MIT Digital Currency Initiative and the University of Brasilia presents

# Cryptocurrency Design and Engineering

Lecture 9: Synchronization and Verification
Taught by: Neha Narula
October 7, 2025
MAS.S62

## Recap

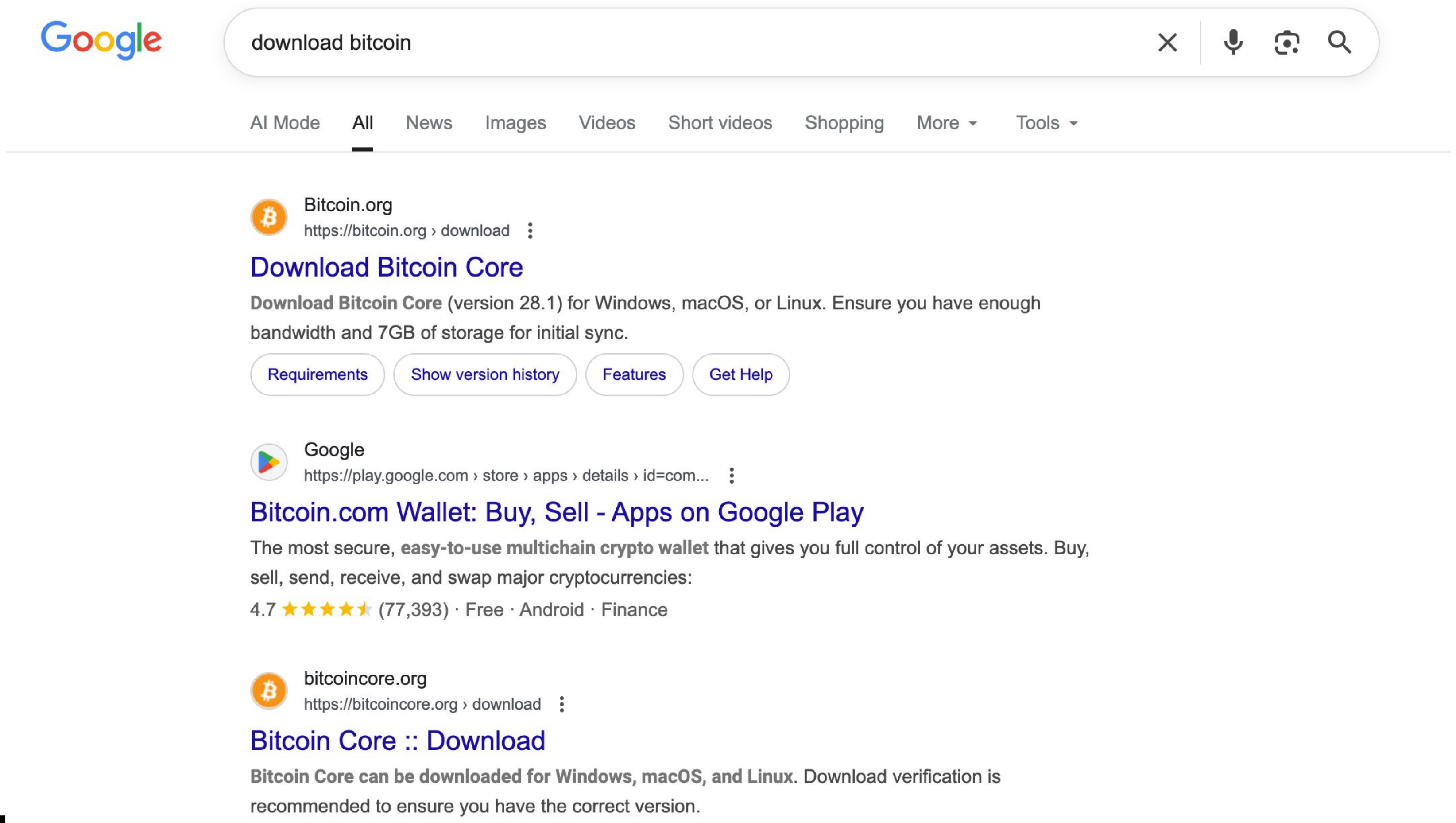
- Goals of proof-of-work
- Validation rules
- Forking, upgrades, and governance

## Synchronization and verification

- How do I learn if I’ve been paid?
  - Look at the blockchain
- How do I learn about the blockchain?
  - Ask the “Bitcoin network”
  - Verify it to make sure it’s “correct”
- How do I continue to learn about the blockchain?
  - Participate in the network

## Steps

1. Download and verify software


download bitcoin

AI Mode | All | News | Images | Videos | Short videos | Shopping | More | Tools

Bitcoin.org
https://bitcoin.org › download

Download Bitcoin Core

**Download Bitcoin Core** (version 28.1) for Windows, macOS, or Linux. Ensure you have enough bandwidth and 7GB of storage for initial sync.

Requirements | Show version history | Features | Get Help

Google
https://play.google.com › store › apps › details › id=com...

Bitcoin.com Wallet: Buy, Sell - Apps on Google Play

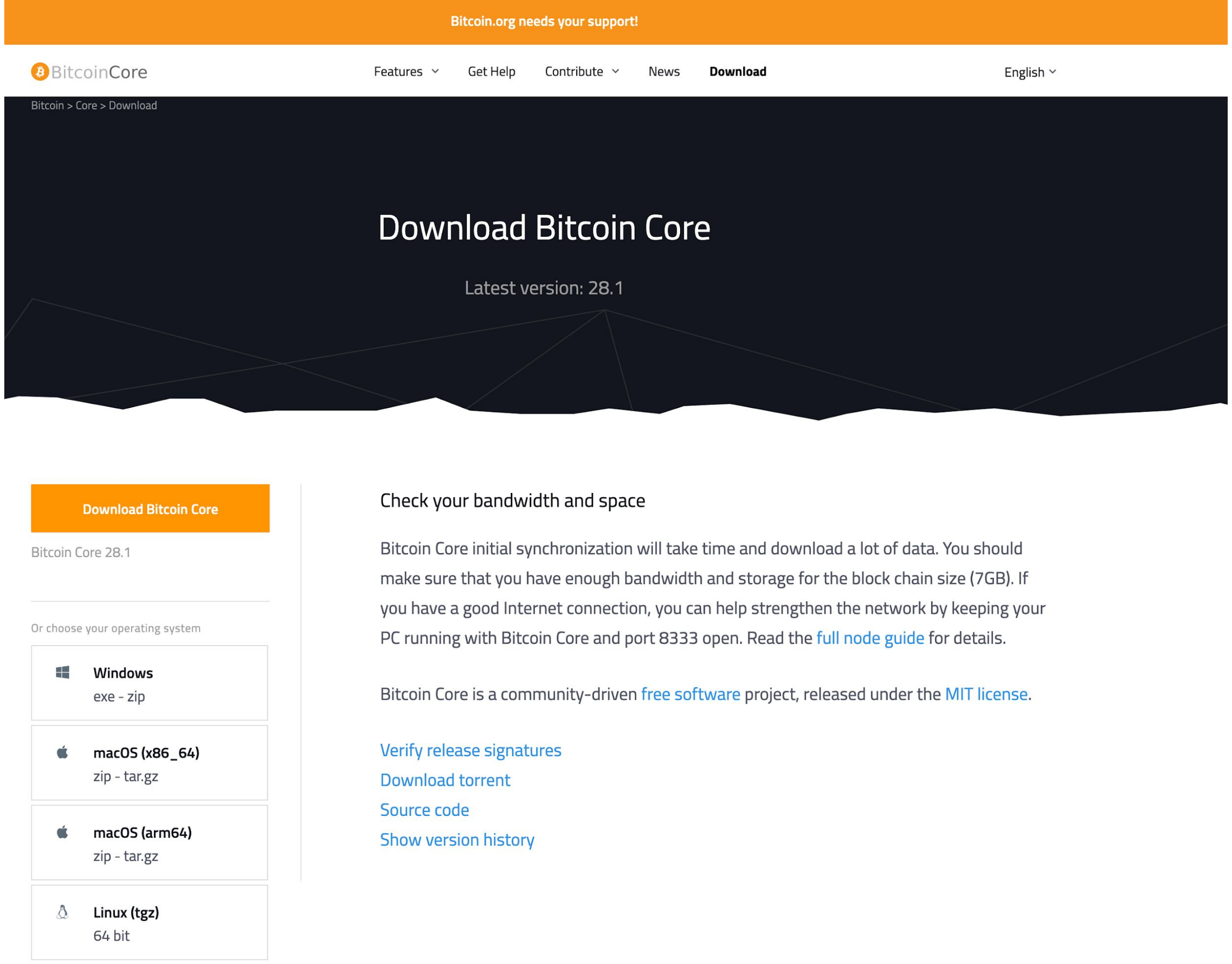
The most secure, **easy-to-use multichain crypto wallet** that gives you full control of your assets. Buy, sell, send, receive, and swap major cryptocurrencies:

4.7 ★★★★½ (77,393) · Free · Android · Finance

bitcoincore.org
https://bitcoincore.org › download

Bitcoin Core :: Download

**Bitcoin Core can be downloaded for Windows, macOS, and Linux.** Download verification is recommended to ensure you have the correct version.


Bitcoin.org needs your support!

BitcoinCore

Features | Get Help | Contribute | News | **Download** | English

Bitcoin > Core > Download

# Download Bitcoin Core

Latest version: 28.1

**Download Bitcoin Core**

Bitcoin Core 28.1

Or choose your operating system

**Windows**
exe - zip

**macOS (x86_64)**
zip - tar.gz

**macOS (arm64)**
zip - tar.gz

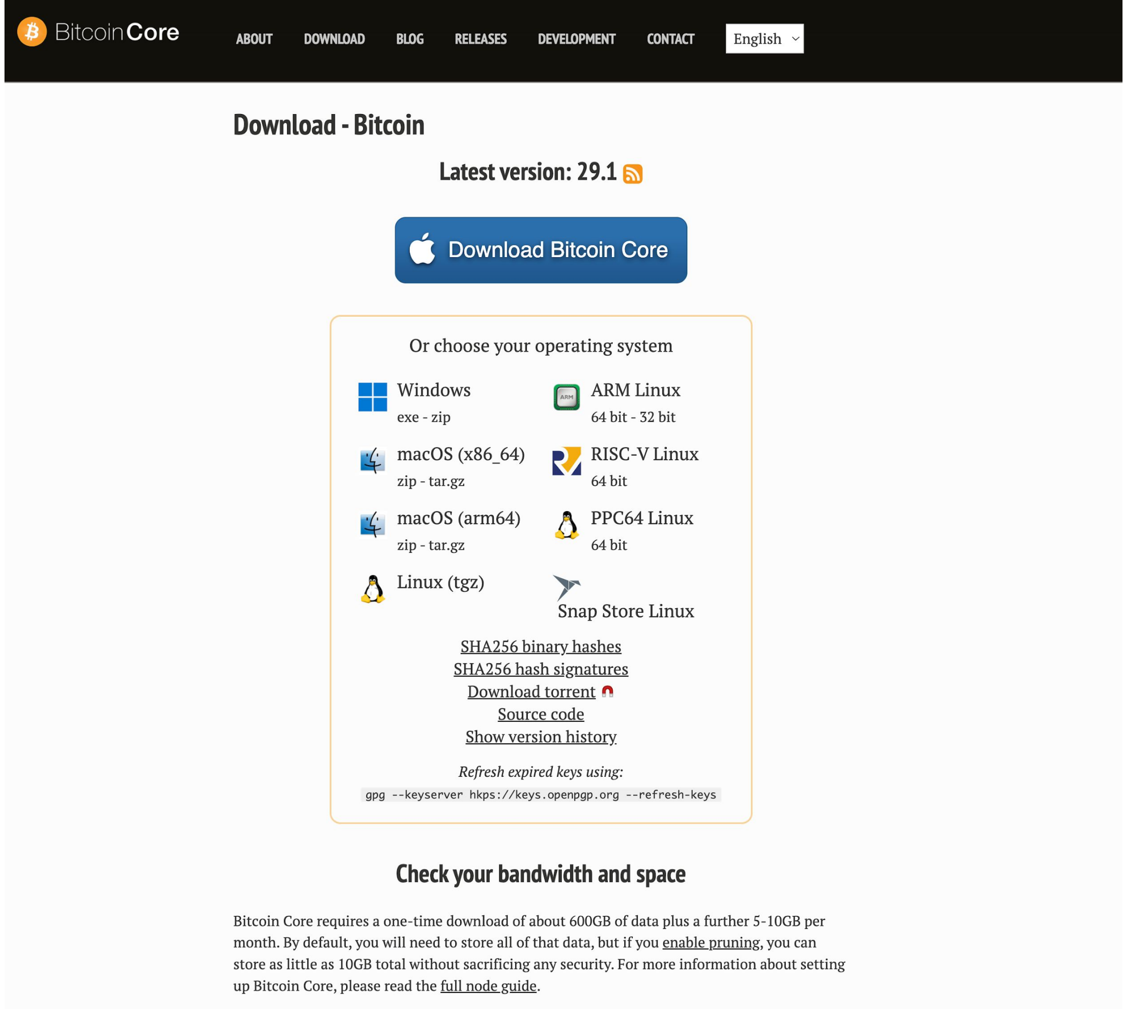
**Linux (tgz)**
64 bit

## Check your bandwidth and space

Bitcoin Core initial synchronization will take time and download a lot of data. You should make sure that you have enough bandwidth and storage for the block chain size (7GB). If you have a good Internet connection, you can help strengthen the network by keeping your PC running with Bitcoin Core and port 8333 open. Read the full node guide for details.

Bitcoin Core is a community-driven free software project, released under the MIT license.

Verify release signatures
Download torrent
Source code
Show version history



## Download - Bitcoin

**Latest version: 29.1**

Download Bitcoin Core

Or choose your operating system

| | |
|---|---|
| Windows<br>exe - zip | ARM Linux<br>64 bit - 32 bit |
| macOS (x86_64)<br>zip - tar.gz | RISC-V Linux<br>64 bit |
| macOS (arm64)<br>zip - tar.gz | PPC64 Linux<br>64 bit |
| Linux (tgz) | Snap Store Linux |

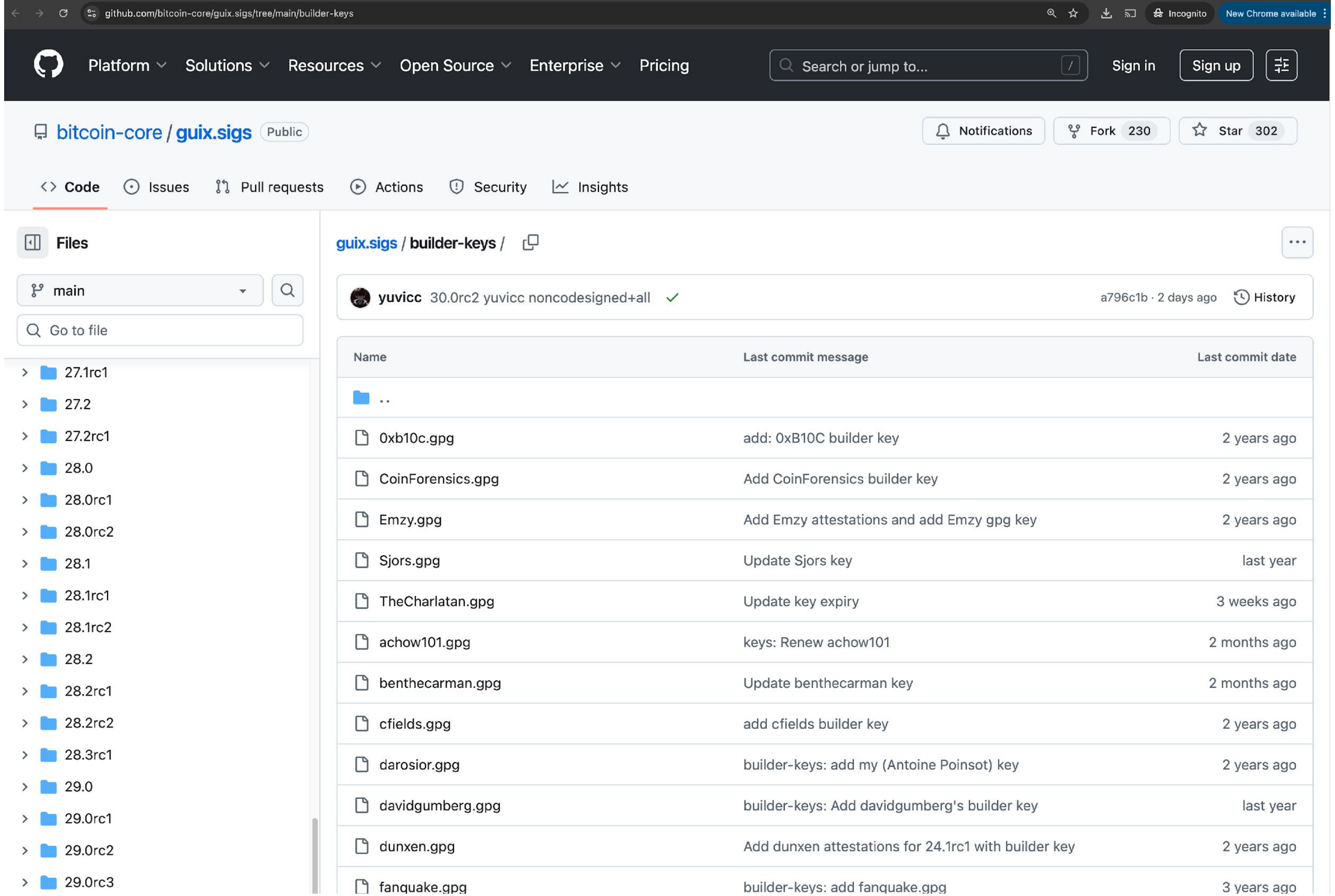
SHA256 binary hashes
SHA256 hash signatures
Download torrent
Source code
Show version history

*Refresh expired keys using:*

```
gpg --keyserver hkps://keys.openpgp.org --refresh-keys
```

**Check your bandwidth and space**

Bitcoin Core requires a one-time download of about 600GB of data plus a further 5-10GB per month. By default, you will need to store all of that data, but if you enable pruning, you can store as little as 10GB total without sacrificing any security. For more information about setting up Bitcoin Core, please read the full node guide.


github.com/bitcoin-core/guix.sigs/tree/main/builder-keys

bitcoin-core / guix.sigs Public

Notifications | Fork 230 | Star 302

Code | Issues | Pull requests | Actions | Security | Insights

Files

main

Go to file

- 27.1rc1
- 27.2
- 27.2rc1
- 28.0
- 28.0rc1
- 28.0rc2
- 28.1
- 28.1rc1
- 28.1rc2
- 28.2
- 28.2rc1
- 28.2rc2
- 28.3rc1
- 29.0
- 29.0rc1
- 29.0rc2
- 29.0rc3

guix.sigs / builder-keys /

yuvicc 30.0rc2 yuvicc noncodesigned+all ✓ a796c1b · 2 days ago History

| Name | Last commit message | Last commit date |
|---|---|---|
| .. | | |
| 0xb10c.gpg | add: 0xB10C builder key | 2 years ago |
| CoinForensics.gpg | Add CoinForensics builder key | 2 years ago |
| Emzy.gpg | Add Emzy attestations and add Emzy gpg key | 2 years ago |
| Sjors.gpg | Update Sjors key | last year |
| TheCharlatan.gpg | Update key expiry | 3 weeks ago |
| achow101.gpg | keys: Renew achow101 | 2 months ago |
| benthecarman.gpg | Update benthecarman key | 2 months ago |
| cfields.gpg | add cfields builder key | 2 years ago |
| darosior.gpg | builder-keys: add my (Antoine Poinsot) key | 2 years ago |
| davidgumberg.gpg | builder-keys: Add davidgumberg's builder key | last year |
| dunxen.gpg | Add dunxen attestations for 24.1rc1 with builder key | 2 years ago |
| fanquake.gpg | builder-keys: add fanquake.gpg | 3 years ago |

## Steps

1. Download and verify software
2. Connect to hardcoded DNS seed peers

# Principles of synchronization

- Don’t know any identities
- Assume everyone is an attacker
- Minimize what you download, maximize what you can verify

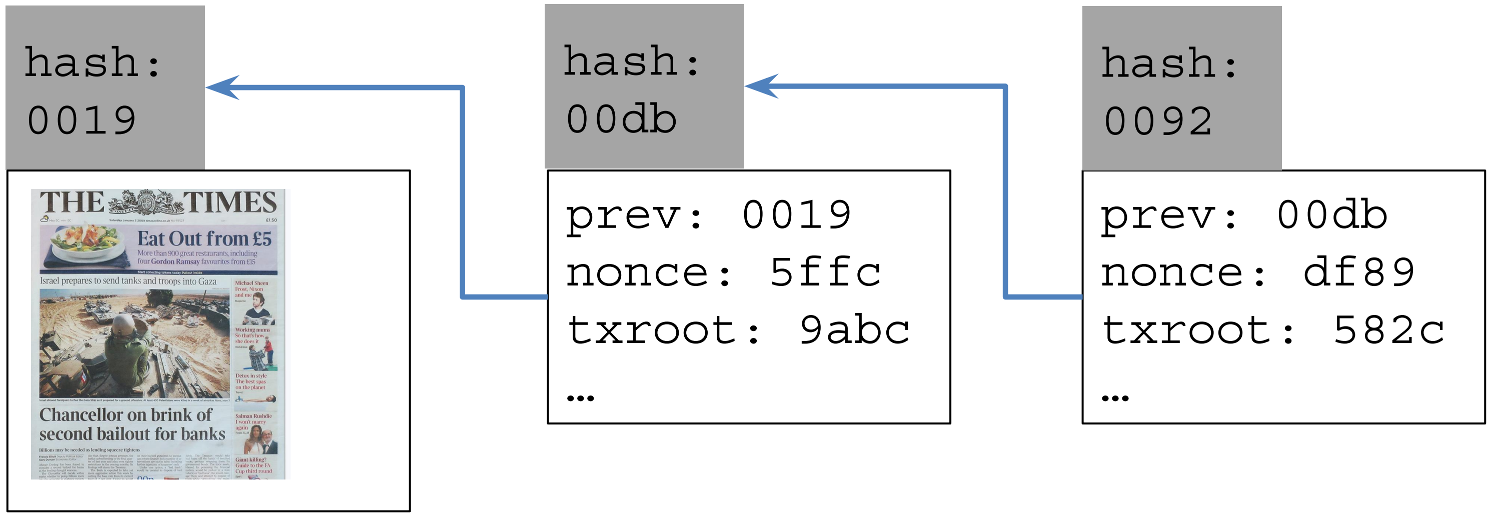
# Types of information to share

- Hello! Here is how I operate
- Here is the blockchain
- Here are other nodes I know about
- Here are some transactions

# Steps

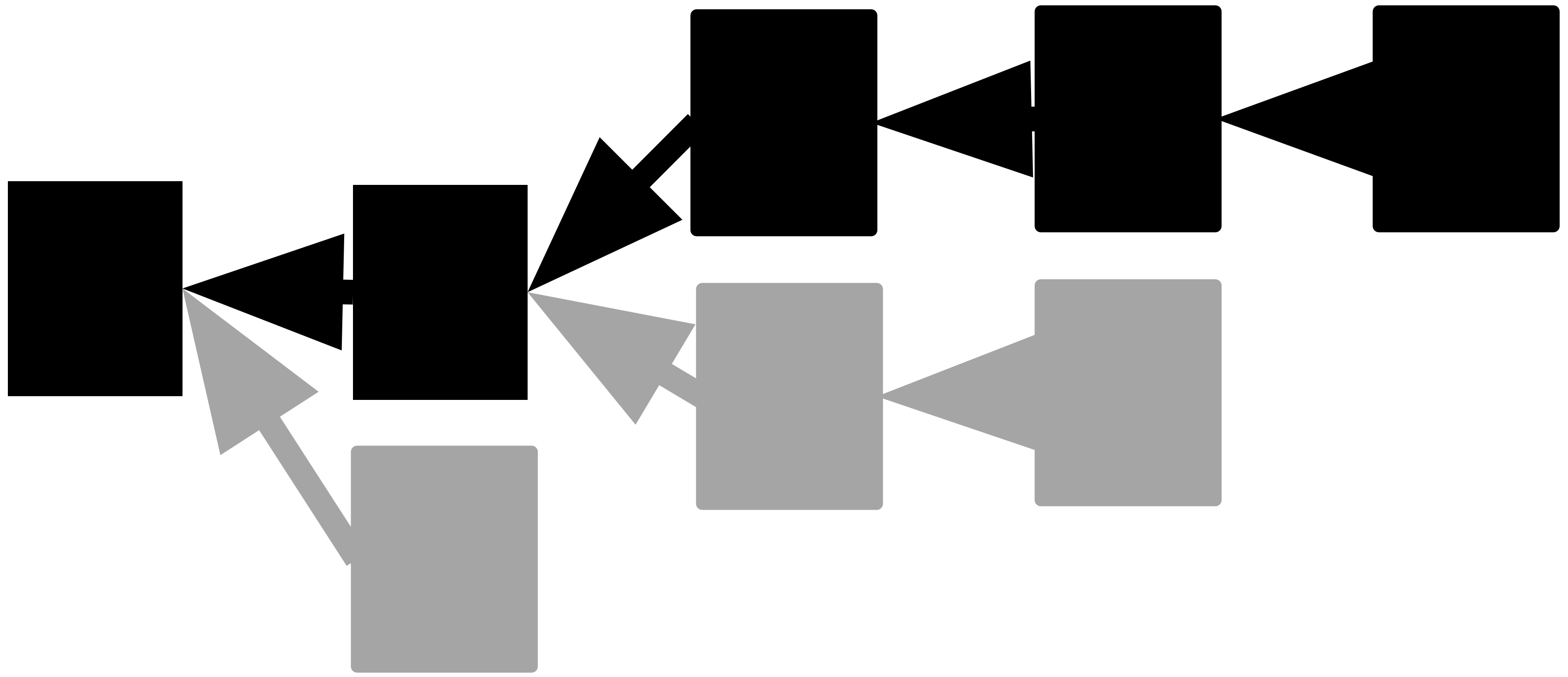
1. Download and verify software
2. Connect to hardcoded DNS seed peers
3. Ask for headers, download and verify

# Blockchain


hash:
0019
THE TIMES
Eat Out from £5
More than 900 great restaurants, including four Gordon Ramsay favourites from £15
Israel prepares to send tanks and troops into Gaza
Michael Sheen Frost, Nixon and me
Working mums So that's how she does it
Detox in style The best spas on the planet
Chancellor on brink of second bailout for banks
Billions may be needed as lending squeeze tightens
Salman Rushdie I won't marry again
Giant killing? Guide to the FA Cup third round
hash:
00db
prev: 0019
nonce: 5ffc
txroot: 9abc
...
hash:
0092
prev: 00db
nonce: df89
txroot: 582c
...

Genesis block

# Actually we store a block header tree



# Block headers

| field | size | purpose |
|---|---|---|
| version | 4B | Block version |
| prev hash | 32B | Hash of previous block |
| Merkle root | 32B | Root of merkle tree of all transactions |
| time | 4B | Unix timestamp |
| difficulty | 4B | Proof-of-work target |
| nonce | 4B | To calculate proof-of-work |

# Header validation rules

- Enough proof of work
- Prev block hash pointers
- Block timestamps
- Correct difficulty

## Steps

1. Download and verify software
2. Connect to hardcoded DNS seed peers
3. Ask for headers, download and verify
4. Ask for blocks, download, verify, and update UTXO set and mempool

# IBD: Initial Block Download

- 600 GB+ of data
- Do you need to download this?
- Do you need to store this?

# Block validity rules

- Block size
- Merkle tree
- For each transaction:
  - Sum(inputs) >= Sum(outputs)
  - For every input
    - Eval(scriptSig+scriptPubKey) == true
    - Output has not already been spent
  - lock_time
- Coinbase transaction preserves supply rules

# Update local datastructures

- UTXO set
- Mempool
- Undo data
- Transaction indexes

## Steady state operation

- IBD: Goal is to maximize bandwidth
- Steady state: minimize latency, partition resistance
  - Learn about all new blocks quickly

# Types of information to share

- Hello! Here is how I operate
- Here is the blockchain
- Here are other nodes I know about
- Here are some transactions

## Existing on the open internet

- The internet is a scary place!
- Any node might be trying to attack you
- Keep a lot of information on peer behavior, maybe disconnect peers
- Risk: eclipse attacks

# Avoiding partitions

- What is a partition?
- Why is a partition dangerous?

# Other ways to verify I got paid

- Ask someone and trust their answer
- Simple Payment Verification (SPV): The reason behind the transaction merkle tree
  - Only can prove inclusion, not exclusion
  - But doesn't require download the entire blockchain