Strategic Report

CIO Office | June 2022

Digital assets: Speculative bubble or real revolution? Part 1/3.
The fundamentals

Cryptocurrencies, such as bitcoin, are the most famous digital asset class. Their market capitalization has exploded in recent years to a value of approximately two trillion Canadian dollars, roughly equivalent to the entire Canadian stock market. Their popularity was once limited to retail investors, but now has spread to some institutional investors and governments. Many skeptics argue that this market has irrational characteristics, particularly because of the staggering growth in digital assets. Is this a speculative bubble or a real revolution? To try to clarify the situation, three strategic reports will be dedicated to digital assets.

This first report will provide a summary of the fundamentals behind digital assets. The second will be dedicated to assessing their fundamental value, while the third will explore the issue of including such assets in a portfolio construction process.

Highlights

- Cryptocurrencies were borne out of a desire to improve the efficiency of transactions between individuals by decentralizing databases. To ensure the integrity of the network, two components are necessary.
- First, a sequence of mathematical steps must be executed to prove the identity of the initiator of a transaction. Second, the transaction history (the blockchain) must be shared by all members of the network. This shared record is updated by a validation mechanism that can take the form of proof-of-work or proof-of-stake. It is this second component that is the main innovation associated with digital assets. Indeed, blockchain is perceived by some as a technology that can have a major impact across several areas.
- Although there are now a wide variety of networks with various associated digital mechanisms and assets, their characteristics relative to conventional systems generally fall into three categories: (1) the ability to settle complex transactions quickly and inexpensively; (2) digital scarcity; and (3) the ability to create smart contracts.

Christophe Faucher-Courchesne
Associate, Quantitative Strategy
CIO Office

Nicolas Charlton
Associate, Quantitative Strategy
CIO Office

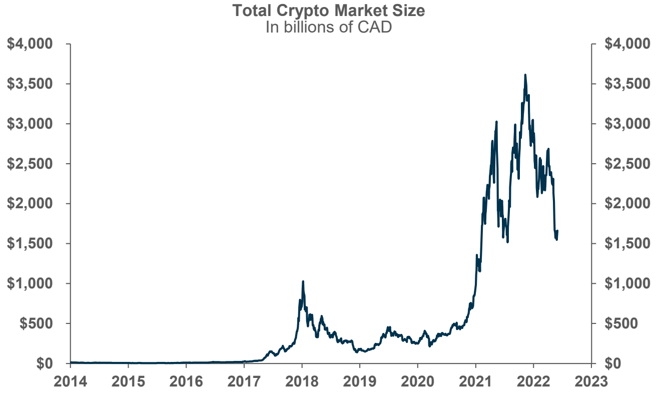
NATIONAL
BANK
INVESTMENTS

Phenomenal growth

The oldest digital assets have not yet celebrated their 15th anniversary. Yet the cryptocurrencies that make up the most famous class of digital assets (of which bitcoin is one) now have a combined market value of close to $1.6 trillion Canadian dollars, roughly equivalent to half of the entire Canadian stock market. Their popularity was once limited to individual investors, but has now spread to some institutional investors and governments. El Salvador and Cuba granted legal tender status to bitcoin in 2021.

However, the popularity of these assets is not unanimous. Some countries, such as China, have simply banned cryptocurrencies. Many skeptics argue that this market has irrational characteristics, especially because of the still rapidly increasing number of digital assets and the size of their market capitalization which have both seen staggering growth (**Chart 1**). There are now more than 19,000 cryptocurrencies in circulation[1] and many other types of digital assets such as non-fungible tokens (NFTs) continue to emerge. Is this a speculative bubble or a real revolution?

1 | Soaring growth of cryptocurrencies



CIO Office (data via Refinitiv)

In an attempt to shed some light on the situation, three strategic reports will be dedicated to the topic of digital assets. This first report will provide a summary of the fundamentals behind digital assets. The second will be dedicated to assessing their fundamental value, while the third will explore the issue of including such assets in a portfolio construction process.

The early days of Bitcoin

In 2008, a paper titled Bitcoin: A Peer-to-Peer Electronic Cash System described a program that would allow users to conduct financial transactions without intermediaries through a robust and decentralized database: the blockchain. Shortly after, in 2009, the program was made available and Bitcoin[2] was born.

The stated purpose of this article was to propose a method to modernize the way transactions are conducted. Indeed, despite the many technological advances of the last few decades, the execution of transactions between clients of different banks, or worse, different countries, is not instantaneous. Even today, these money transfers may incurr significant delays or fees. To illustrate the traditional situation and to better understand the innovation proposed by the original article, let's consider two people, Alice and Bob, who each wish to make a transaction. Alice is a client at Bank A, while Bob is a client at Bank B.

Suppose Alice wants to send $5,000 by cheque[3] to Bob. When Bob cashes the cheque, Bank B must ensure that Alice has the promised amount before adding the amount to Bob's account. However, Bank B's database consists only of its own customers. Since Bank B does not have access to the necessary information about Alice, it must contact Bank A to have it verify the information in Bank A’s own database. Once confirmed, Bank B can make the money available to Bob. This process takes some time and accounts for much of the delay and fees charged.

[1] Data via https://coinmarketcap.com/.

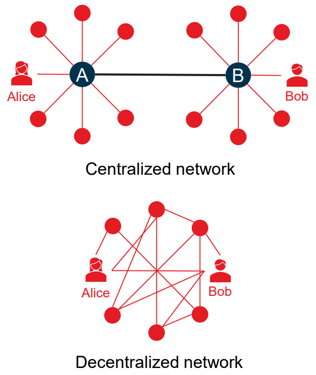
[2] Bitcoin (with a capital letter) refers to the network on which the currency, bitcoin (with a lower-case letter), is traded.

[3] Note that the use of the cheque only serves to illustrate the example without reducing its relevance, as similar processes are involved for the usual electronic transfers.

Bitcoin, a decentralized network

The innovation proposed by the article is based on a database shared by the whole network (**Chart 2**). Indeed, if all the members of a network could verify that Alice possesses $5,000 and that she is indeed the instigator of the transfer request to Bob, the verification would be accelerated.

2 | Centralized vs decentralized networks



Centralized network

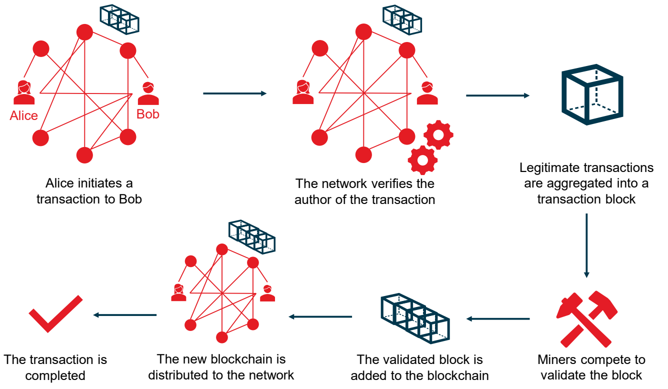
Decentralized network

CIO Office

To do this, two challenges must be overcome. The first challenge is an authentication problem. Alice must be able to prove to the network that she wants to perform a transaction, otherwise another user could forge a transaction on Alice's behalf. The second challenge is network consensus. All members of the network must continually reach a consensus on the balance of each of the network members' accounts to prevent a situation where a user attempts to transfer money they do not possess. The mathematical and computational concepts behind the technology to address these two challenges are complex. Understanding them is certainly not required to hold and trade digital assets, just as it is not necessary to understand the workings of the banking system to hold an account at a financial institution. However, it is relevant to paint a simplified picture of how a transaction (**Chart 3**) with this technology works to better understand the innovations proposed and the interest in digital assets.

The first problem, authenticating the originator of a transaction, is solved by using unique key pairs. Each member of the blockchain network has two keys: a private key and a public key. The private key works like a password and must never be revealed to the network. It allows its holder to make transactions from one account to other accounts. Conversely, the public key is accessible to all members of the network. It is generated from the private key and allows other users to transfer money to the account of its holder. The cryptographic algorithm used to generate the public key makes it easy for the private key holder to generate his public key, but practically impossible for other users to figure out the private key from the public key. These cryptographic concepts are not unique to blockchain or digital assets. On the contrary. They are commonly used on the Internet, and especially have been utilized by HTTPS web pages since the 90s.

3 | Transaction process



Alice initiates a transaction to Bob

The network verifies the author of the transaction

Legitimate transactions are aggregated into a transaction block

Miners compete to validate the block

The validated block is added to the blockchain

The new blockchain is distributed to the network

The transaction is completed

CIO Office

To understand how these keys can authenticate the initiator of a transaction on the blockchain, let's go back to the example of Alice and Bob. Alice wants to send $5,000 to Bob. To do so, she creates a computer file containing the recipient, i.e., Bob's public key, and the message stipulating the amount to be transferred. In order to authenticate the origin of the message, Alice uses a sophisticated electronic signature that is determined by both the message and also her private key. This private key must obviously not be made public. To protect the private key, a series of mathematical operations are used to create a signature. The sequence combines and then transforms the message and the private key into a single value that accompanies the original message. Alice can therefore sign with her private key without revealing it. Moreover, since Alice's signature is unique for each transaction (because the content of the message changes), it is impossible for another user to attempt to forge a transaction by reusing the same signature that Alice provided in the transaction with Bob. In this context, how can the network recognize this is Alice's signature if she does not explicitly reveal her private key?

A second sequence of operations, this time verification, is used by the rest of the network to confirm the authenticity of the signature. The verification function combines Alice's public key (which, remember, is linked to the private key), her signature, and her message. Again, using mathematical operations, it is possible to determine whether the signature produced is indeed linked to Alice's public key and indirectly to her private key. In short, these two functions allow Alice to hide her private key while proving to the whole network through her public key that she holds the private key used to generate the signature. The authentication problem is thus solved using known cryptographic techniques. The second challenge mentioned above is to ensure that all the actors in the network reach consensus on the balance in the various accounts. In other words, it is necessary for each participant to have an identical copy of the transaction history register to prevent a participant from trying to transfer an amount not in their account. This is where the innovation of the blockchain comes into play.

~~Gold~~ bitcoin miners

Which protocol ensures all network participants have the same version of the ledger? This is the question the original Bitcoin article answers by proposing to trust the ledger that required the greatest computational effort. Let's go back to the example of Alice and Bob to illustrate the effort mentioned. Previously, Alice sent a message to the network conveying her intention to transfer $5,000 to Bob. The network then proceeded to verify her signature. After this operation, the transaction proposed by Alice is put on hold for validation. Validation is performed by specific members of the network who are called "miners." These participants aggregate the various proposed transactions into a "block." This block also contains a copy of the most recent version of the ledger, making it possible to preserve the history of previous transactions.

The different miners then compete to try to solve a complex cryptographic problem that is related to the transaction block in question. This problem can only be solved by trial and error, and requires significant computational effort. In contrast, the design of the problem makes it trivial to validate the answer once it is discovered by one of the miners. This validation mechanism is called proof of work. When a miner finds the answer and it is validated by the other miners, the block of transactions is added to the registry and transmitted to all participants. This register is therefore a succession of approved blocks: the famous blockchain. The level of complexity of the problem adapts according to the number of miners, so that a block always requires about ten minutes on average to be approved. This same mechanism offers good protection against potential malicious miners who would try to have fraudulent blocks approved. Indeed, since the official registry is the one that required the most computational effort (and therefore the most blocks approved), malicious miners would need to succeed in getting more blocks approved in their parallel version of the registry than the official one. This is highly unlikely if the number of malicious miners does not represent the majority of miners.

Solving the problem to provide the proof of work requires computing and energy costs. The first successful miner to find the solution that results in validation of the block receives compensation in the form of new assets associated with that blockchain, such as bitcoins. These participants are therefore called miners, analogous with gold, and miner participation increases the number of coins minted. In 2022, Bitcoin miners who manage to find the solution to a block receive 6.25 new bitcoins, which means about $250,000 Canadian dollars.[4] However, the price of bitcoin is not the only factor influencing the reward, as the number of coins obtained by mining is programmed to decrease over time. The total number of bitcoins will be limited to 21 million and 90% of them have already been produced. The last bitcoins should be produced in or around the year 2140. This operation leads to a new concept: digital scarcity.

Cryptocurrencies are multiplying

The combination of the mechanisms associated with key pairs and proof-of-work allows the creation of the decentralized, unmediated network. However, this does not mean the solution is perfect. The proof-of-work validation mechanism is very energy-intensive and limits the number of transactions that can be validated. The Bitcoin network can support less than 10 transactions per second. In comparison, Visa estimates it can support up to 24,000 transactions per second through its centralized system. These technical limitations have given rise to a multitude of different networks and their associated cryptocurrencies. For example, Ether – the second largest cryptocurrency in terms of assets – is expected to replace its validation mechanism this year. Rather than using proof of work like Bitcoin, Ether will use a mechanism called proof of stake. In this mechanism, the miner does not have to solve a complex, energy-intensive mathematical problem, but instead presents a certain amount of cryptocurrency in deposit. The miner can then validate the transaction with a simple task and get his deposit back as well as additional compensation in the form of new Ether coins. However, if an attempt to defraud is detected, the miner loses his deposit.

The presence of other cryptocurrencies is also explained by additional features. Several digital assets allow for the implementation of smart contracts, i.e., transactions that are programmed to execute automatically once certain conditions are met.

Conclusion

In summary, digital assets, of which cryptocurrencies are the most well-known components, were borne out of a desire to improve the efficiency of transactions between individuals by decentralizing databases. To ensure the integrity of the network, two components are necessary.

First, a series of mathematical steps are needed to prove the identity of the initiator of a transaction. Second, the transaction history, the blockchain, must be shared by all members of the network. This record is updated by a validation mechanism that can take the form of a proof of work or a proof of stake. It is this second component that is the main innovation associated with digital assets. Indeed, blockchain is seen by some as a technology that can have a major impact in several areas.

Although there is now a wide variety of networks with various mechanisms and associated digital assets, their characteristics when compared to conventional systems can generally be summarized in three categories: (1) the ability to settle transactions quickly and cheaply; (2) digital scarcity; and (3) the possibility of creating smart contracts. These characteristics allow us to look at the assessment of fundamental value. This topic will be addressed in the next strategic report dedicated to digital assets.

[4] As of June 1, 2022, one bitcoin was trading for approximately $40,000 Canadian.

CIO Office
CIO-Office@nbc.ca

Martin Lefebvre
Chief Investment Officer
martin.lefebvre@bnc.ca

Louis Lajoie
Director
Investment Strategy
louis.lajoie@bnc.ca

Mikhael Deutsch-Heng
Associate
Investment Strategy
mikhael.deutschheng@bnc.ca

Simon-Carl Dunberry
Director
Portfolio Strategy
simon-carl.dunberry@bnc.ca

Zaid Shoufan
Associate
Portfolio Strategy
zaid.shoufan@bnc.ca

Nicolas Charlton
Associate
Quantitative Strategy
nicolas.charlton@bnc.ca

Christophe Faucher-Courchesne
Associate
Quantitative Strategy
christophe.faucher-courchesne@bnc.ca

General

The present document was prepared by National Bank Investments Inc. (NBI), a wholly owned subsidiary of National Bank of Canada. National Bank of Canada is a public company listed on the Toronto Stock Exchange (TSX: NA).

The information and the data supplied in the present document, including those supplied by third parties, are considered accurate at the time of their printing and were obtained from sources which we considered reliable. We reserve the right to modify them without advance notice. This information and data are supplied as informative content only. No representation or guarantee, explicit or implicit, is made as for the exactness, the quality and the complete character of this information and these data. The opinions expressed are not to be construed as solicitation or offer to buy or sell shares mentioned herein and should not be considered as recommendations. The opinions are not intended as investment advice nor are they provided to promote any particular investments and should in no way form the basis for your investment decisions. National Bank Investments Inc. has taken the necessary measures to ensure the quality and accuracy of the information contained herein at the time of publication. It does not, however, guarantee that the information is accurate or complete, and this communication creates no legal or contractual obligation on the part of National Bank Investments Inc.

NBI or its affiliates often act as financial advisor, agent or underwriter for certain issuers mentioned herein and may receive remuneration for its services. As well NBI and its affiliates and/or their officers, directors, representatives, associates, may have a position in the securities mentioned herein and may make purchases and/or sales of these securities from time to time in the open market or otherwise.

This document is for distribution only under such circumstances in Canada and to residents of Canada as may be permitted by applicable law. This document is not directed at you if NBI or any affiliate distributing this document is prohibited or restricted by any legislation or regulation in any jurisdiction from making it available to you. You should satisfy yourself before reading it that NBI is permitted to provide this document to you under relevant legislation and regulations.

Commissions, trailing commissions, management fees and expenses all may be associated with mutual fund investments (the “Funds”). Please read the prospectus of the Funds before investing. The Funds’ securities are not insured by the Canada Deposit Insurance Corporation or by any other government deposit insurer. The Funds are not guaranteed, their values change frequently and past performance may not be repeated.