Cryptocurrencies: From the past to the future

Andrew Odlyzko

School of Mathematics and Digital Technology Center
University of Minnesota
odlyzko@umn.edu
http://www.dtc.umn.edu/~odlyzko

April 27, 2014
What is money? Economists’ answer:

Money’s a matter of functions four,
  a Medium,
  a Measure,
  a Standard,
  a Store.
What is money? Sometimes cowry shells:

2,800 to 3,600 years-old money from China (Wikipedia Commons)
What is money? Sometimes a brand of cigarettes:

Romania in the 1980s (Wikipedia Commons)
What is money? Sometimes immovable stones:

stone coins of Yap (Wikipedia Commons)
Modern digital currencies

- PayPal

- credit cards: charge John Q. Smith’s credit card 1234-5678-9012-3456, expiration 14/14, security code 123, the sum of $123.45
mathematical tools: hash functions, Merkle trees, public key signatures, ...
Bitcoin from 10 miles up: Distributed public record of semi-anonymous transactions

... 
14134725141734693790
45725198356247027078 —owner of secret X is paying
   2345 satoshis to owner of secret Y
42571156992431756855
67460149963429809256
76494901039317156101
27792029715487974367
66142691469882254582
...
Third World: A pioneer in advanced payment systems

M-Pesa African wireless payment system (Wikipedia Commons)
Modern cryptocurrencies:

The future, but how big and how soon?

Technologists propose, society disposes!