TECHNICAL REPORT

All You Want to Know About Bitcoin (But Was Afraid to Ask)

Janek Ratnatunga[1]

Introduction

As discussed in the main article, Bitcoin was conceived as an alternative to Fiat money. As Bitcoin does not have a central government to issue them, it must be mined, just like gold. Bitcoin miners use special software to solve a random maths problem and are issued a certain number of bitcoins in exchange for their effort. This provides a smart way to issue the currency; and creates an incentive for more people to mine. However, just like the gold mining in the old days; Bitcoin mining is not easy. Gold mining required a lot of pickaxes, muscle-power, blood, sweat and tears. Bitcoin mining requires a lot of computing power, time, energy, and cost. Further, there has been a limit placed on how much Bitcoins can be mined (just like technically Gold has a finite limit on earth); and therefore, the more miners that join, the harder it gets to actually mine Bitcoins. Once a Bitcoin is mined, it can be either stored in a personal digital wallet (just like gold kept at home), or deposited in a cryptocurrency exchange (very dangerous if kept for long periods).

Bitcoin Mining

Every Bitcoin miner is essentially a minor 'banker'. Each time the random problem is solved, and their solution is confirmed by other miners already on the Blockchain network, their coins are registered in the ledger. The successful Bitcoin miner becomes part of the decentralised Blockchain's transaction verification and control network. All new and existing Bitcoin transactions are verified by the Bitcoin miners. See Figure 1.

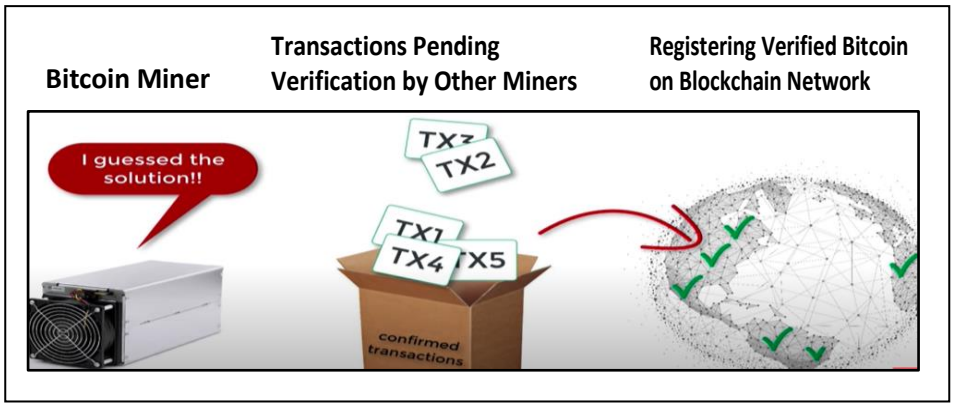

Figure 1: Bitcoin Mining, *Verification and Recording on the Blockchain*

There are only 21 million bitcoins that can be mined in total. Once Bitcoin miners have unlocked all the bitcoins, the planet's supply will essentially be tapped out.

[1] First published: Janek Ratnatunga (2021) "All You Want to Know About Bitcoin (But Was Afraid to Ask)", *On Target*, ICMA Australia Newsletter, 25(2), March-April, pp.12-18.

As of February 14, 2021, 18.638 million Bitcoins have been mined, which leaves 2.362 million yet to be introduced into circulation. Of the existing 18.5 million Bitcoin, around 20 percent —worth around US$140 billion in January 2021 — appear to be in lost or otherwise stranded wallets, according to the cryptocurrency data firm *Chainalysis*.[2]

Early Bitcoins were both a *store of value* ***and*** *a measure of value,* but the values were extremely small. One could buy a cup of coffee at some restaurants which accepted bitcoins in lieu of cash. There is an urban legend that the first transaction was where two bitcoins were used to buy a pizza. It was a bartering system. The early bitcoins were of novelty value as they could not be converted to cash. Today, bitcoin is the 'internet of money'. [This article will cover next the Buying and Selling Bitcoins, and Withdrawing the Cash by converting Bitcoins].

Buying and Selling Bitcoins & Withdrawing Funds

Before considering buying bitcoins, the following table comparing a cryptocurrency account as against traditional bank account needs to be understood; and the following equivalencies in terminology should be recognised:

Traditional Banking	**Bitcoin Trading via Cryptocurrency Exchange**
Your Account Name (KYC Checked by Bank)	Your Account Name (KYC Checked by Exchange)
Your Bank Account Number	Your Cryptocurrency Exchange's Account Recognition Method (e.g., a number/ an email address/an email case, etc.)
Online Banking: Your 'Username'	Your Bitcoin Wallet Address (called, 'Public Key')
Online Banking: Your 'Password'	Your 'Private Key'
Transactions Verification: By bank staff and Recorded in your Bank's Centralised Ledger	Transactions Verification: By Bitcoin Miners and Recorded in The Blockchain's Decentralised Ledger

Before one begins, there are several things that every aspiring Bitcoin investor needs:

1. A personal ***Bitcoin wallet*** (to be kept separate to Cryptocurrency exchange account).
2. A bitcoin address (obtained from the wallet)
3. A cryptocurrency exchange account.
4. Personal identification documents (if you are using a *Know Your Customer (KYC)* platform).
5. A method of payment.

Step 1: *Get a Bitcoin Wallet:*

This manages and stores one's bitcoins. There are many Bitcoin wallets available which you can use to setup a wallet and private key. The *crypto wallet is a program that stores public and private keys* and cooperates with the blockchain to allows users to send and receive digital currency online.

Think of the Bitcoin wallet like a post-box. Anyone can put letters into the post-box (using your public key); but only the postman can take the letters out (using your private key) and then deliver them to a recipient's address. Thus, the public can put bitcoins INTO your wallet using the public key, but only you can take the bitcoins OUT OF your wallet (to sell them; use them to purchase goods or services; or convert to FIAT money) by using the private key.

The functions of a Bitcoin wallet are for:

[2] Nathaniel Popper (2021), "Lost Passwords Lock Millionaires Out of Their Bitcoin Fortunes", *New York Times*, Jan. 14, https://www.nytimes.com/2021/01/12/technology/bitcoin-passwords-wallets-fortunes.html?action=click&module=RelatedLinks&pgtype=Article

- Storing keys
- Digitally Signing Transactions (which require a private key as your digital signature) (see Figure 3)
- Broadcasting Transactions (so that they can be verified by the Bitcoin Miners and entered on the Blockchain Ledger) (see Figure 4).

The main issue in this step is if to use a Software Wallet or a Hardware Wallet. The pro's and con's are as follows:

- *Software Wallets*
  - Run on your computer /Mobile Phone.
  - Good enough for small amounts
  - Free to use.
  - Less secure as linked to the internet.
- *Hardware Wallets*
  - This is a device that connects to your computer when needed only.
  - Good for large amounts.
  - Costs money to buy (AUD $100 to $500)
  - Much safer.

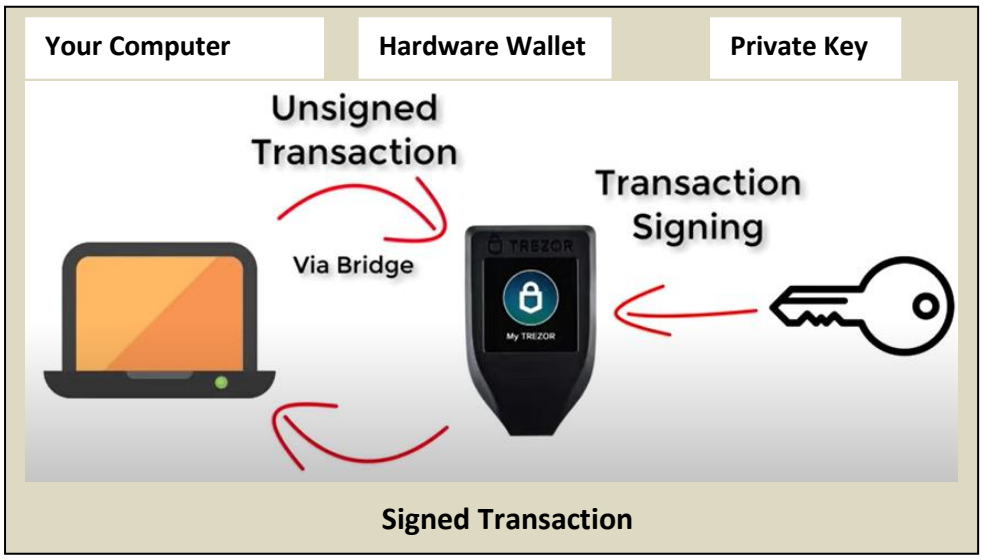

Figure 3: Digitally Signing Transactions

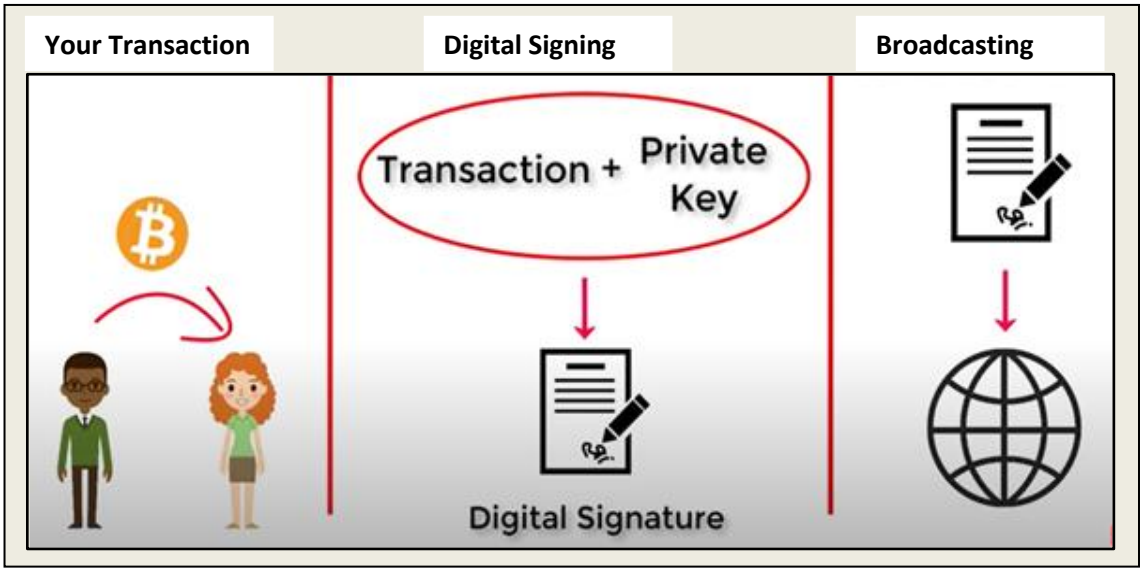

Figure 4: Broadcasting Transactions

Step 2: *Find Your Bitcoin Address.*

Each wallet automatically generates a bitcoin address. This has two parts: A Public and Private Key.

- Your Public key is like your 'user name' in a traditional online bank account.
- Your Private key is like your 'password' in a traditional online bank account.

Public Key

- This is for others to payments to the wallet.
- To get your Public Key, you first must click the Accounts tab toward the top of the screen.
  - This opens your list of cryptocurrency wallets.
  - Your active wallet will have a blue line to the left of the wallet name.
  - To generate your Public Key, click the Receive button.
- You can also find your Bitcoin Cash (BCH) or Bitcoin (BTC) address for receiving payments into your Bitcoin wallet by tapping "Receive" on the bottom toolbar of your hardware wallet.
  - A BTC address is alphanumeric and always starts with a 1 or a 3.
  - Example: This is an example of a receiving address: **3FZbgi29cpjq2GjdwV8eyHuJJnkLtktZc5.**

Private Key

- A Bitcoin private key is a secret number that will enable you to send and receive Bitcoins to and from your wallet.
- Bitcoin wallet has an inbuilt program that will randomly generate a 256-bit long number – This will be your private key.
  - The private key is meant to be secret, hence the word "private" and it is used *to send your Bitcoins to another Bitcoin address.*
  - Additionally, the private key is a 256-bit long number that *looks something like this* **"5Kb8kLf9zgWQnogidDA76MzPL6TsZZY3.**
- Every Bitcoin wallet can have 1 or more private keys stored within the wallet itself.

Step 3: *Obtaining A Cryptocurrency Exchange Account.*

- Signing up for a cryptocurrency exchange will provide you with an account that will allow you to buy, sell, and hold cryptocurrency.
- This cryptocurrency exchange account is like your bank account in a traditional bank, and to set it up you will need to identify yourself and go through *Know Your Customer* (KYC) formalities (see Step 4)
- However, unlike a personal bank account number, some exchanges (e.g., Coinbase) recognise you via your email address or case number (if you have submitted an email case).
- It is generally best practice to use an exchange that allows its users to also withdrawal their crypto to their own personal wallet for safer keeping (There are many exchanges and brokerage platforms that do not allow this – be cautious of these exchanges).
- Other points to check:
  - Accepted countries.
  - Accepted payment methods.
  - Fees
  - Exchange rate.
  - Buying limits.
  - Reputation.
- An important thing to note when creating a cryptocurrency exchange account is to use safe internet practices.
- This includes:
  - using two-factor authentication and

- using a password that is unique and long, including a variety of lowercase letters, capitalised letters, special characters, and numbers.

Step 4: ***Personal Identification Documents (If Using a KYC Platform)***

- There are many types of cryptocurrency exchanges that exist.
  - The ethos of Bitcoin is decentralisation and individual sovereignty.
  - As such, some exchanges allow users to remain anonymous and do not require users to enter personal information.
- Exchanges that allow this operate autonomously and are typically decentralised which means there is no central point of control.
- In other words, there is no CEO and no person or group for any regulatory body to pursue should it have concerns over illegal activity taking place.
- While these types of systems do have the potential to be used for nefarious activities:
  - they also provide services to the unbanked world; i.e., refugees or those living in countries where there is little to no government or banking infrastructure to provide a state identification required for a bank or investment account.
  - Some believe the good in these services outweigh the potential for illegal use as unbanked people now have a means of storing wealth and can use it to climb out of poverty.
- Right now, the most commonly used type of exchanges are not decentralised and ***do require*** KYC. (These exchanges include Coinbase, Kraken, Gemini, to name a few).
- Once you have chosen an exchange, you now need to gather your personal documents.
- Depending on the exchange, the information you may need can depend on the region you live in and the laws within it.
- These may include:
  - pictures of a driver's license or passport,
  - social security number (in USA) or other national identification number,
  - information about your employer and source of funds.
- The process is largely the same as setting up a typical brokerage account in the traditional world.

Step Five: ***Connect to a Method of Payment.***

- After the exchange has ensured your identity and legitimacy, you may now connect a payment option.
- With many of the reputable exchanges, you can connect:
  - To your bank account directly, or
  - To your debit or credit card.
- While you can use a credit card to purchase cryptocurrency, it is generally something that should be avoided due to the volatility that cryptocurrencies can experience.
- It is also possible to get Bitcoin at specialised ATMs and via P2P exchanges (very rare).
- However, be aware that Bitcoin ATMs were increasingly requiring government-issued IDs as of early 2020.

Selling Bitcoins

How to Sell Bitcoin

Cashing out your Bitcoins is not as straightforward as buying them. If you decide to sell your Bitcoins online, you can either do it: (1) Via an exchange; (2) direct trade; or (3) via a peer-to-peer transaction.

Outside of the comfort of your own home, you can: (1) withdraw flat money using a Bitcoin ATM, or (2) sell your Bitcoins in person (p2p).

Selling via an Exchange.

Assuming you already have an account in an Exchange you just simply place a 'sell offer,':
- stating the type of currency that you wish to trade,
- its amount and your asking price per unit.

The exchange will automatically complete the transaction once someone matches your offer.
- After the funds are credited to your account,
- you will need to withdraw them to your connected bank account.

This can sometimes take an excessive amount of time, especially if the exchange is experiencing issues with its banks or facing liquidity problems. Several months before its bankruptcy, the Mt. Gox exchange was experiencing this exact problem. Moreover, some banks just outright refuse to process transactions with funds obtained via cryptocurrency trading.

It is also important to consider a fee you will need to pay in order to use some exchanges. For example, one of the world's biggest cryptocurrency exchanges CEX.io charges:
- a flat fee of $50 for withdrawal via Bank transfer,
- $3.80 if you are withdrawing your funds to a Visa card, and
- 1.2 percent of a transaction + $3.80 if you are using MasterCard.

The withdrawal fees can vary drastically depending on an exchange, but transaction fees are almost always either tiny or non-existent at all. In addition, most exchanges will have a limit on the amount of money you are allowed to store. The limit will increase over time if you stay loyal to a particular exchange.

Finally, it is important to remember that despite offering wallet services, exchanges are by no means a secure and reliable place to store your funds. They are very prone to hacker attacks, and there have also been instances of exchanges shutting down and running away with their users' funds. Therefore, you should take full responsibility for your own funds and store any amount that is not immediately needed in a secure offline wallet.

Direct Trades

Another way of selling your Bitcoins is via a direct trade with another person. This service is accessible on websites usually associated with exchanges, and includes an intermediary facilitating the connection. The steps are as follows:
- First, you will need to register as a seller.
- Apart from setting up your profile, you will need to fully verify your identity.
- Once you are registered, you can post an offer indicating your intention to sell some Bitcoins.
- When a buyer wants to trade with you, you get a notification from the service and from then on you are only interacting with the buyer.
- The website merely serves as a platform to complete the trade.

The process of selling Bitcoins on some of those sites can be quite involved and time-consuming. Therefore, it is imperative to do your research before deciding on a trading platform, and to make sure you have the time and patience required.

Some of the websites offering the option of direct trading are BitBargain, Bittylicious, Coinbase, Openbitcoins, Bitsquare and LocalBitcoins.

Online P2P trading

Peer-to-peer trading marketplaces are a relatively new development in the Bitcoin world. There is no direct exchange of funds taking place. Instead, those websites essentially work as a platform that brings people with different, yet complementary needs together.

The service is designed for the mutual benefit of people who would like to:

- Buy Bitcoins with their credit card, and/or
- Spend their Bitcoins to buy goods from places that do not accept digital currencies as a form of payment.
- As a result, the former gets their flat currency exchanged to BTC, while the latter can buy discounted goods.
- The websites facilitating the service provide users with an escrow service for the transaction, as well as a wallet to store Bitcoins.

All of the platforms offering this service are online-based centralised platforms.

- To be able to sell Bitcoins using those services, you will usually need to fully verify your identification, which obviously voids Bitcoin trading off its anonymity.
- Moreover, once you have managed to sell your BTCs, you will need to withdraw them to your bank account or a bank card.
- Often, this process will take an exceptionally long time and will incur some fees.

Here is an example of how it works.

Bob posts his required wish list including the discount amount he wishes to receive, which normally goes up to 25 percent.

- Jack then accepts the trade and pays for Bob's goods through the marketplace, stating Bob's delivery address.
- Once the goods are delivered, the marketplace releases Jack's money from escrow and transfers the funds into Jack's wallet.

While this system allows Jack to acquire Bitcoins relatively easily using just his bank card, it also charges him quite a high fee for the service.

Some of the websites providing this service are Purse, Brawker and OpenBazaar.

Offline Trading.

Two popular offline trading methods are: (1) Bitcoin ATMs; and (2) Selling Bitcoin in person.

1. Via Bitcoin ATM

Despite looking like traditional cash machines, Bitcoin ATMs are not ATMs in the traditional sense. Instead of connecting to the user's bank account, they are connected to the Internet in order to be able to facilitate Bitcoin transactions.

- Bitcoin ATMs can accept money in cash and exchange it to Bitcoins given as a paper receipt with a QR-code on it or by moving the funds to a wallet on a Blockchain network.
- They usually charge very high transaction fees – e.g., there are media reports citing fees as high as seven percent.

However, Bitcoin ATMs can be quite difficult to locate. In some countries, this requires a money transmitter license, while current regulations in other countries prevent any Bitcoin ATMs from being installed.

2. Selling Bitcoin in person

In many ways, trading digital currency in person is about as easy as it gets. All you need to do to sell your Bitcoins is scan a QR-code on someone's phone and receive cash on the spot.

If you are selling to friends or relatives, you only need to set them up with a Bitcoin wallet, send them the necessary amount and collect your cash. However, if you are dealing with a random person:

- You will most likely go through lengthy rounds of negotiations discussing the price,
- place of meeting and other relevant conditions.

Moreover, you need to take a few things into consideration to ensure your safety and the safety of your funds.

- Verify seller's identity.
- Use Escrow when possible.
- Wait for 3 confirmations before money is released.

Withdrawing Funds

If you are selling Bitcoins online, you will inevitably face the problem of withdrawing funds.

- The most common way to move money is international wire transfer and most prominent exchanges support this method of transferral.
- Recently, however, some exchanges began to accept credit and debit card withdrawals.

Therefore, if you are opening a bank account specifically for withdrawing money made on Bitcoin sales, you need to do your research and chose the bank that best suits your needs.

Summary

New bitcoins need to be mined by solving a cryptographic problem. Other miners already on the Blockchain network, confirm the solution, and the new coins are registered in the blockchain ledger. For those interested in investing in bitcoins, first compare the terminology of a cryptocurrency account as against traditional bank account. Then, before one begins investing, there are several things that every aspiring Bitcoin investor needs: (a) a personal *Bitcoin wallet* (to be kept separate to Cryptocurrency exchange account); (b) a bitcoin address (obtained from the wallet); (c) a cryptocurrency exchange account; (d) personal identification documents (if you are using a *Know Your Customer (KYC)* platform); and (e) a method of payment.

This article provides an in-depth analysis of these steps, and the pitfall that one must be careful of. It also gives a guide to selling bitcoins and withdrawing money to fiat currencies.