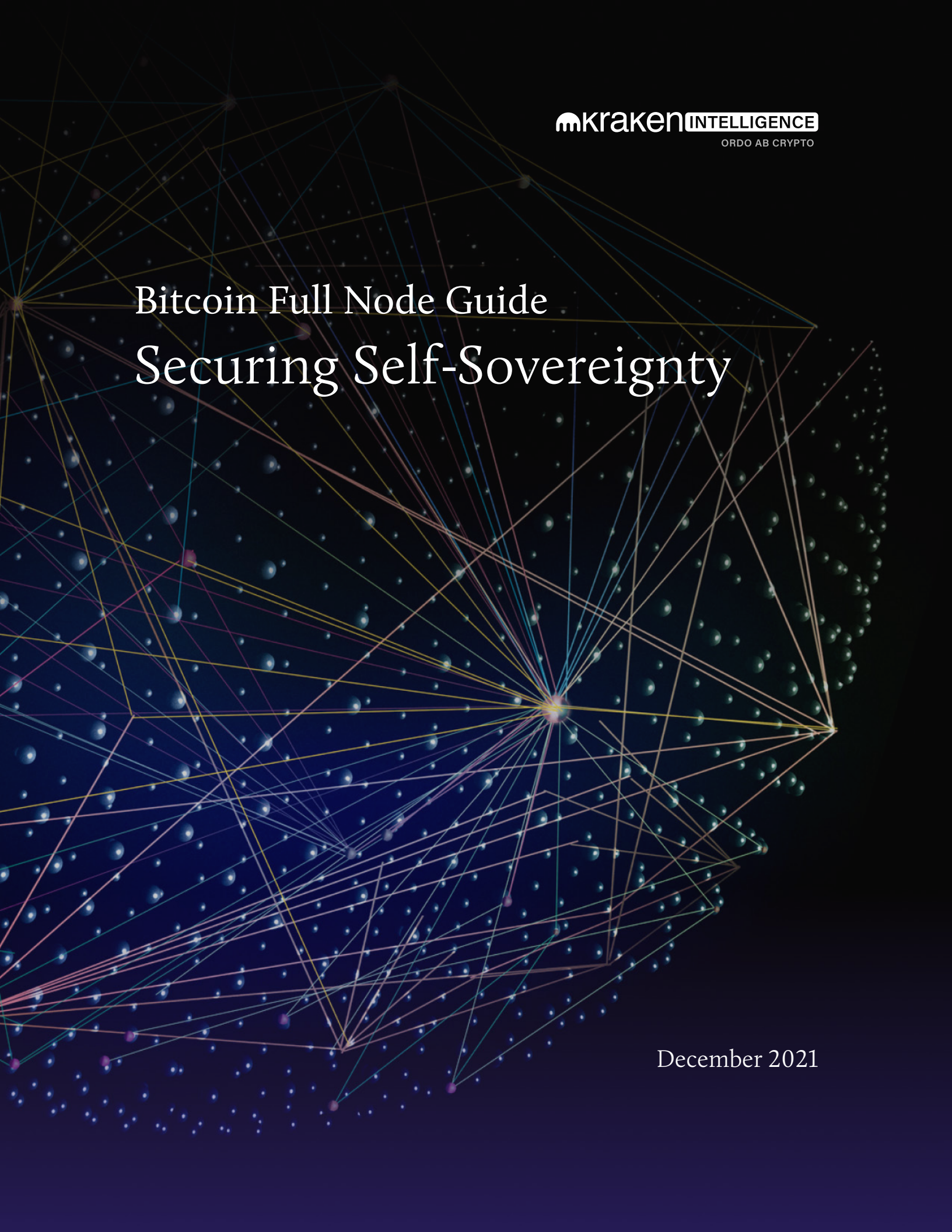


kraken INTELLIGENCE
ORDO AB CRYPTO

Bitcoin Full Node Guide
Securing Self-Sovereignty

December 2021

INTELLIGENCE
ORDO AB CRYPTO

Table of Contents

1.	Introduction
2.	What Is a Full Node?
3.	Step-By-Step: How to Setup and Use a Full Node
4.	Conclusion

Disclosures

This report has been prepared solely for informative purposes and should not be the basis for making investment decisions or be construed as a recommendation to engage in investment transactions or be taken to suggest an investment strategy with respect to any financial instrument or the issuers thereof. This report has not been prepared in accordance with the legal requirements designed to promote the independence of investment research and is not subject to any prohibition on dealing ahead of the dissemination of investment research. Reports issued by Payward, Inc. ("Kraken") or its affiliates are not related to the provision of advisory services regarding investment, tax, legal, financial, accounting, consulting or any other related services and are not recommendations to buy, sell, or hold any asset. The information contained in this report is based on sources considered to be reliable, but not guaranteed to be accurate or complete. Any opinions or estimates expressed herein reflect a judgment made as of this date, and are subject to change without notice. Kraken will not be liable whatsoever for any direct or consequential loss arising from the use of this publication/communication or its contents. Kraken and its affiliates hold positions in digital assets and may now or in the future hold a position in the subject of this research.

1.

Introduction

Bitcoin's reputation as the soundest form of money is largely underpinned by its decentralized blockchain network. The network comprises globally distributed computers, known as "nodes," that connect to each other and are run by anyone in the world with access to a modern-day computer and an internet connection. While roughly 31% of the world is unbanked, Bitcoin is an opportunity for virtually anybody worldwide to become their own bank.[1] Running a full node is the only way to use Bitcoin without reliance on a third party. Full node operators foster Bitcoin and support the network to become more decentralized. They ensure that Bitcoin has no single point of authority or failure that dictates the actions of the rest of the network. Instead, Bitcoin relies on a broad consensus of these full nodes to validate and secure transaction data on the network. Full nodes also allow market participants to transparently view data on the network by publicly hosting a copy of the blockchain.

The primary function of Bitcoin nodes is to ensure blockchain data is valid, secure, and accessible to virtually anyone. Though many assume running a node is a purely altruistic endeavor to bolster the Bitcoin network, using a node to verify transactions offers users by far the best privacy and security assurance. In this report, the Kraken Intelligence team analyzes what a Bitcoin full node is, why you should consider running one, and how to set one up and use it to verify your transactions.

2.

What is a Node?

A node is a device, such as a computer or mobile phone, connected to the Bitcoin network by running Bitcoin's software, also known as the Bitcoin Client. Nodes connect to other computers running the same software (i.e., peer nodes) to create the peer-to-peer Bitcoin network. Most nodes connect via the Internet, but some connect indirectly via satellite, radio, or mesh networks. Nodes fulfill three prominent roles:

Role 1: Store the blockchain ledger's transaction history

All nodes contribute to building and maintaining the blockchain, which is a list of all confirmed Bitcoin transactions, by validating transactions confirmed initially by miners. A copy of all historical transactions is recorded on the Bitcoin blockchain via its network of nodes. Every node keeps a copy of the blockchain and continuously appends it with newly confirmed transactions as they come in.

Role 2: Relay information to other nodes to validate new blocks proposed by miners

Nodes communicate with each other to share the latest transaction information for consensus-building. By sharing information amongst each other, nodes allow everyone on the network to stay up-to-date with what's going on in other parts of the network (e.g., new transactions)—a vital component for overseeing a global digital cryptoasset. Nodes share two types of transactions: confirmed and pending transactions. Confirmed transactions have been validated and added to the blockchain by the miner(s). These transactions are batched in blocks of transactions rather than individually. On the other hand, pending transactions that are not yet added to the blockchain sit in Bitcoin's "mempool" (memory pool). The mempool is effectively a waiting room for pending transactions that are later picked up by miners and included in a block.

Though commonly conflated with "miners," Bitcoin nodes cooperate with Bitcoin miners to maintain the network's integrity. Specifically, nodes ensure no bad actors successfully propose fraudulent transactions before adding them to their mempool. Meanwhile, miners pick up transactions sitting in the mempool and add them to the blockchain. Nodes adjust the mining difficulty to calibrate Bitcoin's average block time, or the time it takes to confirm a new block, to 10 minutes; pseudonymous Bitcoin creator Satoshi Nakamoto called this the "timechain."[2]

Role 3: Follow and enforce the Bitcoin protocol

Each node is programmed to follow the Bitcoin protocol. If a node does not adhere to Bitcoin's rules and shares an invalid block containing one or more fraudulent transactions (e.g., double-spend), other peer nodes reject the "invalid" node from the network. By broadcasting and relaying transactions to other nodes, they can compare blocks proposed by miners to verify their authenticity and effectively weed out bad actors without the need for a centralized intermediary. For instance, if someone broke the rule of sending more bitcoins than they held, all nodes would not validate the transaction.

Some examples of consensus rules include:

- Bitcoin(s) cannot be double-spent under any circumstances.
- Transactions must be signed by the owner(s) of the bitcoin(s) before being spent.
- The block subsidy cannot exceed a certain amount (฿6.25 at the time of publication).
- Transactions and blocks must be in the appropriate data format.

In sum, Bitcoin nodes maintain the reliability of the data stored on the blockchain. Though only one node is necessary to maintain an entire blockchain's history, this system reduces the network to a single point of failure. A blockchain without a decentralized network of nodes is less resilient to threats such as system failures, power outages, or network attacks by malicious actors.

Types of Nodes

Not all nodes are created equal. For instance, nodes containing a full copy of the blockchain ledger used to enforce the network's consensus rules and validate new transactions are full nodes. Most full nodes support the network by validating transactions and blocks before relaying them to more full nodes. Full nodes often serve lightweight nodes, or Simple Payment Verification (SPV) wallets, which only contain a partial copy of the blockchain by allowing them to transmit their transactions to the network through full nodes.

The scope of this report is limited to the two types of nodes defined in the Bitcoin whitepaper—full nodes and SPV clients:

Full Node

A device running software that independently verifies the state of the Bitcoin blockchain by downloading every block and transaction in Bitcoin's nearly 13-year history and checking them against Bitcoin's consensus rules. If a transaction or block violates Bitcoin's consensus rules, a full node will automatically reject it. Full nodes broadcast, verify, and store transactions, effectively acting both as gateways to the network and an information expressway to share network data amongst all participants. Many full nodes also help lightweight nodes by transmitting transactions from the lightweight node's wallet to the network and alerting them when a transaction goes in or out. A single full node will typically connect to eight to ten other nodes.

Figure 1

Full Node

Pros	Cons
Trustless: Does not require trust in a third party to become your own bank. You can conduct borderless transactions that you self-verify to ensure every party acts honestly.	**Data-intensive:** Requires operators to hold +350 GB of data and continuously validate incoming transactions and blocks.
Rule enforcement: Full nodes automatically reject fraudulent transactions, effectively ensuring that no one is breaking the system's rules.	**Maintenance:** Full node operators should upkeep their node, upgrading it as new versions are released, keeping it on to stay in sync with the chain and relay transactions, and ensuring the device's storage is future-proof.
Security: Because you don't need to trust a third party, you can independently verify if any transaction is fraudulent and avoid any potential financial harm.	**Inconvenient:** Carrying around a device with hundreds of GBs of data to verify transactions is cumbersome.
Privacy: Using centralized services often exposes private information that can be leaked publicly.	**Less user-friendly:** The UI is not as straightforward as traditional financial systems. Also, independently verifying transactions requires fundamental knowledge of how Bitcoin works.

Lightweight Node

While full nodes are the cornerstone of the Bitcoin network, lightweight nodes provide market participants easier access to the network. Many lightweight nodes use a method called Simple Payment Verification (SPV), which Satoshi defined in the Bitcoin whitepaper, to verify transactions without downloading the entire blockchain. However, SPV clients can't verify the whole blockchain's transactions. Instead, they only download the block headers only to validate the authenticity of the transactions.[3] These nodes act as intermediaries between the sender and a full node, querying other full nodes when data is required to confirm payment. SPV wallets are significantly cheaper to maintain than full nodes because they don't process large amounts of data through the network. They were historically used in many mobile Bitcoin wallets, though they have since become rarer. SPV clients (e.g., mobile wallets) trust most miners without checking the validity of the blocks they produce. While it would require a majority of miners to mislead an SPV client, they can theoretically make the SPV client

believe anything. However, malicious acts are difficult to execute because full nodes reject invalid blocks. Lightweight nodes typically connect to four other nodes. Though Satoshi described the design for SPV in the 2008 white paper, it wasn't implemented until two years later when Mike Hearn created BitcoinJ, a Java implementation of the Bitcoin protocol.[4] Still, it wasn't until 18 months later that developers published Bitcoin Improvement Proposal (BIP) 37 on November 30th, 2016, providing a specification for "Bloom filtering" of transactions. Put simply, this allowed SPV clients to rely upon the block header to prove the inclusion of a transaction in a block. This provided significantly reduced bandwidth usage, as Satoshi initially described in the whitepaper.

However, not all lightweight nodes function this way. Some light wallets are built to receive their blockchain data from multiple sources. For example, the service would check several block explorers (e.g., blockchain.com, blockchair, blockcypher, and tokenview) to remove the single point of failure within SPV clients. Though it's more unlikely that many block explorers are colluding to trick users, users still must trust others for this data. Multiple block explorers can still lie, or even the third party sourcing data from these block explorers.

Figure 2

Lightweight Node

Pros	Cons
More convenient: Is easily run on any mobile device.	**Less privacy:** SPV clients that use "bloom filtering" have proven issues that can expose private information. Though these issues are managed by splitting bloom filters amongst peers, this step places more load on full nodes. Web wallets that source data from multiple block explorers can also leak private user data.
Cheaper: Consumes less resources since it does not continuously validate pending transactions.	**Less security:** Trust in third parties introduces vulnerabilities, such as a manipulated block explorer that feeds incorrect transaction information to trick an SPV client.
User-friendly: Many lightweight nodes are optimized for beginners, only requiring a basic understanding of Bitcoin addresses.	**Requires trust:** Cannot use Bitcoin without relying on a centralized third party.

Why Run a Full Node?

> *"Trusted third parties are security holes."*
> —Nick Szabo

The saying, "Not your keys, not your coins," also extends to Bitcoin nodes—"Not your node, not your rules." The same way managing your own keys ensures you can't lose your bitcoin due to the malevolence or negligence of a third party, running a full node guarantees you can't be fooled into accepting invalid bitcoin payments. Running a full node allows you to self-verify transactions rather than rely on a third party node. The benefits of running and using your own node include:

Trustlessness When Transacting

Bitcoin was designed to operate without requiring users to trust anyone for the system to function properly. Full nodes remove the need to trust a third party's honesty about the ledger because the operator owns their own copy of the ledger. However, out of convenience, users often end up relying on third parties (e.g., block explorers and wallet service providers) that run full nodes to verify their transactions for them. This implies users must trust that this third party won't feed them unreliable or dishonest information. SPV wallets aren't trustless since they require users to believe that most of the network's hash power is conforming to the rules. Though there are many reliable third-party sources, securing self-sovereignty requires users to self-verify their transactions with their full node. Without a network of nodes ensuring that every transaction and block is valid, it wouldn't be possible for Bitcoin users to know if others are breaking the network's rules, such as double spending transactions or issuing more BTC than the 21 million total supply. To truly become self-sovereign, one cannot rely on others to prove their ownership of coins; it must be self-verified. If you run a full node and nobody looks at the transactions it validates, it is contributing to the network but isn't not helping reduce the need for trust. Bitcoin Core developer Pieter Wuille once said, "One of Bitcoin's strengths—the most important in my opinion even—is the low degree of trust you need in others."

Security

Because full nodes allow users to transact without needing to trust a third party, they also offer the best security model. Trust in a centralized third party inherently comes with inevitable security vulnerabilities, especially in a $1.25T global financial network. For example, a compromised third-party wallet service could make its users a target for bad actors in rare cases. By using a centralized wallet, users place complete trust in the third party to run a node that enforces the network's rules. Even if the third party is established and relatively trustworthy, it can still become compromised by hackers, leak user data that could lead to phishing attacks, or even turn on its user base. By running and using a full node to verify transactions, users effectively shield themselves against fraud on the Bitcoin network. Said differently, if only a few prominent players (e.g., block explorers) were running full nodes, it would only require a malicious intent or an attack against them to change the system's rules because nobody else is validating the authenticity of transactions.

Privacy

Using a centralized wallet or crypto service running its own full node lets the service provider see all the transactions and addresses connected to your wallet. Privacy issues still arise even when using some SPV wallets (lightweight nodes), namely, those that use "Bloom Filtering."[5] Full nodes offer the best privacy as node operators download all the blockchain data and only query for addresses or transactions locally, meaning third parties can't see your search history.

Rule Enforcement

Full nodes autonomously reject rule-breakers as long as they are up and running. Thus, running a fully validating Bitcoin node and using it to verify payments you receive is the only way to enforce the rules to which you agree.

Providing Altruistic Support to the Network's Health

While many misconstrue that miners control the network, in reality, it's the nodes that are in charge. Nodes configured to accept incoming connections altruistically bolster the network by sharing blocks and transactions with other full nodes to help them sync and service data requests from SPV wallets. Put briefly, the network's resilience against attacks is proportional to the number of people actively running full nodes and auditing the network's transactions.

More nodes on the network also strengthen the blockchain against political attack vectors. For instance, if a regulator cracks down on Bitcoin nodes and causes operators in its jurisdiction to shut down operations, nodes outside of the jurisdiction would remain online, defending the network's safety.

Therefore, conducting BTC transactions helps the cryptoasset's offering as a medium of exchange, running a full node bolsters the network, and using a full node to verify your transactions helps you and the ecosystem reduce the need for trust.

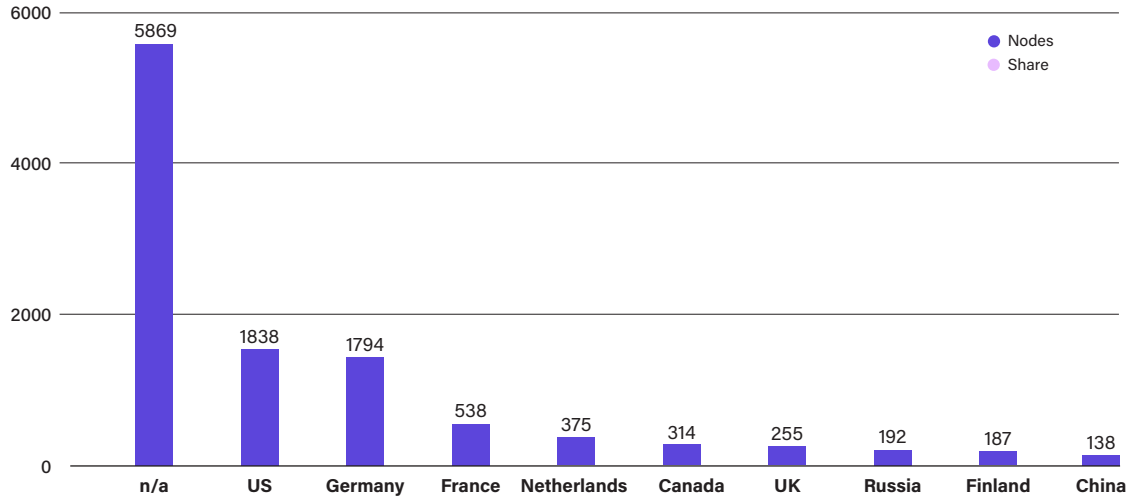
Geographical Distribution of Nodes

There is no foolproof way to count the total number of Bitcoin nodes because they can operate privately, recording blocks and transactions without broadcasting them to the rest of the network. Nodes may lay behind firewalls, or they might not be configured to listen for connections. Moreover, nodes leave and rejoin the network as they please, meaning the total number of nodes is likely much higher than our best estimates, which are limited to active nodes. According to data from Bitnodes, there were 14,078 reachable full nodes on the Bitcoin network at the time of writing.[6] Though individuals can run multiple nodes, this at least means less than 14K people on the network trust a third party to verify their transactions. Though it's challenging to narrow down the geographic distribution of most nodes due to their usage of virtual private networks (VPNs), most identifiable full nodes are situated in the United States (13.86%) and Germany (13.53%), followed by France (4.06%), the Netherlands (2.83%), and Canada (2.37%). The location of more than 44% of reachable

nodes are situated in the United States (13.86%) and Germany (13.53%), followed by France (4.06%), the Netherlands (2.83%), and Canada (2.37%). The location of more than 44% of reachable nodes is unidentifiable due to the use of virtual private networks (VPN), which encrypt internet traffic and disguise online identities.

Figure 3

Global Distribution of Nodes



Source: Kraken Intellegence, Bitnodes

Notably, Bitcoin is not a democracy; consensus is maintained amongst all nodes running the same Bitcoin software and does not include any kind of voting or representation. However, it doesn't require 100% agreement between nodes either. Consensus is an ideal in that there is no absolute agreement between all parties involved in most cases; in a consensus-based system like Bitcoin, changes are only implemented if it's a non-contentious proposal.

Consensus is achieved at the source code level by allowing anyone to propose, review, and comment on changes. Overall consensus in any changes would mean agreement amongst nodes is near-unanimous, though there is no defined threshold. Any changes with a significant portion of disagreement amongst nodes would result in a hard fork

(e.g., Bitcoin Cash). This process ensures equal footing in that no special interests are prioritized over others.

At the blockchain level, consensus is maintained by all nodes running the same software. All active nodes must agree on fundamental rules, including how many new BTC are created per block and the exact state of the chain (i.e., which blocks and transactions make up the blockchain). If nodes disagree on these rules, the network will split, and the blockchain will fork into several chains. Reconciling a chain split is virtually impossible, which is why it takes time to review, agree upon, and implement changes to the network.

Therefore, for Bitcoin to be sufficiently decentralized, it should have a network with nodes distributed worldwide to allow people of all different walks of life to contribute to the Bitcoin network. A globally decentralized network is a feature necessary for a borderless asset.

3.

Step-By-Step: How to Setup and Use a Full Node

Considerations

With Bitcoin, you can be your own bank. However, that also means you're 100% responsible for protecting your coins. Please understand that funds can be permanently lost if mistakes are made when using and interacting with distributed blockchain networks, like Bitcoin. Thus, common rules of thumb include backing up your computer's data and **never** depositing more value in your wallet than you are willing to lose. Of note, it's possible to safely run a full node to support the network and use its wallet, but the users must take **the same precautions** they would take when using any Bitcoin wallet.

Setting up a Bitcoin Core full node is the main focus of this guide. Bitcoin Core is a community-driven free software project released under the MIT license.[7] Over 99% of Bitcoin nodes utilize this software, although at least 6 other software implementations exist. Though Bitcoin Core full nodes can run on outdated computer equipment, it's recommended that a node is set up on a modern-day computer that meets the following minimum requirements:

- A computer running either a Windows, Mac OS X, or Linux operating system.
- 7 GB of free disk space, accessible at a minimum read/write speed of 100 MB/s.[8]
- 2 GB of RAM.
- A broadband Internet connection with upload speeds of at least 400 kilobits (50 kilobytes) per second.

- An unmetered connection, a connection with high upload limits, or a connection you regularly monitor to ensure it doesn't exceed its upload limits. It's common for full nodes on high-speed connections to use 200 GB upload or more a month. Download usage is around 20 GB a month, plus around 350 GB the first time you start your node.
- 6–24 hours a day that your full node can be left running.[9]

Step 0: Select a Device and OS

First, you will want to select a device to install Bitcoin Core, such as:

- A desktop computer or a laptop (Linux, Mac OS X, or Windows 10).
- A Raspberry Pi (Linux).
- A specialized device purchased from a third party manufacturer (typically Linux).
- A compatible Android smartphone or tablet (Android).[10]

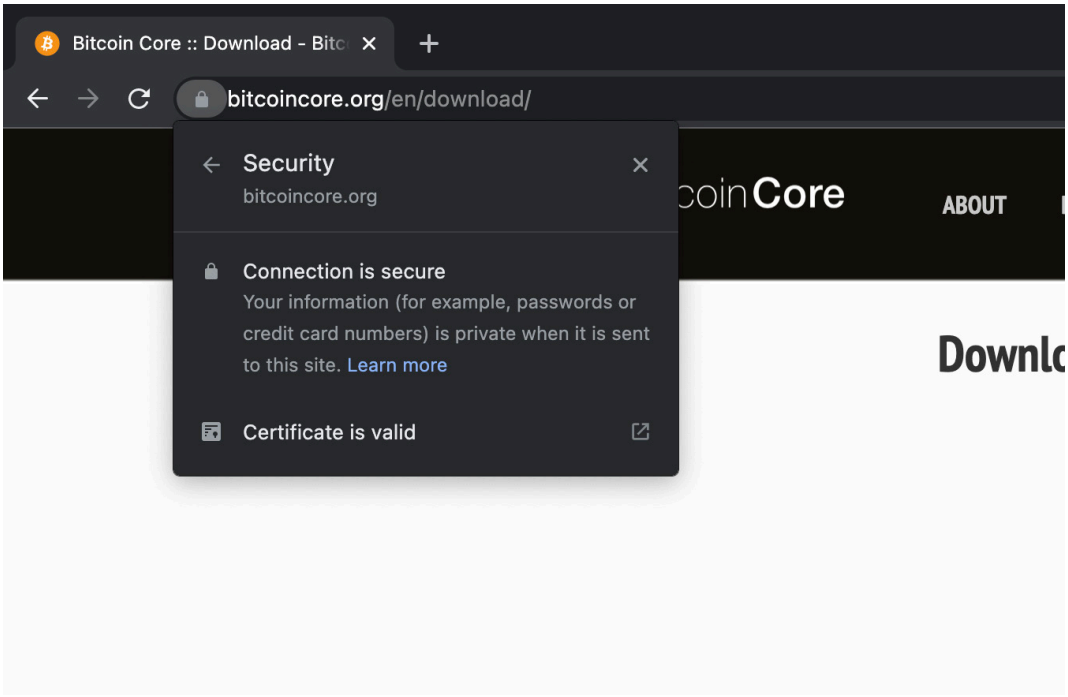
Running a full node on an Android device or Raspberry Pi, which runs on Linux, better suits more tech-savvy users. Thus, we don't cover Bitcoin Core installation on any Linux device in this guide. Utilizing an existing Windows or Mac computer that runs at least six hours a day is recommended for new users looking to run a full node. You should also check your local laws to ensure there are no restrictions for operating a full node.

Once you've selected a device to run your full node on, it's time to download Bitcoin Core.

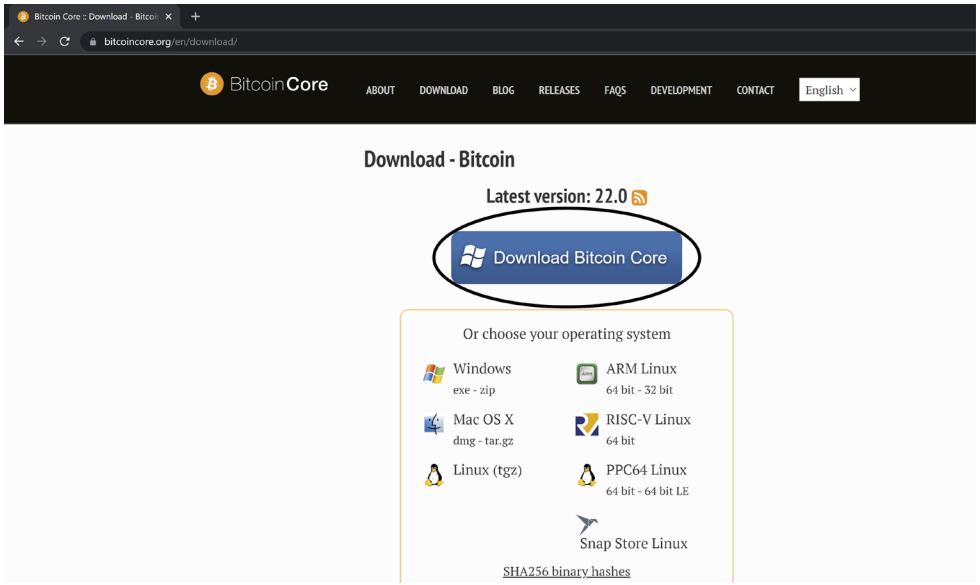
Setting Up on Windows 10

Step 1: Download and Install Bitcoin Core

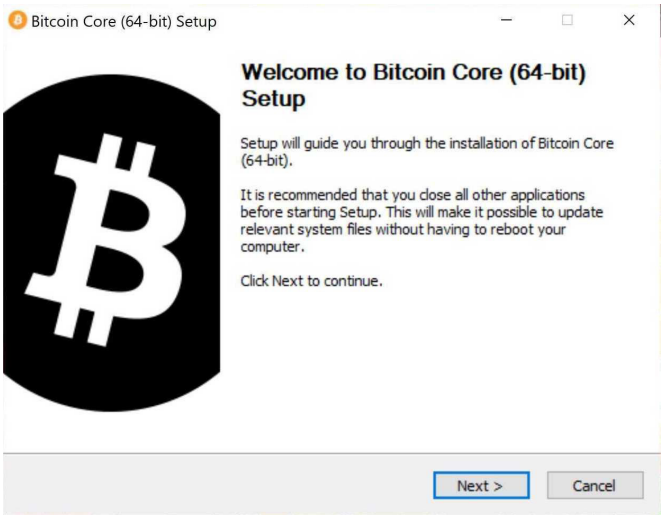
Navigate to Bitcoin Core's **download page**, **always** double-checking URLs to ensure you are on the correct page and verifying you have made a secure connection to the server.[11]



Once you have confirmed that the URL is authentic and verified you have made a secure connection to the server, click the "Download Bitcoin Core" button.



After downloading Bitcoin Core, open the file to install the software.



*Note: Having problems opening Bitcoin Core? Read this **support article**.*[12]

[Optional] Sep 1a: Verify Release Signatures

If you're familiar with Pretty Good Privacy (PGP), an encryption program that provides cryptographic privacy and authentication for data communication, you should verify the release signatures by clicking the "Verify Release Signatures" link on the download page to download a signed list of SHA-256 file hashes. These hashes should be compared with the following fingerprint:

- 01EA 5486 DE18 A882 D4C2 6845 90C8 019E 36C2 E964—All releases after v0.11 are signed by Wladimir J. van der Laan's **releases key** with the fingerprint.[13]

Use PGP to verify the signature on the release signatures file. Then calculate the hash of the archive you downloaded. Lastly, ensure the hash matches those listed in the verified release signatures file.

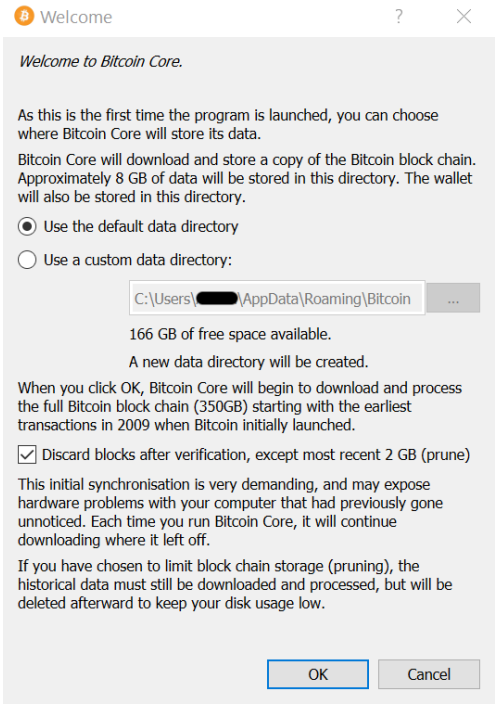
Step 2: Set up Bitcoin Core for the Initial Block Download (IBD)

After downloading and installing the Bitcoin Core software, it's time to download the

Bitcoin blockchain. This is known as the Initial Block Download (IBD), which includes every transaction in the cryptoasset's nearly 13-year history. At the time of writing, the size of the blockchain is 368 GB and growing at an average rate of 0.175 GB per day. Thus, you should choose a device that can both store the existing data as well as the future growth of the Bitcoin blockchain, which is set to reach 1 TB in 2032.

Open the file to run the program to initiate the IBD. The software will prompt you to decide where to store the Bitcoin blockchain on your computer.

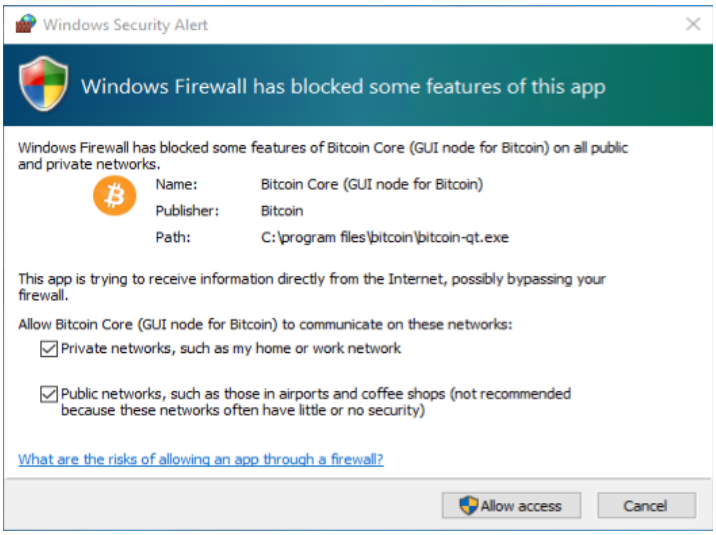
Upon selecting the location to download the Bitcoin blockchain, you will be given the option to choose whether to operate a full node in the standard way by downloading and keeping all the data (368 GB) on your computer or by "pruning," which allows you to run a full node and download and process all the blockchain's data but deletes it immediately afterward to reduce your disk usage. "Pruned" full nodes can reduce the size of the transaction history to roughly 7 GB, about the size required to store roughly 400 songs. If you don't have enough space on your hard drive or just want to refrain from overloading it with 368 GB of data, we recommend running a full node via pruning mode.



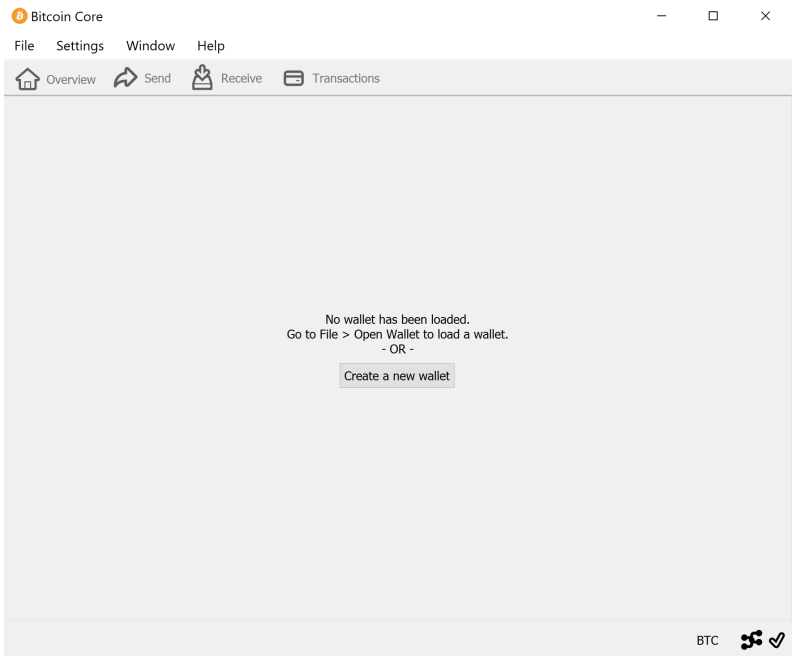
Click “OK” to complete the setup.

Step 3: Configure Firewall to Allow Bitcoin Connection on Public and Private Networks

After setting up the Bitcoin Core client for the IBD, your computer’s firewall will likely notify you that it’s trying to block your connection. If so, disable this by ticking on the following two boxes to allow Bitcoin Core to communicate on both private and public networks.



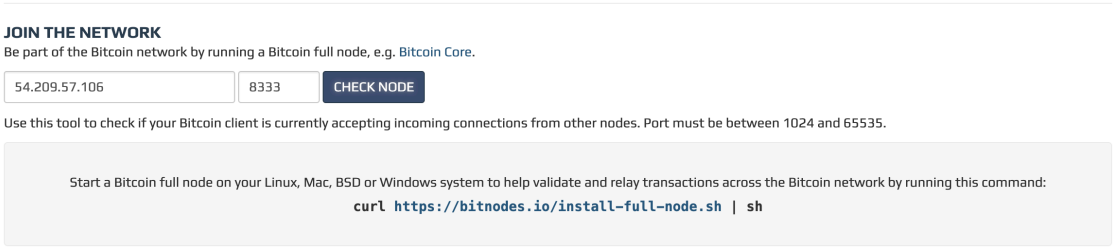
Allowing Bitcoin Core to bypass your computer’s firewall to receive information from the Internet will kickstart the IBD, downloading and validating all blocks and transactions since Bitcoin’s launch on January 3rd, 2009. The IBD is by far the lengthiest part of this process, potentially taking several hours to a few days (depending on hardware and internet speeds) to fully synchronize. Bitcoin Core uses a significant amount of connection bandwidth during the IBD process. However, you can stop Bitcoin Core at any time by closing it and it will resume from the point where it stopped the next time you start it. Notably, the IBD is only needed to be completed on your full node once; after the IBD, your full node will automatically sync with other nodes to update their ledger in real-time.



[Optional] Step 3a: Test Connections and Configure Network if Necessary

Bitcoin Core should work as intended following the IBD; however, operators who want their node to be reachable by other nodes (unnecessary for most users) should test their connections to ensure all is copacetic. To verify if your Bitcoin client is accepting incoming connections from other nodes, visit **Bitnodes.io** and enter your node's IP into the left text box (see image below) and the port into the right-side text box (port must be between 1024 and 65535).[14] Your public IP address can easily be discovered by doing a Google search of "what is my IP address," which will reveal your public IP address as the top search result. Once confirmed that you've inputted the correct IP and port, select the "**Check Node**" button, as displayed in the image below.

Once confirmed that you've inputted the correct IP and port, select the "**Check Node**" button, as displayed in the image below.

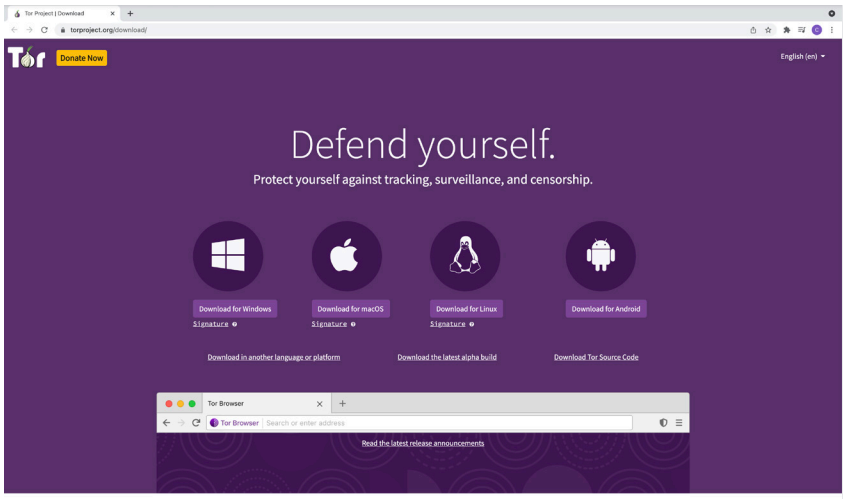


The next screen will display a green or red box. Green means your port is open and running as expected, meaning nothing further is required on your end. However, red indicates your port is closed, and further network configuration is needed to open the port. In this case, you should carefully follow **these instructions** from Bitcoin.org.[15]

[Optional] Step 4b: Connect Your Node to the Tor Network For Privacy and Security

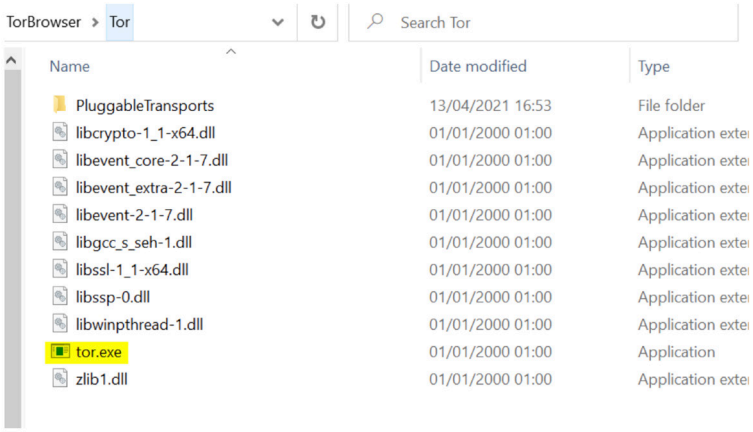
Since Bitcoin's early years, attackers have been frantically searching for different ways to attack the Bitcoin network. Though these attempts to penetrate Bitcoin have been unsuccessful, running a Bitcoin full node that isn't connected to the Tor virtual private network (VPN) may be at risk of being targeted by these bad actors as your node's IP address will be publicly exposed. Tor is a privacy-enhancing tool used by many of the most popular Bitcoin software to preserve user privacy. Though the chances of being targeted are unlikely, it's always best practice to conceal your node's identity as there is no reason to reveal your private information. By running your full node on the anonymous Tor network, blockchain onlookers won't be able to discover that you are operating a full node.

To download and install Tor, navigate to the **open-source project's official website** and select the "Download for Windows" button.[16] However, users should first check their local laws to ensure there are no restrictions for using the Tor network.



Afterward, find the folder where you installed Tor and open the Tor Browser by navigating through the "Browser," "TorBrowser," and "Tor" folders, respectively. Once in "Browser/TorBrowser/Tor," select the "tor.exe" file to open the Tor network browser.

Note: To sync up the Tor network with Bitcoin Core, it's necessary to open "tor.exe" instead of using the dedicated Tor Browser application.



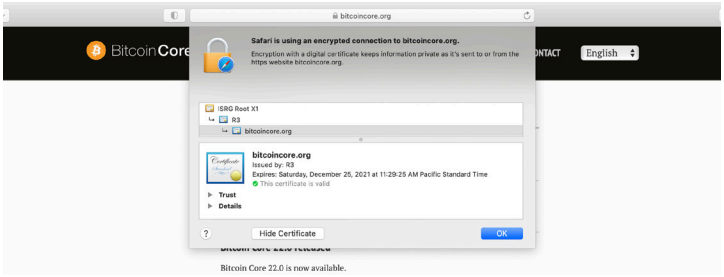
Once "tor.exe" is running, navigate back to the Bitcoin Core client and select "Options" from within the "Settings" menu. Open the "Network" tab, click on the box next to "Connect through SOCKS5 proxy (default proxy)" to select it, and add "127.0.0.1" as the Proxy IP and "9050" as the port. With that, your node should be 100% configured to run over Tor for better privacy and security.

However, your full node won't be connected over the Tor network until your restart the Bitcoin Core client. After rebooting, wait several minutes for your full node to connect to other nodes. If the software indefinitely displays "Connecting to peers" in the bottom left corner of the screen without changing, Bitcoin Core couldn't establish a connection with the Tor network. If this happens, navigate back to network settings in Bitcoin Core and change the Port to "9150" (Tor sometimes uses this Proxy IP for Windows connections).

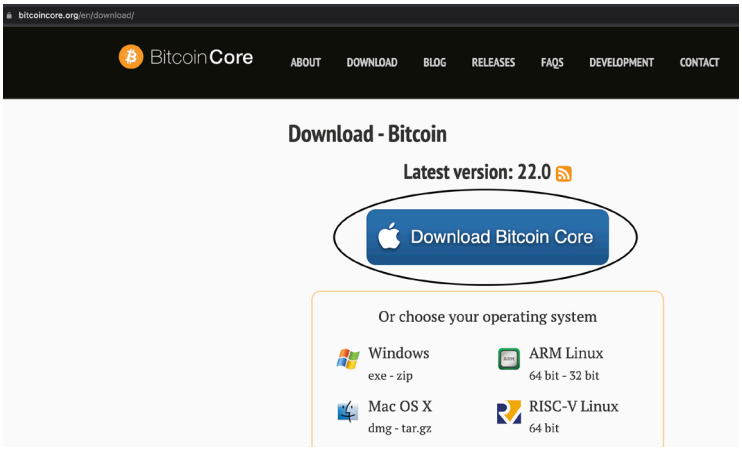
Setting Up on Mac OS X

Step 1: Download and Install Bitcoin Core

Navigate to Bitcoin Core's download page, **always** double-checking URLs to ensure you are on the correct page. Verify you have made a secure connection to the server.[17]



After ensuring that you maintain a secure connection to the site, click on the "Download Bitcoin Core" button to download the Bitcoin Core installer.



[Optional] Step 1a: Verify Release Signatures

If you're familiar with Pretty Good Privacy (PGP), an encryption program that provides cryptographic privacy and authentication for data communication, you should verify the release signatures by clicking the "Verify Release Signatures" link on the download page to download a signed list of SHA-256 file hashes. These hashes should be compared with the following fingerprint:

- 01EA 5486 DE18 A882 D4C2 6845 90C8 019E 36C2 E964—All releases after v0.11 are signed by Wladimir J. van der Laan's **releases key** with the fingerprint.[18]

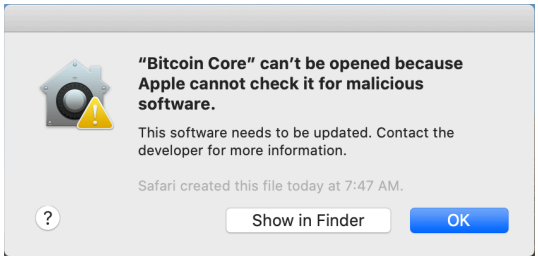
Use PGP to verify the signature on the release signatures file. Then calculate the hash of the archive you downloaded. Lastly, ensure the hash matches those listed in the verified release signatures file.

Step 2: Set up Bitcoin Core for the Initial Block Download (IBD)

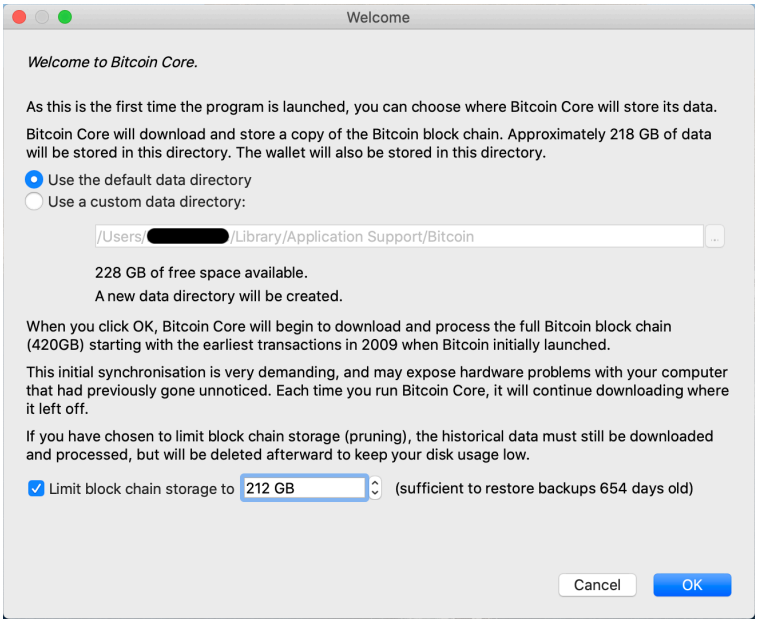
After downloading and installing the Bitcoin Core software, it's time to download the Bitcoin blockchain. This is known as the Initial Block Download (IBD), which includes every transaction in the cryptoasset's nearly 13-year history. At the time of writing, the size of the blockchain is 368 GB and growing at an average rate of 0.175 GB per day. Thus, you should choose a device that can both store the existing data as well as the future growth of the Bitcoin blockchain, which is set to reach 1 TB in 2032.

Open the file after downloading it to your Downloads folder (/Users/<**Your User Name**>/Downloads). Your Mac will then open a Finder window to drag Bitcoin Core to your Applications folder.

Upon running Bitcoin Core, Mac OS X will ask you to confirm that you want to run it. Select the "OK" button on the far right.



Next, you must choose a directory to store the Bitcoin blockchain and your Bitcoin Core wallet. Upon selecting the location to download the Bitcoin blockchain, you will be given the option to choose whether to operate a full node in the standard way by downloading and keeping all the data (368 GB) on your computer or by "pruning," which allows you to run a full node and download and process all the blockchain's data but deletes it immediately afterward to reduce your disk usage. "Pruned" full nodes can reduce the size of the transaction history to 2 GB, about the size required to store roughly 400 songs. For that reason, if you don't have enough space on your hard drive or just want to refrain from overloading it with 368 GB of data, we recommend running a full node via pruning mode.



Click "OK" to finish the setup.

Bitcoin Core will then begin the IBD, downloading and validating all blocks and transactions since Bitcoin's launch on January 3rd, 2009. The IBD is by far the lengthiest part of this process, potentially taking several hours to a few days (depending on hardware and internet speeds) to fully synchronize. Bitcoin Core uses a significant amount of connection bandwidth during the IBD process. However, you can stop Bitcoin Core at any time by closing it and it will resume from the point where it stopped the next time you start it. Notably, the IBD is only needed to be completed on your full node once; after the IBD, your full node will automatically sync with other nodes to update their ledger in real-time.

[Optional] Step 3a: Test Connections and Configure Network if Necessary

Bitcoin Core should work as intended following the IBD; however, operators who want their node to be reachable by other nodes (unnecessary for most users) should test their connections to ensure all is copacetic. To verify if your Bitcoin client is accepting incoming connections from other nodes, visit **Bitnodes.io** and enter your node's IP into the left text box (see image below) and the port into the right-side text box (port must be between 1024 and 65535).[19] Your public IP address can easily be discovered by doing a Google search of "what is my IP address," which will reveal your public IP address as the top search result. Once confirmed that you've inputted the correct IP and port, select the "**Check Node**" button, as displayed in the image below.

The next screen will display a green or red box. Green means your port is open and running as expected, meaning nothing further is required on your end. However, red indicates your port is closed, and further network configuration is needed to open the port. In this case, you should carefully follow **these instructions** from Bitcoin.org.[20]

[Optional] Step 3b: Connect Your Node to the Tor Network For Privacy and Security

Since Bitcoin's early years, attackers have been frantically searching for different ways to attack the Bitcoin network. Though these attempts to penetrate Bitcoin have been unsuccessful, running a Bitcoin full node that isn't connected to the Tor virtual private network (VPN) may be at risk of being targeted by these bad actors as your node's IP address will be publicly exposed. Tor is a privacy-enhancing tool used by many of the most popular Bitcoin software to preserve user privacy. Though the chances of being targeted are unlikely, it's always best practice to conceal your node's identity as there is no reason to reveal your private information. By running your full node on the anonymous Tor network, blockchain onlookers won't be able to discover that you are operating a full node.

To run your Mac OS X-based Bitcoin Full Node over the Tor network, **follow this simple guide.**[21] However, users should first check their local laws to ensure there are no restrictions for using the Tor network.

Pre-Configured Full Node

Pre-configured full nodes are specialized hardware devices that are plug-and-play out of the box. This type of full node setup is best if you want the easiest and most user friendly experience. Some common pre-configured full nodes include:

- **Umbrel**[22]
- **myNode**[23]
- **Lightning in a Box**[24]
- **nodl**[25]
- **RaspiBlitz**[26]
- **The Bitcoin Machine**[27]
- **The Embassy**[28]

Note: If interested in a pre-configured full node, make sure to purchase it from the manufacturer because a middleman can introduce vulnerabilities.

Do-It-Yourself (DIY) Full Node

DIY full nodes are built by the user using specialized hardware and software. This method is best if you don't have a computer with extra disk space that stays on 24/7/365. Node software providers such as Umbrel and MyNode offer easily downloadable software to seamlessly configure DIY full nodes. Though full nodes can run on less, the following equipment is recommended:

- **Raspberry Pi 4** (4–8 GB)[29]
- Micro SD-Card 32GB
- +1 TB Hard Drive or SSD
- Power Supply
- [Optional] Case
- [Optional] Heat sinks and fan

Commonly used DIY full node software includes:

- **myNode**[30]
- **Umbrel**[31]
- **Gordian Server (Mac OS)**[32]
- **Hack0 Build Guide**[33]
- **Node Launcher**[34]
- **Raspberry Pi Node Guide**[35]
- **RaspiBolt Guide**[36]
- **Samourai Dojo**[37]

Mobile Full Node

It's possible to run a Bitcoin full node on an Android device. This option is best for those who want to run a fully validating node out of their pocket, though it will likely drain

your phone's resources while synchronizing. Users have also reported that it eats up mobile data.[38] This software includes:

- ABCore[39]
- Nayuta[40]

How to Use Your Full Node

If you've made it this far by following these steps, congratulations! You have successfully taken a giant leap toward becoming your own bank and securing financial sovereignty. However, the benefits of running a full node aren't fully achieved until you actually use your full node to verify transactions.

Though the most obvious way to use a full node is to use the wallet functionality on the node, this isn't convenient for most users who don't want to carry a full node around. Thus, users commonly synchronize their full nodes with compatible mobile wallets to self-verify on the go! At the time of writing, SPV wallets that support full node functionality include Bread and Samourai Wallet, among many others.

5.

Conclusion

Bitcoin's globally distributed network of full nodes act as both the system's lawmakers and judges, ensuring that Bitcoin's future isn't determined in a centralized manner. Bitcoin full nodes can propose new rules and enforce existing rules about which transactions and blocks are valid to fortify the network against bad actors. If you use a full node for your incoming transactions, you know for certain the legitimacy of any coins you receive. However, most importantly, running and using a full node is the only way to use Bitcoin in a trustless manner. Apart from the personal benefits of running a full node, it also altruistically boosts the network by making it more decentralized and trustless.

In short, full nodes offer Bitcoin users superior security and privacy with the fewest required assumptions while also fortifying the blockchain. The ethos of Bitcoin is to eliminate the need to trust a third party with your wealth or any private information for that matter. Moreover, almost anyone can plug into the Bitcoin network from nearly anywhere in the world, allowing many of the estimated 2.45B unbanked people worldwide to become their own self-sovereign bank. Given that anyone with a modern-day computer and an internet connection can cheaply run a reliable full node, it seems like a no-brainer that securing your financial sovereignty is worth the cost.

Endnotes

1. https://globalfindex.worldbank.org/sites/globalfindex/files/chapters/2017%20Findex%20full%20report_chapter2.pdf
2. https://bitcointalk.org/index.php?topic=382374.msg4108706#msg4108706
3. https://bitcoin.org/bitcoin.pdf
4. https://bitcoinj.org/
5. https://www.youtube.com/watch?v=HScK4pkDNds
6. https://bitnodes.io/
7. http://opensource.org/licenses/mit-license.php
8. https://btcinformation.org/en/full-node#reduce-storage
9. https://bitcoin.org/en/posts/how-to-run-a-full-node#minimum-requirements
10. https://beincrypto.com/run-a-full-bitcoin-node-on-an-android-device/
11. https://bitcoincore.org/en/download/
12. https://blog.pcrisk.com/windows/12622-an-administrator-has-blocked-you-from-running-this-app
13. https://www.google.com/url?q=https://bitcoin.org/laanwj-releases.asc&sa=D&source=docs&ust=1636492669067000&usg=AOvVaw0e0HebLDqsi2H1H3Jwf0jv
14. https://bitnodes.io/#join-the-network
15. https://bitcoin.org/en/full-node#enabling-connections
16. https://www.torproject.org/download/
17. https://bitcoin.org/en/download
18. https://www.google.com/url?q=https://bitcoin.org/laanwj-releases.asc&sa=D&source=docs&ust=1636492669067000&usg=AOvVaw0e0HebLDqsi2H1H3Jwf0jv
19. https://bitnodes.io/#join-the-network
20. https://bitcoin.org/en/full-node#enabling-connections
21. https://www.keepitsimplebitcoin.com/how-to-install-tor/
22. https://thebitcoinmachines.com/product/machine-with-umbrel/
23. https://mynodebtc.com/order_now
24. https://lightninginabox.co/shop/
25. https://shop.nodl.it/en/

26. https://shop.fulmo.org/
27. https://thebitcoinmachines.com/
28. https://start9.com/
29. https://www.raspberrypi.com/products/raspberry-pi-4-model-b/
30. https://mynodebtc.com/download
31. https://getumbrel.com/
32. https://github.com/BlockchainCommons/GordianServer-macOS
33. https://github.com/dgarage/hack0-hardware
34. https://github.com/lightning-power-users/node-launcher
35. https://medium.com/@meeDamian/bitcoin-full-node-on-rbp3-revised-88bb7c8ef1d1
36. https://raspibolt.github.io/raspibolt/
37. https://samouraiwallet.com/dojo
38. https://medium.com/@camilojdl/abcore-review-bitcoin-full-node-for-android-4761bda6a10a
39. https://github.com/greenaddress/abcore
40. https://nayuta.co/core/

We appreciate your feedback! Please visit **https://surveys.kraken.com/jfe/form/SV_8dmJJTfpoyBN4RE** to participate in a brief survey. For all future Kraken Intelligence content, sign up **here**. For comments, suggestions, or questions related to this article or future topics you'd like to learn more about, you may also direct your communication to intel@kraken.com or to your account manager.

Kraken provides access to 92 cryptocurrencies spanning more than 396 markets with advanced trading features, industryleading security, and on-demand client service. With the acquisition of Crypto Facilities, Kraken now offers seamless access to regulated derivatives on 5 cryptocurrencies with up to 50x leverage. Sign up for a free account in minutes at **www.kraken.com/sign-up**. We look forward to welcoming you.

For multi-exchange charting, trading, portfolio tracking, and high resolution historical data, please visit **https://cryptowat.ch**. Create a free Cryptowatch account today at **https://cryptowat.ch/account/create**.

For OTC-related execution services or inquiries, please direct your communication to **otc@kraken.com** or to your account manager.

Disclaimer

The information in this report is provided by, and is the sole opinion of, Kraken's research desk. The information is provided as general market commentary and should not be the basis for making investment decisions or be construed as investment advice with respect to any digital asset or the issuers thereof. Trading digital assets involves significant risk. Any person considering trading digital assets should seek independent advice on the suitability of any particular digital asset. Kraken does not guarantee the accuracy or completeness of the information provided in this report, does not control, endorse or adopt any third party content, and accepts no liability of any kind arising from the use of any information contained in the report, including without limitation, any loss of profit. Kraken expressly disclaims all warranties of accuracy, completeness, merchantability or fitness for a particular purpose with respect to the information in this report. Kraken shall not be responsible for any risks associated with accessing third party websites, including the use of hyperlinks. All market prices, data and other information are based upon selected public market data, reflect prevailing conditions, and research's views as of this date, all of which are subject to change without notice. This report has not been prepared in accordance with the legal requirements designed to promote the independence of investment research and is not subject to any prohibition on dealing ahead of the dissemination of investment research. Kraken and its affiliates hold positions in digital assets and may now or in the future hold a position in the subject of this research. This report is not directed or intended for distribution to, or use by, any person or entity who is a citizen or resident of, or located in a jurisdiction where such distribution or use would be contrary to applicable law or that would subject Kraken and/or its affiliates to any registration or licensing requirement. The digital assets described herein may or may not be eligible for sale in all jurisdictions.