# 1.1 Buying cryptocurrency

**Many institutions choose to rely on third parties, either exchanges or dedicated custodians, in order to hold their cryptocurrency assets.**

As you start your journey, you may be interested in acquiring cryptocurrency. We will walk through a few basic steps to follow in order to do this after considering the legality of cryptocurrency in your jurisdiction:

**Custody cryptocurrency**
To own cryptocurrency, you are required to have a "wallet". A cryptocurrency wallet is how coins and tokens are held or custodied.

There are a couple of options for "custody" of your assets:

- *Third-party service:* You may choose to hold your cryptocurrency with a third party, such as an exchange, which will provide the wallet for you. In this case, you should be aware that you are trusting the security of that exchange with your assets. If the exchange gets hacked, you may have little or no recourse. Generally, to set up a wallet with an exchange, you will need to set up an account using information, including your name, passport or ID number.

- *Self-hosted:* You may choose to self-host your wallet. If you go this route, you will bypass these identification requirements of third-party providers. You will also be taking the security of your assets into your own hands. Be aware that if you lose the necessary materials to access your wallet, you will have no recourse.

The type of cryptocurrency wallet that you will want will depend on the specific needs and features desired. Some cryptocurrency wallets only support specific cryptocurrencies or have limited functionality. This can sometimes mean a trade-off between security and usability. Major differences related to the custody of cryptocurrency include who has access to the private keys of the wallet, how often sensitive data is exposed to the internet, and the type of software or hardware that can be used in setup and maintenance.

Many institutions choose to rely on third parties, either exchanges or dedicated custodians, in order to hold their cryptocurrency assets. This gives them comfort that the ultimate responsibility around the security of their assets lies with a third party. However, this entails deep due diligence to understand the reliability, reputation and recourse provided by that exchange or custodian. Other institutions, particularly those with the requisite security know-how in-house, choose to self-host.

Custodying cryptocurrency is really about the secure custody of a private key, or a string of data akin to a password. Private keys may be represented as a binary code, QR code, mnemonic phrase or other formats. Private keys may be stored in software applications such as mobile apps or desktop applications (typically considered "hot" wallets as they are regularly connected to the internet) or on a specialized, separate hardware device not connected to the internet (also referred to as "cold" storage). There is also the possibility to use a multi-signature wallet, which requires multiple private keys to approve a transaction before assets are transferred (an *m of n* setup). In theory, this can increase the security of funds. There are pros and cons to each type of wallet with differing security, recovery methods and usability.[5]

**Determine a method to acquire cryptocurrency**
Once you have a wallet established, or a way to custody your assets, you will need to acquire your cryptocurrency. There are several methods and platforms to consider:

- Purchasing cryptocurrency as an individual: The most common route is to buy it via a centralized exchange.[6] These exchanges serve as on- and off-ramps and charge fees (ranging from roughly 0.05-5.00%) on each transaction. Different jurisdictions have different exchanges providing liquidity.

- Purchasing cryptocurrency as an institution: You can use a centralized exchange, but often better liquidity and lower fees will be found via an over-the-counter trading desk. You can search for the competitors in these markets based on your jurisdiction.

- Alternative methods: Buying cryptocurrency is not the only way to own cryptocurrency. Other ways to acquire cryptocurrency include participation in the network (mining and staking), earning it (payment for work), airdrops (coins and tokens are randomly distributed to wallets), faucets (a way to collect small quantities of crypto for free), and more.

**Taxation**
Each country taxes digital assets, including cryptocurrency, differently. Keep track of all cryptocurrency transactions to simplify your reconciliation process (when was the transfer made, in what amount, for what goods or services, etc.). Keep in mind that converting one cryptocurrency to another cryptocurrency (e.g. bitcoin to ether) may be considered taxable in some jurisdictions. Spending cryptocurrency to purchase small-value objects such as a coffee may also be taxable as it constitutes a sale of the cryptocurrency.

## 1.2 Making transactions

To make a transaction, you will need a few pieces of information. You will need access to your cryptocurrency. This involves having the information needed to access your funds via the third-party custodian, or having the private key to access the funds in your self-hosted wallet. You will also need the wallet address (or public key) of your counterparty. This might take the form of a string or QR code.

Once you enter the amount you are sending and the address of your counterparty, the system will sign your transaction with your private key (either done by you personally, or by the third party if you chose to use one), broadcast this to the network and show a unique code that represents the transaction called the transaction hash.

## 2.1 Block explorer

A block explorer – a website that tracks all the information inside the blockchain and shows it in intelligible form – is a useful tool for any blockchain user. It acts as a "search engine" for a particular blockchain, allowing users to verify transactions, or check the status of the network.

Most blockchains are transparent, meaning all details of each transaction are publicly broadcasted and recorded and allow for associated metadata to be queried via a block explorer. Traders can verify that transactions have gone through and finalized, agencies can audit and verify reported data, and law enforcement can trace the movement of funds. Individuals can also use block explorers to better understand the degree to which and how blockchains are being used.

## 2.2 Pseudonymity vs anonymity

Most blockchains enable pseudonymity, but not anonymity, meaning they do not guarantee that a user will be unidentifiable.

Pseudonymity means that identities on the blockchain are not directly linked to real-world identifiers such as names, addresses, or identification numbers. When looking at a block explorer, you will not see names of individuals or institutions, but rather strings of data representing those holders' public key addresses. With enough effort, however, most of those addresses can be linked back to identifiers. This can be done via examination of on-chain activity, transaction histories and trails, and analysis of other data such as timestamps and IP addresses associated with transactions.

## 2.3 Privacy

**There are, however, a handful of privacy coins that enable private blockchain transactions.**

As discussed earlier, most blockchains store data in a way that is publicly accessible at any time. There are, however, a handful of privacy coins that enable private blockchain transactions. Two of the best-known projects focusing on this use case are Monero (XMR) and Zcash (ZEC), a fork of the Bitcoin protocol that leverages Zero Knowledge Proofs (ZKPs) to maintain privacy. The basic idea behind ZKPs consists in allowing one party (a prover) to prove to another one (a verifier) the possession of a certain information without revealing that information.

Zcash incorporates transparent "t" and private "z" addresses for sending, receiving, and storing ZEC, thus offering four transaction types from which the user can choose. For example, a transaction facilitated between two "z" addresses is fully shielded. This implies only the fees paid and the occurrence of the transaction appear on the public blockchain, while the addresses, transaction amount and the encrypted memo field are not publicly visible. For auditing and regulatory compliance, Zcash users can use view keys to selectively share address and transaction information.

Monero, on the other hand, only offers fully private transactions. The Monero protocol maintains the privacy of its senders through ring signatures, which do not require a trusted party to perform a setup process. Ring signatures leverage private spend and view keys, as well as public addresses, to facilitate transactions while making it computationally impossible to determine whose key was used to sign. Additionally, stealth addresses guarantee the wallet address of the recipient is never publicly linked to any transaction. The public can nonetheless confirm the legitimacy of the transactions without de-anonymizing the participants through ring confidential transactions. Such privacy coins may face certain liquidity challenges because the current regulatory view on this feature is mixed, thus complicating their listings on exchanges.[7]

## 2.4 Running a node

**Full nodes for any blockchain will place high demands on memory, storage and bandwidth.**

Blockchains are decentralized, distributed databases. These databases are implemented in software and run on a network of nodes. Because cryptocurrency blockchains are permissionless and the code for popular nodes is open source, anyone can participate in the network by running a node.

Reasons for running a node may include:

- *Providing a service to the blockchain network:* Nodes receive transactions, check them against the rules of the protocol and relay them on to other nodes. A diverse and resilient set of nodes is integral to the health and security of the network.

- *Benefits to the host:* Running a node enables the individual or institution to interact directly with the blockchain database without relying on third parties. This may be of particular importance to those who place special value on privacy and security or developers building wallets, block explorers and working on chain analytics.

Running a full node entails downloading, validating, and hosting a full copy of the blockchain database of transactions, going back to the first transaction on the network. *Archive nodes* take this one step further, maintaining a full memory of the state of the blockchain for any given point in time. *Light nodes*, meanwhile, just store block headers, or abridged versions of the transactions in the chain. Light nodes are therefore reliant on full nodes for most data, but that data can be verified against the information contained in the block headers.

There are costs to running nodes. Full nodes for any blockchain will place high demands on memory, storage and bandwidth. All of this can become costly. Nodes generally need to be running for a minimum of six hours per day – and may take days to sync the entire history of the blockchain for the first time. The Bitcoin blockchain demands a minimum of 350 gigabytes of free disk space, 2 gigabytes of memory, and a broadband internet connection with an upload speed of at least 400 kilobits per second. Light nodes make fewer demands on memory and disk space (and can even be run on mobile phones) but are more reliant on network bandwidth.

To judge whether running a full or a light node may be of interest and in order to explore the first steps in doing so, consult the following resources:

- Bitcoin
  - Minimum requirements of a Bitcoin node
  - Bitcoin core

- Ethereum
  - Benefits of an Ethereum node
  - Light client
  - How to set up an Ethereum node

There are also third-party providers who offer node hosting services. This may be a more suitable path if you are with an institution, such as a financial institution, that does not have particular sensitivities around self-hosting and will not be developing applications, or tools that need to directly interact with the blockchain.

## 2.5 Consensus mechanisms and mining

Consensus mechanisms are a critical function that secure permissionless blockchain ledgers and enable the characteristics of immutability and censorship resistance.

Proof of Work (PoW), the mechanism for Bitcoin, is perhaps the best known. PoW mining is the process of computers competing for a reward by executing a cryptographic mining algorithm to meet an output of a predetermined difficulty level. Bitcoin miners hash four inputs using the SHA-256 cryptographic hash function: the transactions of a block; the hash of the previous block; the time stamp; and the nonce (a random number). If the output of this cryptographic function meets a certain difficulty level (i.e. a certain number of leading zero bits), the block is accepted by other nodes on the network and the miner is rewarded.

The culmination of mining results in the appending of new blocks to the blockchain. The newly appended blocks must adhere to the consensus rules of the Bitcoin network or will otherwise be rejected by nodes. The costliness of PoW mining means those who mine bitcoin, but act against the consensus rules of the network, lose significant sums of capital.

**A deeper dive**

- *Difficulty:* Because all miners are competing to append blocks to the Bitcoin network, the difficulty rises as more miners join and drops as miners fall. The difficulty adjusts every 2016 blocks (or every two weeks) and this process keeps miners finding blocks at a rate of roughly one per 10 minutes.

- *Reward:* When a block is successfully appended, a miner can send the first transaction to their own address (known as the coinbase transaction), which compensates the miner with a “block reward”. This block reward consists

**The key inputs to successful mining are low power cost and access to competitive equipment.**

of newly issued bitcoin and all transaction fees from the mined block. The amount of newly issued bitcoin halves every 210,000 blocks, approximately every four years. The block subsidy originally started at 50 bitcoin (BTC) and currently is at 6.25 BTC mined approximately every 10 minutes, or about 900 bitcoin mined every 24 hours (as of April 2021). This algorithm ensures bitcoin is a scarce asset. When bitcoin first launched, for the first four years, approximately 7,200 bitcoin were mined daily.

– *Hashrate:* The speed of solving the cryptographic hash function is the hashrate; the total amount is the network hashrate. If one miner controls around 10% of the Bitcoin network hashrate, they can expect to mine roughly one in ten blocks, and more as their share of the network hashrate increases.

**Attacking the network**

To attack the network, a malicious entity would need to capture 51% of the hash power, allowing the entity to build a longer chain and double spend bitcoin, which they had previously used in a transaction. This would require convincing over 50% of miners to either sell or rent their hash power or someone with more hash power than the current total network hashrate.

**Hardware**

Given the economic incentives, the mining industry is perpetually in an arms race to develop next generation hardware that increases hashrate output. Early bitcoin miners started with central processing units (CPUs), which evolved to graphics processing units (GPUs) and then field programmable gate arrays (FPGAs). But in 2013, single-purpose application specific integrated circuits (ASICs) optimized to hash the SHA-256 algorithm became prevalent. The difficulty level of bitcoin mining was pushed up significantly when ASICs were widely distributed to miners. The hashrate performance of ASICs and consequent difficulty jumps made all other hardware types obsolete. Other types of hardware are still used in the mining of other cryptocurrency protocols, especially those not based on SHA-256.

The key inputs to successful mining are low power cost and access to competitive equipment (ASICs, servers). To build a business of size and scale, particularly for the most popular/competitive cryptocurrencies like bitcoin, miners take on sizable risk in the form of upfront investment and capital expenditure in long-term power contracts, real estate, large volume mining equipment/ASICs, and energy efficient and temperature-controlled data centres to host the mining equipment. The upfront investment is often sized with certain assumptions about crypto market prices, which can be volatile and not guaranteed to materialize.

Given the statistics of success, miners frequently collaborate through participation in a mining pool. Participating in a mining pool enables a miner to have certainty of bitcoin mining rewards on a consistent schedule.

Despite the investment risk and challenges associated with industrial cryptocurrency mining, individuals can set up smaller scale mining operations to participate fully in cryptocurrency networks and may even discover more productivity by mining less mainstream and less competitive cryptocurrencies.

**Getting started with PoW mining**

– *Acquire equipment:* Selection of equipment depends on the triangulation of cost, availability, hashrate performance and power consumption. You may choose either a bitcoin-specific ASIC or hardware that can be used to mine multiple different cryptocurrencies, which have varying algorithms. While it may be difficult to procure equipment from manufacturers, there are secondary markets for used miners available for purchase. As the mining hardware can be loud and hot, often running more than one miner may require finding a data centre hosting location with a low cost of power – factors include the location, source of power (renewable energy based), cost per kilowatt (kWh), as well as whether or not the facility incurs additional costs like cooling requirements to ensure maximum efficiency of the miners.

– *Select and contribute hashrate to mining pool:* Once the hardware is set up, this can be helpful to ensure consistent returns. Factors to selecting a mining pool include cryptocurrency specialization, reputation, size of the pool and its overall percentage of global hashrate, fees paid to the pool and minimum payout sizes.

For alternative coins seeking a less power-intensive approach to securing the network than PoW mining, various consensus models have emerged such as Ethereum's move to Proof of Stake (PoS) and Algorand's Pure Proof of Stake (PPoS), which require miners to stake their native coins to become network validators, ordering transactions and creating new blocks driving all nodes to agreement on the state of the network.

In addition to less power usage, proponents for PoS suggest that barriers to entry are lower as specialized equipment is not required to mine successfully and as more network participants are able to mine with general hardware, the network composition may be more decentralized as well. However, there is some suggestion that PoS may lead to network mining inequality and may unfairly benefit well-resourced network participants since

their ability to mine successfully is directly related to the amount of native coin owned. PPoS seeks to address both PoW's energy consumption and PoS's miner inequity by enabling all network participants the opportunity to propose and validate blocks (with only the probability of mining successfully directly related to the amount of native coin owned). In selecting the consensus mechanism and mining protocol, cryptocurrency networks must trade-off between decentralization, scale and network security.

For more information on the evolution of mining and how to get started, visit:

- Evolution of Mining by Marshall Long, Tales from the Crypt
- Beginner's Guide to Mining, MasterDC
- Choosing a Mining Pool, Make Tech Easier
- Getting Started with Mining, Compass Mining
- Global Hash Rate, BTC.com
- Mempool & Transaction Fees, Mempool.Space
- How Blockchain Works, MIT

## 2.6 Energy consumption

**Permissioned blockchain improves efficiency and latency while also reducing energy consumption.**

As explained above, in order to participate in PoW, significant computational energy is required. Upfront capital expenditure and ongoing electricity bills are costs of running a node to participate in PoW networks (e.g. Bitcoin). Energy consumption depends on the difficulty of the cryptographic puzzle to be solved by a mine in PoW. Nonetheless, the Cambridge Centre for Alternative Finance estimates bitcoin's total electricity consumption to be about 126.98 terawatt hours (TWh) per year.[8]

The proof-of-work scheme is thus compute-intensive and energy demanding, but it is key to addressing the double-spending problem and ensuring the security of the blockchain, as it costs money to attack the network. It is hard to mitigate the energy consumption of PoW blockchains because even if more transactions are added to one block, the cryptographic puzzle difficulty ultimately defines the amount of energy required to participate. In PoW blockchain, energy consumption correlates to market capitalization.[9]

Alternative consensus mechanisms such as PoS consensus and permissioned blockchain consensus consume less energy than PoW blockchains.[10] PoS blockchains are a good alternative to PoW blockchains and entail a participant "staking" capital. This consensus mechanism consumes much less energy and provides adequate security. However, PoS consensus is less battle-tested than PoW so it cannot be said with full certainty that the PoS consensus provides the same security level as PoW.[11] Permissioned blockchain improves efficiency and latency while also reducing energy consumption. Permissioned blockchains are especially suitable for public institutions aiming to decentralize some of their operations. However, they do not give the same flexibility when it comes to decentralization of participants.

Thus, when a user is participating in a blockchain network, they should assess what the economic benefit is of choosing a specific type of consensus mechanism and ensure the energy consumption is weighed sufficiently against benefits.