



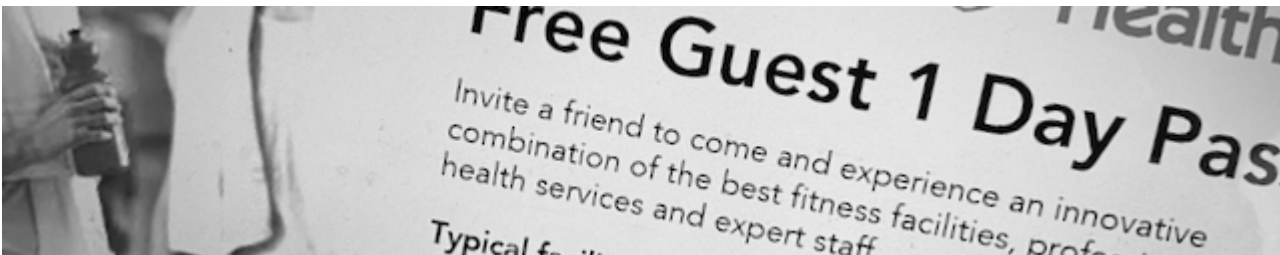
Digital cash 101

Description

Bitcoin is a cryptocurrency, i.e. it is digital money that purportedly carries some of the benefits of cash. You can buy things with it, give it away, invest it, and stash it without involving a bank. But unlike cash, there's no physical paper or coinage.

You could try to design your own banknote, or make a PDF of a real bank note, and email it to a friend but that carries no value, as you still have your own copy of the file, and it can be reproduced and sent again to someone else.

Like real paper money, digital money has to be scarce. When you give some of it away then you no longer have what you had. My local fitness centre used to send me a PDF of a free visitor pass when I answered an online customer satisfaction survey. They stopped doing that as it became obvious that customers could print any number of copies of the free pass and use it more than once.



Simulated, digital versions of paper money are redundant anyway. Our money with the bank is just a series of numbers on a ledger. As you receive or spend money the balance goes up or down, and we trust the bank to keep an accurate and secure record.

But digital currencies are for people who don't want banks to manage, monitor and profit from their transactions. They want the benefits of cash but without the paper or coinage. Transactions with digital currency are also best stored as records in a digital ledger.

A shared ledger

The problem is to provide a ledger that is secure, anonymised, and hidden and out of the purview of a centralised agency like a bank. The solution for cryptocurrencies is to distribute the ledger to the computers (nodes) of a large number of users. Software checks these distributed ledgers against one another in case someone tries to double spend an amount of money, or doctor the record. In fact, nothing gets recorded in the ledger unless all nodes agree it should be there.

The agreement to accept a block of transactions is reached by algorithms at the node computers. These algorithms try to outcompete one another in solving an arbitrary numerical puzzle that requires brute force computing to solve. The node that wins gets some bitcoin as a reward, and the answer to the puzzle gets planted into the block of transactions as a record that it has been verified.

Most of the transaction information in the ledger is in plain sight and can be read on a computer screen, but it's encoded, i.e. encrypted as a series of arbitrary looking alpha-numeric characters. The shared and ordered ledger and its verification apparatus is called a blockchain. Lots of books and online articles explain this further. See my posts: [immutable data](#), [Why hackers have to work hard](#), [An anti-hacker puzzle](#), and [Decode this](#).



What's wrong with digital money

It's well known that cryptocurrencies have certain drawbacks.

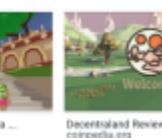
- **Speculation:** The value of cryptocurrencies relative to real (fiat) currency is unstable. Rather than spend the digital money on goods, people tend to buy and sell cryptocurrency in the expectation that it might rise in value. In the early days of its release, the value of bitcoin rose rapidly. It created bitcoin millionaires, and many people of course lost money when its value slumped.
- **Very few merchants accept bitcoin.** They don't have the means to process it, they can't be sure of its value relative to fiat currency, and transactions are not instantaneous. The verification process is slow as node computers reach their consensus to validate a block of transactions. It's hard for cryptocurrencies to compete with the convenience of debit and cash cards, and mobile phone transfer accounts e.g. Kenya's M-PESA (www.remitly.com).



- Verification is costly to the environment. Competition between computer nodes to verify blocks of transactions and thereby earn the nodes money has escalated the computer processing needed to compete. The process requires hardware, power and generates heat as an unsustainable resource burden on the environment. It also concentrates the computational effort to corporations and countries that can afford to support these processes. After all, the verification process only delivers value in so far as it sustains the blockchain. This concentration of economic power has political implications and returns power to the few rather than the many.

Crypto-cultures

Bitcoin was the first successful cryptocurrency and now there are others: Ethereum, Ripple, Litecoin, etc. Apart from their apparent utility, several factors amplify enthusiasm for new cryptocurrencies.



- The story of bitcoin lingers as evidence that cryptocurrencies provide an opportunity to acquire wealth quickly. Some startups in the blockchain world recruit investors by selling “initial coin offerings” (ICOs) as a way to raise startup funds. Investors buy the cryptocurrency at a favourable rate in the hope that their holdings will eventually increase in value.
- Cryptocurrencies entail an ideology (of decentralisation) that is attractive to many. The ideology appeals to both the right and left of politics. For those on the right cryptocurrencies support the idea of unregulated trade, individualism, small government, and self-sufficiency. On the left it suggests a means to greater democracy, people power and a break from large corporations and financial institutions (i.e. capitalism).
- The banking crisis of 2008 eroded the trust of many in banks and financial institutions. That cryptocurrencies are “decentralised,” suggests empowering people over institutions and the democratisation of money. Many people in developing countries are mistrustful of banks, or don’t have the resources to borrow or benefit from what banking offers. Cryptocurrencies

promise a means of empowering the “unbanked.”

- The ubiquitous reach of the Internet delivers, promotes and amplifies the operations of financial products and provides a vehicle for influence campaigns that amplify claims about cryptocurrencies.
- Cryptocurrency is mysterious to the average consumer, but tantalising. There’s plenty of scope for companies to deliver explanations that both clarify and confuse, deliberately or unintentionally. It’s also easy to insert false claims into a narrative dressed up as a cryptocurrency narrative.

As well as enabling legitimate cryptocurrency schemes, these factors create a climate rich with opportunities for scams, get-rich-quick schemes, fraud and fake systems that exploit cryptocurrency narratives (wealth, decentralisation, self-sufficiency, community, opportunity, education) and generate fake digital money schemes, like onecoin. See previous post: [Pseudo-crypto currencies](#).

Category

1. Economics

Tags

1. bitcoin
2. blockchain
3. dagcoin
4. onecoin
5. trumpcoin

Date Created

February 22, 2020

Author

rcoyne99

default watermark