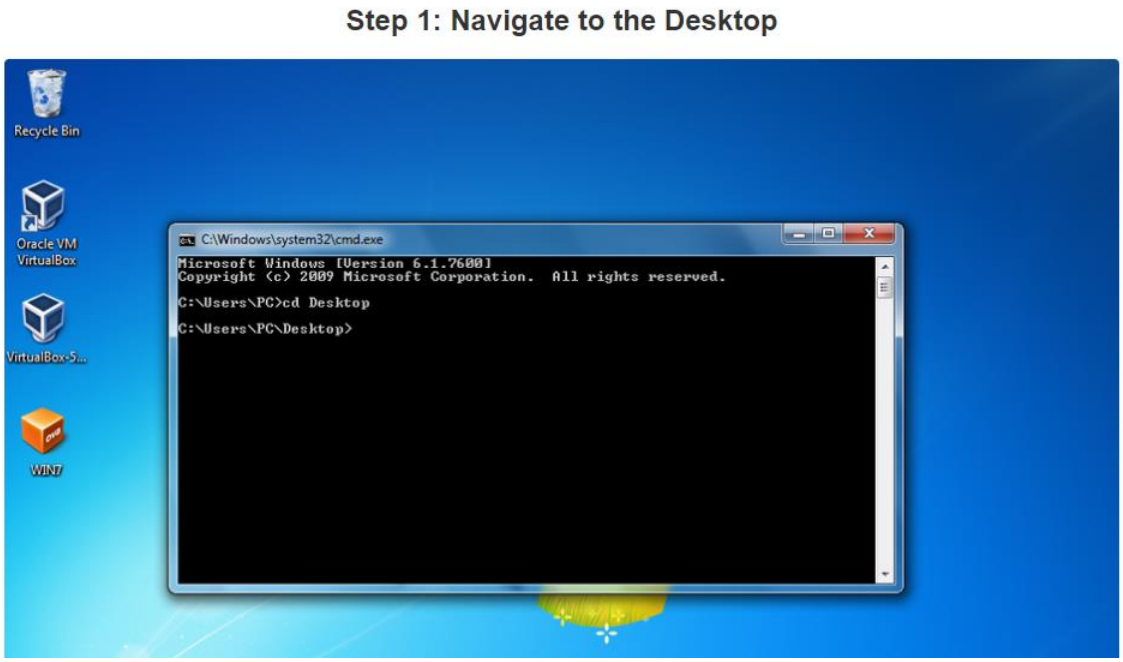
UNIT 4 CREATING AN OWN BLOCK CHAIN

Creating: Basic P2P network, Genesis Blocks and Sharing Blocks – Registering Miners and Creating new blocks – Storing blocks – Creating: Blockchain wallet, API, Command Line Interface – Blockchain Wallet and Transaction: Wallet, Transaction and Colored Coins

Creating:

Basic P2P network:

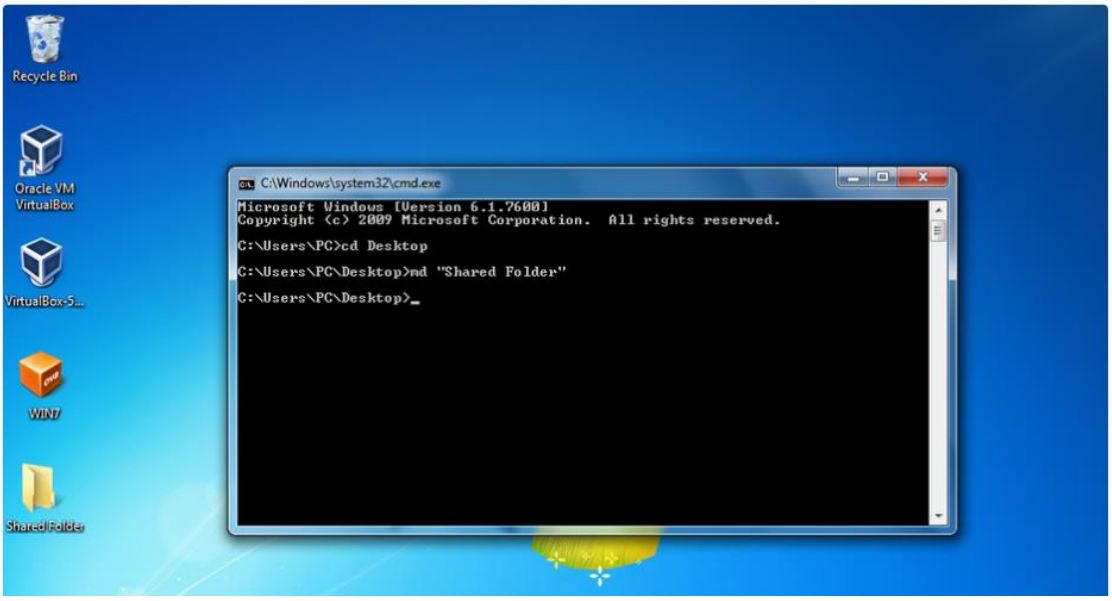
P2P is a technology that is based on a very simple principle, and that is the concept of decentralization. The peer-to-peer architecture of blockchain allows all cryptocurrencies to be transferred worldwide, without the need of any middle-man or intermediaries or central server.



Open command prompt [1] and then use the command <cd Desktop> to change into the desktop directory. This step is simply for convenience so that it is easier to find the folder you're going to be working with .

[1] You can open command prompt by clicking on the windows button at the bottom left and tying <cmd>.

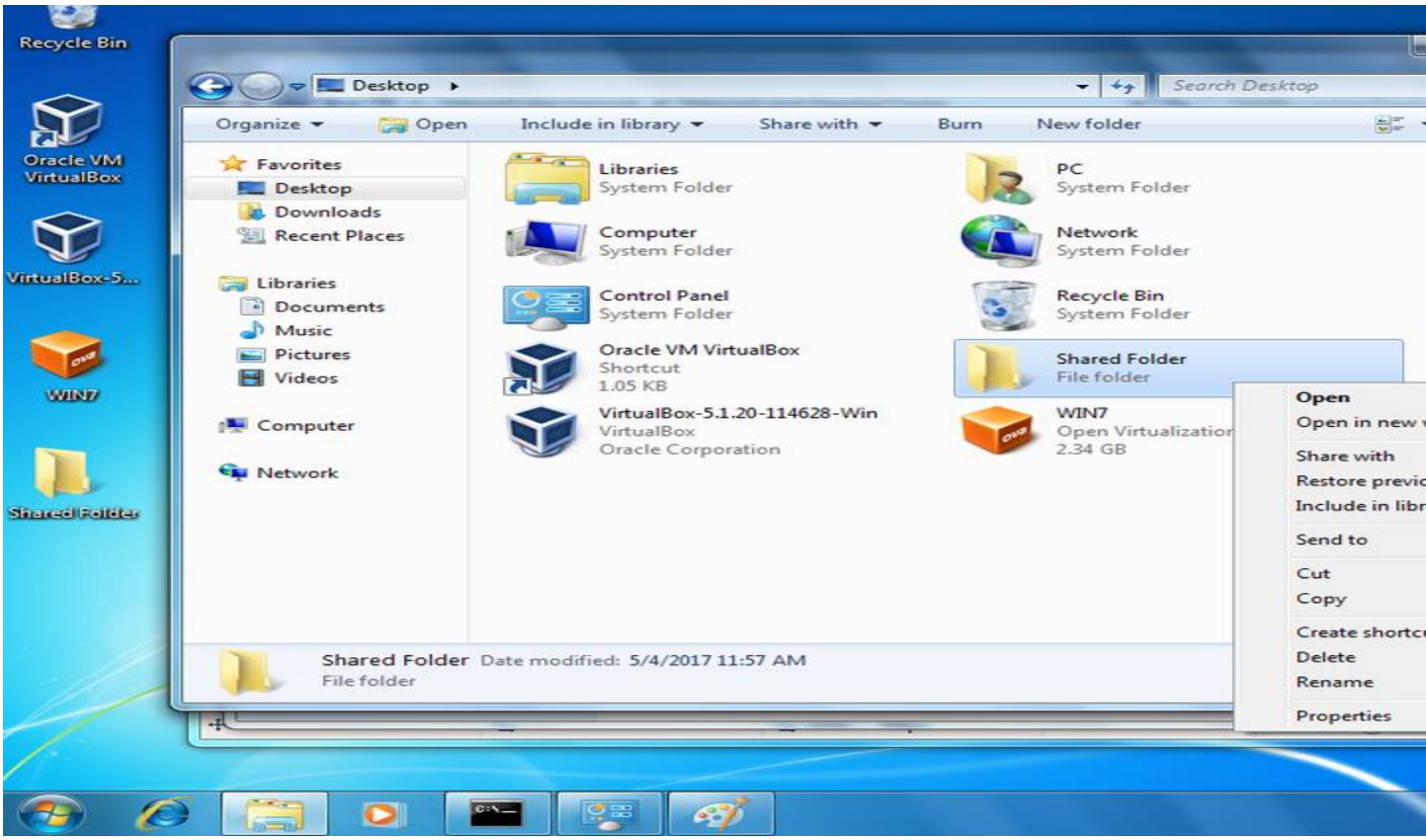
Step 2: Create Your Folder



Use the command <md *folder name*> [2]. Make sure that it is visible on your desktop.

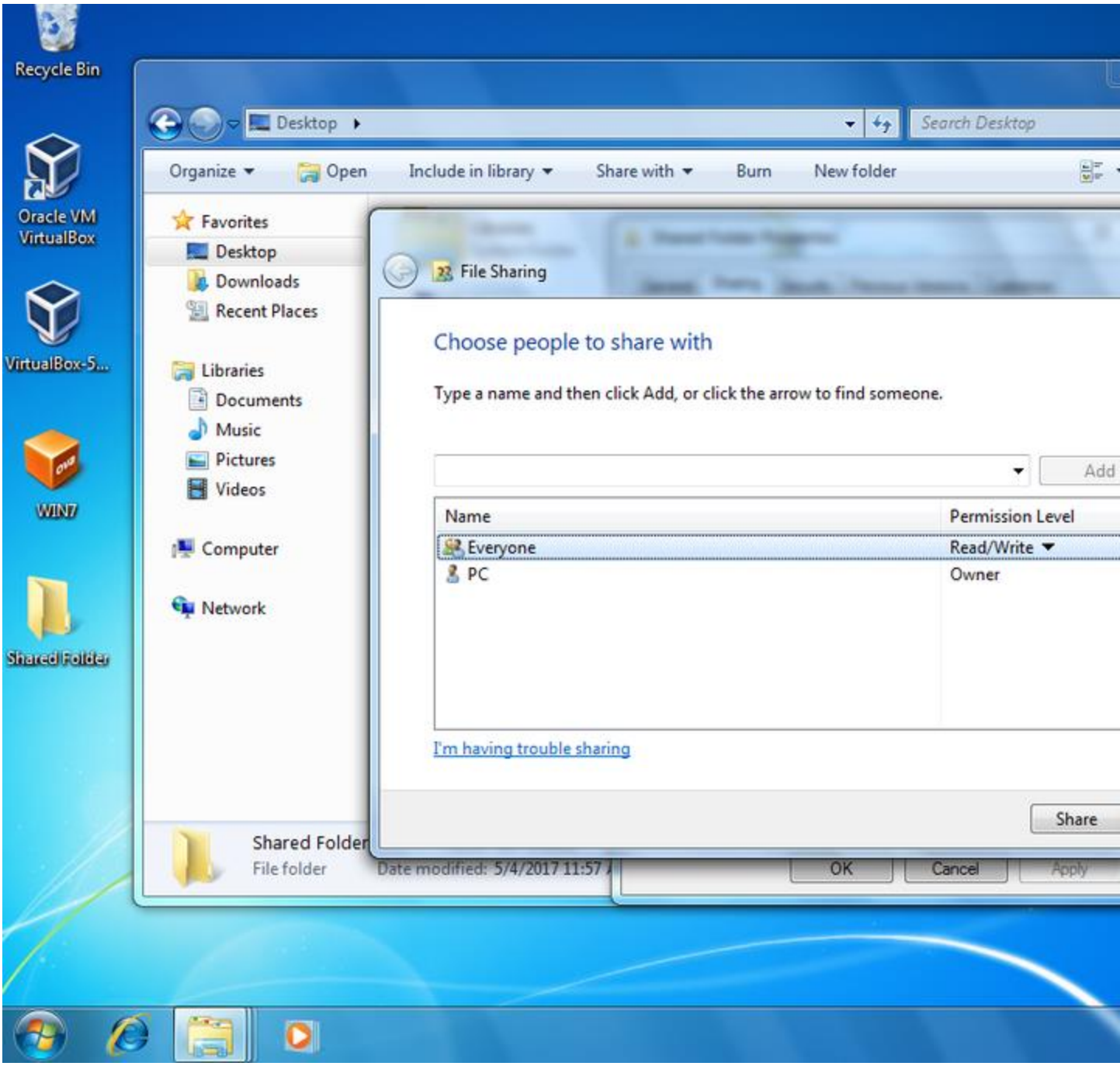
[2] The command md allows you to create a new folder. After tying md press space and type the name of the folder you want to create. If the folder has more than one word in the name make sure to put the name in quotation marks.

Step 3: Navigate to the Folder and Open the Properties



Open the file explorer and go under the Desktop section. Left-click then right-click on the folder. The left-click highlights the folder, and the right-click opens a menu of options. Once the menu of options pops up click on the properties. When you open the properties window go to the sharing section.

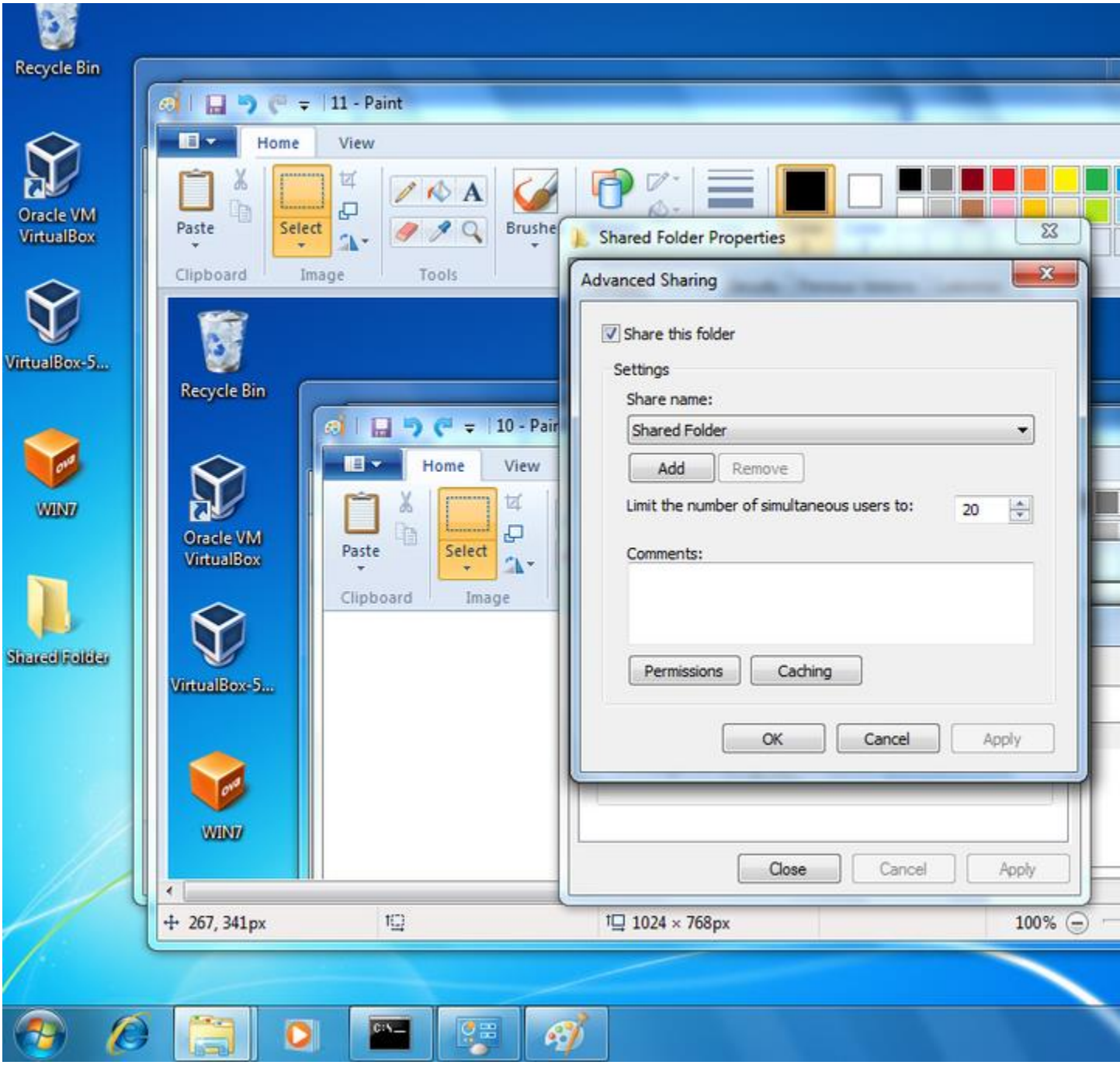
Step 4: Choose Who You Want to Share With.



Type <Everyone> and click add [3]. Once you're done with that click share and then go to the advanced sharing.

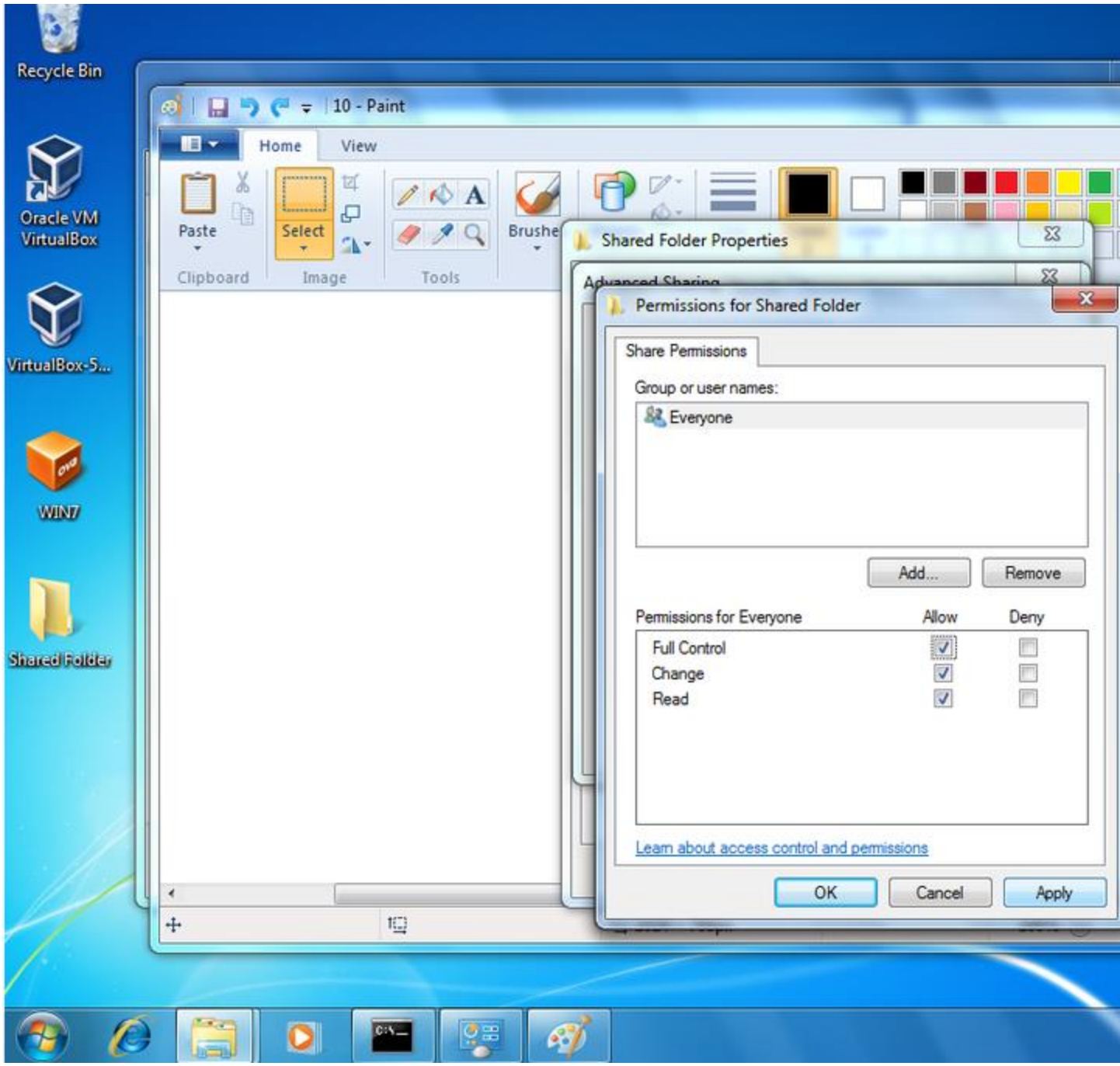
[3] The default setting for the folder is set to only read. This means that if a person accesses the folder they will only be able to view the files and not actually be able to write to the folder.

Step 5: Sharing the Folder



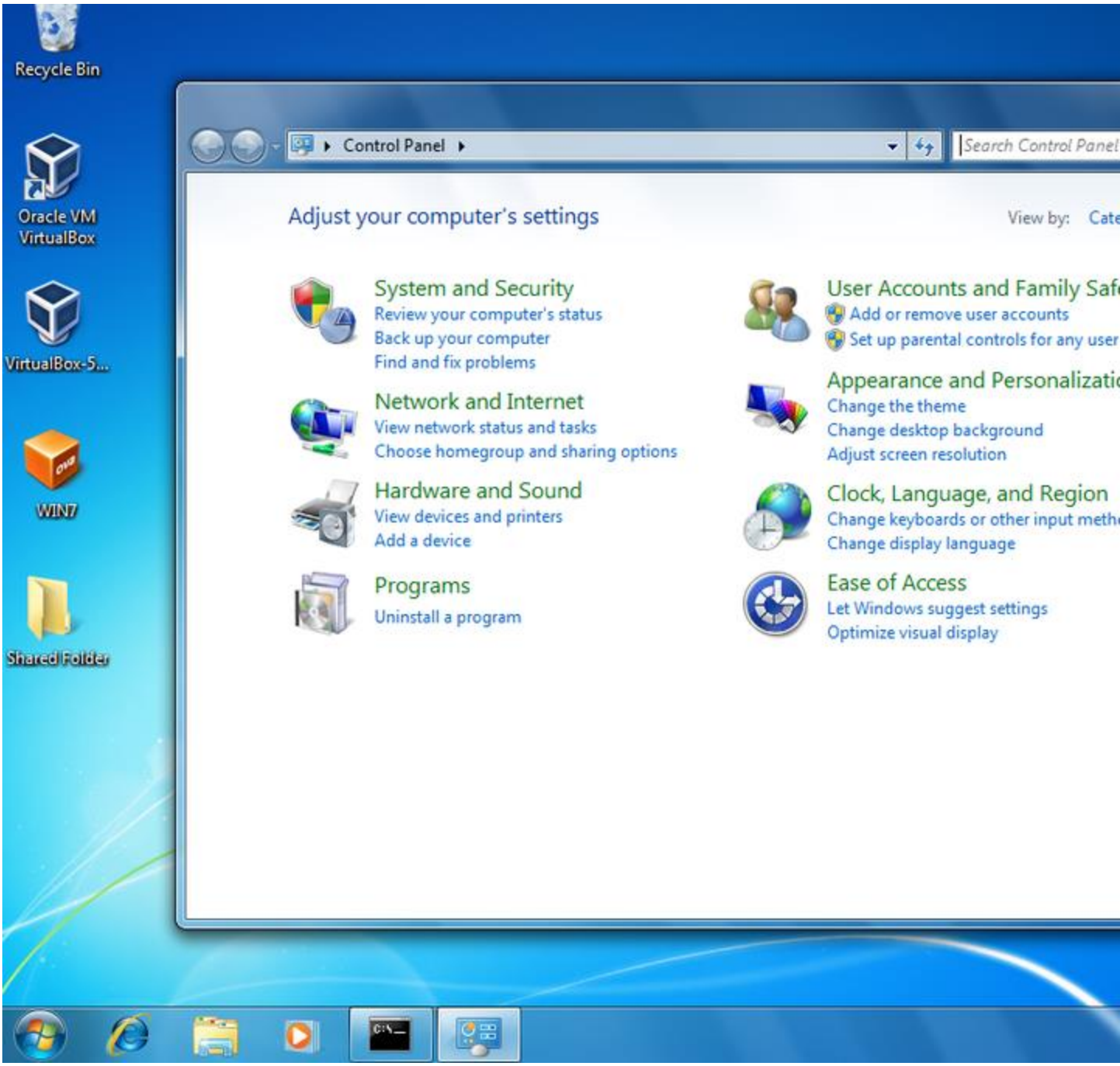
Press the box that lets you share the folder and then go into the permissions section.

Step 6: Permissions



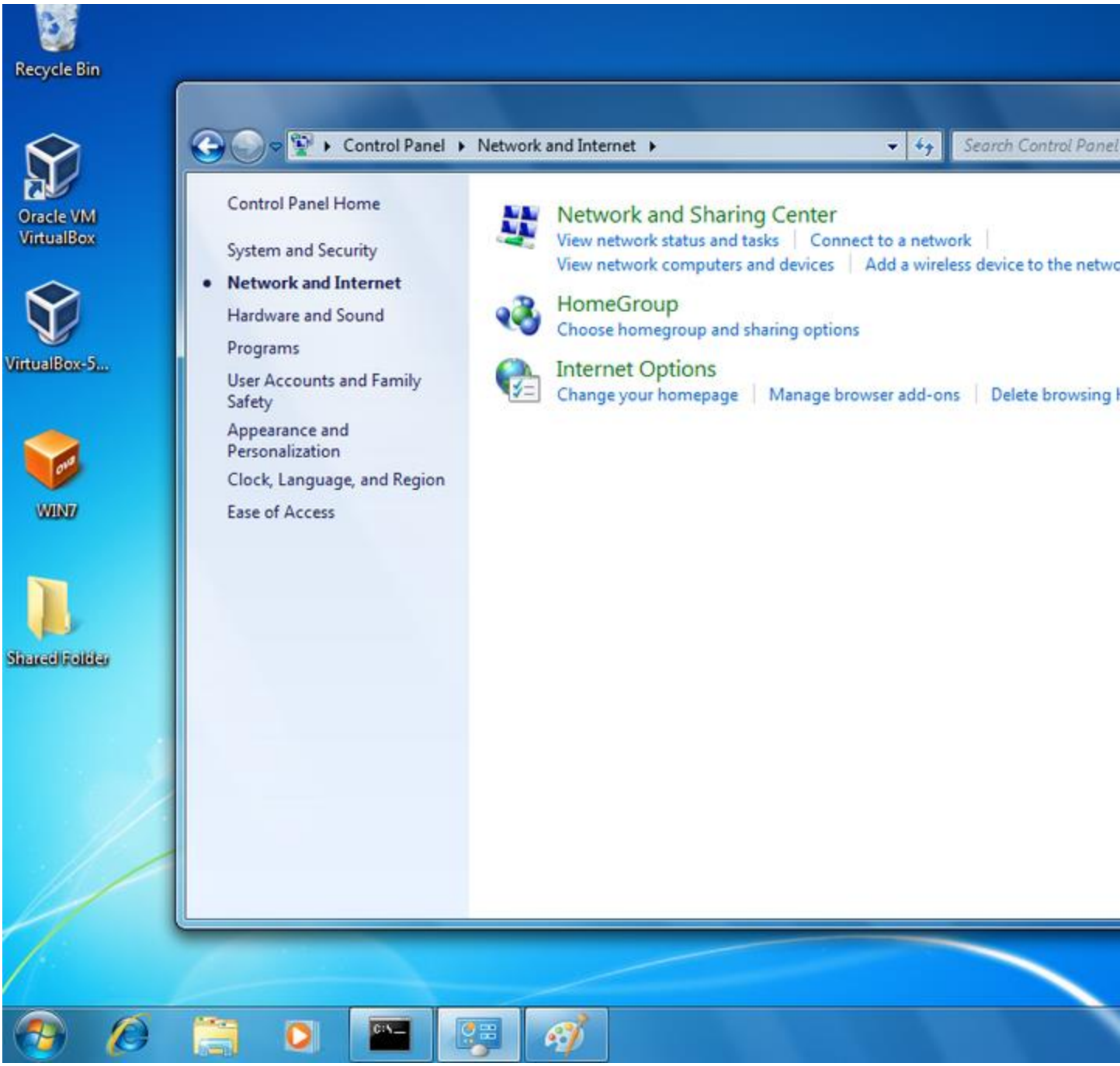
Make sure to give full control to the people that have access to the shared folder. Click Apply then click OK. Once you press OK you'll be back at the advanced sharing page. Press Apply and OK on that page too.

Step 7: Open Control Panel



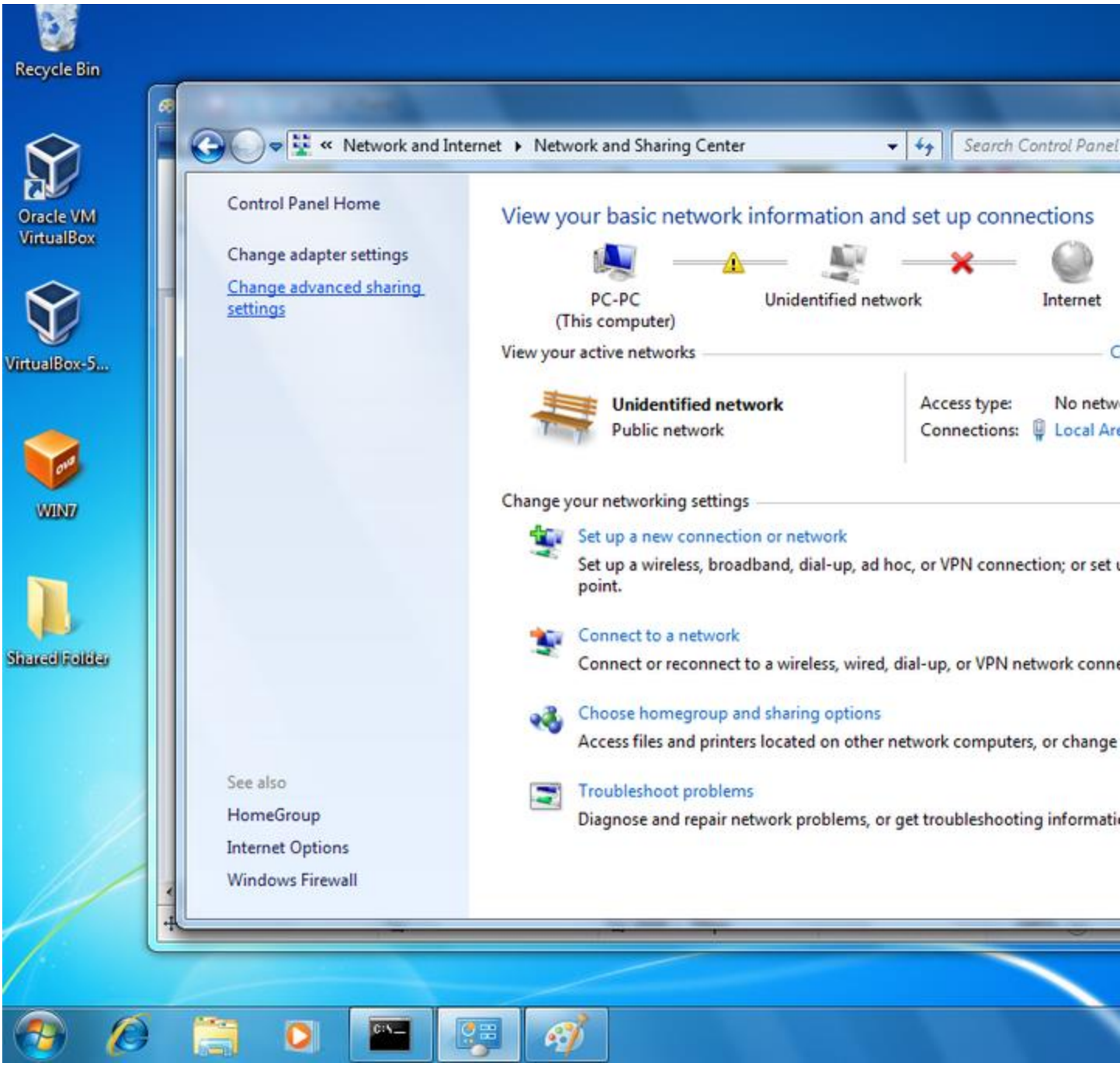
Navigate into the control panel and click on the Network and Internet section.

Step 8: Network and Sharing



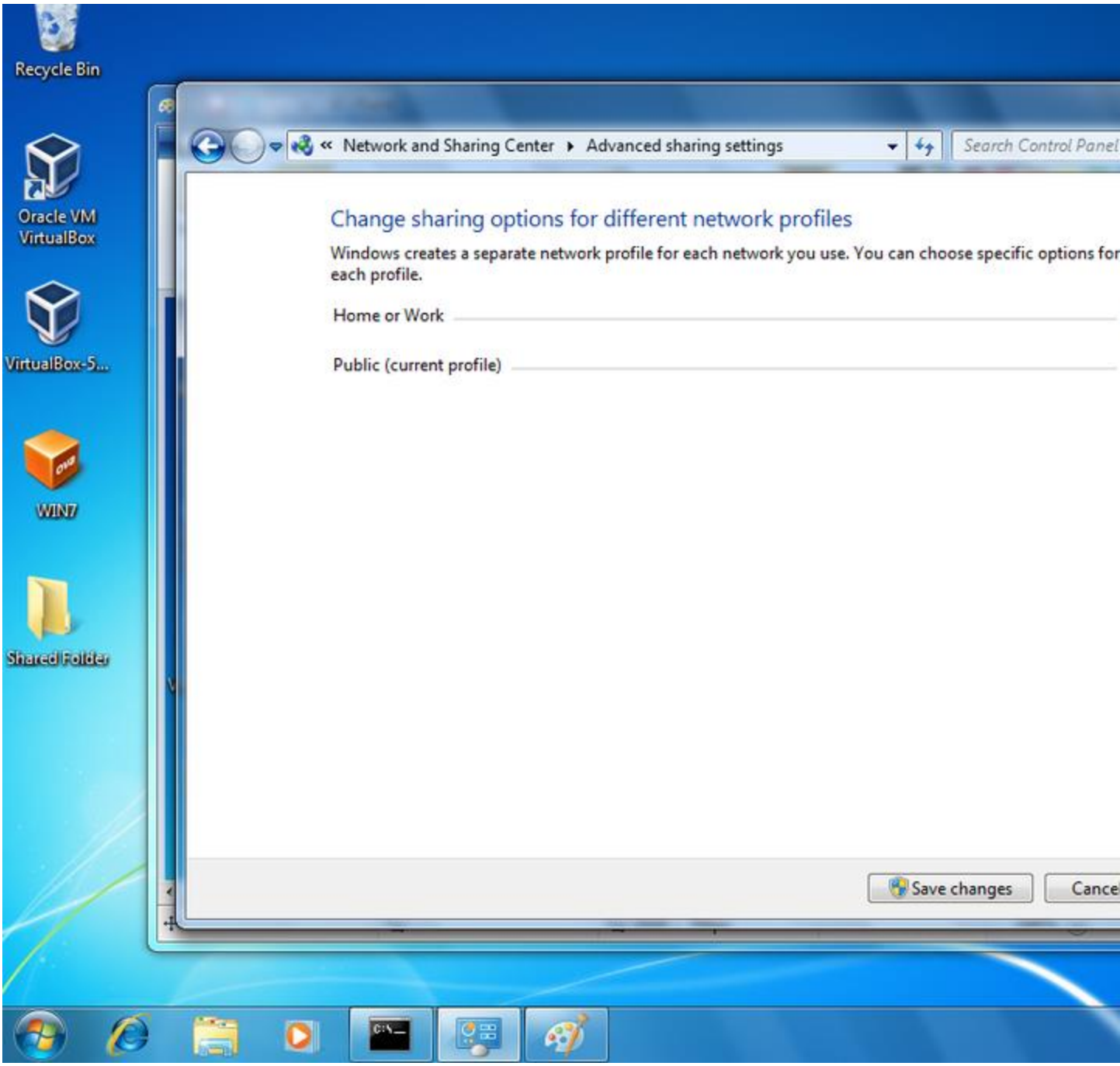
Navigate into the Network and Sharing section.

Step 9: Advanced Sharing



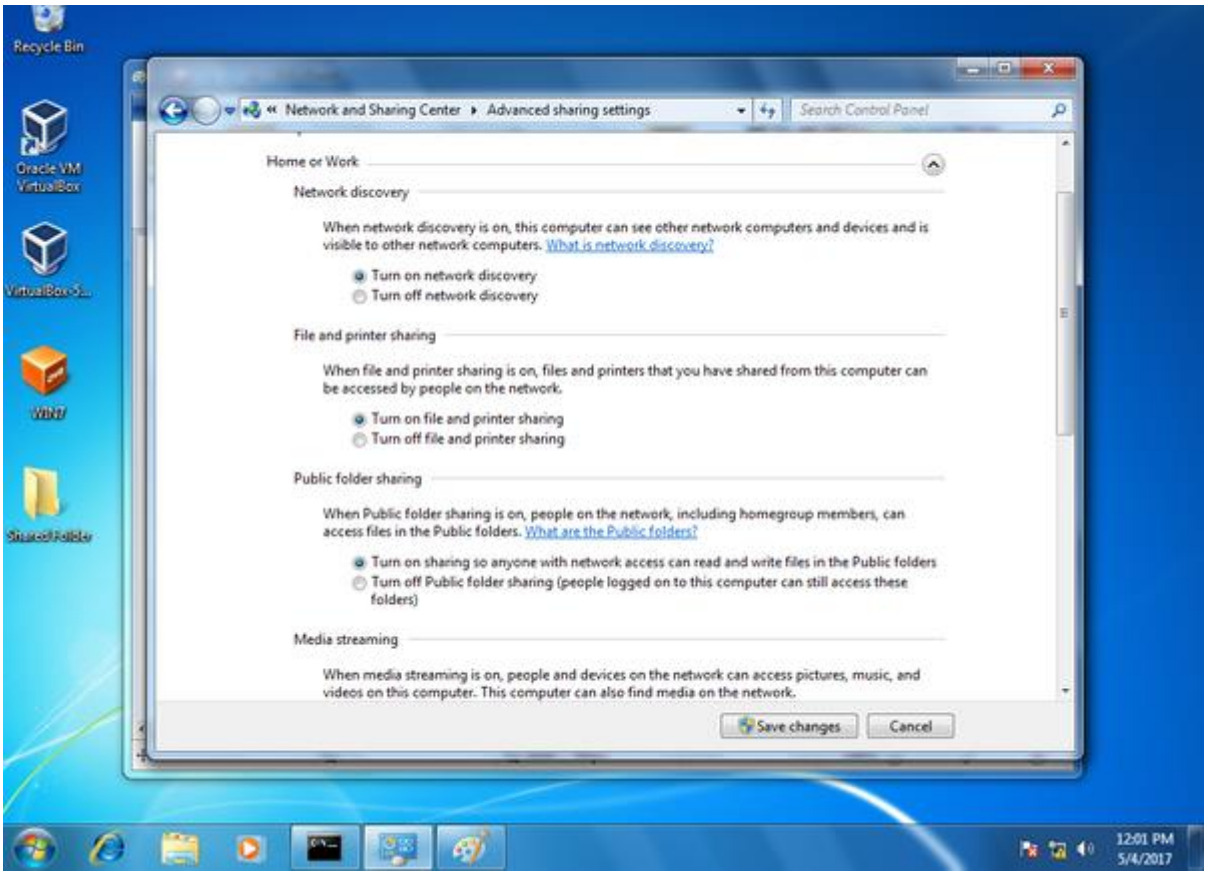
Navigate to the advanced sharing settings.

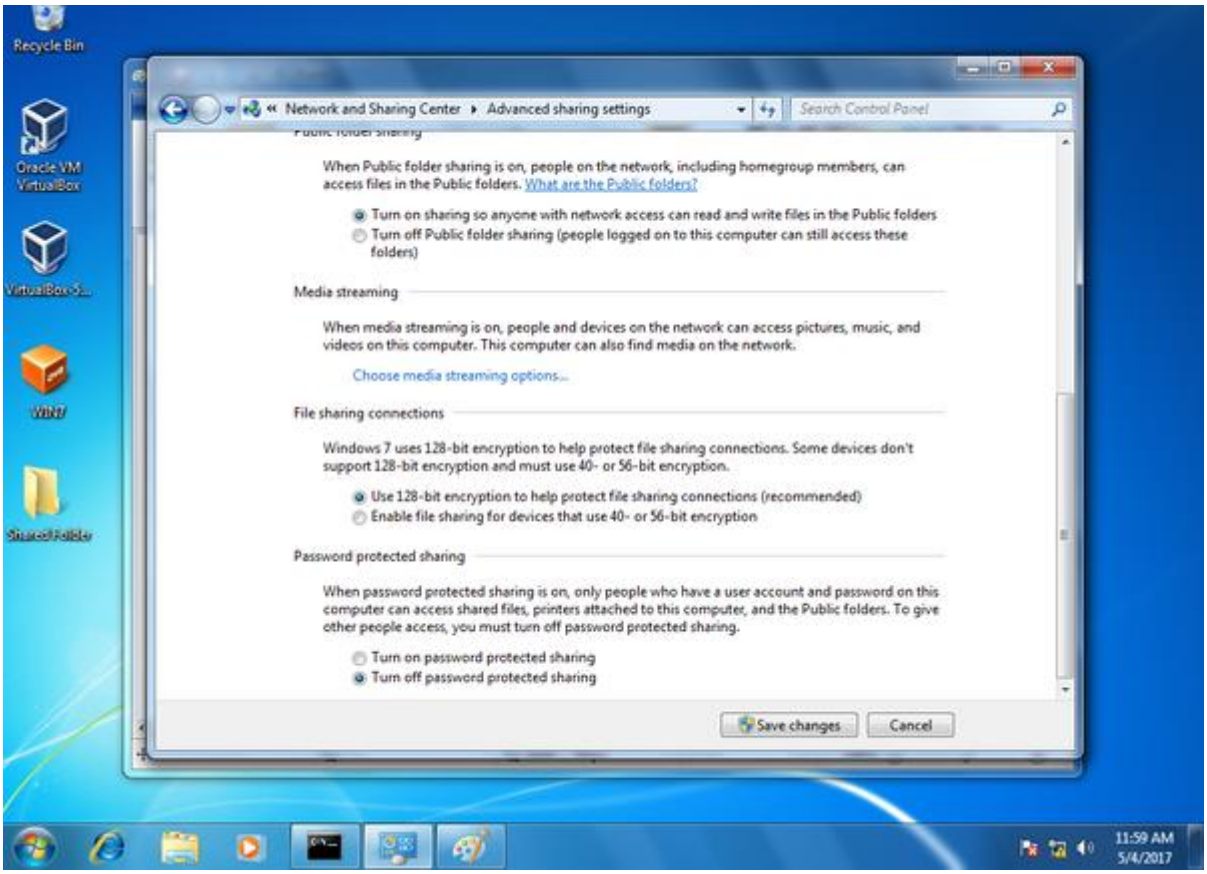
Step 10: Choose Home and Work / Public



There are many settings that need to be changed in both of the options.

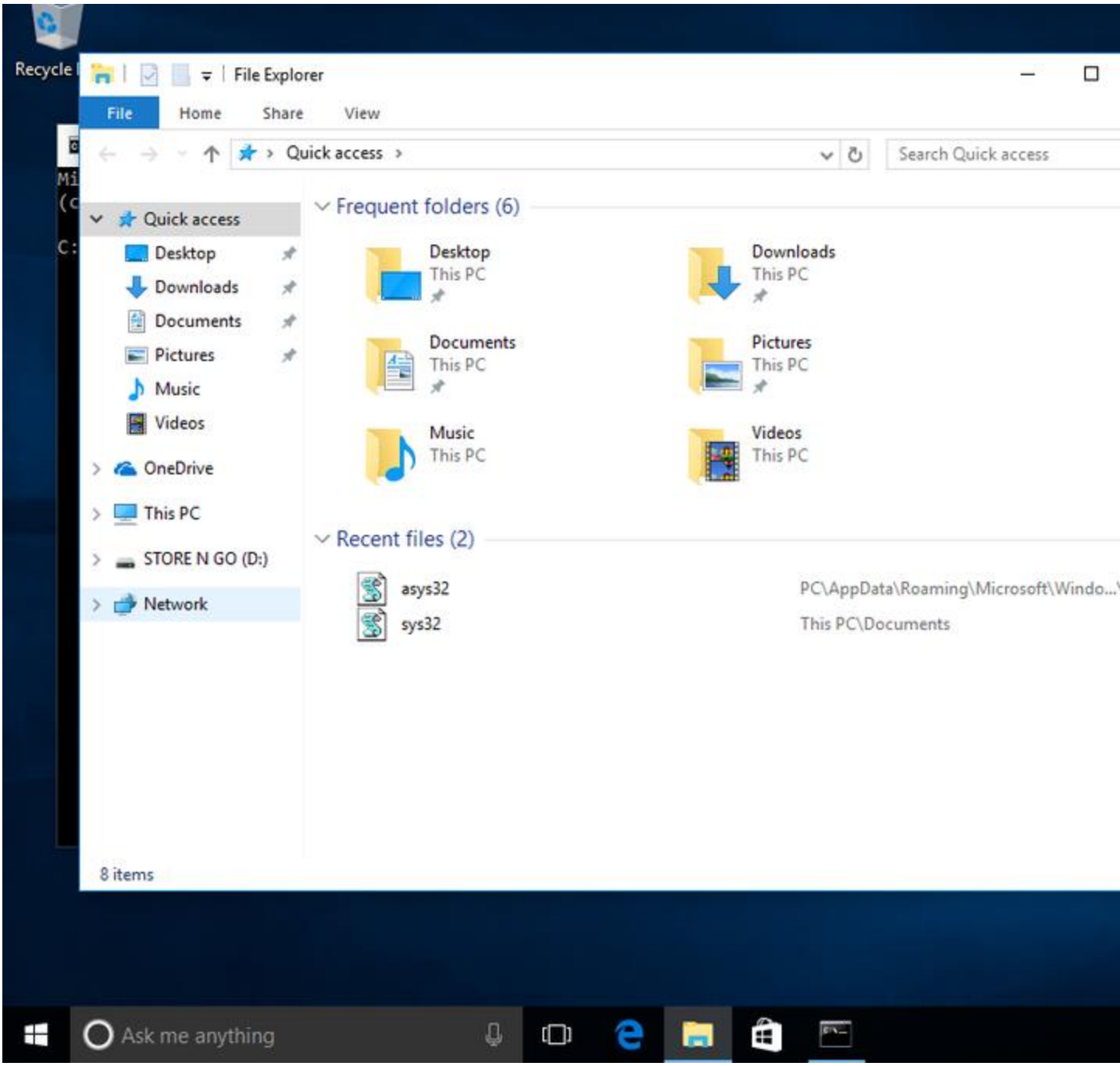
Step 11: Select All Options





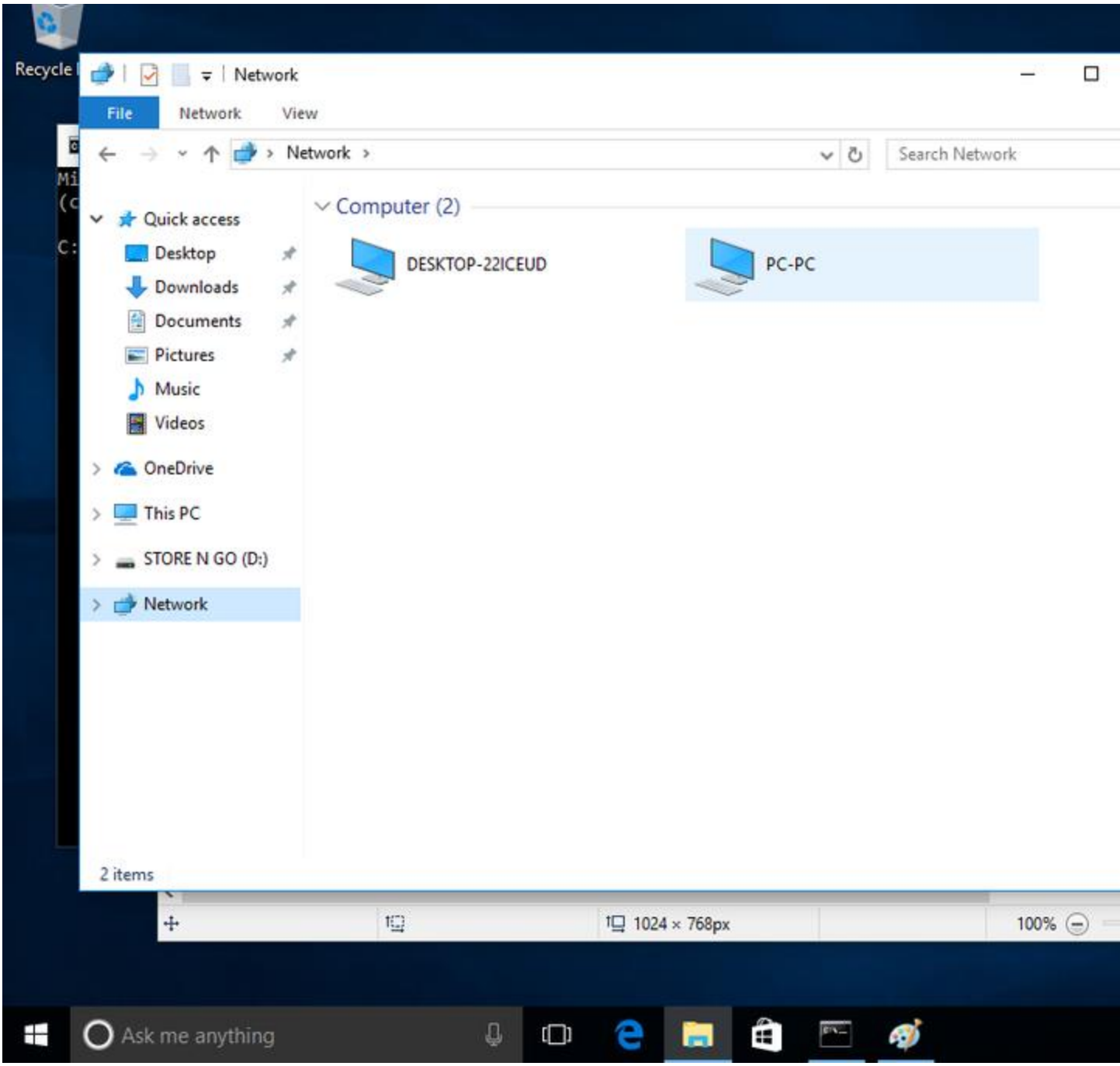
There are going to be many options, the ones you need for the sharing to work are pretty common sense like making sure that your device is allowed to be discovered. And turn off password protected sharing.

Step 12: Go Into Network



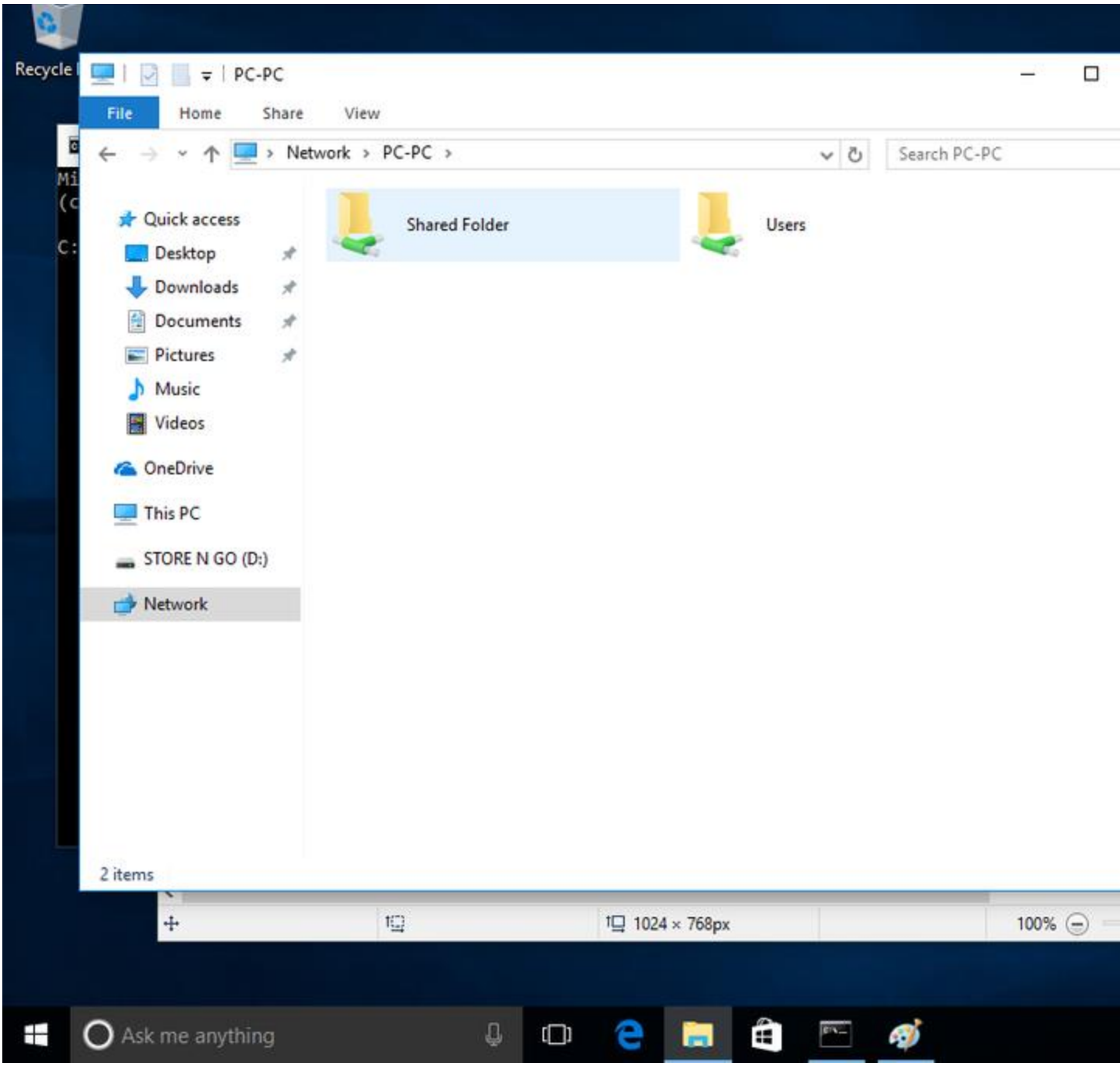
Go onto another computer and open the file explorer. Go into the Network section found on the left hand side at the bottom.

Step 13: Find the Device



Find the original device that the file was shared from.

Step 14: Find the Folder That Was Shared

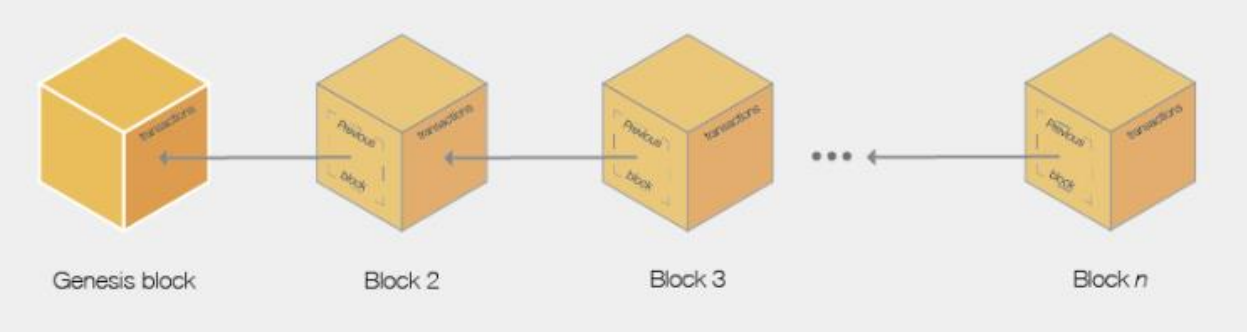


Once you click on the device you will find all the files that were shared from it. You can tell that the folder is shared over the network because it has the green crossroads looking thing under its name.

Genesis Blocks and Sharing Blocks:

Each blockchain application needs a genesis block, which is the very first block of the blockchain.

The genesis block is the first block in any blockchain-based protocol. It is the basis on which additional blocks are added to form a chain of blocks, hence the term blockchain.



This block is sometimes referred to Block 0. Every block in a blockchain stores a reference to the previous block. In the case of Genesis Block, there is no previous block for reference.

In technical terms, it means that the Genesis Block has it's "previous hash" value set to 0. This means that no data was processed before the Genesis Block. All other blocks will have sequential numbers starting by 1, and will have a "previous hash" set to the hash of the previous block.

The hash of genesis block is added to all new transactions in a new block. This combination is used to create its unique hash. This process is repeated until all the new blocks are added to a blockchain.

The number used to refer to the ordering of blocks is known as the block height number. It starts at 0 with the Genesis Block.

Bitcoin genesis block:

The most famous Genesis block was “Bitcoin Chain”,

A coinbase transaction is the first transaction a miner places in a block constructed by them; it is a transaction rewarding the miner in Bitcoins for successfully creating a block to be relayed to the network.

Genesis Block needs:

Without Genesis Block, it would be really difficult for the miners to trust a blockchain and to know when and how it started. This would be extremely impractical.

In theory, there is no real need for a Genesis Block. However, it is necessary to have a starting point that everyone can trust.

As every physical chain must begin with a single physical ring, the Genesis Block is that first, single ring. Or you could see it like the foundation of a building; it may collapse without a solid starting point. You could also view it as the starting point in a race. If every miner just started wherever they wanted, you’d have no consensus point and no basis for trust.

Genesis Block — Block data

The example taken here is the Bitcoin blockchain of the genesis block:

Number of transactions: 1

Transaction fee: $0.00

Block height: 0

Timestamp: 03/02/2009, 18:15

Nonce: 208393

Block difficulty: 1

Block height of a block is the number of blocks in the chain before that given block. Therefore the height of the Genesis block is 0 because no block was placed before it.

Blocks are numbered in a blockchain order. Note that several blocks can have the same height. This could be because of a fork on the network.

The height of a blockchain is the height of the highest block. The highest block in a blockchain is the latest block. For example, at the time of writing, the current block height number of 595130.

Timestamps are generally used to store the date and time of a given event. However, it is important to note that block timestamps are not exactly accurate, and they do not need to be. Block times are accurate only to within an hour or two.

As a miner can change and fake the time of their computer, they are not trusted for chronology. They are simply a rough indicator of when the block was formed by the miner.

Position of a block in the chain does not rely on timestamps.

Nonce or “number used only once” is the number that all miners around the globe are hoping to discover in order to validate a block and receive its mining bonus. Changing the nonce causes a change in the hash. Nonce only applies to blockchains that have a Proof of Work algorithm as consensus algorithm.

Block difficulty is a number that regulates how long it can take for a miner to add a new block to the blockchain.

The difficulty is always fixed at a defined time interval, adjusted once every 2 weeks so that a block can be built at a fixed time interval. So there is a fixed time interval between constructing 2 blocks, which is approximately 10 minutes (in Bitcoin), set by the difficulty of the network.

In technical terms, difficulty is a value that is used to demonstrate, how hard is it to find a hash that will be lower than the target characterized by the system.

Registering Miners and Creating new blocks:

Anyone can apply to become a Blockchain miner. These Blockchain miners install and run a special Blockchain mining software that enables their computers to communicate securely with one another. Once a computer installs the software, joins the network, and begins mining bitcoins, it becomes what is called a 'node.

Step 1: A user signs off on a transaction from their wallet application, attempting to send a certain crypto or token from them to someone else.

Step 2: The transaction is broadcasted by the wallet application and is now awaiting to be picked up by a miner on the according blockchain. As long as it is not picked up, it hovers in a 'pool of unconfirmed transactions'. This pool is a collection of unconfirmed transactions on the network that are waiting to be processed. These unconfirmed transactions are usually not collected in one giant pool, but more often in small subdivided local pools.

Step 3: Miners on the network (sometimes referred to as nodes, but not quite the same!) select transactions from these pools and form them into a 'block'. A block is basically a collection of transactions (at this moment in time, still unconfirmed transactions), in addition to some extra metadata. Every miner constructs their own block of transactions. Multiple miners can select the same transactions to be included in their block.

Step 4: By selecting transactions and adding them to their block, miners create a block of transactions. To add this block of transactions to the blockchain (which means having all the nodes on the blockchain register the transactions in this block), the block first needs a signature (also referred to as a 'proof of work'). This signature is created by solving a very complex mathematical problem that is unique to each block of transactions. Each block has a different mathematical problem, so every miner will work on a different problem unique to the block they formed. Each block's problem is equally hard to solve. In order to solve this mathematical problem, a lot of computational power is used (and thus a lot of electricity). You can compare it to running a calculation on a calculator, only this is much heavier and on done a computer. This is the process referred to as mining. If you want to know more about how the mathematical problem works exactly (it's not actually that complicated), please continue reading below, otherwise, in case you want to keep it a little more simple, skip to step 5.

Step 5: The miner that finds an eligible signature for its block first, broadcasts this block and its signature to all the other miners.

Step 6: Other miners now verify the signature's legitimacy by taking the string of data of the broadcasted block, and hashing it to see if its hash output indeed leads to its included signature of so many zeros (hard to solve, easy to verify, remember?). If it is valid, the other miners will confirm its validity and agree that the block can be added to the blockchain (they reach consensus, aka they all agree with each other, hence the term consensus algorithm). This is also where the definition 'proof of work' comes from. The signature is the 'proof' of the work performed (the computational power that was spent). The block can now be added to the blockchain, and is distributed to all other nodes on the network. The other nodes will accept the block and save it to their transaction data as long as all transactions inside the block can be executed according to the blockchain's history.

Step 7: After a block has been added to the chain, every other block that is added on top of it counts as a 'confirmation' for that block. For example, if my transaction is included in block 502, and the blockchain is 507 blocks long, it means my transaction has 5 confirmations (507–

502). It is referred to as a confirmation because every time another block is added on top of it, the blockchain reaches consensus again on the complete transaction history, including your transaction and your block. You could say that your transaction has been confirmed 5 times by the blockchain at that point. This is also what Etherscan is referring to when showing you your transaction details. The more confirmations your transaction has (aka the deeper the block is embedded in the chain), the harder it is for attackers to alter it (you can read more about how this works here). After a new block is added to the blockchain, all miners need to start over again at step three by forming a new block of transactions. Miners cannot continue (well, they can, but that is quite irrelevant in this article) mining aka solving the problem of the block they were working on earlier because of two reasons:

One: it may contain transactions that have been confirmed by the last block that was added to the blockchain (remember, multiple miners can select/include the same transactions(s) in the block they are solving) already. Any of those transactions initiated again could render them invalid, because the source balance might no longer suffice.

And two: every block needs to add the hash output (signature) of the last block that was added to the blockchain into their metadata. This is what makes it a blockchain. If a miner keeps mining the block they were already working on, other miners will notice that the hash output does not correspond with that of the latest added block on the blockchain, and will therefore reject the block.

Storing Blocks:

Blockchain storage is a way of saving data in a decentralized network, which utilizes the unused hard disk space of users across the world to store files. The decentralized infrastructure is an alternative to centralized cloud storage and can solve many problems found in a centralized system.

Blockchain storage working:

Blockchain relies on distributed ledger technology (DLT). The DLT acts as a decentralized database of information about transactions between various parties. Operations fill the DLT in chronological order and are stored in the ledger as a series of blocks. An interconnected chain is formed between blocks with each one referring to the block before it, thus creating a blockchain

In blockchain storage, files are first broken apart in a process called sharding. Each shard is copied to prevent loss of data should an error occur during transmission. The files are also encrypted with a private key that makes it impossible for it to be viewed by other nodes in the network. The replicated shards are distributed among decentralized nodes all over the world. The interactions are recorded in the blockchain ledger, allowing the system to confirm and

synchronize the transactions across the nodes in the blockchain. Blockchain storage is designed to save these interactions forever and the data can never be changed.

Blockchain storage vs. cloud storage:

Blockchain storage is a potentially cheaper, more secure and more reliable alternative to centralized cloud storage.

Providers of centralized cloud storage prevent data loss by making copies of the data and storing it in different data centers.

The large amount of data that is duplicated in this process can create excessive amounts of surplus information.

Also, cloud storage requires enterprise-grade hardware for its data centers. These factors can make centralized data storage significantly more expensive than blockchain storage.

Blockchain Wallet:

- A blockchain wallet is a digital wallet that allows users to store and manage their Bitcoin, Ether, and other cryptocurrencies.
- Blockchain Wallet can also refer to the wallet service provided by Blockchain, a software company founded by Peter Smith and Nicolas Cary.
- A blockchain wallet allows transfers in cryptocurrencies and the ability to convert them back into a user's local currency.
- A blockchain wallet is a digital wallet that allows users to store, manage, and trade their cryptocurrencies.
- Blockchain Wallet is also the name of a specific wallet service provided by the company Blockchain. This is an E-wallet that allows individuals to store and transfer cryptocurrencies.
- Blockchain Wallet users can manage their balances of Bitcoin, Ether, and other crypto assets.
- Blockchain Wallet charges dynamic fees, meaning that the transaction fees can be different based on factors such as transaction size.
- Blockchain Wallet has a number of security features to prevent theft, including by company insiders.

- E-wallets allow individuals to store cryptocurrencies and other digital assets. In the case of Blockchain Wallet, users can manage their balances of various cryptocurrencies such as the well-known Bitcoin and Ether as well as stellar, Tether, and Paxos Standard.

- Creating an e-wallet with Blockchain Wallet is free, and the account setup process is done online. Individuals must provide an email address and password that will be used to manage the account, and the system will send an automated email requesting that the account be verified.

- Once the wallet is created, the user is provided with a Wallet ID, which is a unique identifier similar to a bank account number.

- Wallet holders can access tier e-wallet by logging into the Blockchain website, or by downloading and accessing a mobile application.

- The Blockchain Wallet interface shows the current wallet balance for crypto-assets and the user's most recent transactions. Users can also access the price charts and see the value of the funds in the chosen local currency of the user. There is also an educational Did You Know section sharing crypto facts and news.

Blockchain Wallet Working:

Users can send a request to another party for a specific amount of bitcoin or other crypto-assets, and the system generates a unique address that can be sent to a third party or converted into a Quick Response code or QR code for short. A QR code is similar to a barcode, which stores financial information and can be read by a digital device.

A unique address is generated each time the user makes a request. Users can also send crypto-assets when someone provides them with a unique address.5 The send-and-receive process is similar to sending or receiving funds through PayPal but uses cryptocurrency instead. PayPal is an online payment provider that acts as a go-between for customers and their banks and credit cards by facilitating online transfers through financial institutions.

Users can also exchange Bitcoin for other crypto-assets and visa-versa, known as swapping. This practice is an easy way to switch out crypto without leaving the security of the Blockchain Wallet.6 Users are shown a quote indicating how much they will receive based on the current exchange rate, with the rate changing depending on how long the user takes to complete the transaction.7 Swaps should take a couple of hours while the transactions are added to each currency's blockchain. However, if it takes longer than six hours, users should contact customer support.8

Blockchain Wallet only allows six crypto-assets for swapping: Bitcoin, Ethereum, Bitcoin Cash, Stellar Lumens, Tether, USD Digital, Wrapped-DGLD.9

Users can also buy or sell crypto through the Buy Crypto interface available to Blockchain Wallet. Buy and sell services are not available in all locations. To make a purchase, a user can either transfer funds from a bank, use a credit or debit card, or use the available cash balance.10 There is a daily limit of $25,000 and a weekly limit of $100,000 as well as a minimum buy order of $5 and a maximum buy order of $25,000.11

Blockchain Wallet Fees

However, it's important to note that the Blockchain Wallet uses a process they call dynamic fees, meaning that the fee charged per transaction can be different based on various factors. Both the transaction size and the conditions of the network at the time of the transaction can greatly impact the size of the fee. Only so many transactions can be processed within a block by the high-powered computers called miners. The miners typically process the transactions that have the highest fees first since it's financially advantageous to them.

Blockchain Wallet offers a priority fee, which could possibly get the transaction processed within an hour. There's also a regular fee, which is cheaper but the transaction would likely take more than an hour. Fees can also be customized by the customer. However, if the customer sets the fee too low, the transfer or transaction could be delayed or rejected.12

Blockchain Wallet Security

Wallet security is an important consideration for users, as a compromised account may result in users losing control of their assets. Blockchain Wallet has several levels of security to protect user funds from any possible attacker, including the company itself.

Passwords

Like other digital services, Blockchain Wallet accounts require passwords for the users' protection. However, the Blockchain company does not store user passwords, and cannot reset the password if lost. This measure prevents company insiders from being able to steal cryptocurrencies. If a user forgets or loses their password, the account can only be recovered with a mnemonic seed.13