

PV204 Security technologies



Bitcoin

Petr Švenda  svenda@fi.muni.cz  [@rngsec](https://twitter.com/rngsec)

Centre for Research on Cryptography and Security, Masaryk University



Three stages of Lecture and Seminar next week

- [before 20.4. 16:00] Preparation before Monday call
 - Video, slides, installation of two mobile wallets
- [20.4. 16:00] Group discussion during the Monday call
 - 40-50 min in breakout rooms
 - 20-30 min collection of results together
 - 10 min bitcoin “giveaway”: on-chain and Lightning transactions
- [till 30.4. 23:59] Own work and assignment

PREPARATION

Preparation before Zoom call (till Monday 20.4. 16:00)

- Watch '*But how does bitcoin actually work?*' by 3Blue1Brown (26min)
 - <https://www.youtube.com/watch?v=bBC-nXj3Ng4>
- Read slides Hello Bitcoin (including notes under every slide)
 - <https://www.hellobitco.in/>, copy of slides also in IS
- Prepare 5 technical questions you would love to know answer to
 - Something that is not clear from slides or not covered
 - Fill it here (No jokes, no trading predictions please 😊)
https://docs.google.com/spreadsheets/d/17mGDZUcExh0dtZyx52wLPvFZNtrDeRTLKWJea_b2Y7Mc/edit?usp=sharing
- Pre-install two wallets on your phone (standard, Lighting)
 - Green: Bitcoin wallet by Blockstream as standard wallet
 - WalletOfSatoshi as Lighting wallet (or BlueWallet/Zap/Muun... if you are more familiar)

MONDAY 20.4. 16:00 CALL



During the Monday call – collaborative discus

- Join discussion with group colleagues (Zoom breakout rooms)
- Try to find answers for the questions from the next slides
 - Note basic points of your findings/answers directly to slides
 - No expectation to do all questions, but cover at least the basic ones
- For every questions:
 - Discuss why and where (usage) it is relevant for Bitcoin (possibly more places)
 - Try to answer using your knowledge, Internet and common sense
- Note down 2-3 surprising observations to mention to whole classroom

QUESTIONS

Questions: Basics

- How can you get some bitcoin(s)? (At least three different options)
- How can I pay you 1btc if I have only one UTXO worth of 5btc?
- Can you get less than 1 bitcoin?
- Can you reverse bitcoin payment if send to wrong address?
- Why “Not your keys, not your bitcoin”? What is non-custodial wallet?
- How can someone steal your bitcoins?
- For what reason are miners consuming a lot of energy?
- How frequently is now block with transactions included to blockchain?
- What will happen if I will try send double-spending tx to Bitcoin network?
- If I will send you bitcoin on-chain, can you tell from whom I got it?
- What is the current inflation rate of Bitcoin? What will it be in one month? Why?

Questions

- Why you should use fresh new address for every receive transaction?
- Why is theoretical maximal limit of on-chain transactions ~6-7tx/sec?
- How is it possible to perform 1000tx/sec between two users (today)?
- When will all bitcoins be mined? What will happen then with mining?
- What will happen if one miner controls 51% of hashrate?
- Why is Bitcoin network not flooded (DOSed) with invalid transactions?
- Can Bitcoin operate without the Internet?
- What is difference between soft- and hard- fork? Why is Bitcoin always aiming for soft-forks only?

Questions

- What will happen if you create pull request to increasing total number of bitcoins from 21M to 100M at <https://github.com/bitcoin/bitcoin>?
- What will happen if such code change is accepted by Bitcoin core developer?
- Can I operate full Bitcoin node without owning any bitcoin?
- Can you receive bitcoins without operating full node?
- What attacks are possible if I'm using Bitcoin wallet which is not connected to my trusted full node?
- What will happen if someone manages to compute SHA256 with specified number prefix zeros (mining puzzle) 1000x faster than now?

Questions

- What will happen to Bitcoin security if quantum computer powerful enough to break 256b ECC is build?
- When will Proof of Stake replace Proof of Work in Bitcoin?
- What is a difference between public key and Bitcoin address?
- What ECC curve is used for Bitcoin?
- What happens when private key for some UTXO is permanently lost?
- How you can you make your relatives to inherit your bitcoins?
- Why is open-source important for Bitcoin to work?

Questions

- How high fee is required for transaction to be included to block?
- What information is one leaking when browsing transactions using 3rd party block explorers?
- Why is coinbase transaction (miner's reward) spendable only after 100 blocks?

Get some satsoshies (on-chain)

- Example of well-designed wallet is GreenWallet by Blockstream
 - Install wallet on mobile phone and backup your recovery seed (BIP32)
- I will send you \$2 worth of Bitcoin on-chain, if you will promise (and fulfill 😊) to send me \$1 back later via Lightning
 - Generate new receive address, show me QR Code
- When sending, you can set custom fee starting from 1.0 sat/vbyte
 - Standard transaction has ~260vbytes => ~\$0.02 (but may take long to confirm)
- Note: Lightning wallets frequently contains also standard wallets
 - E.g., BlueWallet, Muun wallet

Get some satsoshies via Lighting network

- I will send 3000 satsoshies to one member of your project group
- She/he will send 1000 to each of the remaining members
- Poor-man option: Custodial wallet (beware, is **custodial!**)
 - Wallet of Satoshi (Android, iOS), Setup time: instant installation and use
- Better option: Non-custodial wallet connected to hosted Lighting wallet
 - Blue Wallet, you need to have at least some on-chain btc (at least 30k sats == 0.0003 btc)
 - Your wallet holds the private keys, but channels are opened by trusted service
 - Setup time: Takes up to several hours before ready (on-chain transactions)
- Best option: Setup your own full node and own Lighting node
 - E.g., Raspi4 + 1TB HDD + mynodebtc.com image + mobile wallet (BlueWallet, Zap, RTL...)
 - Similar to previous option, but Lighting wallet now connects to your Lighting node
 - Setup time: Days before your full node is synchronized, then several hours to open channel

Further reading

- Mastering Bitcoin (Andreas M. Antonopoulos and others)
 - <https://github.com/bitcoinbook/bitcoinbook>
- List of interesting resources
 - <https://blockonomi.com/bitcoin-educational-resources/>

OWN WORK AND ASSIGNMENT

P2P Bitcoin network map <https://bitnodes.io/>

GLOBAL BITCOIN NODES DISTRIBUTION

Reachable nodes as of Sun Apr 12 2020
11:13:21 GMT+0200 (Central European Summer Time).

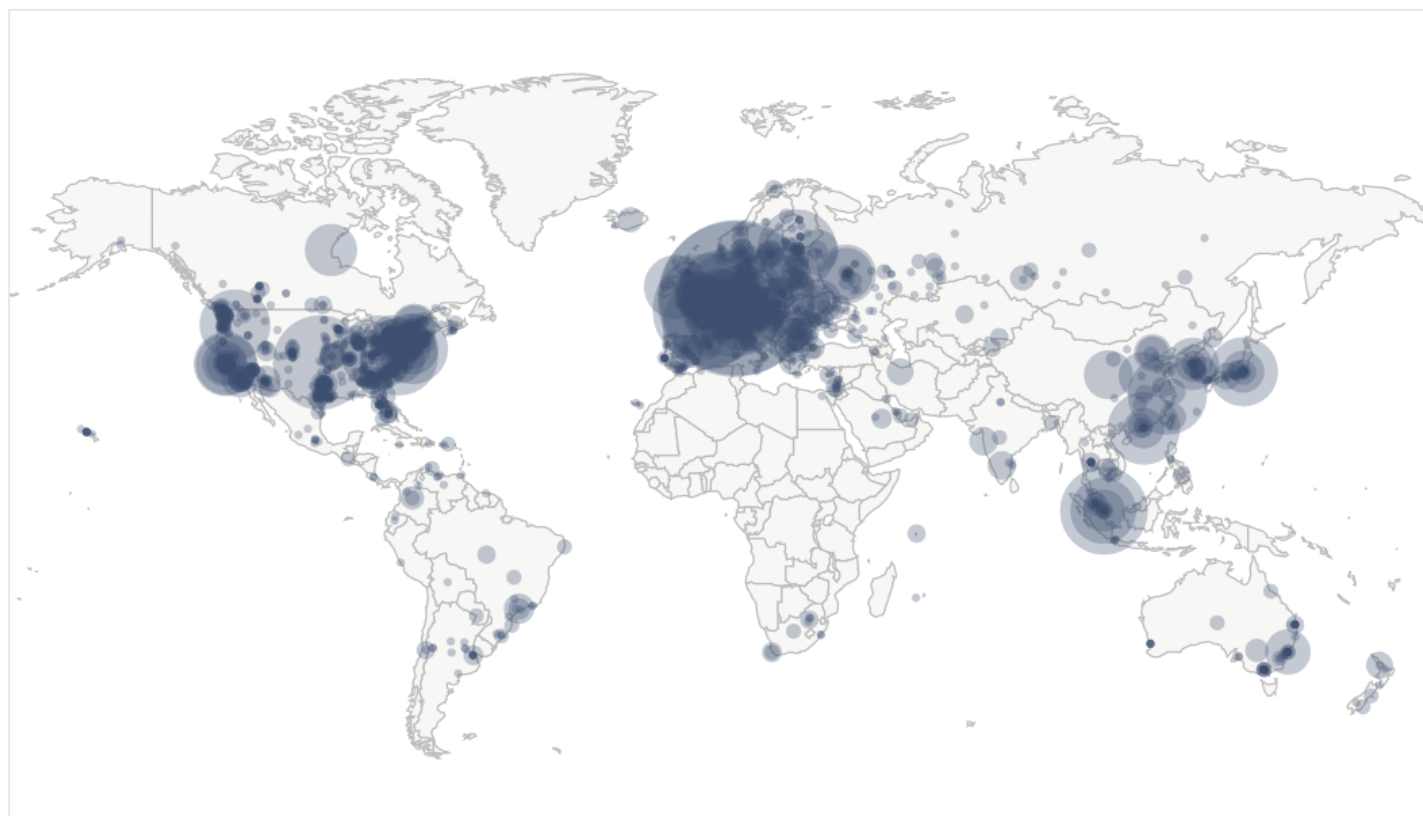
9967 NODES

[24-hour charts »](#)

Top 10 countries with their respective number of reachable nodes are as follow.

RANK	COUNTRY	NODES
1	United States	2018 (20.25%)
2	Germany	1807 (18.13%)
3	n/a	1751 (17.57%)
4	France	585 (5.87%)
5	Netherlands	456 (4.58%)
6	Canada	325 (3.26%)
7	United Kingdom	260 (2.61%)
8	Singapore	256 (2.57%)
9	China	231 (2.32%)
10	Russian Federation	221 (2.22%)

[More \(101\) »](#)



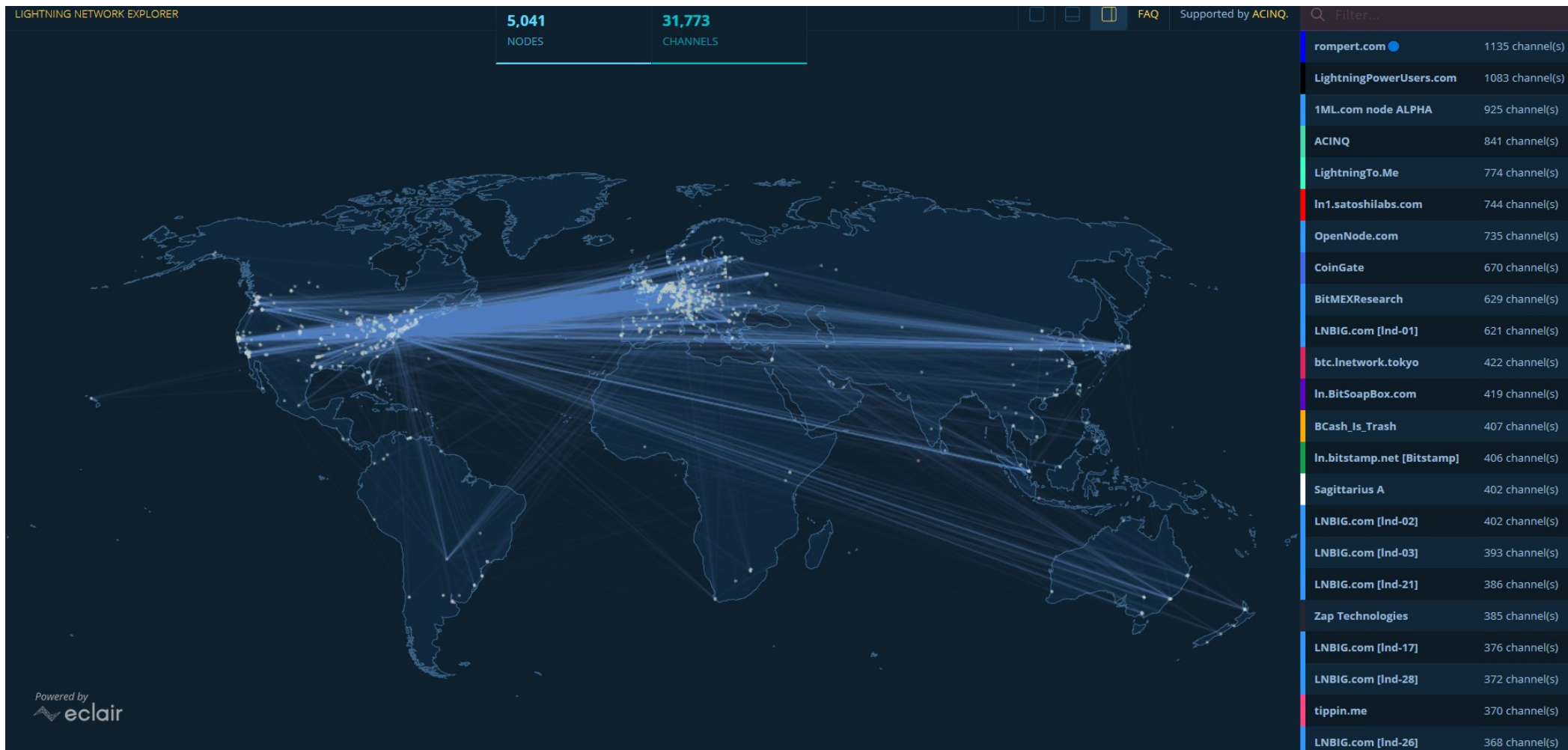
Map shows concentration of reachable Bitcoin nodes found in countries around the world.

[LIVE MAP](#)

Networks in Bitcoin (Mainnet, Testnet, Regtest)

- Mainnet – main, global production network
- Testnet – testing network (global, some mining happens...)
 - Restarted from time to time, contains many different types and versions of TXs
- Regtest – local instance of Bitcoin network
 - Used for local testing (integration, regression, debugging)
 - Blockchain started from block 0, you are the only miner
 - (mined bitcoins unusable on Mainnet)
 - You can insert own transactions, decide on mining new blocks, debug...
- Lightning – second layer network atop of Mainnet

Lightning network <https://explorer.acinq.co/>



Own work: Using API of full node

- Install full Bitcoin node
 - Bitcoin core, <https://bitcoincore.org/bin/bitcoin-core-0.19.1/>
- Download few blocks from real P2P network
 - Observe and document peers to which you connected (number, version, IP)
 - Analyze first few blocks from blockchain using Bitcoin/blocks/blk00000.dat and compare to info provided by online Block explorers
- Run local regtest network
 - Analyze basic of regtest blockchain
 - Mine some blocks
 - Analyze your wallet
 - Make transaction on regtest

```
>bitcoin-cli -regtest getbalance  
50.00000000
```

Bitcoin -regtest

- Run local network (bitcoin daemon)
 - `bitcoind -regtest`
- Obtain new address for future mined bitcoins (=> `miner_address`)
 - `bitcoin-cli -regtest getnewaddress`
- Mine 101 blocks
 - `bitcoin-cli -regtest generatetoaddress 101 miner_address`
- Check your balance
 - `bitcoin-cli -regtest getbalance`
- Send previously mined bitcoins to new address (`getnewaddress->new_address`)
 - `bitcoin-cli -regtest sendtoaddress new_address 10.00`
- Mine additional to block to include new TX into blockchain...
 - <https://bitcoin.org/en/developer-examples>, <https://bitcoin.org/en/developer-reference#bitcoin-core-apis>

ASSIGNMENT

Assignment 7.1: Bitcoin network CLI

- Describe steps to create transaction with three outputs to three different addresses
 - List sequence of commands, add corresponding CLI screenshots
 - List raw resulting transaction
- Answer the following questions
 - Why bitcoins from regtest cannot be used on mainnet?
 - How is address on regtest different from mainnet?
 - When is mempool changing during your steps?

Assignment 7.2: Bitcoin transaction graph analysis

- During the online lecture, some bitcoins were sent on-chain
 - The first transaction I made will be called “original”
 - Txid = f236bf1c11eea0f1d1d757ce31bd8dae8a400d5e3ef1a103b38e37081937ff2f
- Reconstruct and visualize graph of txs before and after “original”
- Answer the following questions
 - What is transaction ID (txid) and output index (vout) of “original” transaction?
 - How much bitcoins I owned before sending it to first student?
 - P.S. If you at some some deduce that I own more than 30 bitcoins, you are wrong 😊
 - From where “original” tx comes from (txid, additional analysis and discussion)?
 - How much fee was paid to create “original” UTXO?
 - What type of address was used? Was Segwit used?

Assignment 7: Bitcoin

- Produce short text/pdf description of solution
 - Provide steps for bitcoin regtest operations
 - Provide visualization of transactions graph
 - Provide answers to questions asked
- Submit before 30.4.2020 23:59 into IS HW vault
 - Soft deadline: -1.5 points for every started 24 hours


IF YOU LIKE TO DIG DEEPER


<https://mynodebtc.com>





myNode

Core Services


Bitcoin
 Running


Lightning
 Running



Electrum Server
 Running



Tor
 Private Connections
 Remote Access
 Premium Feature



VPN
 Premium Feature


Services


Apps



RTL
 Lightning Wallet



BTC Pay Server
 Merchant Tool
 Premium Feature



LND Hub


LND Connect
 Lightning Tool


Explorer
 BTC RPC Explorer


Dojo
 Disabled


Whirlpool
 Disabled


Mempool.Space
 Mempool Viewer
 Premium Feature

Operating own Bitcoin full node with Lightning

- Download presync part of blockchain from other mynodes (2 days)
- Download the rest of blocks from Bitcoin P2P network (1-2 days)
- Enable Lightning, create new wallet, send some sats to it (on-chain)
- Download Lightning wallet (e.g., BlueWallet, Zap)
- Pair Lightning wallet with your node
- Open channel to some other node
 - E.g., Lightning Node Suggestions at <https://store.blockstream.com/>
 - Opening channel performs one on-chain transaction
- *Analyze all other options in mynodebtc web GUI!*
- *Enable Electrum Server, Enable BTC RPC Explorer, Browse transactions...*