We are pleased to revive *F&D*'s popular "Back-to-Basics" series, which we discontinued at the end of 2015. In this series, we explain the economic terms that our readers encounter on a daily basis. Check out the "Back-to-Basics" videos, too, at www.fandd.org.

# What Are Cryptocurrencies?

## A potential new form of money offers benefits while posing risks

**Antoine Bouveret and Vikram Haksar**

**HUNDREDS OF THEM** have sprouted, with fanciful names like Primecoin, Dash, and Verge. They have developed cult-like followings among the tech-savvy. Their values fluctuate wildly. Some people say these mysterious bits of computer code will someday replace money as we know it. What exactly are these cryptocurrencies, and what makes people think they are worth anything at all? To answer these questions, let's first look at how money evolved.



### Uses of money

Money serves as a store of value, a means of exchange for goods and services, and a unit of account that measures value. Before money, human societies exchanged goods and services directly—a bushel of grain for a pig, say. This was not very efficient. As societies grew more complex, commodity monies were developed—from seashells to copper, silver, and gold. Some states introduced fiat money—which has no intrinsic value other than the promise to pay—such as paper money in eighth century China under the Tang dynasty.

Most early forms of fiat money were neither very stable nor widely accepted, as people did not believe the issuer would honor its commitment to redeem the money. Governments were tempted to print more money to buy goods or raise wages, which fueled inflation (think of people moving cash around in wheelbarrows in post–World War I Germany). Modern central banks seek to maintain price stability by regulating the supply of money on behalf of governments.

### Bookkeeping and ledgers

An increasingly extensive and complex financial system gave rise to the need for trusted intermediaries and credible accounting systems. The development of double-entry bookkeeping in Renaissance Italy was a major innovation that strengthened the role of large private banks. In modern times, central banks emerged at the apex of payment systems. With computerized bank ledgers, the coordinating role of central banks increased.

How do such ledgers work? Financial institutions adjust the positions of their account holders in their internal ledgers, while the central bank validates transactions among financial institutions in a central ledger. For example, Mehrnaz uses money from her account in bank A to buy goods from Mary, who has an account in bank B. Bank A debits the money from Mehrnaz's account. The central bank moves money from bank A to bank B and records the transaction in its central ledger. Bank B then adds the money to Mary's account. As you can see, the system is based on trust in the central bank and in its ability to safeguard the integrity of the central ledger and ensure that the same money is not spent twice.

ART: THE NOUN PROJECT / MASSUPA KAEWGAHYA

With many cryptocurrencies, on the other hand, there is no need for a trusted central agent. Instead, they rely on distributed ledger technology, such as blockchain, to construct a ledger (effectively a database) that is maintained across a network. To ensure that the same cryptocurrency is not spent twice, each member of the network verifies and validates transactions using technologies derived from computing and cryptography. Once a decentralized consensus is achieved among members of the network, the transaction is added to the ledger, which is validated. The ledger provides a complete history of the transactions associated with a particular cryptocurrency that is permanent and cannot be manipulated by a single entity. This ability to achieve consensus on the validity of transactions between accounts in a distributed network is a foundational technological shift.

Network members who verify and validate transactions are usually rewarded with newly minted cryptocurrency. Many cryptocurrencies are also pseudo-anonymous: holders of the currency have two keys. One is public, such as an account number; another, private key is required to complete a transaction. So, to continue the previous example, Mehrnaz wants to buy goods from Mary using a cryptocurrency. To do so, she initiates a transaction with her private key. Mehrnaz is identified in the network by her public key, ABC, and Mary is identified by hers, XYZ. Network members verify that ABC has the money she wants to transfer to XYZ by solving a cryptography puzzle. Once the puzzle is solved, the transaction is validated, a new block representing the transaction is added to the blockchain, and the money is transferred from ABC's wallet to XYZ's.

## Benefits, risks

Now that we understand the technology, let's return to the genesis of cryptocurrencies. The first one, Bitcoin, was introduced in 2009 by a programmer (or group of programmers) using the pseudonym Satoshi Nakamoto. As of April 2018, there were more than 1,500 cryptocurrencies, according to coinmarketcap.com; along with Bitcoin, Ether and Ripple are the most widely used.

Despite the hype, cryptocurrencies still don't fulfill the basic functions of money as a store of value, means of exchange, and unit of account. Because their value is highly volatile, they have little use so far as a unit of account or a store of value. Limited acceptance for payment restricts their use as a medium of exchange. Unlike with fiat money, the cost of producing many cryptocurrencies is high, reflecting the large amount of energy needed to power the computers that solve the cryptographic puzzles. Finally, decentralized issuance implies that there is no entity backing the asset, so acceptance is based entirely on users' trust.

**Distributed ledger technology could reduce the cost of international transfers, including remittances, and foster financial inclusion.**

Cryptocurrencies and their underlying technologies offer benefits but also carry risks. Distributed ledger technology could reduce the cost of international transfers, including remittances, and foster financial inclusion. Some payment services now make overseas transfers in a matter of hours, not days. The technology can provide benefits beyond the financial system. For example, it can be used to securely store important records, such as medical histories and land deeds. On the other hand, the pseudo-anonymity of many cryptocurrencies makes them vulnerable to use in money laundering and terrorism financing, if no intermediary checks the integrity of transactions or the identity of the people making them. Cryptocurrencies could also eventually present challenges for central banks were they to affect control over the money supply and therefore the conduct of monetary policy. FD

**ANTOINE BOUVERET** is an economist and **VIKRAM HAKSAR** an assistant director in the IMF's Strategy, Policy, and Review Department.