CRYPTOCURRENCY

Stephen Marshall

Introduction

In general, Bitcoin and cryptocurrency are now a widely known and accepted phenomenon with a large portion of the population being involved in the buying and selling of these alternate forms of currencies or at the very least being familiar with their existence and the many ways in which a blockchain solution can benefit them as individuals. Indeed, cryptocurrency has been widely recognised around the globe as one of the great technological advancements of recent times as highlighted by the following quote regarding the Bitcoin platform:

> "Bitcoin is a remarkable cryptographic achievement. The ability to create something which is not duplicable in the digital world has enormous value. The Bitcoin architecture, literally the ability to having these ledgers that can't be replicated is an amazing advancement."
>
> Eric Schmidt, Executive Chairman of Google, March 2014.

The challenge remains for merchants and business owners as to how to utilise or incorporate these alternate forms of currency into their existing payment frameworks. Additionally, how to streamline their processes so that customers are not unnecessarily burdened with too many of the technical aspects which exist in these environments and that they can quickly and easily avail themselves of the products and services being offered, as with traditional payment methods, but without the need for onerous bank fees and transaction charges.

For some background and context on how cryptocurrency came to be where it is today, it is worth briefly considering its creation and inception. Bitcoin was invented in 2009 by a person (or group) who called himself Satoshi Nakamoto. His stated goal was to create "a new electronic cash system" that was "completely decentralised with no server or central authority." After cultivating the concept and technology, in 2011, Nakamoto turned over the source code and domains to others in the bitcoin community and subsequently vanished.

Each Bitcoin is contained in a computer file which is stored as a 'digital wallet' app on a smartphone or computer. People can send Bitcoins (or part of one) to your digital wallet and you can send Bitcoins to other people. Without getting into the technical details, Bitcoin works on a vast public ledger, also called a blockchain, where all confirmed transactions are included as so-called 'blocks.' As each block enters the system it is broadcast to the peer-to-peer computer network of users for validation. In this way, all users are aware of each transaction which prevents stealing and double-spending - where someone spends the same currency twice. The process also helps blockchain users trust the system.

Whenever someone sends a transaction it is broadcast instantly to the network and verified by the 'miners' (Those who have specific hardware equipment, which is used to perform calculations necessary to maintain the Bitcoin system). Miners are constantly working to confirm individual transactions and include them in the next block of transactions in the chain. Once a new block is verified, all the transactions within it are permanently recorded on the blockchain. Rewards are paid

out in Bitcoin to miners who confirm transactions and verify the next block as a way to incentivise productivity on the network.

With Bitcoin Core's price increasing over the years and reaching billions of dollars in market capitalisation, all kinds of people see its value and appeal. This brings out both the good and bad in human nature and unfortunately with the bad, comes scammers. The bottom line is scammers also want to profit somehow from Bitcoin Core but through nefarious means.

Cryptocurrency has no central point of control, as most traditional currencies do, and is sustained by individuals in the widespread cryptocurrency community. Its usefulness as a payment platform can be attributed to some key properties:

- Irreversible
- Pseudonymous
- Fast
- Global
- Secure
- Decentralised

How is cryptocurrency stored

Cryptocurrency is usually stored using a 'Wallet' - a wallet is an app or program that allows you to send and receive cryptocurrency. Wallets also keep track of your balance which is held in one or more addresses. Generally, wallets also have a feature that keeps a history of your transactions. There are many different wallets across various platforms and whilst they all share certain basic functionality, features vary from one wallet to another.

To say that Bitcoins are stored in a wallet is not quite giving the entire picture. Bitcoins are not stored anywhere. Bitcoin balances are maintained using public and private "keys" which are long strings of numbers and letters linked through the mathematical encryption algorithm used to create them; it is these keys that are stored in the wallet. The public key (comparable to an international bank account number or IBAN) serves as the address published to the world and to which others may send Bitcoins.

Backing up the keys in your wallet ensures that, if all else fails, you can restore your cryptocurrency. Wallets have hidden private keys and if you only have a backup for your visible addresses you will not be able to restore all of your money, so it is wise to back up your entire wallet.

How to buy and Sell

You'll need to use an exchange to buy and sell cryptocurrency. There are plenty of exchanges around it is a just a matter of finding one that supports the cryptocurrency that you are looking to purchase, as well as the fiat currency that you wish to spend. If there are multiple possibilities, you can then

move on to evaluate and compare the trading and transfer fees to find the option which best suits your requirements.

Bitcoin exchanges are similar to foreign exchange markets. While exchanges offer wallet capabilities to users, it is not their primary business. Since wallets must be secure, exchanges do not encourage storing large amounts of Bitcoin or for long periods. Therefore, it is advisable to transfer your Bitcoins to a secure wallet because security must be your top priority when choosing a Bitcoin wallet.

Volatility

Volatility is a vital concept to understand since it measures risks. For investors and traders understanding their risk tolerance is always the first step before engaging in any form of investment. In recent years, the price of cryptocurrencies have vigorously fluctuated from end to end, with many considering cryptocurrencies to be a highly unstable market full of speculation and uncertainty. It must be mentioned that the level of risks that one chooses to undertake is highly correlated to the potential returns that he would acquire. In other words, a higher risk investment is associated with a greater probability of generating higher returns while a low-risk investment would yield a smaller rate of returns.

Security and risks

Cryptocurrency and their exchanges are entirely digital and, as with any virtual system, are at risk from hackers, malware and operational glitches. If a thief gains access to a cryptocurrency owner's computer hard drive and steals his private encryption key, he could transfer the stolen cryptocurrency to another account. Users can prevent this only if cryptocurrency is stored on a computer which is not connected to the internet, or else by choosing to use a paper wallet e.g. printing out the private keys and addresses and not keeping them on a computer at all.

Trading with Bit coin

Since cryptocurrency can be exchanged for traditional or fiat currency (e.g. USD GBP etc), it is possible to use cryptocurrencies to facilitate the exchange of one fiat currency for another. This is achieved by purchasing the cryptocurrency with one type of currency, for example USD, and then selling the cryptocurrency for another type of currency, GBP for example. In this scenario, you have effectively traded USD to GBP with the cryptocurrency acting as a common resource with which to achieve the transfer of one currency to another. It is important to consider the exchange rate and applicable fees for this type of transaction and compare them to those which would be applicable to a traditional currency exchange transaction.

Stephen Marshall
Director

June 2019