

Key Issue

Of modems and pixie dust – blockchain demystified

We often hear from enthusiasts about the revolutionary potential of blockchain, the technology that underlies the Bitcoin virtual currency. But what can we really do with blockchain, and what possible perils and pitfalls exist? In this article I will look at a few potential blockchain use cases that are relevant to libraries and librarians, and clear up some blockchain myths and misconceptions.

Keywords

Blockchain; distributed ledger; reproducibility; provenance

Everything that is old is new again

Do you remember the 1990s? The early days of the web and the internet as a mass phenomenon? The screech of the 19.2K modem handshake, and the expectant wait as interlaced JPEGs slowly cantilevered into view? CRTs became LCDs, phone lines went wireless, the computer shrank until it fitted into our pockets, and here we are today. So much has changed, but we have largely managed to keep pace, and indeed it feels completely normal to have a pocket supercomputer that uses artificial intelligence to connect us to the world's information.

If you believe the hype, there is a similarly profound change happening right now around a family of technologies known colloquially as blockchain.¹ Blockchain is the 'distributed ledger' technology which forms the basis of the Bitcoin virtual currency,² and a whole host of people are looking into other applications for it. You might remember some folk back in the early days of the web breathlessly predicting that our lives would be forever transformed by the Internet, back when the only decent connectivity was at universities and research institutes and the vast majority of people had only ever typed 'www' by accident. Confusingly, Blockchain is also the trading name of the blockchain.com currency exchange, which lets you buy and sell virtual currencies like Bitcoin. Whilst Blockchain (the company) uses blockchain (the technology), the two are not synonymous and there are many other open source and proprietary distributed ledger implementations.

And as interest in all things internet snowballed, we saw countless cases of over-hyped companies; of teams struggling to deliver products using the technology of the day; and honest to goodness scams from hucksters and snake oil salesmen. Remember the dot-com boom and bust?³ We are at that point round about now with blockchain and so-called cryptocurrencies like Bitcoin. Following a period of irrational exuberance, a lot of investors and early adopters are starting to ask themselves, 'What is this stuff really good for?' In a recent House of Commons Treasury Committee inquiry,⁴ blockchain was described by one witness as a 'magic wand pixie dust' fad.⁵



MARTIN HAMILTON

Futurist
Jisc

'investors and early adopters are starting to ask themselves, "What is this stuff really good for?"'

Ranganathan shrugged

Librarians and information professionals might not feel that they have very much in common with the libertarians that crowd the blockchain message boards, and with good reason. It is difficult to imagine two more different groups – and like matter and anti-matter, bringing the two together is likely to cause fireworks. Taking their lead from author Ayn Rand's philosophy that unfettered self-interest is good and altruism is destructive, libertarian blockchain enthusiasts tend to view the technology in terms of the new freedoms that they believe it will create – first and foremost the freedom to trade without government interference, enabling and empowering the Randian 'sovereign individual'.⁶ By contrast, in the domain of libraries and scholarly communications we tend to place the highest value on activities that benefit society as a whole, such as Ranganathan's Laws of Library Science and his development of the Colon Classification.⁷

Beyond the hype, virtual currencies are nothing new, from supermarket loyalty points to frequent flier miles and complementary currencies like the Bristol Pound (which is intended to support local businesses) to the Fureai Kippu system in Japan,⁸ which issues credits in exchange for assistance to senior citizens. Cryptocurrency advocates would say that Bitcoin and its imitators are different in two highly significant ways: they operate at global scale, and they are truly decentralized, meaning that there is no one entity exercising overall control. Perhaps most crucially, there is no obvious way to link in to government tax collection mechanisms, and from the tax collector's perspective it can be extremely difficult to work out who the parties are to a transaction. Virtual currencies also hint at a world where it might become increasingly difficult for companies to build highly detailed profiles of customers.

Right now, at the end of 2018, there are nearly 2,000 cryptocurrencies⁹ – most aiming to compete with Bitcoin, with some focused on particular use cases like Fureai Kippu. Much key blockchain software is open source, meaning that anyone can use or modify it with few strings attached. This has led to a proliferation of Bitcoin clones and products derived from the popular Ethereum software. It might seem paradoxical to give away the keys to the kingdom, but this model underpins products used by billions, like Android phones and the Chrome browser.

'openness has led to waves of innovation around blockchain'

This openness has led to waves of innovation around blockchain, fuelled by millions of dollars of venture capital investment. Most notable was the introduction of smart contracts in the Ethereum blockchain system. Smart contracts are chunks of code that can be automatically triggered to carry out an activity when certain conditions are met. Examples include changing the owner of a property after funds have been transferred, or automating business processes like supply chain management.¹⁰

Honey, I blockchained the library

There are any number of reasons why libraries might want to experiment with blockchain technologies. I have picked out three here to illustrate some potential use cases and Brock¹¹ has a more exhaustive list of research areas where blockchain shows promise:

- ***Master bibliography of every publication by an academic***

At present this information is found in a wide variety of databases and online services, with no one single canonical source. Many academics invest considerable time in ensuring that public profiles such as Google Scholar and ResearchGate are up to date, but there are a large number of ways that a researcher and their work may be discovered, and most researchers do not have the time or inclination to join and maintain a profile, bibliography, etc. on each of the popular services. Institutional profile pages are sometimes constructed automatically from products like Symplectic Elements, but even then a certain amount of manual curation is required and this data does not follow the researcher should they move to another institution. In an ideal world, there would just be a single researcher profile listing and linking to all of their publications.

- **Record of when and where research outputs are cited**

For better or worse, we still set great store by the number of publications a researcher is responsible for, the journals they appear in and the extent to which their work is held in high esteem by the research community in their discipline. The increasing take-up of Digital Object Identifiers (DOIs) for research outputs is making it easier to find citations, but uptake is far from universal and it is somewhat labour intensive to trawl through databases of scholarly communications searching for the DOI of each of your papers. The perfect situation would be one in which the publications, data sets, software, etc. listed on an academic's researcher profile (as above) would automatically be updated as new citations were made. This would help to raise awareness of the impact of the work, and also help researchers to find potential collaborators or competitors.

- **A truly personal digital identity that you own and control, choosing which data about yourself you release, and who to release it to**

At the moment our notions of a professional digital identity are rooted in the institutional user ID, with associated systems and services such as research information systems publishing academic profiles and lists of publications. These are typically viewed in a highly transactional way and destroyed when researchers move from one institution to another, although formal research outputs may persist in institutional repositories. Many researchers seeking greater permanence have opted to use personal digital identities such as consumer-oriented Google and Microsoft accounts as their primary means of communicating with their peers, collaborating on projects and sharing results. These come with their own set of trade-offs, as services can be withdrawn or radically changed without contractual safeguards, e.g. Google Reader and Google Plus. In an ideal world, from the researcher's perspective, they would own and control this digital identity rather than be subject to the whims of institutions and cloud providers.

'the fact that it exists does not automatically mean that we should be looking to see where we can apply it'

It is worth noting that blockchain-based approaches may well augment or displace existing solutions. For example, ORCID has stated that it is interested in exploring the potential of blockchain.¹²

But we are at risk of confirmation bias here. Blockchain is a family of technologies, and the fact that it exists does not automatically mean that we should be looking to see where we can apply it. It is far more important to consider the fundamental, existential problems facing libraries and information professionals before looking at whether any specific technology can help address them.

Attack of the 50-foot blockchain

Blockchain enthusiasts will tell you that in the future everything will be on the blockchain, but there isn't 'a' blockchain. Instead, there is a Wild West of competing products and services, often from early stage startups. Some of these are true to the Bitcoin open and decentralized ethos, but the vast majority involve some form of enclosure, with your data only accessible through a vendor's app. What happens to your data if the vendor ceases to trade, gets taken over, or has trouble paying their hosting bills? Your data may be distributed across thousands of computers around the internet, but if the only way of getting to it is through that app, then you may never see it again.

Another popular misconception is that you can put just about anything 'on the blockchain'. After all, is it not a storage system a bit like Dropbox or Google Drive? The reality can be quite complex and fraught, because many blockchain implementations are not really designed to be used this way. Storing a large object such as a MPEG movie or a PDF of a PhD thesis on a blockchain tends to require it to be chopped up into lots of small chunks, with each one stored individually as a block of data. The blockchain itself consists of these blocks of data plus references to the related data. Some blockchain implementations have quite small block sizes, e.g. the original Bitcoin blockchain uses 1MB blocks. This

4 approach can also be very expensive because you have to pay for each Bitcoin transaction, and transaction fees are both variable and difficult to predict. Fees peaked at US\$55 in December 2017 but have plummeted at the time of writing due to the collapse of the cryptocurrency market.¹³ Some blockchain implementations do not have these limitations, but this diversity quickly gets technically complex and it can be difficult to know which are the right questions to ask when evaluating a potential blockchain solution.

You could keep the object somewhere else, and use the blockchain for record keeping – using it as a distributed ledger rather than a database per se. It is easy to glibly say ‘somewhere else’, but in reality it is important that you get to the bottom of how your data will be kept safe and secure. It could be anything from a hyperscale cloud provider’s data centre, to being split up into chunks and ‘sharded’ across thousands of people’s PCs using a technology like the interplanetary file system (IPFS).¹⁴

Sharding raises its head again in another way: as transactions are added to a blockchain, the amount of RAM, CPU and storage needed to hold a copy of the blockchain database on a computer will increase. The core Bitcoin blockchain had reached 183GB in size by September 2018,¹⁵ making it infeasible to run a Bitcoin server process or ‘node’ for many people due to resource constraints on consumer-grade laptops and PCs. Blockchain researchers are working on a variety of sharding solutions involving lesser or subsidiary nodes that do not have to hold the entire blockchain database, but these have yet to be widely deployed. Each blockchain node has to update its ledger before a transaction is confirmed, and this can take several hours.

Many blockchain implementations are still inherently cryptocurrencies, and consequently hobbled by variations of the bitcoin ‘mining’ process. If you wondered where Bitcoins come from, the answer is that your computer essentially comes up with a random number, and calculates its digital fingerprint (or hash) over and over again until the fingerprint matches one generated by the Bitcoin network. It is estimated that the Bitcoin network now uses as much electricity as Ireland,¹⁶ but there are other blockchain implementations that are not so resource intensive.

‘It is estimated that the Bitcoin network now uses as much electricity as Ireland’

What’s a librarian to do?

Blockchain and other distributed ledger technologies are interesting and hold potential for solving wicked problems that the sector struggles with, such as provenance of research results, tracking citations and reproducibility of research results. However, as you have seen, there are many traps for the unwary, such as transaction costs, block size limitations, issues around resource consumption and the enclosure of blockchain within wholly proprietary systems. The most important thing is to go into any blockchain engagement with your eyes wide open, and be prepared to disengage rapidly. For example, if your institution was looking at issuing qualifications online using a blockchain-based approach, it would be important to have a Plan B (such as issuing paper certificates or PDFs).

‘distributed ledger technologies ... hold potential for solving wicked problems that the sector struggles with’

At Jisc we have been collaborating with the Open University’s Knowledge Media Institute on its Open Blockchain initiative.¹⁷ We are very interested in talking to librarians and information scientists about R&D around potential applications of blockchain and distributed ledgers, and would love to hear from you.

Abbreviations and Acronyms

A list of the abbreviations and acronyms used in this and other *Insights* articles can be accessed here – click on the URL below and then select the ‘full list of industry A&As’ link: <http://www.uksg.org/publications#aa>

Competing interests

The author has declared no competing interests.

References

1. Wikipedia entry for blockchain:
<https://en.m.wikipedia.org/wiki/Blockchain> (accessed 20 November 2018).
2. Wikipedia entry for Bitcoin:
<https://en.m.wikipedia.org/wiki/Bitcoin> (accessed 20 November 2018).
3. Howcroft D, Richardson H and Wilson M, 'Now you see it... Now you don't' – Myths of the Dot.com Market. In *Proceedings of the 9th European Conference on Information Systems*, 2001:
<http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.481.5756&rep=rep1&type=pdf> (accessed 20 November 2018).
4. UK Parliament, *Crypto-assets* – report of House of Commons Treasury Committee enquiry, September 2018:
<https://publications.parliament.uk/pa/cm201719/cmselect/cmtreasy/910/910.pdf> (accessed 20 November 2018).
5. Kelly J, Blockchain insiders tell us why we don't need the blockchain, *Financial Times*, 2 May 2018:
<https://ftalphaville.ft.com/2018/05/02/1525253799000/Blockchain-insiders-tell-us-why-we-don-t-need-blockchain/> (accessed 21 September 2018).
6. Hunt L H, Thus Spake Howard Roark: Nietzschean Ideas in The Fountainhead, *Philosophy and Literature*, 2006, 30(1), 79–101; DOI:
<https://doi.org/10.1353/phl.2006.0012> (accessed 20 November 2018).
7. Naun C C, Ranganathan's importance, *The Australian Library Journal*, 1994, 43(4), 219–225; DOI:
<https://doi.org/10.1080/00049670.1994.10755691> (accessed 30 November 2018).
8. Seyfang G and Longhurst N, Growing green money? Mapping community currencies for sustainable development. *Ecological Economics*, February 2013, 86, 65–77; DOI:
<https://doi.org/10.1016/j.ecolecon.2012.11.003> (accessed 20 November 2018). Open access pre-print available from:
<https://core.ac.uk/download/pdf/9838084.pdf> (accessed 30 November 2018).
9. Coinmarketcap – List of active cryptocurrencies 2018:
<https://coinmarketcap.com/all/views/all/> (accessed 20 November 2018).
10. Gutierrez J R, What are smart contracts and how do they work? (Examples & Challenges), *Cryptovest*, 2018:
<https://cryptovest.com/education/what-are-smart-contracts-and-how-do-they-work-examples--challenges/> (accessed 30 November 2018).
11. Brock J, Mapping the blockchain for science landscape, *Hacker Noon*, Medium, 2018:
<https://hackernoon.com/mapping-the-blockchain-for-science-landscape-546b61bfbd1> (accessed 20 November 2018).
12. Peters R, 7 March 2018, Why We Need to Explore Blockchain Technology to Connect Researchers and Research, Robert Peters's Blog:
<https://orcid.org/blog/2018/03/07/why-we-need-explore-blockchain-technology-connect-researchers-and-research> (accessed 30 November 2018).
13. Peterson B, The cost of bitcoin payments is skyrocketing because the network is totally overloaded, *Business Insider*, 2017:
<http://uk.businessinsider.com/bitcoin-payment-mining-fees-hit-new-high-2017-12> (accessed 20 November 2018).
14. Coral Health (2018) Learn to securely share files on the blockchain with IPFS! (Technical walkthrough and discussion), Medium:
<https://medium.com/@mycoralhealth/learn-to-securely-share-files-on-the-blockchain-with-ipfs-219ee47df54c> (accessed 20 November 2018).
15. Blockchain.com – Blockchain Size live chart:
<https://www.blockchain.com/en/charts/blocks-size> (accessed 30 November 2018).
16. Leonard J, Bitcoin now uses as much energy as Ireland and could match Austria by end of 2018, *Computing*, 2018:
<https://www.computing.co.uk/ctg/news/3032588/bitcoin-now-uses-as-much-energy-as-ireland-and-could-equal-austria-by-end-of-2018> (accessed 30 November 2018).
17. Open University – Open Blockchain initiative, 2018:
<https://blockchain.open.ac.uk/> (accessed 20 November 2018).

Article copyright: © 2019 Martin Hamilton. This is an open access article distributed under the terms of the [Creative Commons Attribution Licence](#), which permits unrestricted use and distribution provided the original author and source are credited.

Martin Hamilton
Futurist
Jisc, GB
E-mail: martin.hamilton@jisc.ac.uk



ORCID ID: <http://orcid.org/0000-0002-7269-3737>

To cite this article:

Hamilton M, Of modems and pixie dust – blockchain demystified, *Insights*, 2019, 32: 2, 1–5; DOI: <https://doi.org/10.1629/uksg.447>

Submitted on 25 September 2018 Accepted on 19 November 2018 Published on 09 January 2019

Published by UKSG in association with Ubiquity Press.