Hannah Carter

Hugo Vaca Pereira

Money and Banking

12 February 2023

The Economics of Bitcoin and Similar private digital currencies

Are private digital currencies money? Gerald P. Dwyer thinks that maybe they can be. In his journal article "The economics of Bitcoin and similar private digital currencies," he argues that the use of peer-to-peer networks and open source software can bring about an equilibrium in which digital currency has a positive value. However, he stills fails to solve the main obstacle in the way of digital currencies' realization of true money status: the double-spending problem.

From the beginning, Dwyer establishes the reality of the double-spending problem: "a digital representation of currency requires that it not be possible to create multiple copies and spend the same digital currency two or more times." However, the medium of Bitcoin and other private digital currencies, known as "bits," are simple to produce on a computer, and there is no central authority to certify that particular pieces of currency have not already been spent. Instead, the currencies rely on networks of peer-to-peer authentication. Public-key cryptography is used to keep track of transactions and the amount of bitcoins owned by individuals, each of whom also has their own digital signature–or private key–in order to verify themselves. The database of Bitcoin, the "block chain," is kept and updated on multiple websites and records every trade of currency between "miners," with the correct chain always being the longest one. A rule limiting the number of bitcoins combined with the use of this peer-to-peer network makes it fairly easy to determine whether additional bitcoins are being added to the amount denoted by the system. An equilibrium of zero requires that the marginal cost of production of bitcoins is zero and that the

individual holders are relatively indifferent between various digital currencies. A positive equilibrium would require that all private currencies are highly liquid and distinguishable between themselves, in order to prevent them from being perfect substitutes.

Is it possible for Bitcoin to achieve the status of money? In my opinion, highly unlikely. Dwyer states how currency being distinguishable is a defining factor, but the fact that new private digital currencies are created all the time makes this extremely difficult: distinguishing between a potentially innumerable number of currencies will only make them harder to exchange. Whether or not these currencies can function as media of exchange for actual goods and services is also debatable because the block chains contain no information on transfers, and thus determining the volume of those exchanges is left to estimation. Even if these issues are resolved, there is still no solution to the double-spending problem; and based on current trends, there probably will not be one in the near future. Valid transactions, or additions to the block chain, can occur in a matter of seconds, but the risk of double spending is not reduced to a low level for ten or more minutes when they are included in a block or chain. Due to this, the risk of double-spending in fast transactions can never be eliminated. Considering that research has shown a recent trend towards smaller transactions and faster spending, it is a logical possibility that this problem could only increase within digital currency networks going forward. Without an answer to double-spending, private digital currencies like Bitcoin can never be considered true stores of value, and thus never reach the status of money.