BITCOIN BUTLERS

Best Practices for Bitcoin Owners - 2021

Bitcoin is a unique asset. One of the properties that makes it so special is that it exists only in the digital realm where it is secured by cryptography and passwords. No one can ever take physical ownership of it. Because of this trait, all owners of Bitcoin need to understand the Best Practices required for securely holding it long-term and ultimately treating it as a multi-generational asset to be passed along to your heirs.

In this document, we will explore the Best Practices that apply equally to new users as well as someone who may have owned Bitcoin since it was $10 in 2011. These ideas are, as the name implies, intended to be the “best” practices. However, these are not the only practices, and will not apply to every situation. With that in mind, you must understand that Bitcoin is a bearer asset, and if you make a mistake, you may never be able to access your Bitcoin. Bitcoin does not have a customer service number to help you, and it does not allow for any do-overs. The good news is that with the implementation of the Best Practices, even a new user with virtually no understanding of Bitcoin can protect themselves and their loved ones from unnecessary loss of their Bitcoin. Additionally, we anticipate that new and innovative ways to maintain these Best Practices will constantly be entering the Bitcoin space. Our goal is to evaluate these solutions and keep this guide updated to reflect the latest technology.

The five Best Practices for long-term ownership of Bitcoin are as follows:

1. Buy Bitcoin from a reputable exchange
2. Store Bitcoin in a multi-sig wallet
3. Create a strong inheritance plan
4. Run your own full node on the Bitcoin network
5. Review and maintain your storage and inheritance plans at least annually

Best Practice #1 - Buy Bitcoin From a Reputable Exchange

On its surface this may seem like an obvious rule, and maybe it is, but that does not mean that it should not be one of the Best Practices. In fact, making sure that your funds actually get converted from fiat money to Bitcoin is arguably one of the most important rules. If you try and convert $10,000 to Bitcoin and instead you are robbed or cheated in the process, you will immediately understand the value of “Best Practice #1”.

The Bitcoin landscape has changed a great deal since Mt. Gox closed their doors in 2014. Buying from a reputable exchange only helps strengthen the Bitcoin ecosystem, which ultimately benefits everyone.

There are numerous trusted exchanges all over the world which can convert fiat money into Bitcoin. Unfortunately, there are many situations where a buyer might not choose one of these safer paths. Some buyers might want to find the lowest service fee possible, and those buyers might look for an exchange that charges lower fees. While you can always find ways to buy Bitcoin with lower fees, you also need to consider the counterparty risk of the transaction. A 1% fee for a $10,000 purchase of Bitcoin will cost you $100, and a half a percent fee will cost you $50, so the net difference is quite small. But, if trying to save $50 for every $10,000 you convert to Bitcoin puts you in a situation where at the end of the day you have nothing, then obviously it was not worth the savings.

The exchanges do as their name implies - they exchange fiat currency to Bitcoin and Bitcoin back to fiat currency. Before exchanges existed, it was rather difficult to buy Bitcoin. Mt. Gox, one of the first and most notable exchanges, was hacked and in the process, 740,000 Bitcoins were lost. The value of those coins as of this writing is over $30 Billion, and Mt. Gox was forced to shut down because of this hack. The Bitcoin landscape has changed a great deal since Mt. Gox closed their doors in 2014. Buying from a reputable exchange only helps strengthen the Bitcoin ecosystem, which ultimately benefits everyone.

Another pitfall to avoid when purchasing Bitcoin is “paper Bitcoin”. Paper Bitcoin is purchased from applications such as PayPal, Square, Robinhood, and Cash App. These apps offer an easy and convenient way to convert your fiat currency to Bitcoin, but they do not permit you to remove the Bitcoin from their platform and store it in your own wallet with your own keys. One of the most important tenets of Bitcoin is “Not your keys, not your Bitcoin”. This simply means that if you do not control the keys to your Bitcoin wallet, then someone else does. As your understanding of Bitcoin improves, the more you will understand why this is simply a terrible idea. We will explore more about how to best store Bitcoin in Best Practice #2 - Store Bitcoin in a multi-sig wallet.

There are also those that might prefer to buy Bitcoin “privately” to avoid the Know Your Customer/Anti Money Laundering Rules in the US (KYC/AML). The goal here is to own Bitcoin anonymously. Purchasing Bitcoin this way typically involves meeting in person with someone found online or through mutual contacts. Upon meeting, you hand them cash, and they send you an equivalent amount of Bitcoin. It is generally in your best interests and a best practice to comply with the laws regarding financial transactions in your particular jurisdiction. Additionally, meeting someone you don’t know (or don’t know well) to buy Bitcoin at a specific time and place creates an attack vector that could result in theft of your cash or possibly physical harm.

The various Bitcoin exchanges have pros and cons. These include the ability to both buy and sell Bitcoin (some are only buying services), the amount of time before you can withdraw your Bitcoin to your own wallet, various buying limits, the ability to set up recurring buying plans and the ability to handle institutional accounts for buying through an IRA, trust, or other corporate entity. Finding an exchange that meets your needs and supporting that exchange by paying fees will help ensure that they are around for the long term. At the time of this writing, the following are some of the most trusted exchanges in the United States - Swan Bitcoin, CoinBase, Kraken, Gemini, and Binance US. There are also numerous over the counter (OTC) buying platforms for those looking to acquire large amounts with lower fees.

Lastly, there is an increasing presence of OTC buying services that are integrated into some of the leading multi-sig wallet providers. These service offerings are quite new and need to be more thoroughly evaluated before they can be considered a Best Practice.

Best Practice #2 - Store Your Bitcoin in a Multi-sig Wallet

There are numerous ways to store your Bitcoin. Deciding on the right storage method can be quite confusing, especially if you are new to the space. Once you understand the differences between the various options it becomes obvious why the use of a multi-signature or multi-key wallet ("multi-sig") is the best storage practice.

> ***Your "keys" are simply a complex password that is required to spend your Bitcoin…it is best to avoid using any method of storing your keys that contains a single point of failure or rests too much responsibility with a third party.***

Bitcoin resides in one and only one location, on the Bitcoin network. You will never take physical possession of Bitcoin like you could with a stack of hundred-dollar bills or a bar of gold. More accurately, your Bitcoin holdings represent a collection of unspent Bitcoin transactions, known as UTXO's, that only the holder of your keys can spend. In other words, the Bitcoin blockchain keeps an immutable list of every transaction that has ever taken place on the network. Your balance on the network is the difference between the Bitcoin you've acquired and the Bitcoin you've spent.

Your "keys" are simply a complex password that is required to spend your Bitcoin. Since your password is critical to accessing your coins, it is best to avoid using any method of storing your keys that contains a single point of failure or rests too much responsibility with a third party. A multi-sig wallet is a solution that provides multiple keys to provide redundant security and avoid single points of failure. This is the safest way to safeguard and "store" your Bitcoin. Before we delve into multi-sig, we will discuss the other most common storage options for Bitcoin owners. To simplify the idea of a wallet, we are going to use the analogy of a mailbox, since that is a more familiar concept that is easier to grasp.

Imagine a mailbox that can receive gold coins that have been sent to you. This mailbox has a public slot where coins can be dropped, but a key is required to open it to retrieve your coins. Those coins can be spent, sold, or exchanged for cash by whoever is in possession of them. Therefore, it is vital that the mailbox is secure. Since the coins you are receiving have significant value, you do not want anyone to be able to open that mailbox and remove the coins without your permission. You must make sure that this mailbox has a strong lock, and more importantly that you are in control of the key(s) to that lock.

You have choices as to where your mailbox resides. If you rent a mailbox from a third party, such as a UPS Store, or open a PO Box at your local post office, there is risk that another party will have access to your mailbox. If that third party were to decide to open your mailbox and take your gold, then you would be left with nothing. Additionally, if that third party is engaged in any fraudulent or other illegal activity, law enforcement authorities might decide to seize their operations and with it, all your gold coins.

This scenario most closely resembles a cryptocurrency exchange or other online storage methods known as "hot wallets". If the owner of the exchange decides to flee the country and take all the money out of everyone's account, they can do so. If the owner of the exchange were to get into trouble with the authorities, the government could come in and seize all assets in their possession, including yours. If you think either of these scenarios are just an example, they are not. This has happened and continues to happen in the real world. Here is a recent story where the owner of an exchange in Turkey allegedly fled the country with $2 billion.

One of the most important things you can do when owning Bitcoin is to take custody of your private keys and not leave it on an exchange or in a wallet that is hosted externally. Again, "not your keys, not your Bitcoin", means that if you do not have the private keys to your Bitcoin, you do not have custody of your coins, and it is for this reason that leaving your Bitcoin on an exchange or hot wallet is not advisable. Holding your own Bitcoin in a manner that does not require your private keys to be stored anywhere online is referred to as "cold storage". Other than small amounts of Bitcoin or amounts that are in transit from hot to cold storage, we recommend avoiding hot wallets whenever possible.

The next type of mailbox is located directly on your property, and you are the only one with a key. This certainly increases the security, but if you lose that key, your mailbox and whatever is in it is likely locked forever. Also, if someone else steals your key they can take your gold. While this mailbox is certainly better than one that is kept off site, it still has the weakness of a single point of failure that can keep you from accessing your gold coins. This scenario most closely resembles a hardware wallet.

A hardware wallet is a small device that contains the private key required to spend your Bitcoin. It usually connects via USB to your computer. As of this writing, the most popular hardware wallets are made by Ledger, Trezor, and COLDCARD. By using the private key stored on one of these devices, you can receive Bitcoin to an address you control which will allow you to unlock your Bitcoin later. Without this key, no one can access and spend your Bitcoin. Unfortunately, this method has some significant weaknesses and vulnerabilities.

When you set up a single key hardware wallet, you will be prompted to write down a set of either 12 or 24 words known as a "seed phrase". This seed phrase is unique to your device and serves as a backup of your private key if the related hardware device is lost or damaged. This seed phrase can be stored as a backup in one or more locations. If something were to happen to your physical key, you can restore it by entering those 12 or 24 words into the appropriate application. While this method is critical to effectively use and protect a hardware wallet, it is subject to risk.

If someone steals your hardware wallet, they may have a hard time doing anything nefarious with it. The most common hardware wallets are usually protected by a PIN code of 6 to 9 numbers. So even if someone were to obtain physical custody of your hardware key, unless they knew your PIN they would be unable to access your Bitcoin. This is one layer of protection, and it certainly helps, but it is not a level of security that is acceptable for anything more than small amounts of Bitcoin that you understand are not fully protected. If anyone gets your seed words, regardless of where they are stored, they can recreate your wallet and spend your Bitcoin without needing the PIN.

The third type of mailbox is one that requires any two of three total keys to open. It has significantly more security than the other two mailboxes, and it gives you the ability to keep multiple keys in multiple locations. For example, you can keep one key at your home and one at your office. Even if someone broke into your home and stole your key, they could not open the mailbox because two keys are required to open it. The third key can be stored with a third party. This third party cannot access your mailbox because they only have one key, but should you lose or damage one of your other keys, you would still have access to your mailbox.

This type of mailbox is analogous to a two-of-three multi-sig wallet setup that provides a strong basic level of security and will protect against nearly all of the losses you might experience. It is much more secure than not having the mailbox in your possession, and since it requires two keys to unlock it, it is far more secure than a single key.

The fourth type of mailbox is one that requires three keys to open. It adds even more security and allows you to have five or six keys that are geographically distributed. Should something happen to one or even two of the keys, any three of the remaining keys can open your mailbox. You can have a company or other trusted party hold one of your keys, and should there be an issue, there would be more than one person who could help you. This is a more robust form of multi-sig, and while it may protect you in certain specific instances, it requires more oversight and maintenance than a two-of-three setup.

The storage of Bitcoin keys will only improve over time, but for now and the foreseeable future, multi-sig is best way to store the private keys to your Bitcoin. Multi-sig is easy to implement thanks to user friendly solutions from providers like Unchained Capital and Casa. These solutions not only protect your Bitcoin with a sophisticated level of security, they also allow for user errors or the loss or destruction of a key without the irretrievable loss of your Bitcoin. If managed and maintained correctly, they also remove single points of failure from the equation.

One last bit of advice regarding the movement of Bitcoin from one wallet to another is to confirm every address character for character. Whether Bitcoin is being sent from an exchange to cold storage, between your own wallets, or to/from another party, you should take the time to confirm every character in the wallet address prior to sending any Bitcoin. It is not advisable to rely on scanned QR code addresses, as they can be hacked by malicious actors and provide an incorrect wallet address. You are better off copying and pasting the address and confirming that the address generated by the receiving wallet matches the address where the funds are being sent. This may require having the party who is sending or receiving the Bitcoin also confirm each character of the case-sensitive address. It should only take about 30 seconds to confirm the address. There is no way to undo a transfer once it has been sent, so this is an easy way to ensure that your Bitcoin is being sent to the correct place.

Best Practice #3 - Create a Strong Inheritance Plan

There may not be another area of the Bitcoin ecosystem that is as underdeveloped and less implemented than inheritance planning. Bitcoin is often talked about as being a multi-generational asset, but very few in the Bitcoin community have an inheritance plan for their Bitcoin. This means if they die, their Bitcoin dies with them. It is estimated that 4% of all Bitcoin is lost each year due to poor storage or poor inheritance planning. Inheritance planning is also the most difficult part of the Bitcoin Best Practices as it requires a unique solution for each person or family. However, it is critical that you implement a strong inheritance plan with no single point of failure if you wish to pass your Bitcoin on to your heirs. We all want to provide for and protect our families, and there is never a time that your family will need your assets more than when you are no longer there for them.

> ***While there is certainly an amount of effort and energy required to implement a strong inheritance plan for your Bitcoin, your overall inheritance plan will be improved significantly. Your Bitcoin inheritance plan will help protect and ensure the proper distribution of your analog assets as well.***

Inheritance planning for Bitcoin comes down to two critical needs:

1. Ensuring that your heirs will be able to access your assets
2. Ensuring that your assets are distributed according to your wishes

Each of these critical needs requires a unique and often custom configuration based on multiple factors. This may include family dynamics, storage method(s), the technical ability of the user and their heirs, and navigating through any trusts or other asset protection vehicles that may be in place. Everyone's situation is different, so everyone's plan is somewhat different. This may seem overwhelming, particularly to new users and those unfamiliar with estate planning. However, with a bit of effort, it is quite manageable. Additionally, there are services, including Bitcoin Butlers, that can help with this part.

The first focus of inheritance planning is making sure your heirs can get access to your assets. If you have implemented Best Practice #2, your Bitcoin will be stored securely in a multi-sig wallet. Thus, you will need to make sure that your heirs have a foolproof roadmap in place so that they can access your wallet. Otherwise, your Bitcoin will be lost forever and will never be distributed to your heirs. The roadmap that you construct should enable your heirs to easily access your keys, and like everything else with Bitcoin, users should be careful to avoid single points of failure.

The second part of inheritance planning is ensuring that you have an unexploitable way to distribute your assets to your heirs in the manner set forth in your will. It is not particularly difficult to get an heir the keys to your Bitcoin. However, depending on your storage and inheritance plan, that heir may have the ability to transfer all of your Bitcoin to themself or somewhere other than where you intended. Therefore, it is critical that you implement a plan that prevents one heir from taking sole custody of your Bitcoin. You should create a mechanism where at least two people are needed to transfer any Bitcoin out of your wallet to your heirs.

While there is certainly an amount of effort and energy required to implement a strong inheritance plan for your Bitcoin, your overall inheritance plan will be improved significantly. Your Bitcoin inheritance plan will help protect and ensure the proper distribution of your analog assets as well. In other words, by creating a strong plan for your digital assets, you will also create a stronger plan for your analog assets. Additionally, most of the required work will be completed up front. Once your initial plan is in place, any adjustments you may need to make going forward are usually minor and easy to implement.

There are many lessons that can be learned from lack of inheritance planning, but few are more heartbreaking than Matthew Mellon, who died with an estimated $500 million worth of digital assets that his three children could not recover. Mr. Mellon set up a strong storage solution for his assets, but he did not set up the inheritance plan for his children, and so his family did not have access to those funds when he unexpectedly passed away. Just a few hours of planning could have created a drastically better future for his children. Anyone who owns Bitcoin should heed the lessons from this tragic story and be sure to implement and maintain a strong inheritance plan.

Best Practice #4 - Run Your Own Bitcoin Node

When you look at your traditional bank or brokerage statements, the balances shown are obligations the bank or broker has to you. While the assets listed may be yours, it does not mean that you will ever be able to take custody of them. With Bitcoin, you can run a node that will allow you to verify that your Bitcoin is indeed your Bitcoin. Unlike the bank or brokerage statements, when you view your balance directly from your node you are not seeing an IOU.

There are numerous reasons to run a Bitcoin node, but one of the most important is that it gives you true visibility into the status of your coins.

It is your actual Bitcoin balance that is being verified on the network in real time. This gives you proof that it is *your* Bitcoin. You do not need the bank or broker to send it to you. It is already in your possession, and you can spend it at will.

There are numerous reasons to run a Bitcoin node, but one of the most important is that it gives you true visibility into the status of your coins. If you think of your Bitcoin as being held in a secure safe, running a node and setting up a watch-only wallet is like having a security camera inside that safe. You can watch the feed from the camera 24 hours a day to make sure your assets are still there. Of course, you can see the holdings in a particular wallet through the wallet's software platform, but this requires relying on a third party to tell you the balance. The ability to verify this independently is one of the great features of Bitcoin. With other assets, the verification process is much more complex and often impossible.

A watch-only wallet gives you the actual Bitcoin balance in any of your wallets. You can think of it as providing a real time balance for your account, much like you might see from a bank or brokerage house. The difference is that you have full control of these funds, and do not need a check mailed to you or funds wired to you to have true possession of your money. Setting up the watch-only wallet does require some expertise, but there are services available that can help you do so, including Bitcoin Butlers. In addition to setting up wallets directly on your node, you are also able to use the node to verify and obtain the status of transactions from your own local version of the blockchain.

Running a node may seem overwhelming or overly complicated, but in fact it is quite easy. There are several nodes that you can buy pre-assembled and preloaded with the required software. You can simply plug them in and create your account. These prebuilt nodes range in cost from $350 to $600, or you can buy $250-$300 worth of readily available hardware and assemble one in under an hour with almost no technical expertise required. These nodes take up the same space as a paperback book, and they easily connect to your internet router. Additionally, there is no need for a screen, as you will gain access through any computer or mobile device connected to the same network as the node. Once this little device is plugged in and set up, it requires practically no maintenance. It is small, silent and can be set up out of the way. It is an incredibly powerful and beneficial tool.

A node combined with a watch-only wallet and the ability to directly validate transactions is the most reliable way to ensure that your Bitcoin is secure and that the balance is in line with your expectations. It takes a bit of time and effort to set it up, but once it is running it requires almost no maintenance and it should last for several years. If used for around 5 years, it will cost the equivalent of $5-10 a month to have comprehensive visibility into the safety and security of your Bitcoin. Another benefit of running a node is that it contributes to the overall security and decentralization of the network by storing an up-to-date copy of the entire blockchain and validating new transactions in real time as they occur. Lastly, it also allows you to run a lightning network node which is a powerful payment platform that is seeing increasing levels of adoption. Read more about it here.

Best Practice #5 - Review And Maintain Your Storage And Inheritance Plans At Least Annually

The annual maintenance process will not only help you ensure that your security and inheritance plan are in good order, but it will also provide you with a greater sense of comfort.

Once you have the first four parts of the Bitcoin Best Practices in place, the last element is simply the maintenance of your will, storage and inheritance plans. It is irresponsible to simply put things in place at a particular point in time and then assume that they will be there for you in a time of need many years into the future. Part of the maintenance process is to educate your heirs and trusted people on the steps required to access your Bitcoin. However, it is important to note that you need to exercise caution when exposing anyone to the steps needed to unlock your Bitcoin. Nobody should have the ability to spend your Bitcoin without your permission. It is only after you are gone that the full roadmap to your Bitcoin should be available to your heirs and other trusted people.

The first step in this process is to keep your will updated. You need to account for any changes in your marital status, beneficiaries, health, objectives, and family dynamics as well as any other factors that would require a change to your will. Modifying a will is not particularly complex or difficult, and it can prevent a range of unwanted issues in the future.

The second step in the process is confirming your access to each Bitcoin wallet key, which means getting them all from the geographically dispersed secure locations where they are stored. This annual exercise will help you better understand the steps and processes that your heirs may have to go through to get the necessary keys to your Bitcoin. In some situations, it is even advisable to take one of your heirs with you. It is one thing to have a key stored in a safe in a remote location, it is another thing to successfully access that safe. Any weaknesses or issues that you encounter need to be addressed immediately and incorporated into your inheritance plan.

The third step is making sure that each physical key device is functioning correctly and can connect to your account. Different wallet providers have different ways to do this, but the trusted wallet providers and certainly all of the multi-sig wallet providers have a way for you to confirm that your devices are functioning properly. After you have gathered the necessary keys in your multi-sig setup, you simply need to run though a few diagnostics which should take no more than about 30 minutes. This is also a good time to educate your spouse or other heirs on the process. You can think of this process as a training exercise for your heirs.

Lastly, every year or two, you want to make sure to swap out the letters being held by your trusted parties in a [tamper evident bag.](#) A strong inheritance plan involves a trusted person or people to hold a key and/or other information that will assist you in the event of your death. These items might include written instructions, physical wallet keys, or other critical items. This should be given to these individuals in a tamper evident bag to be swapped out periodically. The trusted people should return the prior sealed bag to you, and you should verify that no one has tampered with it. If they are unable to locate the envelope or if there is evidence of tampering, you need to immediately make sure to change relevant passwords and lock down any secure items to which they have access. You also need to find a new trusted person, since this person has now become untrustworthy.

There is a common theme in the Bitcoin ecosystem, “Don’t trust, verify”, and with annual maintenance of your storage system you will verify that everything is in good order. The same applies to the annual review of your inheritance plan. You will verify that your trusted people are acting in accordance with your expectations and needs. This process will not only help you ensure that your security and inheritance plan are in good order, but it will also provide you with a greater sense of comfort. This sense of comfort will also be shared by your spouse and your heirs, but most importantly, it will ensure that if something happens to you, that your loved ones will have the assets you intended to pass on to them and that they are not lost forever.