



# Giving Currency to Not Using Currency

Many transactions are done online, but most are based on standard currencies. Bitcoin is one example of a digital payment system, or cryptocurrency, that exists only electronically, preserves its users' anonymity, and has no central player such as a bank or government in control. It relies on a network of shared computers to process and verify each transaction, each of which is encrypted using mathematical formulas and entered into an electronic ledger, called a *blockchain*. The blockchain connects transactions and ensures that a bitcoin owner can't spend the same unit of value ("coin") twice. Each bitcoin owner has a private number that the mathematical formulas make easy to use but impossible in practice to discover. Thus, although

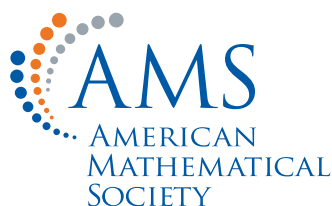


bitcoins may seem less secure than hard currency, they are far less vulnerable to theft or counterfeiting as long as the private number is kept secret.

Listen Up!



MM/134.s



The **Mathematical Moments** program promotes appreciation and understanding of the role mathematics plays in science, nature, technology, and human culture.

[www.ams.org/mathmoments](http://www.ams.org/mathmoments)