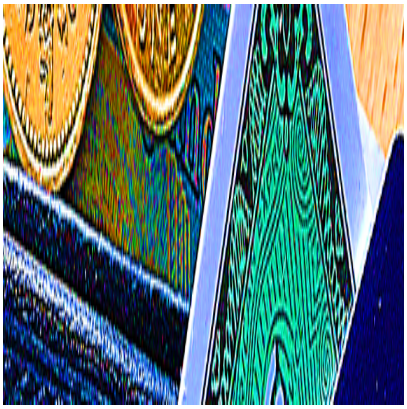

Digital money

Description

Digital money attempts to keep financial transactions reliable and trustworthy without the need for a bank. To achieve this it does two things that computer networks do well: distribute and encrypt.

If I create a painting then itâ??s a one off. If I sell it then I pass on ownership of the painting to the buyer. The buyer takes possession of the physical object to hang on a wall, store in a vault, or sell on to someone else. Once I have given a painting to someone I canâ??t give the same painting to them again, nor can I give it to someone else as well.

Cash, as in the case of notes and coins, is a bit like trading in paintings. Notes and coins are unique items, one offs, that we can exchange and pass around. Forgeries happen, but in general, cash currency is reliable. If I give a Â£10 note to someone I canâ??t give it to them again and call it Â£20, or give it again to someone else. Once it is spent itâ??s gone from my possession. The advantage of cash is that, once in circulation it requires no central management. Cash, like other physical goods, takes care of itself in a distributed economy.

But cash is cumbersome to carry around, especially in large quantities. You can lose the notes and coins, and someone can steal them.

Ledgers

Long before we had computers, there were ledgers, i.e. records of financial transactions, reducing the need to always have cash to hand. Companies would generate funds that they would hand over to some centralised, trusted agent, such as a bank. The funds would appear on the bankâ??s ledger (database of transactions).

As a company payed one of its workers, the bank record would show a drop in the balance on the companyâ??s ledger, and a corresponding increase in the employeeâ??s ledger. Via bank transfers, direct debits, debit card and other online transactions, money circulates as records on spreadsheets under the management of banks.

Thereâ??s an overhead. Banks take management fees. They lend money out to you and others, and do other things with it. Itâ??s fair to say that trust in banks dropped since the 2008 financial crisis. Digital money is an attempt to wrest control of money from banks. It attempts to combine the benefits of cash with those of digital ledgers, but to diminish the need for banks.

Instead of circulating Â£10 notes, why not have digital images of Â£10 notes and circulate those? Itâ??s obvious. Like other digital products, digital images are not unique, and can be copied. You could pay someone with an image of a Â£10 note, but thereâ??s no guarantee itâ??s an original, nor that you havenâ??t already given it to someone else.

Cash notes have unique serial numbers. In the world of digital money, no one is thinking in terms of images of cash notes. So all you need is something like a serial number. A unit of digital currency can be as abstract as a string of characters. As itâ??s processed on computer systems it doesnâ??t need to look anything like money. The trick to ensuring the uniqueness and integrity of a transaction in digital money is to encrypt the digital cash unit. According to the seminal paper on digital cash by â??Satoshi Nakamotoâ??:

> â??What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party.â?•

So the challenge is to create a digital string that can be stored in a computer database but is unique, it can be recorded, but itâ??s value canâ??t be duplicated. Nor can it be spent again by the same person. Nor can the ledger be hacked with fake transactions by an outside party.

Distributed ledgers

Transactions take place within networks of computers belonging to people using the digital currency (e.g. bitcoin). Digital cash systems such as bitcoin exploit computational techniques that have no direct analogue in the world of finance (prior to computers), as far as I can see. It involves computers in the network racing to solve a digital puzzle in order to validate a transaction and its rightful place in a chain of transactions (i.e. a cash item is only being spent once). A helpful blog post by Michael Nielson provides the clearest attempt Iâ??ve yet read to explain this process.

The whole digital money method is meant to run peer-to-peer, where computers are in direct communication with each other, without going through 3rd party servers. Duplicating the same ledger across large numbers of computers (with no central bank) creates storage issues for those PCs (or smartphones). Thatâ??s one of a number of interesting technical challenges addressed by the developers of unhackable digital money.

Bitcoin politics

Irrespective of the technical issues, and understanding how it all works, there are fascinating political, legal, social, privacy and ethical issues surrounding the aims of digital money. The idea of decentralised commerce sounds suitably liberal and democratic. But by some readings, it harbours an undercurrent of right-wing, anti-establishment self-reliance.

For David Golumbia, digital currencies â??emerge from the profoundly ideological and overtly conspiratorial anti-Central Bank rhetoric propagated by the extremist right in the U.S.â• (119). So digital money is arguably money for anti-establishment â??preppersâ• suspicious of the â??deep state,â• and other alt-right bogeymen. Also see post: Self-reliance and the accessorized self.

References

- Golumbia, D. (2015), â??Bitcoin as Politics: Distributed Right-Wing Extremismâ??, in G. Lovink, N. Tkacz and P. de Vries (eds), *Moneylab Reader: An Intervention in Digital Economy*: 117-31, Amsterdam: Institute of Network Cultures.
- Nakamoto, S. (2008), â??Bitcoin: A Peer-to-Peer Electronic Cash Systemâ??. *Bitcoin*. Available online: https://bitcoin.org/bitcoin.pdf (accessed 19 June 2017).
- Nielson, M. (2013), â??How the Bitcoin Protocol Actually Worksâ??. *Data-Driven Intelligence*, 6 December 2013. Available online: http://www.michaelnielsen.org/ddi/how-the-bitcoin-protocol-actually-works/ (accessed 16 June 2017).

Category

1. Economics

Tags

1. bitcoin
2. blockchain
3. ciphercity
4. money
5. politics

Date Created
June 19, 2017
Author

rcoyne99