UNIVERSITY of NICOSIA

MSc in Digital Currency

DFIN-511: Introduction to Digital Currencies

Session 5
Bitcoin in practice Part 2
Bitcoin Core,
Constructing a transaction, Segwit, Lightning network, Mining pools

DFIN-511: Introduction to Digital Currencies

UNIVERSITY of NICOSIA

Objectives of Session 5

- Understanding Bitcoin Core and how it works
- Understand the functionality of Bitcoin Core
- Get more familiar with the mining process and mining pools

- ***This is the last of the three introductory sessions on the technical aspects around the emerging field of cryptocurrencies. Exploring transactions over the basic Bitcoin client is the goal of this session, along with introducing scaling proposals such as SegWit and the Lightning Network.***
- ***In the next sessions we'll explore alternative currencies (altcoins) and alternate uses of the blockchain and then switch back to more business oriented subjects, under the view of cryptocurrencies.***

Agenda

1. Bitcoin Core
2. Bitcoin core functionality
3. Mining and mining pools
4. Segregated Witness
5. Lightning Network
6. A fork in the Road (a primer)
7. Conclusions
8. Further Reading

1. Bitcoin Core

Bitcoind

- Bitcoind was the first client in the history of Bitcoin and it is a full client that implements the Bitcoin protocol. It is operated from the command line and can be used to send remote procedure call (RPC)-based commands. It is now mostly useful for programmers and advanced users

- Bitcoind was available for most existing popular operating systems, including Windows, Linux, and MacOS. In addition, it could also be adapted or extended by building from its source code that is found in the Bitcoin github repository (https://github.com/bitcoin/bitcoin).

- In order to install and operate bitcoind you needed experience with the command line. More advanced command line operations within Bitcoin Core will be covered later in other modules of the MSc program.

Bitcoin Core

- Bitcoin Core (previously known as Bitcoin-Qt) is the third Bitcoin client, written in C++, developed by Wladimir J. van der Laan and based on the original reference code by Satoshi Nakamoto.

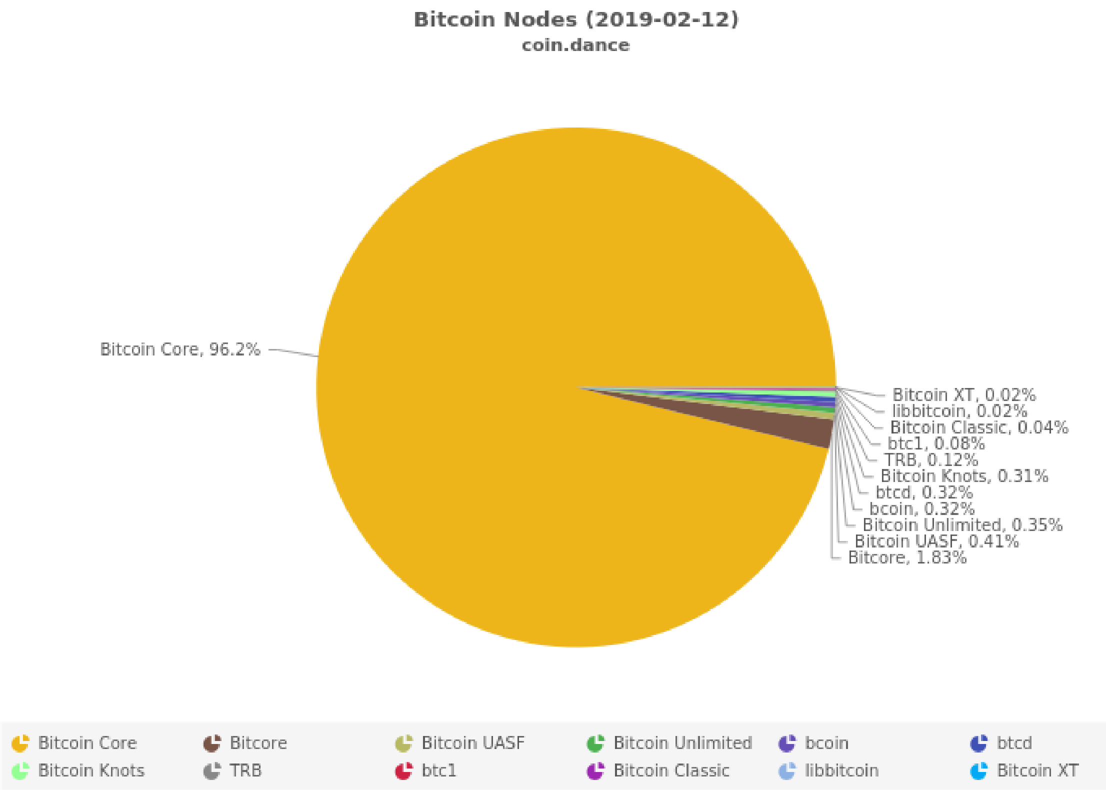
- It has been bundled with bitcoind since version 0.5 and can be considered to be a Graphical User Interface (GUI) front-end to bitcoind.

- Besides Bitcoin Core, other implementations also exist:
  - Bitcoin Unlimited, which is a fork of the Bitcoin Core reference client with the intention of providing a voice to all stakeholders in the Bitcoin ecosystem. The project seeks to remove existing practical barriers by allowing nodes to choose the maximum block size they accept as valid. More information here. It is also a full node implementation for the Bitcoin Cash network.
  - Users indicate which block size limit they prefer, find the limit via majority consensus and track the largest proof-of-work, regardless of block size. In case of a block of >1 megabyte in size accepted by Bitcoin Unlimited and rejected by nodes with a block size limit, a fork occurs. This will force two separate blockchains with Bitcoin Unlimited nodes following the chain with the largest proof-of-work.

Bitcoin Core 0.17.1

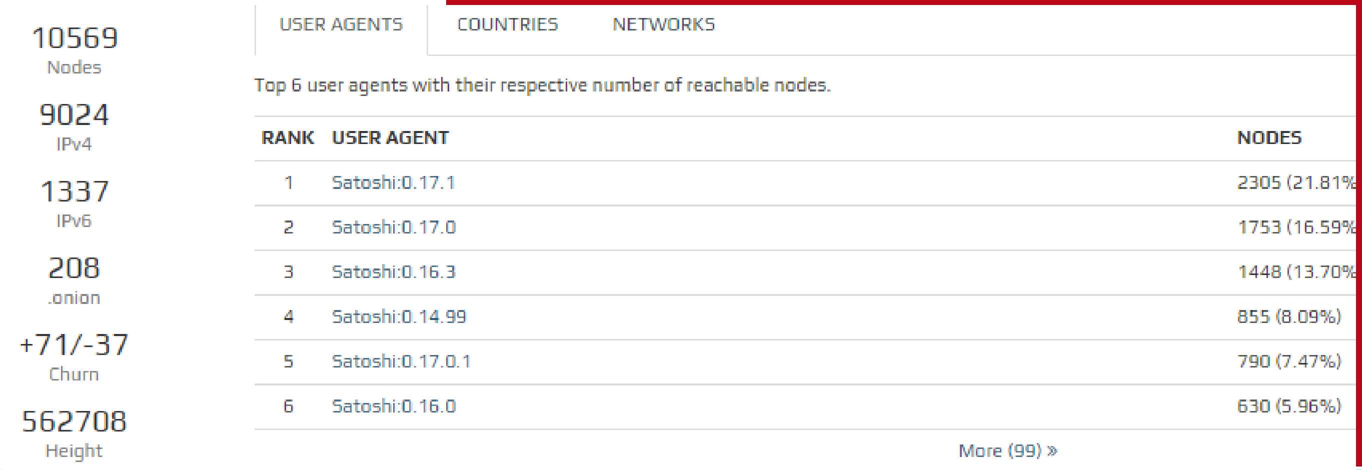
- New versions of Bitcoin Core are typically released every 2-3 months enhancing some minor performance improvements.
- A detailed guide towards upgrading your client to the **latest version (0.17.1)** can be found here:
  - https://bitcoin.org/en/release/v0.17.1#how-to-upgrade
- Important Improvements incorporated in previous releases (0.16.1 & 0.16.0) can be found here and here
- The most notable had to do with:
  - Full support for Segwit in wallet and user interfaces
  - Full support for Segwit addresses
  - Creation of HD-wallets by default
  - Replace-by-Fee as the Default Sending Option
  - Removal of miner block size option
- A denial-of-service vulnerability exploitable by miners was discovered in Bitcoin Core versions 0.14.0 up to 0.16.2. It was then immediately recommended to upgrade any of the vulnerable versions to 0.16.3.

Node Distribution



According to https://coin.dance/nodes the number of Bitcoin Core nodes kept increasing until late 2017 but since then no significant fluctuation on the number of nodes is witnessed. What is the main reason behind this?

Sources: coin.dance and https://bitnodes.earn.com/nodes/?q=



10569
Nodes

9024
IPv4

1337
IPv6

208
.onion

+71/-37
Churn

562708
Height

USER AGENTS | COUNTRIES | NETWORKS

Top 6 user agents with their respective number of reachable nodes.

RANK	USER AGENT	NODES
1	Satoshi:0.17.1	2305 (21.81%
2	Satoshi:0.17.0	1753 (16.59%
3	Satoshi:0.16.3	1448 (13.70%
4	Satoshi:0.14.99	855 (8.09%)
5	Satoshi:0.17.0.1	790 (7.47%)
6	Satoshi:0.16.0	630 (5.96%)

More (99) »

2. Bitcoin Core functionality

Bitcoin Installation

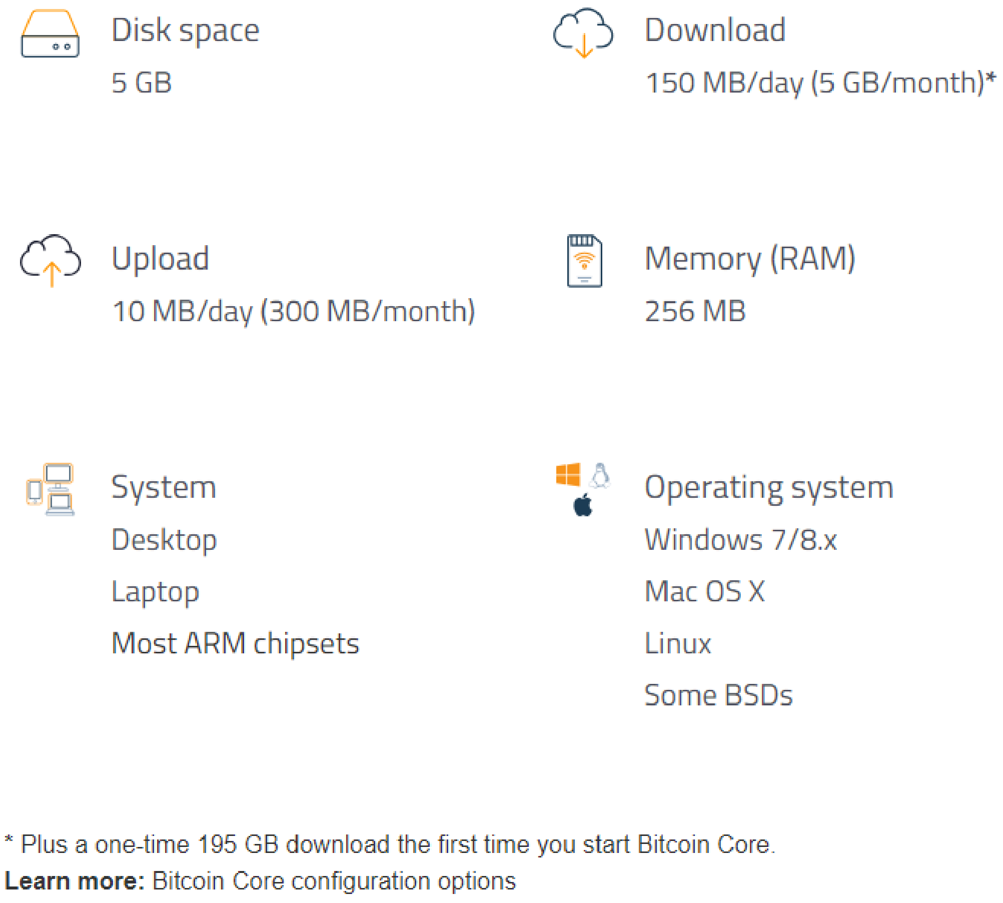
You can download the appropriate Bitcoin installer from https://bitcoin.org/en/download

After installation you will have to wait until the initial synchronization of the entire Bitcoin blockchain is done, which may take, depending on your bandwidth and the number of connected Bitcoin nodes, several days.

In an older computer, the full node may never synchronize as the files may eventually seem to get corrupted.

It is recommended for users who wish to download and experiment with Bitcoin Core, to ensure that they have the storage and bandwidth capabilities.

Bitcoin Core Minimum Requirements



Disk space
5 GB

Download
150 MB/day (5 GB/month)*

Upload
10 MB/day (300 MB/month)

Memory (RAM)
256 MB

System
Desktop
Laptop
Most ARM chipsets

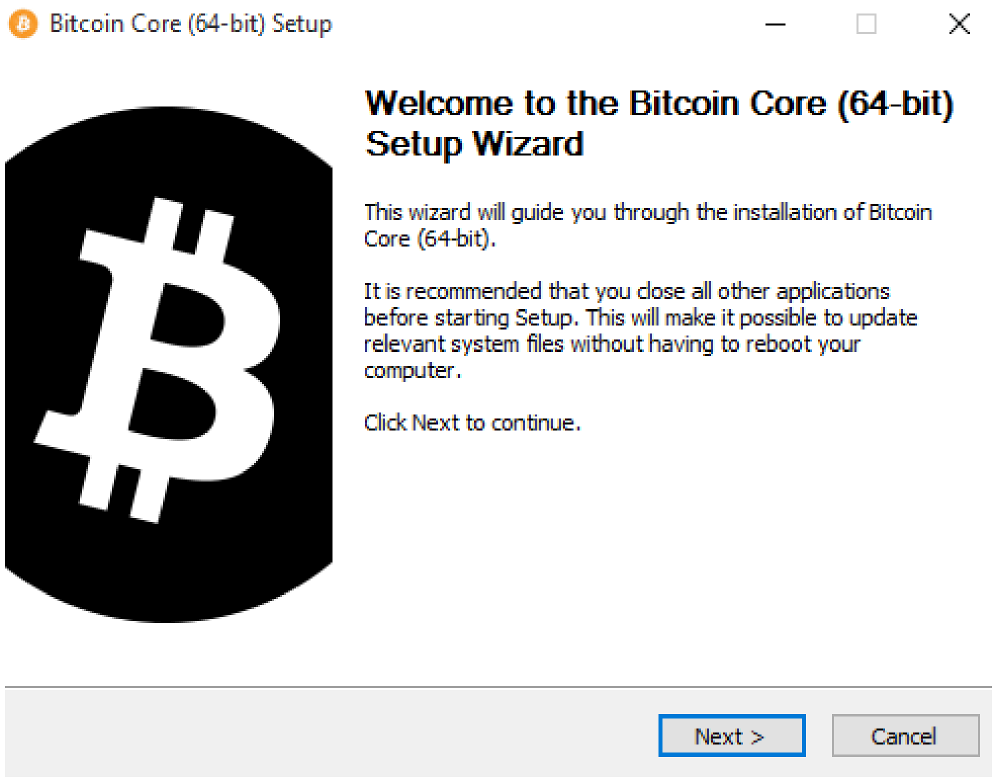
Operating system
Windows 7/8.x
Mac OS X
Linux
Some BSDs

* Plus a one-time 195 GB download the first time you start Bitcoin Core.

Learn more: Bitcoin Core configuration options

Bitcoin Core

- Demonstration in Windows (Source: https://bitcoin.org/en/full-node#windows-10)



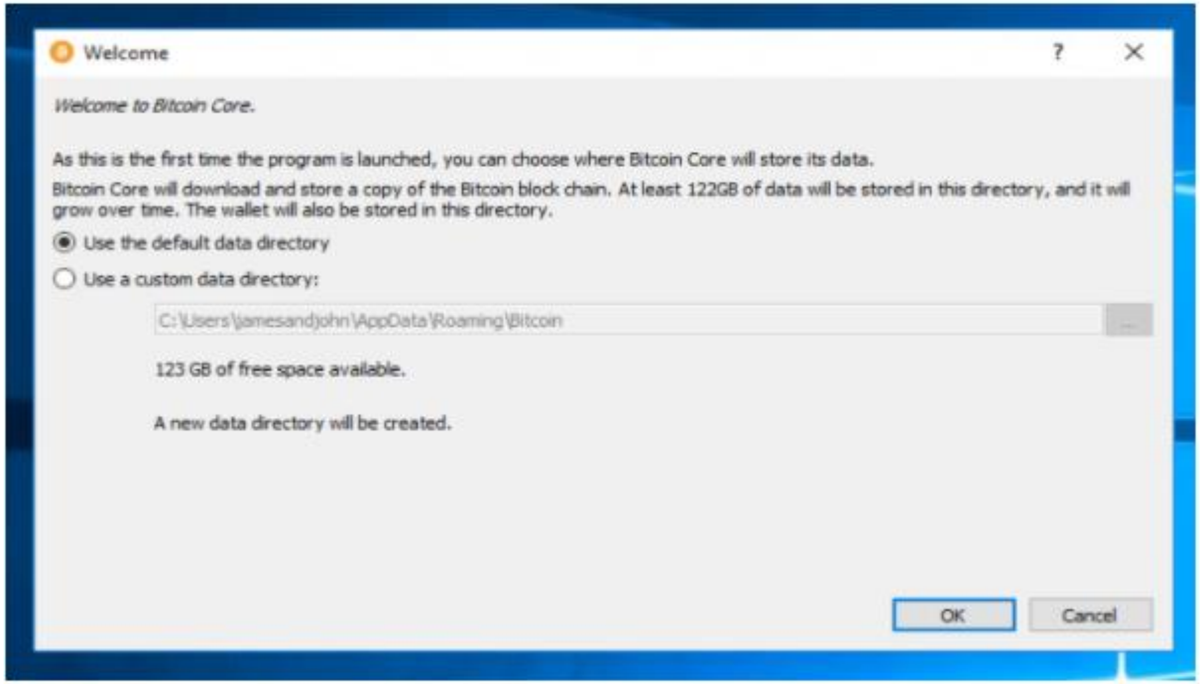
Welcome to the Bitcoin Core (64-bit) Setup Wizard

This wizard will guide you through the installation of Bitcoin Core (64-bit).

It is recommended that you close all other applications before starting Setup. This will make it possible to update relevant system files without having to reboot your computer.

Click Next to continue.

You will be prompted to choose a directory to store the Bitcoin block chain and your wallet. Unless you have a separate partition or drive you want to use, click Ok to use the default.



Welcome to Bitcoin Core.

As this is the first time the program is launched, you can choose where Bitcoin Core will store its data.

Bitcoin Core will download and store a copy of the Bitcoin block chain. At least 122GB of data will be stored in this directory, and it will grow over time. The wallet will also be stored in this directory.

● Use the default data directory

○ Use a custom data directory:

C:\Users\jamesandjohn\AppData\Roaming\Bitcoin

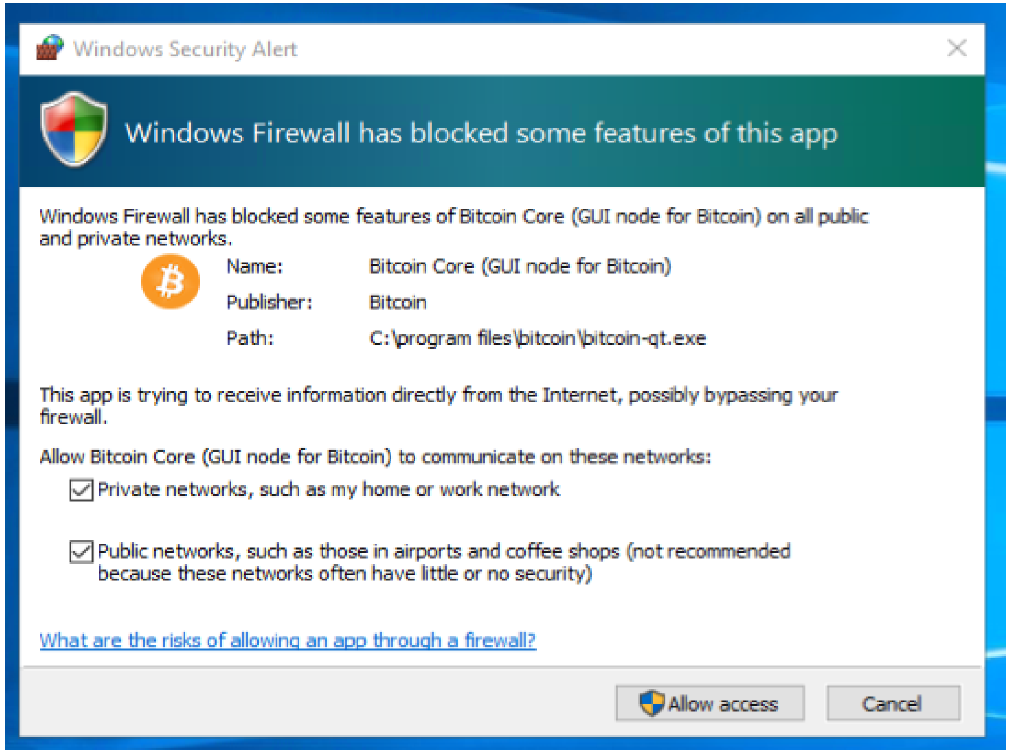
123 GB of free space available.

A new data directory will be created.

Bitcoin Core

- Demonstration in Windows (Source: https://bitcoin.org/en/full-node#windows-10)

Your firewall may block Bitcoin Core from making outbound connections. It's safe to allow Bitcoin Core to use all networks. (Note: you will still need to configure inbound connections as described later in the Network Configuration section.)



Windows Firewall has blocked some features of this app

Windows Firewall has blocked some features of Bitcoin Core (GUI node for Bitcoin) on all public and private networks.

Name: Bitcoin Core (GUI node for Bitcoin)

Publisher: Bitcoin

Path: C:\program files\bitcoin\bitcoin-qt.exe

This app is trying to receive information directly from the Internet, possibly bypassing your firewall.

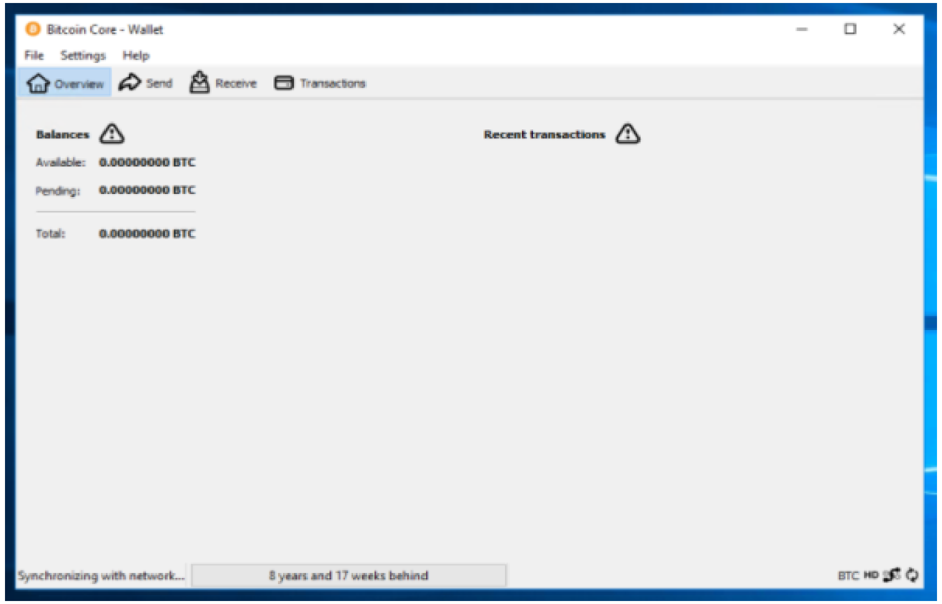
Allow Bitcoin Core (GUI node for Bitcoin) to communicate on these networks:

☑ Private networks, such as my home or work network

☑ Public networks, such as those in airports and coffee shops (not recommended because these networks often have little or no security)

What are the risks of allowing an app through a firewall?

Bitcoin Core GUI will begin to download the block chain. This step will take at least several days, and it may take much more time on a slow Internet connection or with a slow computer. During the download, Bitcoin Core will use a significant part of your connection bandwidth. You can stop Bitcoin Core at any time by closing it; it will resume from the point where it stopped the next time you start it.



Balances ⚠

Available: 0.00000000 BTC

Pending: 0.00000000 BTC

Total: 0.00000000 BTC

Recent transactions ⚠

Synchronizing with network... 8 years and 17 weeks behind

After download is complete, you may use Bitcoin Core as your wallet or you can just let it run to help support the Bitcoin network.

*Inbound connections must be allowed to support the Bitcoin network. To allow inbound connections, perform the following additional steps: https://bitcoin.org/en/full-node#network-configuration

Bitcoin clients

Continuing with the Windows demonstration, the “Bitcoin” folder in a user’s “AppData” folder in Windows is very important because it stores (among others):

- The Bitcoin configuration file (the user is able to generate it: https://jlopp.github.io/bitcoin-core-config-generator/)
- Your Bitcoin wallet (the wallet.dat file)
- The “blocks” folder which stores a full copy of the Bitcoin blockchain, whose current size is about 200GB

Command Line Interface (CLI)

The complete reference to the Bitcoin client Application Programming Interface (API) can be found here: https://bitcoincore.org/en/doc/0.17.0/

Using the command line interface you can:

- Get information about the status of the Bitcoin network
- Manage your wallet
- Explore and decode transactions
- Explore blocks
- Create, sign and submit transactions with unspent outputs

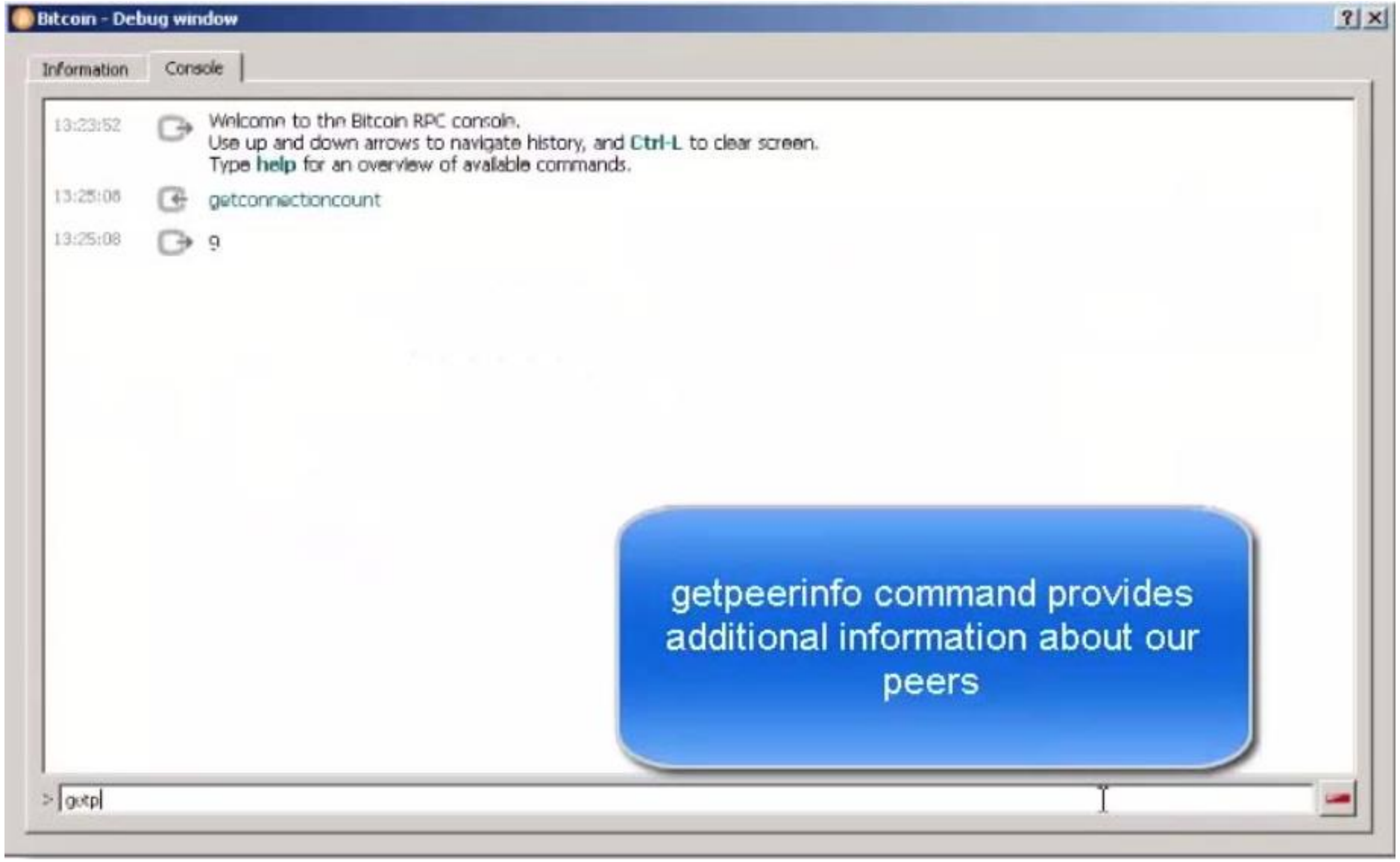
Bitcoin Core – Getting network information

Commands to use:

Command	Description
getconnectioncount	Returns the number of connections to other nodes.
getpeerinfo	Returns data about each connected node.
getdifficulty	Returns the proof-of-work difficulty as a multiple of the minimum difficulty.
getblockcount	Returns the number of blocks in the longest block chain.
getmininginfo	Returns an object containing mining-related information: • blocks • currentblocksize • currentblocktx • difficulty • pooledtx • chain • warnings • networkhashps
generatetoaddress	Mine blocks immediately to a specified address (before the RPC call returns)

Bitcoin Core – Getting network information

Video illustration below:



```
13:23:52   Welcome to the Bitcoin RPC console.
           Use up and down arrows to navigate history, and Ctrl-L to clear screen.
           Type help for an overview of available commands.
13:25:08   getconnectioncount
13:25:08   9
> getp
```

getpeerinfo command provides additional information about our peers

Managing your wallet (CLI)

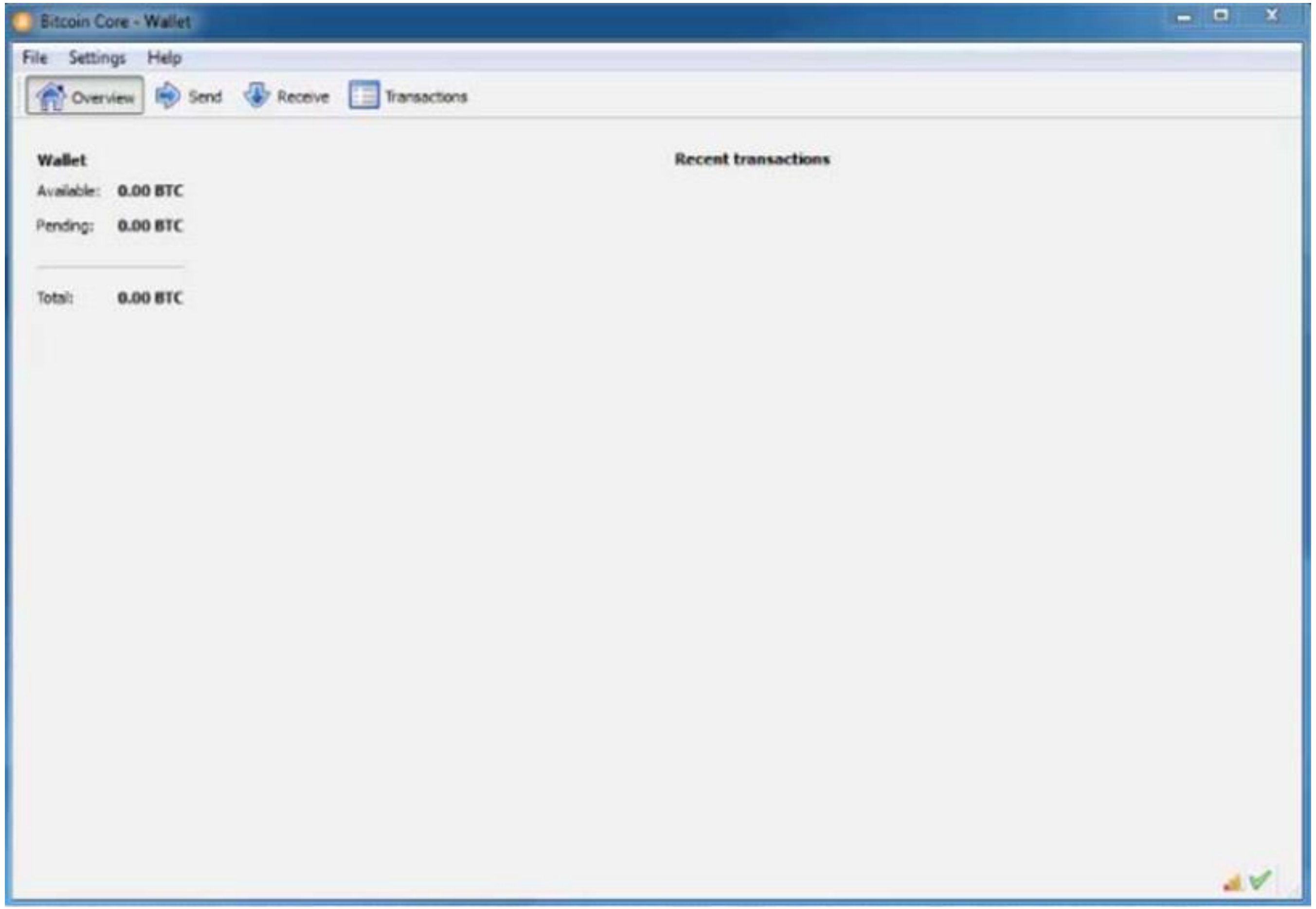
Command	Parameters	Description
getnewaddress	[account]	Returns a new bitcoin address for receiving payments. If [account] is specified payments received with the address will be credited to [account].
dumpprivkey	<bitcoinaddress>	Reveals the private key corresponding to <bitcoinaddress>
importprivkey	<bitcoinprivkey> [label] [rescan=true]	Adds a private key (as returned by dumpprivkey) to your wallet. This may take a while, as a rescan is done, looking for existing transactions. Note: There's no need to import public key, as in ECDSA (unlike RSA) this can be computed from the private key.
getaccountaddress	<account>	Returns the current bitcoin address for receiving payments to this account. If <account> does not exist, it will be created along with an associated new address that will be returned.
getreceivedbyaddress	<bitcoinaddress> [minconf=1]	Returns the amount received by <bitcoinaddress> in transactions with at least [minconf] confirmations. It correctly handles the case where someone has sent to the address in multiple transactions. Keep in mind that addresses are only ever used for receiving transactions. Works only for addresses in the local wallet, external addresses will always show 0.

Managing your wallet (CLI)

Command	Parameters	Description
listtransactions	[account] [count=10] [from=0]	Returns up to [count] most recent transactions skipping the first [from] transactions for account [account]. If [account] not provided it'll return recent transactions from all accounts.
getaddressesbyaccount	<account>	Returns the list of addresses for the given account.
encryptwallet	<passphrase>	Encrypts the wallet with <passphrase>
walletlock		Removes the wallet encryption key from memory, locking the wallet. After calling this method, you will need to call walletpassphrase again before being able to call any methods which require the wallet to be unlocked.
walletpassphrase	<passphrase> <timeout>	Stores the wallet decryption key in memory for <timeout> seconds.
walletpassphrasechange	<oldpassphrase> <newpassphrase>	Changes the wallet passphrase from <oldpassphrase> to <newpassphrase>.

Managing your wallet (CLI) - Vanitygen

Video illustration below:



Wallet

Available: **0.00 BTC**

Pending: **0.00 BTC**

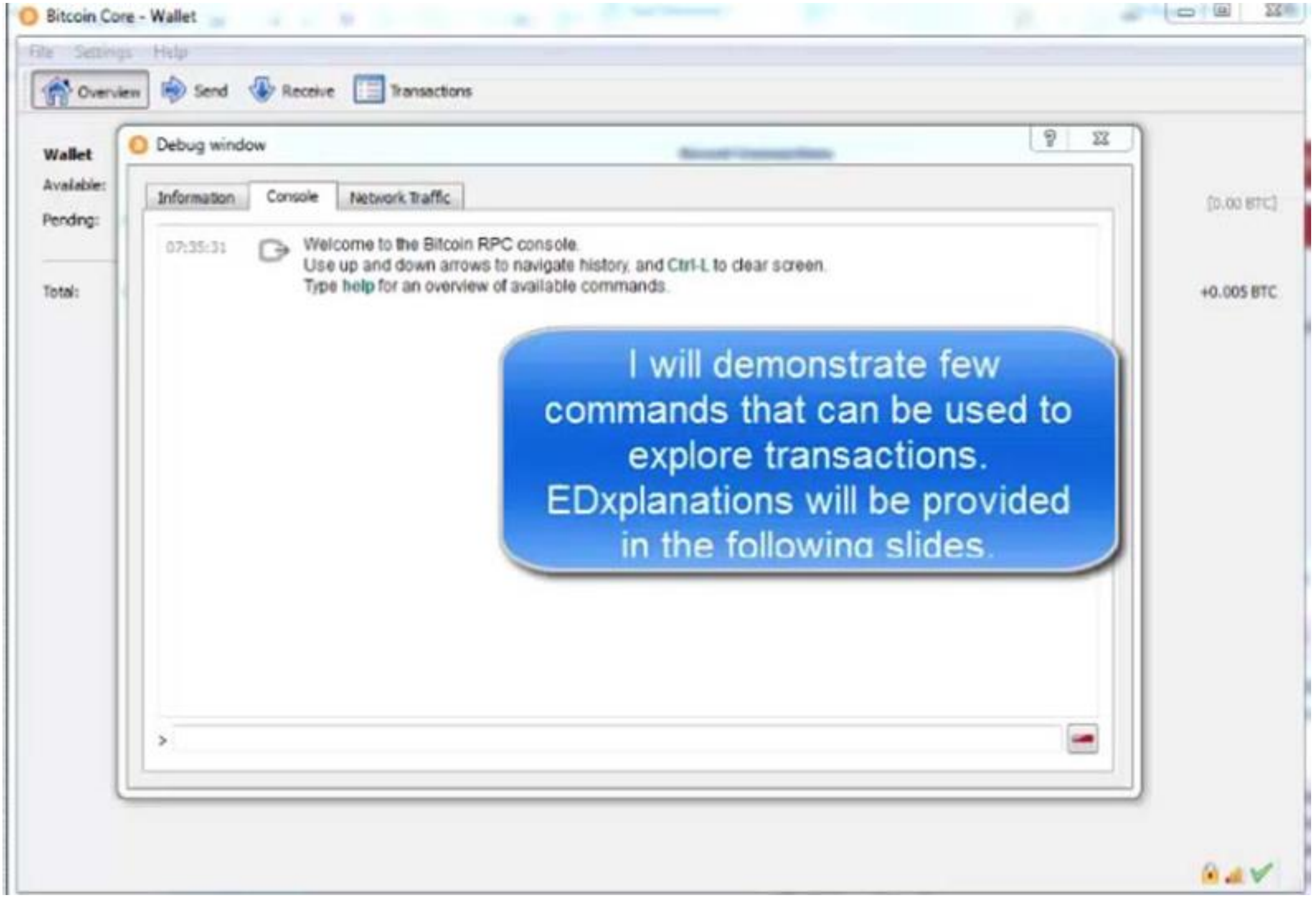
Total: **0.00 BTC**

Managing your wallet (CLI)

Command	Parameters	Description
gettransaction	<txid>	Returns an object about the given transaction containing: • "amount" : total amount of the transaction • "confirmations" : number of confirmations of the transaction • "txid" : the transaction ID • "time" : time associated with the transaction[1]. • "details" - An array of objects containing: • "account" • "address" • "category" • "amount" • "fee"
getrawtransaction	<txid> [verbose=0]	Returns raw transaction representation for given transaction id.
decoderawtransaction	<hex string>	Produces a human-readable JSON object for a raw transaction
getaccountaddress	<account>	Returns the current bitcoin address for receiving payments to this account. If <account> does not exist, it will be created along with an associated new address that will be returned.
getreceivedbyaddress	<bitcoinaddress> [minconf=1]	Returns the amount received by <bitcoinaddress> in transactions with at least [minconf] confirmations. It correctly handles the case where someone has sent to the address in multiple transactions. Keep in mind that addresses are only ever used for receiving transactions. Works only for addresses in the local wallet, external addresses will always show 0.

Managing your wallet (CLI) - Vanitygen

Video illustration below:



```
07:35:31   Welcome to the Bitcoin RPC console.
           Use up and down arrows to navigate history, and Ctrl-L to clear screen.
           Type help for an overview of available commands.
```

I will demonstrate few commands that can be used to explore transactions. EDxplanations will be provided in the following slides.

Exploring Transactions (CLI)

```
getrawtransaction
0408953d670d0f268b70f449772bd3d1c1b80c690be6f3017e3f9bdaa01c0b6c

0100000002918 1c1d7b6b4fc7e2f1f1ee43dfeb778468292a7b49a3e26c9c70b2
68fbc9ade000000006c493046022100cc2a0d920c154014d4e7f93878307b1b5a
eab8bba25288e1f00573fe05cf8aac022100b8269506e5c431d55bbe4c6850e98
3db8b9d9016cdece8dd7555a4ebf22816ba012102c8515f4e0512378032d44d5e
d3888bcd50be103ee26e0279f52a1fb935bb8f71ffffffff0e4d456390086dd62
2ce8be50672de7943d2a1d0ee78593a6b4e5c7a9cb6c9c3000000008a47304402
200f9e6e9bacd1f0d44525265455e92014faba5931a0ee8517664777d38c090d9
5022000905089d5bfcf8509589984f9b79182ea1bcbf6e6ae16f765efd8390f3c
835201410468 1901c41fe94cabc8e809ca1f830fd6bc953d88254337db8ab1db9
448ecd8bb2fec05f74f38abb05f4fd5d7040f9c011365967c24672514c2a40f20
dde07094ffffffff0220a10700000000001976a9148b87c4f4c177a46de7d50b7
dd9840c16caa4728088acc07a100000000000001976a91452dadb8a8948da050406
72a11eacaecd916aa39288ac00000000
```

The gettransaction command returns a transaction in a simplified form.

To retrieve the full transaction code we can use two commands: getrawtransaction and decoderawtransaction.

The getrawtransaction command uses the transaction ID as a parameter and returns the full transaction as a “raw” hex string, exactly as it is on the Bitcoin network.

Exploring Transactions (CLI)

```
decoderawtransaction 0100000029181c1d7b6b4fc7e2f1f1ee43dfeb…
```

```
{
"txid" :
"0408953d670d0f268b70f449772bd3d1c1b80c690be6f3017e3f9bdaa01c0b6c",
"version" : 1,
"locktime" : 0,
"vin" : [
{
"txid" :
"de9abc8f260bc7c9263e9ab4a792824678b7fe3de41e1f2f7efcb4b6d7c18191",
"vout" : 0,
"scriptSig" : {
"asm" :
"3046022100cc2a0d920c154014d4e7f93878307b1b5aeab8bba25288e1f00573fe05cf8a
ac022100b8269506e5c431d55bbe4c6850e983db8b9d9016cdece8dd7555a4ebf22816ba0
1 02c8515f4e0512378032d44d5ed3888bcd50be103ee26e0279f52a1fb935bb8f71",
"hex" :
"493046022100cc2a0d920c154014d4e7f93878307b1b5aeab8bba25288e1f00573fe05cf
8aac022100b8269506e5c431d55bbe4c6850e983db8b9d9016cdece8dd7555a4ebf22816b
a012102c8515f4e0512378032d44d5ed3888bcd50be103ee26e0279f52a1fb935bb8f71"
},
"sequence" : 4294967295
},
{
"txid" :
"c3c9b69c7a5c4e6b3a5978eed0a1d24379de7206e58bce22d66d089063454d0e",
"vout" : 0,
"scriptSig" : {
"asm" :
"304402200f9e6e9bacd1f0d44525265455e92014faba5931a0ee8517664777d38c0
```

The decoderawtransaction command shows all the parts of this transaction, including the transaction inputs and outputs.

Exploring Transactions (CLI)

```
"vin" : [
{
"txid" : "de9abc8f260bc7c9263e9ab4a792824678b7fe3de41e1f2f7efcb4b6d7c18191",
"vout" : 0,
"scriptSig" : {
"asm" :
"3046022100cc2a0d920c154014d4e7f93878307b1b5aeab8bba25288e1f00573fe05cf8aac0
22100b8269506e5c431d55bbe4c6850e983db8b9d9016cdece8dd7555a4ebf22816ba01
02c8515f4e0512378032d44d5ed3888bcd50be103ee26e0279f52a1fb935bb8f71",
"hex" : "49304…"
},
"sequence" : 4294967295
},
{
"txid" : "c3c9b69c7a5c4e6b3a5978eed0a1d24379de7206e58bce22d66d089063454d0e",
"vout" : 0,
"scriptSig" : {
"asm" :
"304402200f9e6e9bacd1f0d44525265455e92014faba5931a0ee8517664777d38c090d95022
000905089d5bfcf8509589984f9b79182ea1bcbf6e6ae16f765efd8390f3c835201
04681901c41fe94cabc8e809ca1f830fd6bc953d88254337db8ab1db9448ecd8bb2fec05f74f
38abb05f4fd5d7040f9c011365967c24672514c2a40f20dde07094",
"hex" : "4730…"
},
"sequence" : 4294967295
}
],
```

This transaction has two inputs as outputs of previously confirmed transactions with IDs starting with de9a and c3c9 respectively

Exploring Transactions (CLI)

and one output of 5 mBits to our new 1Dima... address.

```
"vout" : [
{
"value" : 0.00500000,
"n" : 0,
"scriptPubKey" : {
"asm" : "OP_DUP OP_HASH160 8b87c4f4c177a46de7d50b7dd9840c16caa47280
OP_EQUALVERIFY OP_CHECKSIG",
"hex" : "76a9148b87c4f4c177a46de7d50b7dd9840c16caa4728088ac",
"reqSigs" : 1,
"type" : "pubkeyhash",
"addresses" : [
"1Dima5vfScYn342c7SfcX2pFYSu3rqhtKz"
]
```

Exploring Transactions (CLI)

```
gettransaction
0408953d670d0f268b70f449772bd3d1c1b80c690be6f3017e3f9bdaa01c0b6c
{
"amount" : -0.01080000,
"fee" : 0.01080000,
"confirmations" : 2,
"blockhash" :
"0000000000000000232049 9cc4e60f5a515a03b088925f78b728bdf79ed5ac86",
"blockindex" : 189,
"blocktime" : 1399872120,
"txid" :
"0408953d670d0f268b70f449772bd3d1c1b80c690be6f3017e3f9bdaa01c0b6c",
"walletconflicts" : [
],
"time" : 1399871859,
"timereceived" : 1399871859,
"details" : [
{
…
```

Once the transaction is confirmed, by inclusion in the block, the gettransaction command returns additional information, showing the block hash (identifier) and block index for the block in which the transaction was included.

Multi-signature transactions

Bitcoin has a feature called “multi-signature”, in which a transaction must have multiple independent approvals before the funds can be spent. Multi-signature (or “multisig”) transactions prevent thieves from stealing the contents of a wallet by simply gaining access to a single key-pair.

The most common scheme for multi-signature transactions is to employ an “M-of-N scheme”, for instance, 2-of-3, in which case, at least 2 people (i.e. signers) must approve a transaction.

The way this works is that 3 public keys are listed as potential signers of a transaction, and at least 2 of those must be used to create a transaction’s signature in order to spend it.

There is a limitation of 15 public keys that can be used to sign a transaction, and any combination of the “M-of-N scheme” may be used. However, currently the “2-of-3 scheme” is the most practical.

Some popular multisig wallets can be found here: https://coinsutra.com/best-multi-signature-bitcoin-wallets/

Multi-signature transactions

The general form of a multisig (“M-of-N”) transaction script looks like:

“M <Public Key 1> <Public Key 2> … <Public Key N> N OP_CHECKMULTISIG”

In the case of a “2-of-3” multisig transaction the script looks like:

“2 <Public Key A> <Public Key B> <Public Key C> 3 OP_CHECKMULTISIG”

The above forms a “locking script”, which can only be unlocked by an equivalent “unlocking script”, which contains 2 or more signatures computed from the signer’s private keys and corresponding to the listed public keys, as follows:

“OP_0 <Signature B> <Signature C>”

The above “locking” and “unlocking” script, together form a “validation script” which serves to enable multisig wallets:

“OP_0 <Signature B> <Signature C>

2 <Public Key A> <Public Key B> <Public Key C> 3 OP_CHECKMULTISIG”

(Validation script)

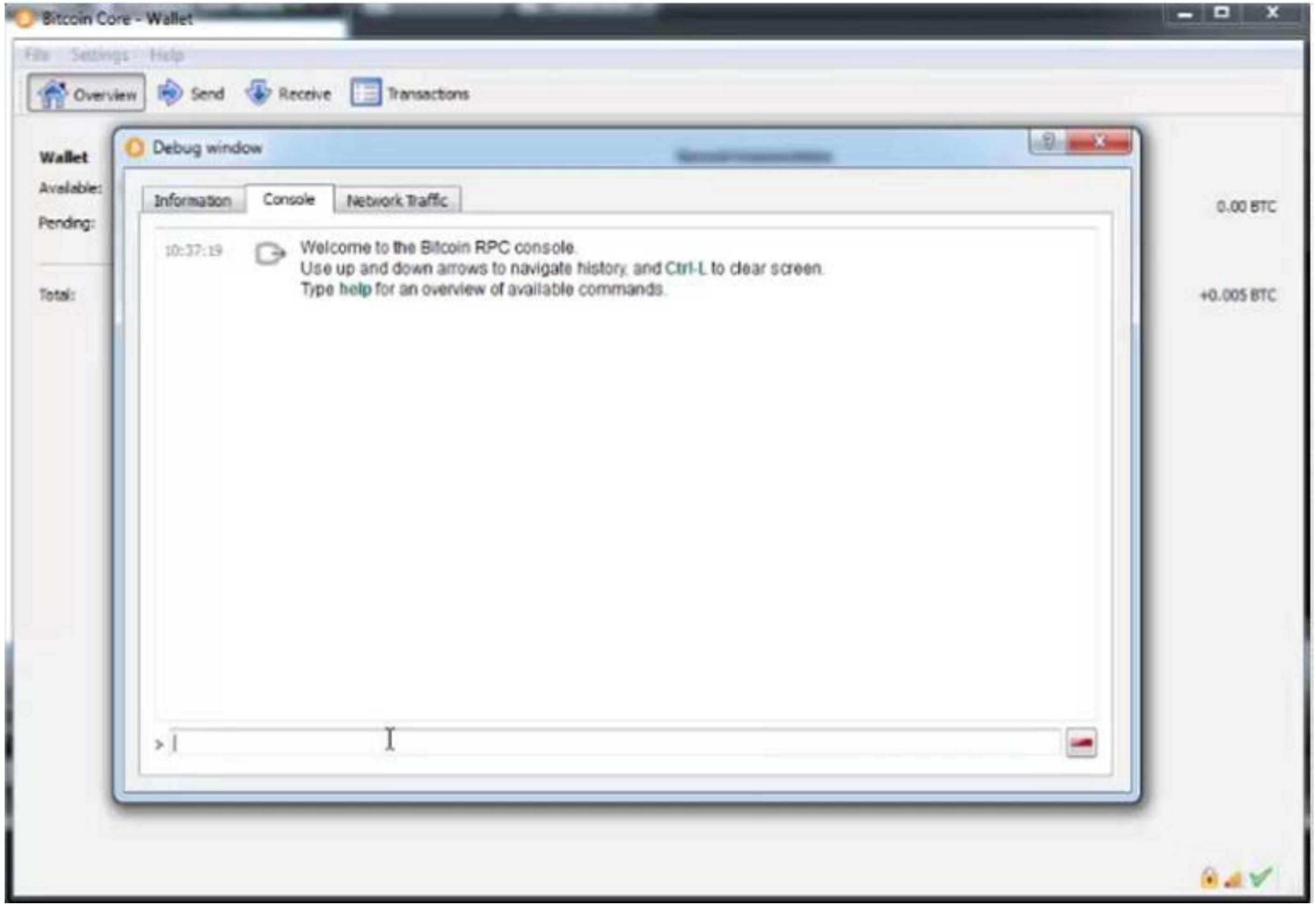
Exploring Blocks (CLI)

Commands to use:

Command	Parameters	Description
getblock	<hash>	Returns information about the block with the given hash.
getblockhash	<index>	Returns hash of block in best-block-chain at <index>; index 0 is the genesis block

Managing your wallet (CLI)

Video illustration below:



Wallet
Available: 0.00 BTC
Pending:
Total: +0.005 BTC

```
10:37:19   Welcome to the Bitcoin RPC console.
           Use up and down arrows to navigate history, and Ctrl-L to clear screen.
           Type help for an overview of available commands.

>
```

Exploring Blocks (CLI)

```
gettransaction
0408953d670d0f268b70f449772bd3d1c1b80c690be6f3017e3f9bdaa01c0b6c
{
"amount" : -0.01080000,
"fee" : 0.01080000,
"confirmations" : 2,
"blockhash" :
"00000000000000002320499cc4e60f5a515a03b088925f78b728bdf79ed5ac86",
"blockindex" : 189,
"blocktime" : 1399872120,
"txid" :
"0408953d670d0f268b70f449772bd3d1c1b80c690be6f3017e3f9bdaa01c0b6c",
"walletconflicts" : [
],
"time" : 1399871859,
"timereceived" : 1399871859,
"details" : [
{
…
```

We are now going to analyze the block we obtained earlier.

Exploring Blocks (CLI)

```
getblock
000000000000000002320499cc4e60f5a515a03b088925f78b728bdf79ed5ac86
{
"hash" :
"000000000000000002320499cc4e60f5a515a03b088925f78b728bdf79ed5ac86",
"confirmations" : 20,
"size" : 144825,
"height" : 300323,
"version" : 2,
"merkleroot" :
"5c782440831d895dbe2851999d403f08a59768a633de027288403efa472081c8",
"tx" : [
"5a127914b627a7657759c0a09df974d11d6712bd707731e9bb6b7b675d326aeb",
"050347e8a6babdd74fc60809c29f16d1bc23f0f5dd2ac329499b57166e197e18",
"999972c1afe4c311e46e475a661dc83397cd3896c79f7cda4374d0372433de9a",
…
"161cb709e9b9e15617d0827af6282fee53484fe9ca4a575258989d8809256fd8"
],
"time" : 1399872120,
"nonce" : 1602350785,
"bits" : "1900896c",
"difficulty" : 8000872135.96816350,
"chainwork" :
"000000000000000000000000000000000000000000005cd4f1cdf66447a1f6c4",
"previousblockhash" :
"00000000000000000044340d7a81d3165439ddbabc94521754f00daeaaa0aae09b",
"nextblockhash" :
"000000000000000001ad17972576160667dd6f246045ff03e50716242d68faf7"
}
```

As you can see, this block contains many transactions.

Exploring Blocks (CLI)

```
"998342493e6deb9efda2250878a86b42b74fbdd99365e5074d9d7517f6f92e50",
"1f74548a6b92149b2dd523928ebfc830aa80f9f01bca94f281a934e647696981",
"4fa2eb6c33189190fc515066c0a38da9573583f3b795fe2f0b75147278b3c037",
"15766c8dee6053f2d36bba568497850ca0d39d782d239816261d7bef9b3d25b3",
"0408953d670d0f268b70f449772bd3d1c1b80c690be6f3017e3f9bdaa01c0b6c",
"8062654f3f2de78537da07784a199e6724a5ea43a281b7f7536d9d2ad2a468a6",
"b90e6279b0e4bf697d71a0129bbc76e993e72c397f411b796935c56f5e58d12b",
"22246aaaa62afa3d191df40226dfcb3a64fe3e426b67525d4eb1d906a6f9ef87",
"33d20b9bbbf7ea35f070aabc8a34db51ba0fa172dcaac114fb00b28f31c8cbf3",
"0cf5e8f7fbc9dc0d853c8699abd5ce8f1ff497da8b1acc819d07a7d2ae54dc30",
```

Our transaction can also be found in this block.

Exploring Blocks (CLI)

```
getblockhash 0
000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f

getblock
000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f
{
"hash" :
"000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f",
"confirmations" : 300344,
"size" : 285,
"height" : 0,
"version" : 1,
"merkleroot" :
"4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b",
"tx" : [
"4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b"
],
"time" : 1231006505,
"nonce" : 2083236893,
"bits" : "1d00ffff",
"difficulty" : 1.00000000,
"chainwork" :
"0000000000000000000000000000000000000000000000000000000100010001",
"nextblockhash" :
"00000000839a8e6886ab5951d76f411475428afc90947ee320161bbf18eb6048"
}
```

We can retrieve block by index ("block height"), where "0" is the height of the Genesis block.

The Genesis block only contains one
transaction (the coinbase transaction). Prior to the first Bitcoin transaction (found on block 170), all blocks only contained the coinbase transaction.

This is how bitcoins are being generated.

Exploring transactions

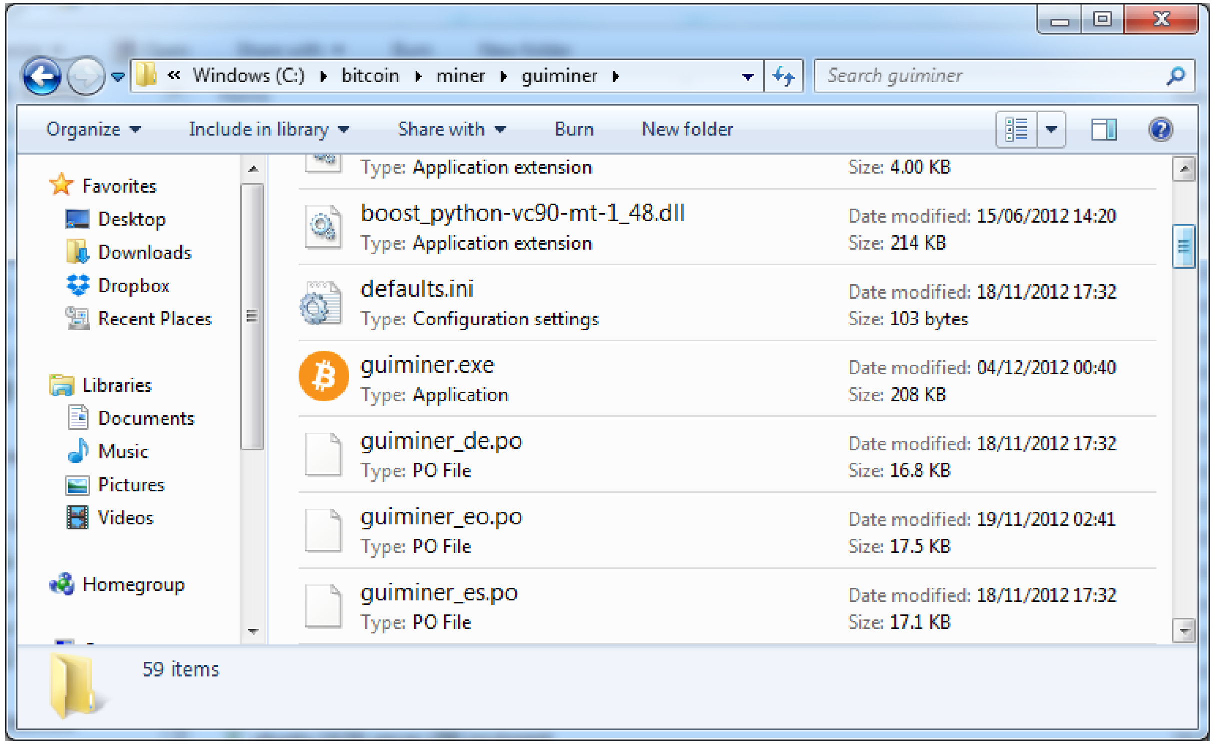
- New bitcoins are generated by miners.
- Miners also confirm our transactions.
- The basics of mining were previously discussed in Session 3.
- Over the next pages, we are going to discuss practical issues related to mining.

3. Mining and mining pools

What is mining?

- The easiest way was to download GUI-miner from http://guiminer.org/. You download a self-extracting archive. When you run it you have to specify the desired location, for example, c:\bitcoin\miner\.

- After extracting you will have a guiminer folder with the following content:



Type: Application extension Size: 4.00 KB

boost_python-vc90-mt-1_48.dll
Type: Application extension Date modified: 15/06/2012 14:20 Size: 214 KB

defaults.ini
Type: Configuration settings Date modified: 18/11/2012 17:32 Size: 103 bytes

guiminer.exe
Type: Application Date modified: 04/12/2012 00:40 Size: 208 KB

guiminer_de.po
Type: PO File Date modified: 18/11/2012 17:32 Size: 16.8 KB

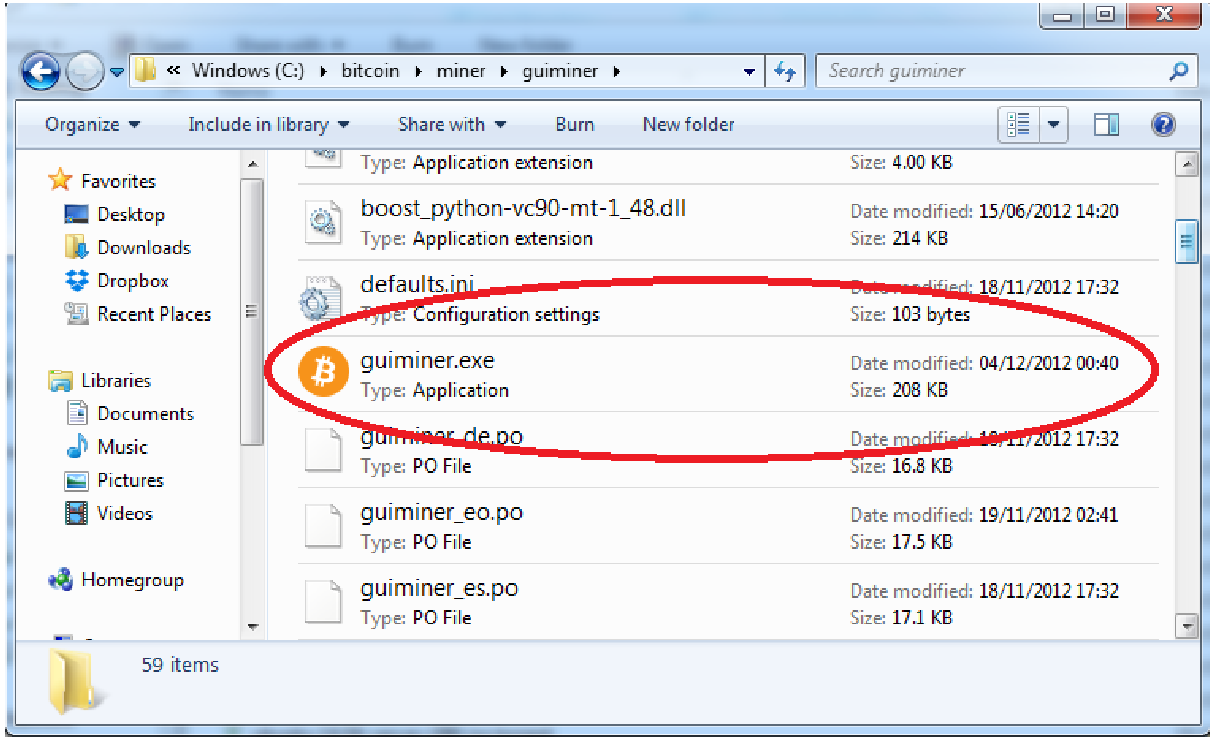
guiminer_eo.po
Type: PO File Date modified: 19/11/2012 02:41 Size: 17.5 KB

guiminer_es.po
Type: PO File Date modified: 18/11/2012 17:32 Size: 17.1 KB

59 items

What is mining?

- You can create a shortcut for guiminer.exe



Type: Application extension Size: 4.00 KB

boost_python-vc90-mt-1_48.dll Date modified: 15/06/2012 14:20
Type: Application extension Size: 214 KB

defaults.ini Date modified: 18/11/2012 17:32
Type: Configuration settings Size: 103 bytes

guiminer.exe Date modified: 04/12/2012 00:40
Type: Application Size: 208 KB

guiminer_de.po Date modified: 18/11/2012 17:32
Type: PO File Size: 16.8 KB

guiminer_eo.po Date modified: 19/11/2012 02:41
Type: PO File Size: 17.5 KB

guiminer_es.po Date modified: 18/11/2012 17:32
Type: PO File Size: 17.1 KB

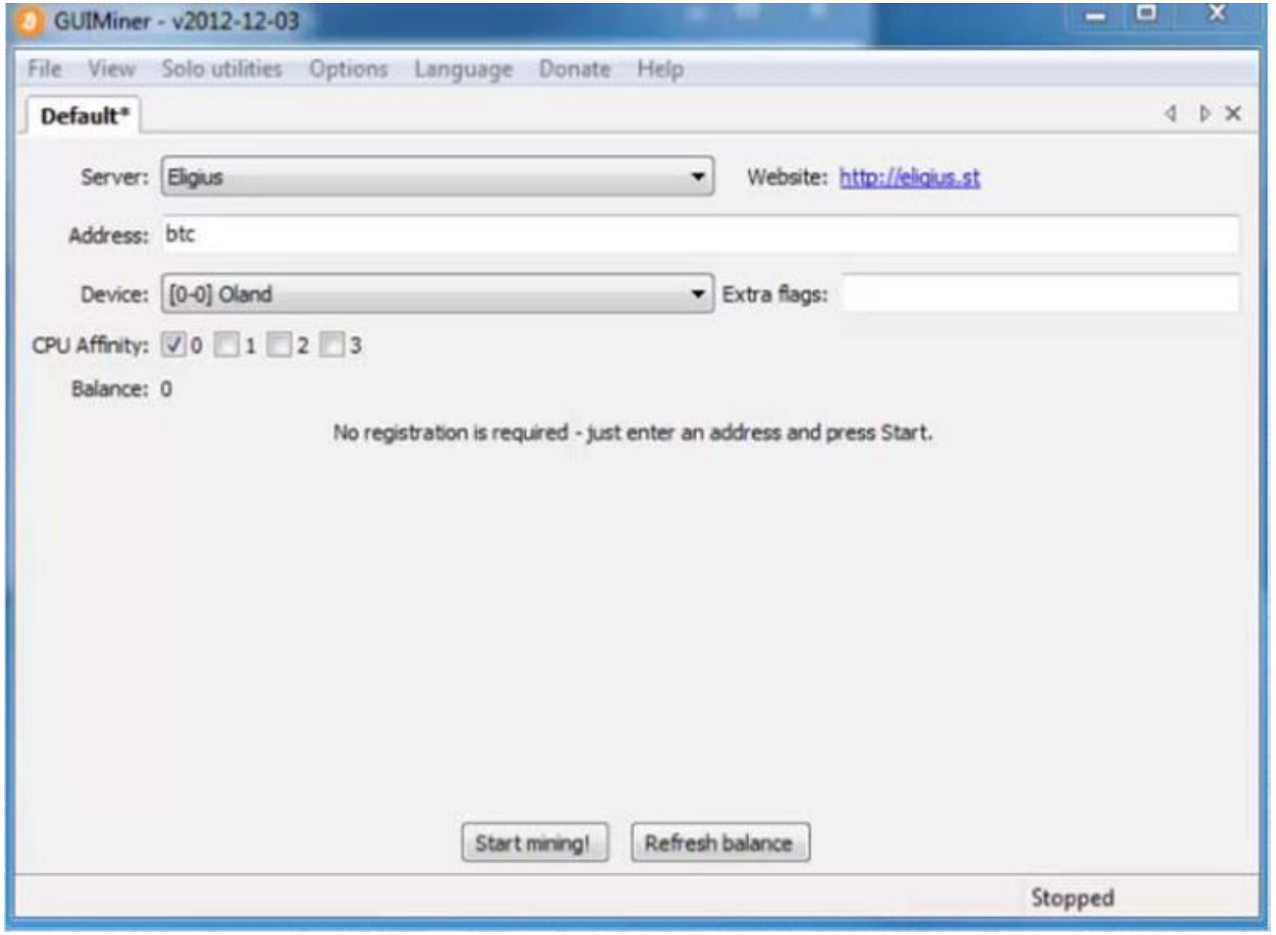
59 items

What is mining? Solo Mining

- The difference between solo mining and pool mining was discussed earlier in Session 3. In order to implement solo mining you need to have Bitcoin Core installed and synchronized.
- When running in server mode core accepts RPC calls from other programs, including the miner. The miner can use the getblocktemplate RPC call.
- getblocktemplate returns a whole template for the next block to be generated.
- When a solution is found the miner submits it to the network.

What is mining? Solo Mining

Video illustration below:



Server: Eligius

Website: http://eligius.st

Address: btc

Device: [0-0] Oland

Extra flags:

CPU Affinity: ☑ 0 □ 1 □ 2 □ 3

Balance: 0

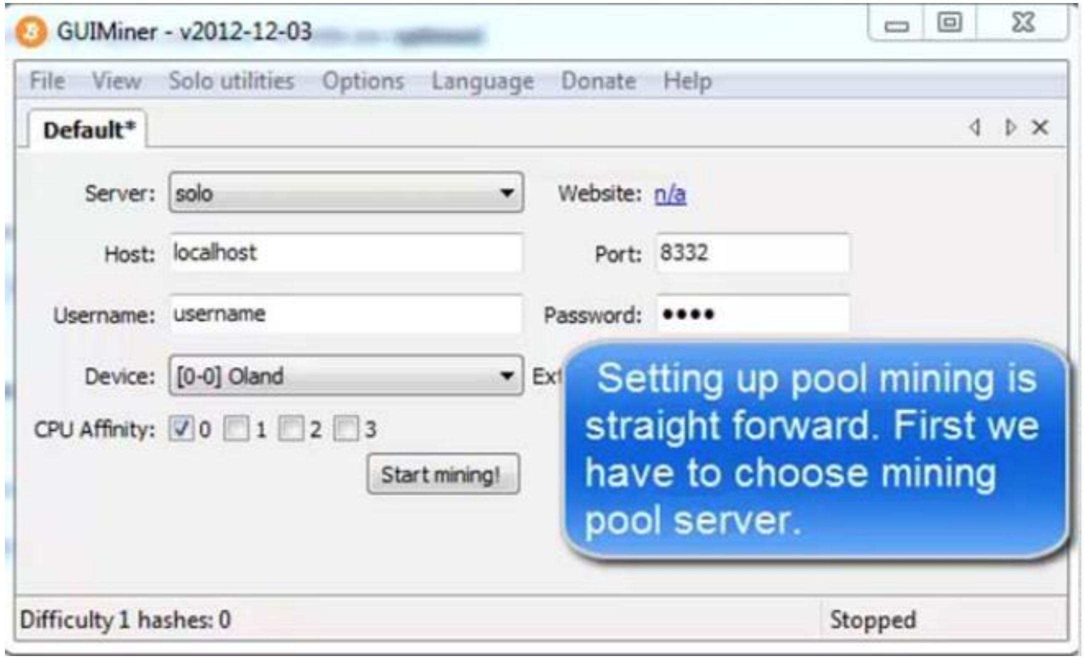
No registration is required - just enter an address and press Start.

Stopped

Mining - Pool mining

- Pool mining doesn’t require having a full client. However you have to create an account with one of the mining pools. We have discussed pool selection earlier in Session 3.
- As an example, we created an account with bitcoin.cz (now known as slushpool). The registration procedure depends on the chosen pool.

Video illustration:



Server: solo

Website: n/a

Host: localhost

Port: 8332

Username: username

Password: ••••

Device: [0-0] Oland

Ext

CPU Affinity: ☑ 0 □ 1 □ 2 □ 3

Setting up pool mining is straight forward. First we have to choose mining pool server.

Difficulty 1 hashes: 0

Stopped

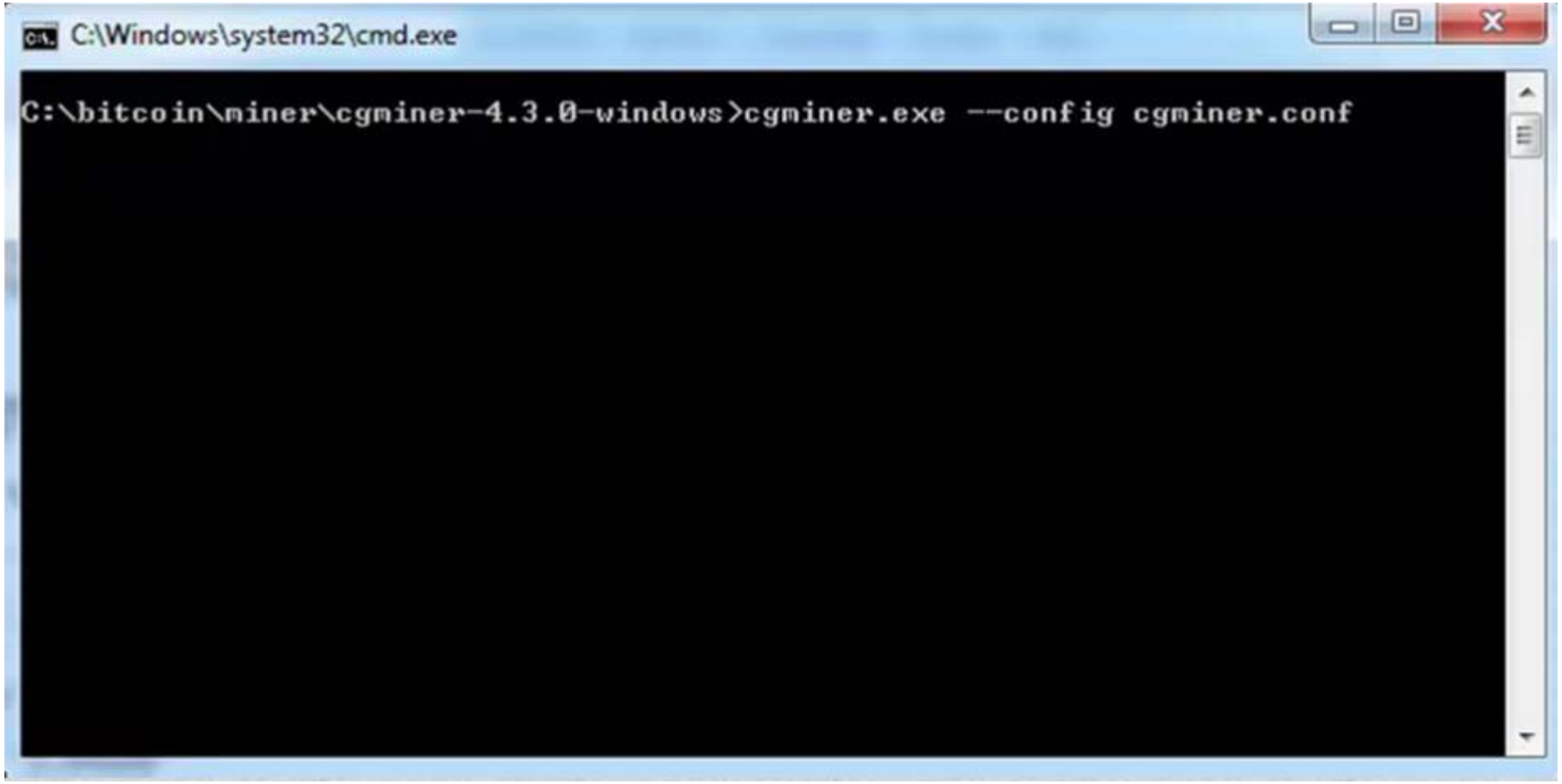
Mining - ASIC Mining

- So far we used our CPUs in order to do the mining calculations. This was the case in the earlier days when the mining difficulty was low. Today CPU mining cannot provide any level of meaningful performance. Far more calculations can be performed with specially designed ASICs. ASIC stands for **Application Specific Integrated Circuit.**

- ASIC miners can be standalone devices that are connected to the network. Such miners are relatively expensive and contain dozens of ASIC chips.

Mining - ASIC Mining

In the video example below, the miner reports work progress and performance statistics.



```
C:\bitcoin\miner\cgminer-4.3.0-windows>cgminer.exe --config cgminer.conf
```

Mining - GPU mining

- GPU mining is another type of mining where the GPU (Graphics Processing Unit) is used to perform mining calculations. GPU miners are usually based on custom-built PCs that may have up to 6 graphics cards. GPU mining is faster than CPU mining, and consumes a lot of power.

- The significantly higher output of ASICs combined with their low energy consumption per hash (by comparison), has made them the method of choice when mining bitcoins. GPUs are hardly used for Bitcoin mining anymore, though they are used to mine other coins like Monero

4. Segregated Witness (segwit)

Segregated Witness

An idea of Pieter Wuille, first presented at the Scaling Bitcoin workshops in Hong Kong in early December 2015, "Segregated Witness" or segwit is an optimization proposal implemented in August 23, 2017, with the aim to improve Bitcoin's performance in a number of ways.

As we've seen in previous sessions, simply put, transactions in Bitcoin have two main types of information contained within them:

- One part is what sum is transferred from where to where, in the form of inputs and outputs
- Proof that those transferences are authorized by the respective private key holders and they can be validly performed

This last part is the "Witness" part.

The basic idea behind segwit is that removing this from the transaction, enables more transactions to be recorded to the blockchain and thus a higher transaction throughput i.e. separate signature data from tx identifier data. Lets take a deeper look at what this means, and what other benefits or risks are associated with this change

Transaction malleability

- Bitcoin transactions revisited: Andreas want to send 5BTC to Antonis
  - **Andreas broadcasts a request to the network**: The request contains Antonis' public address, the amount being sent (5BTC) and a transaction fee for the miners. It also contains Andreas**' private key signature** proving that he owns 5BTC to send. This is the **witness data**.
  - **Miners process the transaction**. All the above information is encrypted and the transaction ID is formed.
  - **The transaction queues until is it processed and included in a block**.
  - **The block is confirmed** and broadcasted to the network. Antonis receives 5BTC from Andreas.
- Transaction malleability could be used by Antonis to fool Andreas making him send 10BTC instead of 5BTC i.e. Antonis to change Andreas' witness data before the transaction is confirmed.
- This will produce a **new** TX ID without changing the transaction itself (which is still 5BTC being sent from Andreas to Antonis but with the initial TX ID). When this transaction is confirmed, it will cancel the original one. Even though Antonis has received 5BTC he will tell Andreas that the transaction has not gone thorough. Andreas will check for the initial TX ID and see that the original transaction did not go through and then Andreas will send Antonis 5BTC more! Antonis now has 10BTC.

Transaction malleability

- SegWit simply removes witness data from the transaction
- All witness data of a block are encrypted on a segwit sidechain when calculating the TX ID. Even if the signature data is modified the TX ID remains the same. The root code is stored on the main blockchain.
- Via this way, the Bitcoin network scalability has also improved as witness data used to make up more than 60% of each block.
- As more transaction information can now be included in a block, after the implementation of segwit, confirmation times were much quicker.
- Fun fact:
  - Mt.Gox has blamed the transaction malleability flaw in 2014 for suspended withdrawals

https://www.coindesk.com/price-drops-mt-gox-blames-bitcoin-flaw-withdrawal-delays

Further explanation on Segwit: https://www.buybitcoinworldwide.com/segwit/

Segregated Witness

Benefits and costs identified are as follows :

- More transactions per second since the “witness part” isn’t included in the blockchain
- Decrease transaction fees
- Backward compatible – it is a soft fork
- No “transaction malleability” for segwit transactions
- Potential for fraud proofs for SPV (light) wallets
- Witness part to be included in “add-on” blocks verified as part of a miners’ coinbase transaction
- The whole value chain within Bitcoin, miners, nodes, wallets, etc needs to upgrade to gain maximum benefits
- If every transaction propagated was “segwit enabled” we could see a potential increase in blocksize to ~1.7m (although the witness information will still need to be relayed between nodes and miners)

For more information on Segregated Witness adoption and functionalities, see here

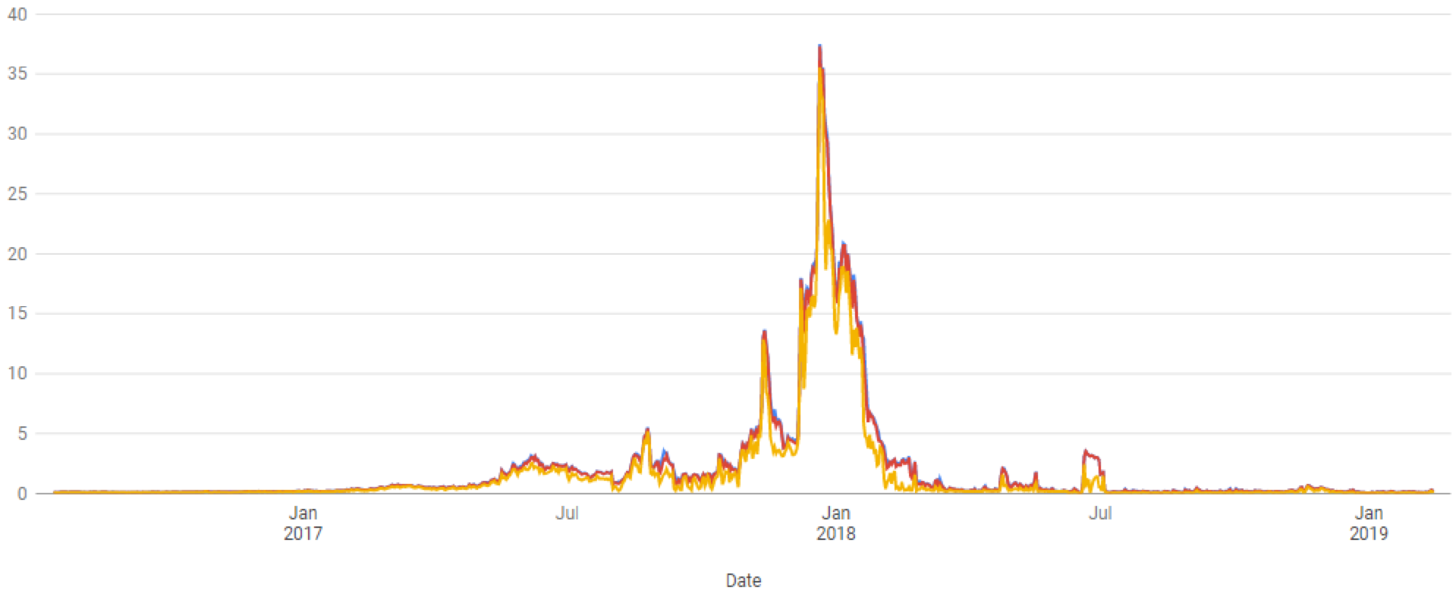
Segregated Witness – Adoption

- The majority of crypto exchanges and wallets are now implementing the concept, over the past months we had some major updates:
  - SegWit has been implemented in Coinbase, Bitfinex and many wallets
    https://usethebitcoin.com/segregated-witness-implemented-coinbase-bitfinex-bitcoin-network-upgrading/
    https://captainaltcoin.com/bitcoin-segwit-wallets/

  - Bitcoin Core versions from 0.16.0 onwards include full SegWit support
    https://cointelegraph.com/news/segwit-gets-its-big-debut-as-latest-bitcoin-core-version-introduces-full-support

  - SegWit adoption still holds back from 100%
    https://www.coindesk.com/one-year-later-whats-holding-back-segwit-adoption-on-bitcoin

Dollars per TX



Source:
https://bitcoinfees.info/

SegWit2x

- Lead Developer – Jeff Garzik
- Was expected to activate in November 2017
- What was expected: Approximately 90 days after the activation of SegWit, a block between 1MB-2MB in size would be generated by miners as an attempt to increase network capacity. The majority of the Bitcoin network was expected to continue mining on top of this block
- Without significant miners' support, the project has failed. A successful hard fork could create another version of Bitcoin
- Mike Belshe, CEO of Bitgo, announced the cancellation via a post(see link below) to the Bitcoin-SegWit2x mailing list.
- https://lists.linuxfoundation.org/pipermail/bitcoin-segwit2x/2017-November/000685.html

5. Lightning Network

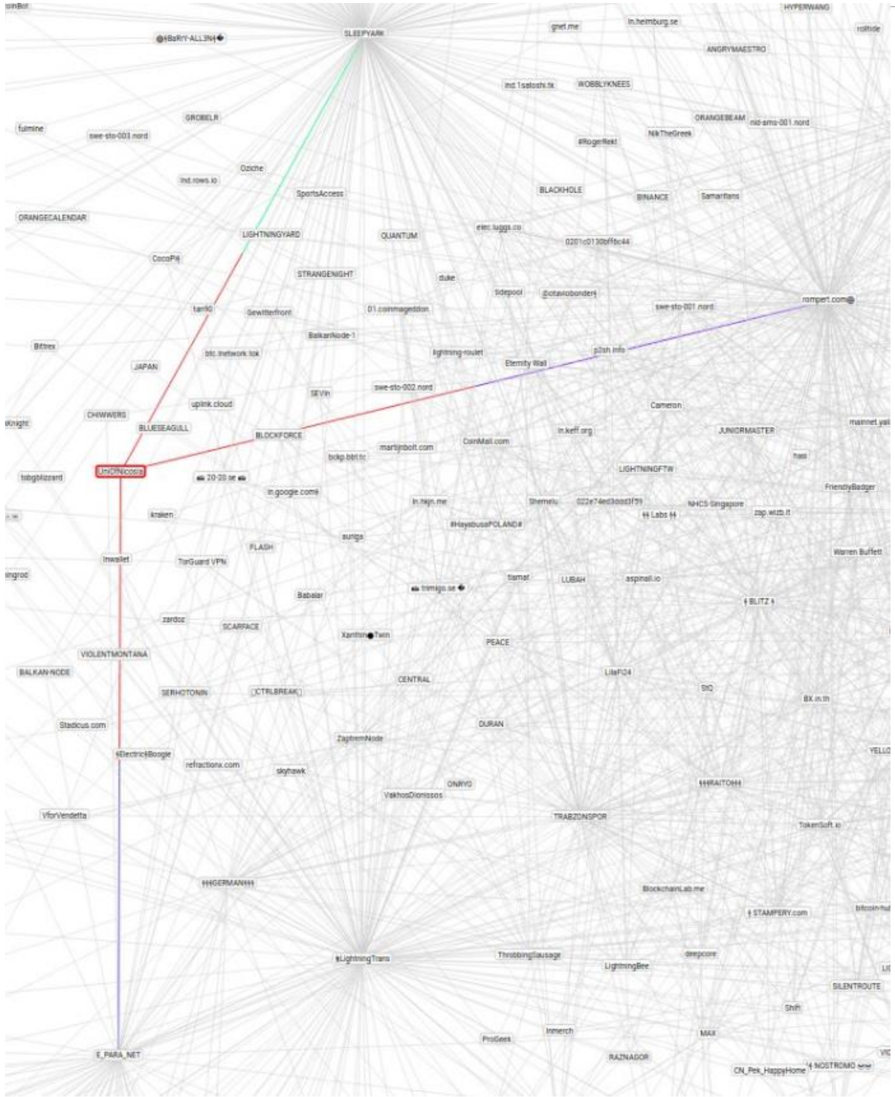
Lightning Network

- The idea is that not all transactions need to be recorded on the Blockchain
  - If 2 people make multiple transactions between them there is no need to record all the transactions on the Blockchain which ultimately makes the network “heavier”.
  - A **payment channel** between these people can be created. The opening of this channel is recorded on the Blockchain. Participants will then transact through the payment channel (off-chain – no blockchain transactions at this point) as much as they wish.
  - When participants decide to close the channel, only the final balance of the transactions will be recorded on the blockchain.
- Another hypothetical scenario: Person A, Person B, Person C
- 2 payment channels exist: Channel between A-B & Channel between B-C
- If A wants to send 1 bitcoin to C:
  - B will send 1 bitcoin to C ,and
  - A will send 1 bitcoin to B for reimbursement.

Payment Channels

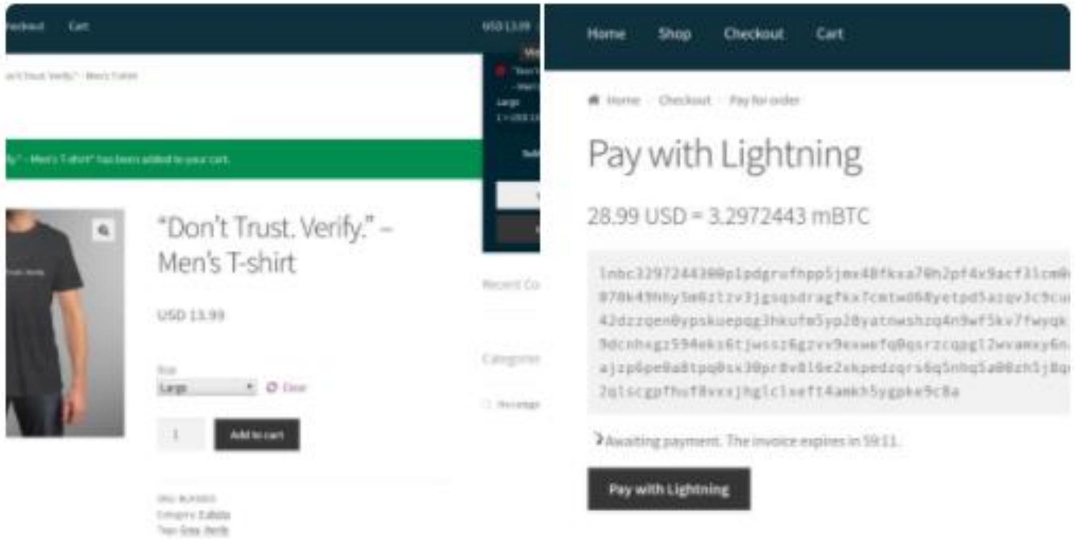
- Funds are locked in a payment channel (think of them as safety box). These funds are used for transactions between the 2 participants
- Participants open up a channel, by committing a certain amount of Bitcoins.
- A “promise of ownership” for a certain amount of bitcoins is transferred between the two participants in the channel when they want to transact. This can happen multiple times
- Anyone of the two participants may decide to close the channel at any given time
- Closing a channel would mean that a transaction concerning the final balance of the participants will be recorded on the Blockchain i.e. each participant’s share of the “safety box” is recorded on the blockchain forever

Lightning Network - UNIC



- The University of Nicosia is running on Lightning Mainnet
- Where is lightning used? https://bitcoinist.com/lightning-network-bitcoin-cities/

UNIC's first purchase on Lightning, 1 T-shirt, size Large



“Don't Trust. Verify.” – Men's T-shirt

USD 13.99

Size: Large

1

Add to cart

Home Shop Checkout Cart

Home / Checkout / Pay for order

Pay with Lightning

28.99 USD = 3.2972443 mBTC

```
lnbc3297244300p1pdgrufnpp5jmx48fkxa70n2pf4x9acf31cm0
870k49hhy5m0z1zv3jgsqsdragfkx7cmtw064yetpd5azqv3c9cu
42dzzqen0ypskuepqg3hkufm5yp20yatnwshzq4n9wf5kv7fwyqk
9dcnhegz594eks6tjwssz6gzvv9exwefq0qsrzcqpg12wvamxy6n
ajzp6pe0a8tpq0sx30pr8v816e2xkpedzqrs6q5nhq5a08zh5j8q
2q1scgpfhuf8vxxjhg1c1xeft4amkh5ygpke9c8a
```

Awaiting payment. The invoice expires in 59:11.

Pay with Lightning

5. A fork in the Road (a primer)

Forks come in different types

A detailed discussion on forks would take the space of a whole session and is beyond the scope of this course. The short answer to what a fork is, is that it is a method to upgrade the network.

> “They vote with their CPU power, expressing their acceptance of valid blocks by working on extending them and rejecting invalid blocks by refusing to work on them. Any needed rules and incentives can be enforced with this consensus mechanism”
>
> - Satoshi Nakamoto, Bitcoin Whitepaper

Soft Forks : A soft fork is a change to the Bitcoin protocol wherein updated nodes start operating with new rules, and old nodes never see these changes. Old nodes still keep receiving new blocks and will recognize them as valid, so we can say that a soft fork is backwards-compatible. Soft forked nodes might not make too much sense of what is happening in the updated parts of the network, but they’re still part of it.

Hard Forks : This is a permanent divergence in the block chain towards a new ruleset that old nodes can’t follow (can’t validate blocks any longer). Hard forked nodes see that something crucial has happened since no or fewer blocks (that are valid to them), are coming in, and they have to make an active choice whether to upgrade to a newer version (join the hard fork) or continue along their existing path, building blocks on the old chain.

This is a more Bitcoin-centric week. Other scalability proposals such as the establishment of Bitcoin Cash and Ethereum sharding will be discussed during the following weeks.

6. Conclusions

Conclusions

- The Bitcoin Core client synchronizes with the Bitcoin network and the blockchain (i.e. blocks of transactions) and, therefore, is able to validate those transactions
- Bitcoin Core can be controlled through the CLI (Command Line Interface)
- Bitcoin Core can work as a server and provide services (APIs) to other programs like graphical interfaces or miner
- Solo mining required an installation of Bitcoin Core.
- Pool mining requires an account with one of the mining pools but no local Bitcoin Core.
- CPU mining does not provide any meaningful performance anymore.
- GPU mining is power consuming and largely obsolete unless mining some altcoins like Monero.
- ASIC mining provides the best results for Bitcoin mining, but might not be available for other cryptocurrencies.

Conclusions

- Segregated Witness (SegWit) is an already implemented soft fork on Bitcoin which addresses malleability and scalability issues
- Lightning Network supports the idea of moving the value from the ownership of the Bitcoins to the “promise of ownership” of the Bitcoins.
- Average transaction fees for Bitcoin have recently dropped as a result of many factors, including segwit adoption
- SegWit2x supporters backed up a 2MB block increase, alongside the activation of Segregated Witness, but the project failed due to limited adoption

7. Further Reading

Some Further Reading

- Bitcoin Core

https://en.bitcoin.it/wiki/Bitcoin_Core

- Lightning Network Explained and Adoption

https://cointelegraph.com/explained/lightning-network-explained

https://www.coindesk.com/merchants-bitcoin-lightning-network/

https://blockonomi.com/lightning-network-advances-hurdles/

https://www.coindesk.com/bitcoins-lightning-torch-has-blazed-through-37-countries-so-far

- SegWit Introduction

https://blockgeeks.com/guides/what-is-segwit/

- Comparison of mining pools and hardware

https://en.bitcoin.it/wiki/Comparison_of_mining_pools
https://www.buybitcoinworldwide.com/mining/hardware/

Some Further Reading

- Bitcoin Core 0.17.1

https://bitcoin.org/en/release/v0.17.1

- Consensus Rule Changes

https://bitcoin.org/en/developer-guide#consensus-rule-changes

- Blocksize Arguments :
  - https://en.bitcoin.it/wiki/Block_size_limit_controversy
  - http://bitcoin.stackexchange.com/questions/36085/what-are-the-arguments-for-and-against-the-increase-of-the-block-size-limit
- SegWit addresses
  - https://ethereumworldnews.com/segwit-reach-historical-peaks/
  - https://bitcointechtalk.com/transaction-malleability-explained-b7e240236fc7

UNIVERSITY of NICOSIA

Questions?

Contact us:

Twitter: @mscdigital
Course Support: digitalcurrency@unic.ac.cy
IT & Live Session support: dl.it@unic.ac.cy