WILSON MEMO

Wilson Center
Congressional Relations

Wilson Center
SCIENCE AND TECHNOLOGY INNOVATION PROGRAM

CryptoMaster Briefing: The Cryptocurrency Codex

Cryptocurrency Basics

Cryptocurrency is electronic money. For centuries, society has used "money" as a medium of exchange for goods and services–an alternative to the barter system.

Early on, money took the form of gold and silver coins. At one time, the US dollar was backed by gold. Today, fiat currencies, like the dollar, are the prevailing form of money in the world.

Fiat currencies have value because a government has declared them "legal tender" and people believe they have value. Ownership of fiat currency is recorded by central authorities, in centralized ledgers. This ownership can be represented by attractively designed pieces of paper (e.g. the dollar bill).

The idea for cryptocurrency is based on the notion that the same principle that allows paper to be used as money can be applied to an alphanumeric string– also known as a "**hash**" (e.g. "a2g893dh"). If people are willing to accept this hash in return for goods and services, it can serve the function of an alternative form of money. The hash exists electronically as a data entry on a ledger.

Cryptocurrency is a digital asset. The current infrastructure bill defines digital assets as "any digital representation of value which is recorded on a cryptographically secured distributed ledger or any similar technology as specified by the [Treasury] Secretary." **Unlike the US dollar, anybody can create a cryptocurrency.**

Cryptocurrency is stored in "digital wallets". The cryptocurrency held in those wallets can be traded on **exchanges**, through "**brokers**," or directly between counterparts. Digital wallets have a certain degree of anonymity. The record of what wallet holds a hash is kept on ledgers that might be updated and validated by record keepers called "**miners**."

This record keeping system is called the "**blockchain**." Miners record the hash's movement between senders and receivers on a ledger which is distributed. Each time a hash moves, the "miners" may be "rewarded" (paid) for keeping the record system intact. The movement of the hash (the cryptocurrency), and its history of exchange between wallets is encoded (or encrypted) into the hash itself. Each hash is therefore unique, thereby eliminating the "double spend problem" (like the security features and serial numbers on dollar bills). There is no central authority keeping the records of who owns what– the community keeps the records with perhaps thousands of computers or "nodes" storing information. As such, the blockchain is viewed by many as more immutable than a centralized storage system as the record of ownership and transaction is maintained across a "**distributed ledger**." The distributed ledger can be used to store other information and programs as well. For instance, we could build into the blockchain conditions for the movement of a hash (a so called "**smart contract**").

As a cryptocurrency gains traction, its value relative to fiat currency or other assets (physical or digital) may rise. Cryptocurrencies, therefore, might be exchanged for fiat currency, goods, or services, at a profit.

Debrief from Wilson Experts

Meg King & Alan Rechtschaffen

Director of Wilson Center Science and Technology Innovation Program (STIP). Learn more about Ms. King here.

Wilson Center Trustee, Private Investor, Senior Lecturer of Laws at New York University. Learn more about Mr. Rechtschaffen here.