Despite the Downsides of a Number of Cryptocurrencies, the Underlying Technology Continues to Show Its Potential

Cryptocurrencies continue to evolve rapidly and largely go beyond the scope of just Bitcoin, which has made headlines on a regular basis in recent years. There are now more than 1,600 cryptocurrencies in circulation, around 10 times more than the number of national currencies.

Following a surge in many of their prices last year, major corrections were observed. This still-elusive asset class is plagued by many issues. That said, the underlying technology remains promising for facilitating and reducing the cost of many types of transactions. Even central banks are exploring its potential. Here we refer to Distributed Ledger Technology. It consists of virtual ledgers shared simultaneously between many computers around the world, enabling transactions to be validated in a decentralized manner.

The Roller Coaster Keeps On Going...

The dizzying rise in the value of Bitcoin and of many other of its peers garnered a lot of attention in 2017. However, this trend did not continue in 2018. After closing in on US$20,000 in December 2017, the value of one Bitcoin plummeted and is now worth around US$7,000 (graph 1). Ether and Ripple, in second and third place in terms of outstanding, also fell after posting an even steeper climb than Bitcoin (graph 2).

Even central banks are exploring its potential. Here we refer to Distributed Ledger Technology. It consists of virtual ledgers shared simultaneously between many computers around the world, enabling transactions to be validated in a decentralized manner.

This is not the first time that Bitcoin and other cryptocurrencies have seen dramatic increases and sharp drops. On average, their volatility is far greater than that of other asset classes (graph 3 on page 2). The value of cryptocurrencies is very sensitive to changing demand, which may fluctuate for many reasons. This sensitivity is exacerbated by a supply that changes little over time, unlike for national currencies. The supply of a cryptocurrency...
is predetermined by the computer program that runs it. For example, there are currently 17 million Bitcoins in circulation, and only 12.5 are added every ten minutes. In about two years, this pace will be cut in half, and the supply will eventually be capped at 21 million Bitcoins.

**Gains May Be Tougher to Come By**

The programmed scarcity of cryptocurrencies may seem to hold promise of more large gains in the future, provided that demand is there. By analyzing how Bitcoin has evolved since being created in 2009, we see that the most substantial gains might have already happened.

Last year was a record one for Bitcoin’s value, but its annual rise has already been much faster (graph 4). Roughly speaking, Bitcoin’s value increased 20 fold in 2017 between its trough and its peak. Although considerable, this is 10 times smaller than the increase observed in 2011, when Bitcoin’s value rose from about US$0.10 to more than US$20. Similarly, 2013 was also a banner year, with the annual change in Bitcoin’s value close to 5 times the pace of the change observed in 2017.

**Proliferation of Cryptocurrencies**

The slower growth in Bitcoin’s value may have been linked to the proliferation of cryptocurrencies. There are currently more than 1,600, and rising. Therefore, even if the supply of Bitcoin increases very slowly, the supply generated by other cryptocurrencies is a substitute that may meet the growing demand.

What must also be considered is that rising cryptocurrency values means that buying large quantities of cryptocurrencies is increasingly difficult. Today, it takes a lot more subscribers and large investments to create a scarcity effect that would give the currencies a significant boost. In 2011, when one Bitcoin was worth US$0.10, it took US$1,000 to buy 10,000 Bitcoins; today, it would take approximately US$70M.

**A Lot of Downsides**

Aside from their volatility and the uncertainty surrounding their future performance, many other factors may keep demand for cryptocurrencies from expanding. The absence of a legal framework and protection mechanisms is still a big problem. Cryptocurrency users have little recourse in the event of loss, theft or fraud. Moreover, hacked exchange platforms have been frequent headline news in recent months, which may have undermined user confidence. These platforms are used to exchange cryptocurrencies against standard currencies or against other cryptocurrencies. There are also concerns about potential price manipulation.

Among other things, the ease of use and practicality of cryptocurrencies can be questioned. A lost password could be enough to lose access to your virtual wallet. Extra caution must also be exercised during transactions because they cannot be cancelled or reversed, unless the other party involved agrees to cooperate. In particular, this means carefully checking each transaction amount. The difficulty in conceptualizing prices in Bitcoin, Ether or Litecoin, to name just a few, may lead to costly errors. If you are paying for coffee with Bitcoin, you have to make sure that the decimal is in the right place. A $2.00 coffee would be equal to two ten-thousandths of a Bitcoin (0.0002 BTC). You also need to find a store that accepts payment in cryptocurrencies; there are still few that do. Transaction times and fees can be other disincentives, particularly for transactions involving Bitcoin, whose network is at near capacity. To prioritize the processing of a transaction, a high enough fee must be paid. It should be noted that this fee will fluctuate depending on traffic. A substantial increase in fees was noted in December 2017 (graph 5 on page 3).

Bitcoin network saturation is an issue for which many developers are working to find solutions. Since the network is not governed by a central organization, changes are difficult to implement.

---

1. [https://coinmarketcap.com/all/views/all/](https://coinmarketcap.com/all/views/all/)
When changes are accepted by only part of the network, this may lead to the creation of a new cryptocurrency. That is why today there is Bitcoin XT (created in August 2015), Bitcoin Unlimited (created in January 2016), Bitcoin Cash (created in August 2017) and Bitcoin Gold (created in October 2017).

Growing Electricity Needs
Cryptocurrencies run on computer networks made up of legions of computers around the world. The Digiconomist website publishes electricity consumption estimates for Bitcoin and Ethereum networks. According to these estimates, the Bitcoin network consumes about 70 terawatt hours annually, compared to some 20 terawatt hours consumed by the Ethereum network (graph 6). Combined, these two networks consume the equivalent in electricity of a country like Belgium or Finland.

GRAPH 5
Bitcoin network saturation in December resulted in high transaction fees

Average transaction fee paid in the Bitcoin network

Source: bitcoinfees.info

These estimates may seem high at first glance, even exaggerated, but other information nevertheless tends to confirm this emerging industry’s high demand for electricity. We need only look at the interest shown recently in Quebec’s low electricity costs, which forced Hydro-Québec to hit the brakes. There were more than 300 requests from companies operating in the cryptocurrency sector. These requests apparently totalled roughly 18,000 megawatts of power, which would mean more than 150 terawatt hours in annual energy consumption, assuming usage 24 hours a day, 365 days a year.

Let there be no mistake, all electronic payment methods consume energy. On the Bitcoin network, however, this energy is estimated at close to 1,000 kilowatt hours per transaction, enough energy to power a 1,500-watt baseboard heater for 28 days. The Ethereum network is more frugal, with estimated consumption of just over 80 kilowatt hours per transaction. This much energy could nonetheless recharge a Tesla vehicle.

To add to the problem, networks such as the Bitcoin and Ethereum networks provide a substantial incentive to connect more computers if the value of cryptocurrencies increases. Those who validate transaction blocks are rewarded. They collect transaction fees, but more than anything, they have a chance to get their hands on new cryptocurrency units. On the Bitcoin network, 12.5 new Bitcoins are issued to the owner of the first computer to validate a block of transactions, which on average takes 10 minutes. On the Ethereum network, 5 Ethers are distributed that way every 15 seconds. Understandably, if the value of cryptocurrencies increases, the potential earnings for those who validate transactions increase as well.

More connected computers does not necessarily mean that more transactions will be processed. This limit is set by computer programs governing cryptocurrencies. The level of difficulty in validating transaction blocks is automatically adjusted to offset the growing number of connected computers.

Graph 6
Mining cryptocurrencies requires a lot of electricity

Source: digiconomist.net

However, not all cryptocurrency networks operate this way. For example, the Ripple, Iota or Credits networks do not allow connected computers to benefit from the creation of new cryptocurrency units.

In Search of Identity
When Bitcoin and its other peers emerged, they were quickly referred to as currency. However, they do not really have the required characteristics. A currency must be used as a unit of account, that is, as a reference point to express the prices of all goods and services. It must also be used as a store of value and as a means of transactions.

The high volatility of Bitcoin and its peers reduces their usefulness as a unit of account. It would be too difficult to track how the prices of goods and services change over time. That volatility also prevents them from being considered as a store of value, the

---

main purpose of which is the accumulation of funds that might be spent later. The risk level must be low to protect purchasing power. Lastly, since cryptocurrencies are still not used very extensively to buy goods and services, it can hardly be said that they are a true means of transactions. Furthermore, network saturation, as is the case with the Bitcoin network, is a major limiting factor.

If they are not truly currencies, what are they then? Because of the scarcity effect that Bitcoin and its peers are trying to reproduce, some will compare them to gold. Individuals or companies that connect computers on cryptocurrency networks are called “miners” in that sector’s jargon. That said, the proliferation of cryptocurrencies disables the comparison with gold, for which no substitute really exists. What’s more, there is no demand to use cryptocurrencies in manufacturing processes, as is rather the case for any resource, including gold.

As the Bank of Canada Governor suggested in a speech delivered in December 2017, perhaps another name should be found for cryptocurrencies. He also likened this type of instrument to gambling: “[...] perhaps the most one can say is that buying these things means buying risk, which makes it closer to gambling than investing.”

**Varied Applications**

The fast evolution of cryptocurrencies makes them even more difficult to classify into a single asset class. Varied applications arise from Distributed Ledger Technology.

The term “token” is increasingly used in parallel with the development of new applications. These tokens can be issued as part of crowdfunding or rewards programs. Companies can also hold pre-sales of their products or services by issuing tokens. In more complex cases, tokens will be akin to securities. This could be a form of participation in the capital of a company.

In analogy to IPOs (Initial Public Offerings), the acronym ICO (Initial Coin Offering) is commonly used to refer to new token issuances. Again, caution should be exercised. These could be very risky investments because they often finance startup projects or companies. Being well informed is important. However, the available documentation could be incomplete, if not unclear. There are no specific regulations governing all ICOs. Securities rules may apply to some of them, but that varies from one country to the next. Lastly, some ICOs may be fraudulent, as the funds raised could be diverted for other purposes. To raise the public’s awareness of the risks surrounding ICOs, the U.S. Securities and Exchange Commission created a false ICO in May with HoweyCoins.3 Those who wanted to buy it were redirected to a site with information on the risks surrounding this type of investment.

Despite the downsides, the development of multiple applications with Distributed Ledger Technology opens the way for broader uses that could entail better oversight from a legal perspective. For example, the Australian Securities Exchange announced in December 2017 that it wanted to use this new technology to replace its current exchange platform in the next few years.4

**Will Central Banks Join the Parade?**

An application that could revolutionize payment methods would mean that national currencies, such as the Canadian dollar, the U.S. dollar and the euro, would be traded on cryptocurrencies-inspired platforms. Several central banks are currently looking into this. The national currencies would essentially be the same, except that they would also be traded virtually using distributed ledgers.5

This new way of holding and trading currency could be a substitute for the use of cash. The commonality would be particularly important from the point of view of central bank accounting. A unit of virtual currency or a unit of paper currency would both be recorded on the liability side of a central bank’s balance sheet. Just like for cash, the central bank would not be obligated to pay interest on this liability. It would, in turn, earn income from the securities held in its assets.

In a context where cash could be used to an even lesser extent, central banks might benefit from issuing currency in a new format to avoid revenue losses. If central banks’ liabilities decrease, their assets and interest income will too. The decrease in cash in circulation is particularly evident in Sweden (graph 7).

**GRAPH 7**

The amount of cash in circulation is dropping quickly in Sweden

---


In that respect, the Bank of Sweden (Riksbank) might be the first central bank to issue its currency in a virtual format, just as it was the first to issue paper currency in Europe in 1658.

However, issuing a national currency in a virtual format poses some issues, especially its potential use by organized crime. This would depend on the degree of confidentiality on the networks. Like cash, national cryptocurrencies evolving in a confidential environment could become a very popular payment method for illicit transactions. This could also be the case for the underground economy in general. One way of working around the problem would be to cap the amounts held in virtual wallets.

**The Experiment Continues!**

For all intents and purposes, it could be said that the Bitcoin and other cryptocurrency networks are a sort of lab experiment where a new technology can be tested. This experiment has now entered a new phase with the development of multiple applications. The next step could well be broader use of distributed ledgers in our everyday transactions. Stock exchanges have already taken a step in that direction, or are contemplating doing so. Some central banks are also considering the usefulness of issuing currency in a virtual format.

Of course, many details have yet to be ironed out, but there should be cost savings. This is, after all, the great promise of this technology. Networks such as the Bitcoin network, whose size is still limited and which uses a great deal of energy, do not appear to be viable in the long term, unless major changes are introduced. The networks must be designed to quickly process large quantities of transactions, at a low cost, while maintaining a high degree of security for users. This also entails legal security, with customized protection mechanisms.

Hendrix Vachon, Senior Economist