



Updated February 7, 2018

Financial Innovation: “Cryptocurrencies”

A “cryptocurrency” (sometimes referred to as *virtual currency*, a term that can also refer to a broader class of electronic money) acts as money in an electronic payment system in which transactions are validated by a decentralized network of computers rather than a third-party intermediary, such as a bank. The use of this financial technology (or *fintech*) potentially creates certain benefits, poses certain risks, and raises a number of questions for policymakers. This In Focus examines cryptocurrencies and related policy issues.

Background

A central difficulty with sending payments electronically is the “double spending problem.” Sending an electronic message or digital file directly from a payer to a payee in the hopes that it will act as a transfer of value is problematic, because payees cannot confirm that a payer has not sent that same message or file to multiple other payees. Because money in such a system can be double (or any number of times) spent, it would not retain its value.

Traditionally, this problem has been resolved by involving at least one centralized, trusted intermediary—such as a private bank, government central bank, or other financial institution. The trusted intermediaries maintain ledgers of accounts recording how much money each participant has. To make payment, an electronic message or messages are sent to an intermediary or to and between various intermediaries, instructing each to make the necessary changes to their ledgers to transfer value from one account to the other.

In 2008, Bitcoin created a new solution to the double-spending problem through the use of *blockchain technology*, which is now frequently used to enable other various cryptocurrencies, such as Ether, Alpha Coin, and Papyrus. Blockchain uses cryptography, file sharing and user agreement to ensure that *each* transaction is secure, that the *groups* of transactions that form blocks are secure, and that *the entire ledger* (or blockchain) is secure. Through this system, parties that do not trust each other can nevertheless exchange value without a centralized intermediary, because they trust the decentralized network and its cryptographic protocols.

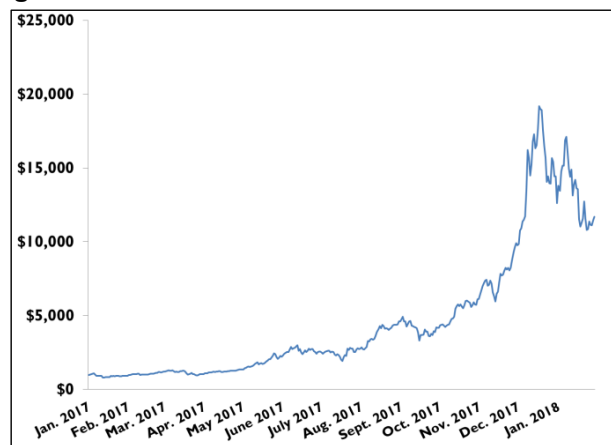
Cryptocurrencies act as money in these virtual platforms that maintain digital ledgers, which appear virtually impossible to falsely manipulate. The transfer of a cryptocurrency from one member of a network to another represents a valid transfer of value. The transfers are validated by the network’s members and not by a centralized third-party or a payment system that involves such intermediaries.

Payers and payees in these networks are typically identified by a pseudonym (often a string of numbers and characters), called an *address*, which is linked to a *public key*. They also need a password, called a *private key*, in order to process a transaction. The address identifies to the users of the blockchain that the identity controlling the public key owns cryptocurrency, which can only be used when they apply their private key to it. Because of the platforms’ security protocols, losing the public or private key often means losing access to the cryptocurrency. Together the public and private keys are sometimes called a *wallet* in which an individual’s cryptocurrencies are stored when the individual is not using them in transactions.

People may “mine” certain cryptocurrencies, earning newly created units of the currencies by performing certain work for the platform, such as validating incoming transactions. Alternatively, people can acquire cryptocurrencies on exchanges with payment of official government-backed currencies or other cryptocurrencies. Although cryptocurrency ledgers are believed to be mathematically secure, vulnerabilities in wallets and exchanges have been exploited, causing losses for individuals and exchanges.

One likely reason cryptocurrencies have recently become a prominent issue is the sudden appreciation (and subsequent depreciation) in value of many of them. For example, according to one company that tracks prices, the value of a Bitcoin rose 1,884% from \$968 at the beginning of 2017 to \$19,194 at its peak in December 2017, as shown in **Figure 1**. The value then fell 44% to \$10,797 a little more than a month later.

Figure 1. Value of Bitcoin



Source: Bitcoin.com accessed on January 30, 2018.

Potential Benefits

As discussed above, traditional monetary and electronic payment systems involve a number of intermediaries such as government central banks and private financial institutions. To carry out transactions, these institutions

operate and maintain extensive electronic networks and other infrastructure, employ workers, and require time to finalize transactions. To meet costs and earn profits, users of the systems are charged fees. Cryptocurrencies aim to provide a payment system that is more efficient, faster, and less costly. In addition, the pseudonymity of transactions offers greater privacy that could be valued by some users.

Potential Obstacles

It is not clear if cryptocurrencies will be able to deliver these hoped-for efficiencies, because they currently face certain limitations. For money to be effective, it must serve as a medium of exchange widely accepted across the economy and act as a “store of value.” Unlike the U.S. dollar or other government backed currencies, cryptocurrencies are not legal tender, meaning creditors are not legally required to accept them to settle debts. In addition, consumers may be hesitant to place their trust in a decentralized computer network of pseudonymous participants that many do not completely understand. These characteristics may impede the widespread adoption of cryptocurrencies. Furthermore, the values of many cryptocurrencies have recently been highly volatile, potentially making them a poor store of value.

In addition, even if a cryptocurrency is able to achieve widespread acceptance and a stable value, the system is not costless. The fast processing of payments requires performing computations, which are extremely difficult and require investment in computers and servers and the consumption of electricity. Given these costs, whether or under what conditions greater efficiency than the existing system can be achieved is uncertain.

Policy Issues

Cryptocurrency transactions involve money transfers, exchanges, and investment products. Policymakers have created an existing regulatory framework to address risks related to these activities. Because these currencies are new and evolving, it is not yet clear how effective the tools and authorities available to regulators are when applied to cryptocurrencies.

Some observers argue that certain regulations restrict the adoption and use of beneficial cryptocurrencies and should be relaxed. In contrast, others argue that current regulation provides inadequate protections against potential risks and that regulation should be strengthened.

Crime. The pseudonymous and decentralized nature of cryptocurrency transactions could provide an additional means to launder money, evade taxes, fund terrorists, or bypass financial sanctions the U.S. government has imposed on other countries.

The Department of the Treasury’s Financial Crimes Enforcement Network (FinCEN) has issued guidance explaining how regulations designed to curtail these activities apply to the use of virtual currencies. FinCEN has indicated that *exchangers* (people engaged in the business of exchanging virtual currency for real currency, funds, or other virtual currency) and *administrators* (people engaged in the business putting virtual currency into circulation and

who have the authority to withdrawal currencies from circulation) qualify as *money services businesses* (MSBs) subject to federal regulation. Among other things, MSBs must register with and report suspicious transactions to FinCEN and maintain anti-money laundering compliance programs.

Taxes. The Internal Revenue Service has issued guidance stating that virtual currencies should be treated as *property* (as opposed to *currency*), meaning that users owe taxes on any realized gains whenever they dispose of virtual currency, including when they use it to purchase goods and services. The guidance further indicates that when an employee is paid in virtual currency, it will be taxed as wages.

Consumer Protection. Because consumers are not necessarily familiar with cryptocurrencies, they could be charged excessive fees when using or exchanging the currencies; deceived about their true value; or unaware of the risks of loss of value or electronic theft. Cryptocurrency exchanges may be required to obtain money transmitter licenses from the states in which they operate, and to abide by any consumer protection requirements imposed on money transmitters by state law.

Investor Protection. Cryptocurrencies have or may become the underlying asset in certain financial products—including initial coin offerings (ICOs) wherein cryptocurrencies are sold to raise capital; exchange traded funds (ETFs) wherein a fund invests in a portfolio of cryptocurrencies; and futures contracts wherein parties agree to buy, sell, or trade cryptocurrencies at a future date. In these cases, questions about investor protections have been raised. Some observers are concerned these products create the opportunity for investors to take on risks they do not understand or to become victims of fraud. The Securities and Exchange Commission (SEC) has indicated that depending on their specific features, ICOs may result in offerings of “securities” subject to federal regulation. The SEC also regulates the majority of ETFs, and has sought public comment on proposals related to Bitcoin-based ETFs. The Commodities Futures Trading Commission regulates derivatives contracts in virtual currencies, and exchanges on which such contracts trade. Both agencies have issued statements outlining their general approach to the regulation of virtual currency products.

CRS Products

CRS Report R43339, *Bitcoin: Questions, Answers, and Analysis of Legal Issues*, by Edward V. Murphy and M. Maureen Murphy

CRS Legal Sidebar WSLG1856, *For First Time, FinCEN Imposes Penalty on Foreign-Based Virtual Currency Exchange for Violations of Anti-Money Laundering Laws*, by M. Maureen Murphy

David W. Perkins, Analyst in Macroeconomic Policy

IF10824

Disclaimer

This document was prepared by the Congressional Research Service (CRS). CRS serves as nonpartisan shared staff to congressional committees and Members of Congress. It operates solely at the behest of and under the direction of Congress. Information in a CRS Report should not be relied upon for purposes other than public understanding of information that has been provided by CRS to Members of Congress in connection with CRS’s institutional role. CRS Reports, as a work of the United States Government, are not subject to copyright protection in the United States. Any CRS Report may be reproduced and distributed in its entirety without permission from CRS. However, as a CRS Report may include copyrighted images or material from a third party, you may need to obtain the permission of the copyright holder if you wish to copy or otherwise use copyrighted material.