Decentralized E-Money (Bitcoin)

What is decentralized e-money?

Decentralized e-money is stored and flows through a peer-to-peer computer network that directly links users, much like a chat room. No single user controls the network.

There is no centralized issuer of such products or a trusted third party that manages them. This means that they are independent of central banks, financial institutions and Internet platforms. Decentralized e-money is not backed by any particular good or service, and is not redeemable into national currencies.

Bitcoin is an example of a decentralized e-money innovation. Bitcoin was launched in 2009, and since then, many other similar digital currencies have been created, including Litecoin, Peercoin, Ripple and Nxt.

Decentralized e-money such as Bitcoin arose because cryptography and technology have solved two problems, counterfeiting and double spending, that would have made a decentralized digital currency impossible. The use of cryptography is one of the reasons why the various types of decentralized e-money are typically called "cryptocurrencies."

Authenticity

As with today's polymer bank notes, to ensure the value of a currency, you need to check that it is authentic. The same is true of cryptocurrencies.

To confirm the authenticity of a cryptocurrency, you need to verify the electronic record that supports it. There are now well-established information technologies to help you do that.

Double spending

You also want to make sure that the cryptocurrency you receive has not already been spent—that the person sending it to you has not previously sent the same unit of the cryptocurrency to someone else.

Preventing this problem is particularly challenging in decentralized e-money, because there is no centralized platform or institution to verify the transaction and take steps against double spending.

Now, thanks to cryptographic tools, network users can trust the validity of the cryptocurrency despite the absence of a trusted third party.

Are cryptocurrencies "money"?

The commonly held definition of money includes three criteria:

(i) Money should be generally accepted as a medium of exchange.

(ii) Money should be a unit of account so that we can compare the costs of goods and services over time and between merchants.

(iii) Money should be a store of value that stays stable over time.

Using those criteria for Bitcoin and other cryptocurrencies, we see that they fall short of today's definition of "money."

This text, and other backgrounders on topics related to the Bank of Canada's work, can be found at: bankofcanada.ca—search for "backgrounders."

© Bank of Canada 2014

As a medium of exchange

Only a few retailers accept Bitcoin as payment for goods and services. In Canada, in early 2014, there may be only about 200 retailers that accept Bitcoin. While this number is likely growing, at present, Bitcoin is not "generally accepted" as a medium of exchange.

As a unit of account

Even retailers that accept Bitcoin tend to display their prices in state currencies such as the Canadian dollar and only translate them into Bitcoin at the point of sale. This suggests that Bitcoin is not a unit of measurement that could be used to compare the value of a good or service offered over time or by different merchants.

As a store of value

Cryptocurrencies such as Bitcoin are highly volatile. For example, the value of Bitcoin is 40 times more variable than the value of the U.S. dollar. People are unlikely to want to save or invest money in a cryptocurrency whose value could swing wildly over a short period of time. The same is true for merchants, who are unlikely to accept a "medium of exchange" that is so volatile in value.

Potential risks of using cryptocurrencies

Bitcoin users need to be aware of the potential financial risks to which they might be exposed, in light of the volatility of Bitcoin prices and the risk of failure of Bitcoin exchanges, such as Mt. Gox. As well, given that cryptocurrencies such as Bitcoin are not regulated and do not have a centralized issuer, users bear all of the risks themselves and have no legal recourse should they wish to reverse a Bitcoin transaction.

April 2014