Block that is being analyzed for this assignment is the 818968th in its order and we shall refer to this Bitcoin Block as BB from now on.

The number refers to the block's "height" or its order in the blockchain.

Here are the details of our block BB as presented in https://www.blockchain.com/explorer/blocks/btc/818968:



Details

Hash	00000-ace44	Depth	1
Capacity	130.91%	Size	1,372,717
Distance	25m 1s	Version	0×23a16000
BTC	11,650.0289	Merkle Root	f8-61
Value	$444,056,578	Difficulty	67,957,790,298,897.88
Value Today	$444,473,532	Nonce	2,360,465,427
Average Value	9.1229670198 BTC	Bits	386,147,408
Median Value	0.01242014 BTC	Weight	3,993,448 WU
Input Value	11,650.40 BTC	Minted	6.25 BTC
Output Value	11,656.65 BTC	Reward	6.62284445 BTC
Transactions	1,277	Mined on	Nov 29, 2023, 10:04:36 AM
Witness Tx's	1,119	Height	818,968
Inputs	8,240	Confirmations	1
Outputs	3,102	Fee Range	0-388 sat/vByte
Fees	0.37284445 BTC	Average Fee	0.00029197
Fees Kb	0.0002716 BTC	Median Fee	0.00008544
Fees kWU	0.0000934 BTC	Miner	AntPool

Hash is the unique identifier for the block. This is a crucial part for the block's integrity.

Capacity is a value of a block's transaction capacity. Segregated Witness (SegWit) protocol allows transactions beyond the standard capacity which makes it possible for this value to be over 100%.

Distance refers to the time since the block was mined.

The value BTC is the accumulative amount of the transactions within this block.

Value and Value Today numbers tell the total amount of all transactions in the block at the time of mining. The latter one is the fixed number according to today's BTC price.

Average Value & Median Value refer to the average and median transaction value inside the block. As larger transaction might ramp up the Average Value up, the Median Value gives more accurate information of the sizes of the transactions in general.

Input Value & Output Value. Input value is the total amount of BTC transferred from senders addresses to this block and Output Value is the same other way around. The output is a bit less because of transaction fees.

Transactions is the number of transactions included in this block. Witness Tx’s is the number of SegWit transactions. SegWit protocol makes BTC more scalable by allowing more transactions within the block.

Output & Input are the number of output and input transactions inside this block.

Fees refer to the amount of fees payed by users who want their transactions to be included in the block. Fees kb is a measure of how much users are paying for each kilobyte of transaction space they use in the block. Fees kWu means the same thing but is weighted according to the SegWit protocol.

Depth is the total amount of confirmations meaning that only one block has been added since the creation of this block.

Size is the size of the block in bytes. The size deterems how many transactions the block can include.

Version is a version number of the block used to signal readiness for network upgrades or to indicate which rules were followed in constructing the block.

Merkle root is a single hash to represent all the blocks transactions and used in verifying transactions.

Difficulty is the level of difficulty for finding a new hash for the next block.

Nonce - “Random value that can be adjusted to satisfy the proof of work”. The value itself represents a successful attempt to create a block hash.

Bits is a target threshold for valid block hash.

Weigh - Weigh units related to SegWit protocol.

Minted is the amount of BTC granted as a reward to the miner who mined the block.

Total reward is the minted amount minus transaction fees.

Mined is the date when this block was mined and added to the block chain.

Height is the name and order number of the block in the chain.

Confirmations is the number of block that has been added to the chain.

Free range indicates the variability of transaction fees in the block.

Average fee is the mean transaction fee paid per byte for the transactions within the block.

Median fee gives a more typical value of transaction fees within the block.

Miner is the mining pool that successfully mined the block.

Summary

This is my first iteration of studying Bitcoin technical features and a lot of these aforementioned terms are still a bit hard to understand completely.

What is more clear to me is the theory behind the added value through proof of work and CPU usage and how the blockchain works through the hash mechanism.