An Introduction to Bitcoin and Other Virtual Currencies

A message from the BMO Nesbitt Burns Portfolio Advisory Team: This article is designed to provide awareness about virtual currencies, also referred to as "cryptocurrencies." We acknowledge that the value of bitcoin and other virtual currencies has increased exponentially over a relatively short period of time. These dramatic increases in value are viewed as both a flag of caution, and area worthy of further research. As a team, we currently do not support virtual currency trading given the information we have available. However, we do believe it is valuable to remain knowledgeable as market dynamics continue to be affected by technological change and emerging tech investment themes.

What is a virtual currency?

All virtual currencies are also digital currencies or digital money, and do not exist in a tangible form, meaning they are accessed and transacted with electronically. A virtual currency differs from a digital currency by the way in which it is issued and supported, as well as its usability. Decentralized virtual currencies utilize cryptography to secure their record of transactions, which are stored in an online publically available ledger called a blockchain. An example of a blockchain is Bitcoin (capital B, Bitcoin), which is the name of both the underlying technology and the unit of virtual currency itself (lower case b, bitcoin). Bitcoin is the world's first blockchain and has existed for just over nine years. Entries recorded on a blockchain such as the Bitcoin are considered to be immutable (i.e., very difficult to tamper with or change without the decentralized Bitcoin community knowing). Other examples of decentralized blockchains are Ethereum and Litecoin, which share some similarities with Bitcoin.

Depending on whom you ask, virtual currencies can be considered a currency, an asset, or a commodity, similar to gold. Arguably, virtual currencies have similar characteristics to traditional fiat currencies (i.e., a store of value, a medium of exchange, and a unit of account). Unlike traditional currencies, virtual currencies are not controlled or regulated by any single authority and are, therefore, decentralized. Transactions are conducted in a peer-to-peer network without the need for intermediaries such as central banks or financial institutions.

Virtual currencies, such as bitcoin, can be used to purchase goods and services or to hold as a store of value, and transfer value seamlessly across international borders. At the moment, there are more than one thousand operational virtual currencies, each offering something different.

How does supply work?

Virtual currency "miners" run powerful computer processors that serve to verify transactions on the blockchain protocol. Mining is incentivized through the concurrent creation of new currency units rewarded to the miners for successful verification. Think of miners as a classroom of students taking a math quiz every 10 minutes, with the first student to achieve 100 per cent receiving a reward of newly minted currency units each time. (Keep in mind that not all virtual currencies operate on the same mining protocol, and some lesser known virtual currencies have eliminated the mining process altogether.)

Bitcoin is one such virtual currency that requires the mining process; however, the total number of units that can be created is limited, much like the total available supply of gold. In the case of Bitcoin, the total supply is capped at 21 million, but with this being said each bitcoin is divisible by 100 million with its smallest divisible unit referred to as a "Satoshi." The last bitcoins are anticipated to be mined in 2140 with incentive then moving solely to the monetization of the verification process, as opposed to the creation of new units.

Continued

How does demand work?

Once created, virtual currencies can be used to trade or conduct transactions in the global economy, with more and more retailers and businesses accepting virtual currencies by the day. Typically, virtual currencies are accessed through a user's virtual currency wallet held on a virtual exchange or hard wallet device (similar to a USB stick.) These are accessible via mobile phone or laptop computer. Each wallet contains the user's public and private keys. The public key is similar to an email address and the private key is effectively the password.

In using the Bitcoin blockchain as an example, a transaction will state, "John gives 'X number' of bitcoin to Sarah." This transaction is signed (approved) by John's private key and sent to Sarah's public key (wallet address). After verification by the miners, the transaction is completed and added as part of a block to the Bitcoin blockchain. This block will house certain information confirming the transaction took place alongside other transactions bundled together with it. Not all transactional information is stored in the block; however, the approximate time stamp of when the transaction took place and the wallet addresses of those involved (not the names of the individuals) are included.

Buying and selling bitcoin and other virtual currencies

Individuals currently cannot purchase or sell bitcoin and other virtual currencies from their local bank branch or through their financial professionals. Generally, virtual currencies are purchased and sold via a third party exchange, such as Coinbase, foreign brokerage, Bitcoin ATM, or peer-to-peer website such as Local Bitcoins. Typically, users will create a wallet linked to their bank account or credit card to purchase and sell virtual currencies. Some exchanges and brokerages will accept wires, e-mail money transfers, and other payment methods, and the rates between buyers and sellers can differ significantly. Bitcoin ATMs ("BTMs"), generally only accept cash and charge higher fees for their convenience. However, BTMs typically have limits on the amount of virtual currency units that can be purchased. While there are many ways to purchase and sell, the use of blockchain technology ensures there is only one ledger, per virtual currency, recording all of the transactions.

The use of virtual currencies continues to grow as the emerging digital economy gains prominence in Canada and worldwide. We encourage investors to stay informed as technological advances that marry currency and the online sphere become more accessible.

BMO Wealth Management
BMO Nesbitt Burns

ID1602 (12/17)