

Bitcoin: What You Should Know

Topics Discussed:

- ⇒ Introduction
- ⇒ What is Bitcoin?
- ⇒ Statistical Data
- ⇒ How Are Bitcoin Transactions Processed/Recorded
- ⇒ Bitcoin Mining
- ⇒ Features of Bitcoin
- ⇒ How Are Bitcoins Acquired?
- ⇒ Can Bitcoins Be Converted Into Money?
- ⇒ Drawbacks to Bitcoin
- ⇒ Is It Secured?
- ⇒ How Is Bitcoin Regulated?
- ⇒ References

INTRODUCTION

Bitcoin may have been referenced at an AML/CFT training or conference that you attended, or you may have seen it in the news or on social media. It may have caused you to ask: What is Bitcoin? How does it work? Is it legal? How is it used? How is it regulated? Is it secured? and many other questions. This newsletter serves to answer these questions about Bitcoin. **Please note that this newsletter in no way serves to promote or advertise Bitcoin.**

The Financial Services Regulatory Commission (FSRC) is aware that Bitcoin is being offered to and used by individuals in this jurisdiction. Being the ultimate Regulatory Body for AML/CFT, the FSRC wants to ensure that the General Public is provided with detailed information about Bitcoin before buying into the network.

What is Bitcoin?

Bitcoin is a form of digital currency, otherwise known as 'cryptocurrency'. Bitcoin operates independently of a central authority, instead it is supported by a decentralized peer to peer (P2P) network of computers across the internet which acts as servers to process the financial transactions of this currency. Transaction management and money issuance are carried out collectively by the network.

Once you own bitcoins, what you actually control is a private digital key that allows you access to your bitcoins.

STATISTICAL DATA

As at the end of November 2017, one (1) bitcoin is valued at approximately US\$11,000.00 and approximately 16,700,000 bitcoins are in circulation with a market total of approximately US\$185 billion.

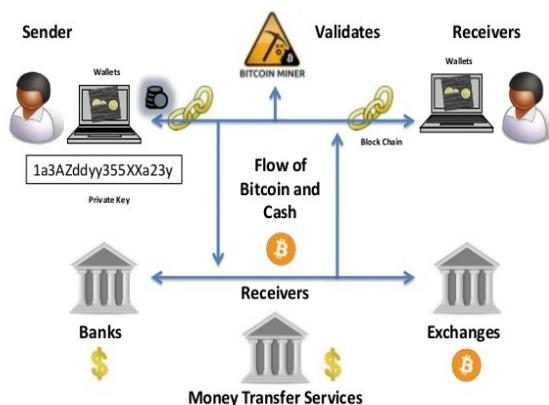
HOW ARE BITCOIN TRANSACTIONS PROCESSED/RECORDED

Bitcoins are purely virtual, which leads persons to question how transactions are carried out using the currency. A **transaction** is a transfer of Bitcoin value from one 'wallet' to another that is broadcasted to the network and collected into blocks. A **wallet** is a small personal database that is used to store bitcoins on a computer drive, Smartphone, tablet or a cloud service. There are three (3) types of wallets: 1) a software wallet (installed on your computer); 2) a mobile wallet (stored on your mobile device); and 3) a Web wallet (located on the website of a service provider that hosts bitcoins).

Bitcoins can be used to purchase goods and services online. The transactions comprise of an amount, an input (sending address), an output (receiving address) and private keys. A user simply enters a receiving address and his/her private digital key, the transaction is then sent and verified by the miners using the Bitcoin Blockchain. The **Blockchain** is a public ledger of account that keeps track of every transaction made on the network since Bitcoin's inception.

BITCOIN MINING

Mining is an important and integral part of keeping Bitcoin stable and secured. The process involves specialized computers solving algorithmic equations or hash functions. The miners confirm blocks of transactions on the Blockchain and are rewarded Bitcoins in exchange for solving the problem and verifying the transaction. Miners are also rewarded network fees when they harvest new bitcoins.



FEATURES OF BITCOIN

1. Bitcoin has similar characteristics to money in terms of durability, portability, scarcity, divisibility and recognisability and is based on the properties of mathematics rather than on physical properties like gold and silver or trust in central authorities (like fiat currencies).
2. The value of a Bitcoin is determined by supply and demand and is fully virtual.
3. As a decentralized currency, Bitcoin is free from government interference and manipulation.
4. **Anonymity** - Unless users publicize their wallet addresses, no one can trace transactions back to them. Only the wallet owners, will know how many Bitcoins they have.
5. **Bitcoin has a maximum 21 million limit:** The total number of Bitcoins that will be issued is capped at 21 million. The Bitcoin “mining” process presently creates 25 Bitcoins every 10 minutes (the number created will be halved every four years), so that limit will not be reached until the year 2140.
6. **Low Transaction Costs** - small fees are paid to three groups of Bitcoin services: the servers (nodes) who support the network of miners, the online exchanges that convert bitcoins into money and the mining pools that one may join. The owners of some server nodes will charge one-time transaction fees of a few cents every time money is sent across their nodes, and online exchanges will similarly charge when bitcoins are cashed in for dollars or euros. Additionally, most mining pools will either charge a small support fee or ask for a small donation from the people who join their pools. In the end, while there are nominal costs to use Bitcoin, the transaction fees and mining pool donations are much cheaper than conventional banking or wire transfer fees.

HOW ARE BITCOINS ACQUIRED

There are a variety of ways to acquire bitcoins:

1. Accept bitcoins as payment for goods or services.
2. Bitcoins can be purchased from applications such as Bitit, Cubits, or Coinbase.
3. The most common way to buy bitcoins are the Bitcoin Exchanges.
4. Bitcoin ATMs can be used to purchase Bitcoins.
5. Participate in a mining pool or solo mining.



CAN BITCOINS BE CONVERTED INTO MONEY?

Bitcoins cannot necessarily be converted into cash, as the currency is purely virtual. To exchange Bitcoins for cash, one will actually have to sell their Bitcoins. The image above depicts a Bitcoin ATM. Two way Bitcoin ATMs can be used to buy or sell bitcoins in exchange for cash.

BE INFORMED! BE AWARE! BE VIGILANT!

DRAWBACKS TO BITCOIN

Some of the drawbacks to Bitcoins are as follows:

- * **Volatility** – The price of a Bitcoin has been increasingly volatile, making it difficult to assess its real value and increasing the risk of losses for investors in the cryptocurrency. Despite Bitcoins considerable volatility (swings in the value of the currency), some large companies such as Microsoft and Paypal accept bitcoin as a payment option.
- * **Bitcoin has limited acceptance:** It has limited acceptance so far and cannot be used at many brick-and-mortar storefronts, though that may eventually change if it continues to gain traction and more awareness.
- * **Bitcoin transactions have limitations:** A Bitcoin transaction can take as long as 10 minutes to confirm. Transactions are also irreversible and can only be refunded by the Bitcoin recipient. These limitations do not exist with conventional currencies, where debit and credit transactions are confirmed within seconds; certain transactions can also be reversed for valid reasons by the originator, without having to rely on the recipient's largesse.
- * **Bitcoin balances are not insured:** This means that if you lose your Bitcoins for any reason – for example, your hard drive crashes, or a hacker steals the digital wallet in which your Bitcoins are stored, or the Bitcoin exchange where you held a balance went out of business – you have little recourse.

IS IT SECURED

To date there have not been any hacks or security breaches to the Bitcoin network itself. However, there are a number of cases where personal wallets have been hacked. For example, the case of Mt. Gox, which was a Bitcoin exchange based in Japan. By 2013 and into 2014, the Company was handling over 70% of all bitcoin transactions worldwide, as the largest bitcoin intermediary and the world's leading bitcoin exchange. However, in 2014, Mt. Gox announced that approximately 850,000 bitcoins belonging to customers and the Company were likely stolen, an amount valued at more than \$450 million at the time. As a result, the Company suspended trading and filed for bankruptcy.

HOW IS BITCOIN REGULATED?

With conventional money transactions, Financial Institutions are obligated by law to apply AML/CFT controls including customer due diligence and transaction monitoring. Bitcoin, being a cryptocurrency, can be used to conceal or disguise the illicit origin of funds, thus facilitating money laundering, terrorist financing and tax evasion. Its tracibility is limited due to user anonymity and anonymizing service providers that complicate the transaction chain. It is for these reasons that governments across the world are working to establish measures to regulate the use of virtual currencies. However, due to the complexity of Bitcoin, use of the cryptocurrency is yet to be successfully regulated. As a result, the trading of Bitcoin has been banned in some countries such as China and Russia.

Reference:

- <https://bitcoin.org/en/>
- <https://www.wired.com/2016/03/must-understand-bitcoin-regulate/>
- Virtual Currencies and Beyond: Initial Considerations, IMF Staff Discussion Note, January 2016