Can blockchain withstand skepticism? An inquiry

Kent Anderson*
CEO, RedLink

1. Introduction

Blockchain has captured the interest of the scholarly communication community, and most of us are grappling with questions: What is it? What does it offer? What are the pros and cons? There is a lot of hype (pros), but the cons (skepticism) are not given equal time. So, with permission from Kent Anderson, we are reprinting his thought-provoking blog that was published earlier this year in *The Scholarly Kitchen* [1].

2. Blockchain

The hype over blockchain - a new technology that has generated what one observer has called a "mind virus" [2] - has infected scholarly communications, with companies claiming to bring blockchain to scientific research [3], conferences about the technology and its potential implications [4], and even an interview earlier this week on this blog echoing claims about its "revolutionary" nature and potential to reduce expenses and save us work [5]. It's interesting to see how some new technologies make everyone do backflips while others that can offer even greater utility and long-term value do not. Case in point – USB drives. Introduced in 2000, these were never that sexy, but have proven to be consistently useful, and continue to serve their main purpose to this day.

For whatever reason, blockchain has sex appeal in spades, with Bitcoin, Silicon Valley bros, disruptors, and technologists all aligned around its cool capabilities. There is also a certain libertarian appeal to blockchain, as its relative anonymity (better described as pseudonymity) is cited by some as having the potential to take the Internet back to its anarchic and individualistic days. I'm also told that blockchain has solved one of the biggest problems in computer science, the Byzantine Generals' Problem, representing a significant technical breakthrough [6]. That probably earned it some fans.

---

*E-mail: kanderson@redlink.com.

Others are nonplussed. As Paul Ford wrote in *BusinessWeek* [2]:

Most things that the blockchain promises to do can be done more easily with other technologies … the blockchain freaks have a world in their heads, and they won't rest until it's real.

Blockchain has huge potential to decentralize data. Internet visionaries have long been talking about decentralized data, data intermediaries, and data ownership [7]. Yet, there are those who dare to question the paradigm of decentralized data as an infallible good [8], noting:

- Several technical disadvantages inherent to any decentralized system, such as computational limitations (it's hard to add up data you don't have), susceptibility to network unreliability, slower speeds due to reliance on network speeds, and duplicative data that may or may not be synchronized.
- The lack of economies of scale to defray the costs of decentralized systems (yes, decentralization may be more expensive).
- The cognitive burden of people managing their own data, and how unlikely it is for this to work reliably for long periods of time at scale.
- The tendency for even decentralized systems to assume characteristics of centralized systems because people start using the same pathways.

To this last point, in the recent interview here about blockchain [9], this tendency to common pathways, which is akin to centralization in practical terms, can be seen when Martijn Roelandse stated:

The envisioned end-game for this initiative is a platform … maintained by an Amsterdam-based startup.

This perspective was later confirmed in a separate comment [10] by the other participant in the interview, Joris van Rossum. Researchers have also found that cryptocurrencies are less decentralized than advertised [11] owing to a number of the factors mentioned above. Perhaps it's better to accept that some degree of centralization will often make sense, economically, functionally, or socially.

Blockchain technology is a framework that comes with a ledger that can be modified to fit a particular use-case. Modifications incorporate a set of rules for the encapsulation of data and associated data permissions. There are hundreds of ledgers geared towards different use cases. By itself, blockchain does nothing.

For example, with Bitcoin, the most well-known blockchain use-case, the particular implementation allows anyone to participate as a "miner" of coins simply by joining the blockchain and contributing their computing power. Bitcoin works as long as more than half of the participating database maintainers are "good guys" – that is, can be trusted to keep miscreants in check, and will do the right thing to maintain data integrity.

Blockchain is used for other cryptocurrencies (which may be mislabeled themselves – more below), as individuals can make a bid on a segment of the currency pseudonymously, withdraw shares of the currency under their blockchain address pseudonym, and serve as a miner for the currency using only this pseudonym. Everyone trusts the value of the cryptocurrency because blockchain ensures that every transaction is captured, even if the participants aren't known to one another.

This approach is already running into regulatory headwinds as the EU rolls out the General Data Protection Regulation (GDPR). Regulators have to take blockchain both seriously and literally as a

technology. Michèle Finck, a lecturer in EU law at the University of Oxford, is quoted in *BusinessWeek* in an article entitled, "Is Your Blockchain Business Doomed?" [12] stating:

Blockchains, as currently designed, are incompatible with the GDPR.

A lot of things clearly need to be sorted out with blockchain and GDPR. What is "personal information" – a person's public blockchain address? In general, encrypted data is viewed as personal data, making much of blockchain susceptible to GDPR regulation. This may lead to redundant systems, as companies have to build traditional databases to manage any personally identifiable information off a blockchain, which could remove some of the purported benefits of blockchain. Also, blockchain address pseudonyms are only as secure as any system resolving them to real identities, which web trackers, cookies, and beacons can unmask rather simply [13].

Does a ledger system without administrative roles and possessing pseudonymous features seem appropriate for scholarly communications? What do we not want to attribute openly? In the interview about blockchain on the *Kitchen* earlier, you can see the interviewees trying to reconcile the two concepts – pseudonyms and attribution – as they talk about peer review, data sharing, reviewer recognition, and citations. This is a possible side-effect of presuming blockchain as the technical solution. Take, for example, this passage [14]:

… blockchain as a datastore with no central owner where information can be stored pseudonymously could support the creation of a shared … authoritative database of scientific events. Here traditional activities such as publications and citations could be stored, along with currently opaque and unrecognized activities, such as peer review. A data store incorporating all scientific events would make science more transparent and reproducible, and allow for more comprehensive and reliable metrics.

There is a side salad of words here, so let's try to discern more precisely what the speaker is saying by addressing the three nouns – "citations", "publications", and "metrics". Immediately, we can see some issues with pseudonymously stored data. How can you count pseudonymous citations or publications? Who would trust or even publish a pseudonymous publication, with the author's identity hidden even from the editors and publishers? Why do these even need to be stored in this manner?

It's entirely possible that there are simpler ways to address security and identity, such as two-step authentication, which appears robust enough to prevent anyone from hacking the Twitter account of the President of the United States (a fact that still boggles my mind – there must be a large number of hackers attempting to penetrate this single account, day in and day out).

This conflation of concepts occurs quite often if you read carefully. For instance, ARTiFACTS (see: https://artifacts.ai/), which boasts that it is "leveraging blockchain technology", also states that researchers can "[r]eceive attribution for all [their] relevant work (and provide the same to others)". Now, this all can be true if ARTiFACTS is leveraging portions of blockchain and creating a variant of the type of ledger system that makes blockchain distinctive. But what benefit, beyond sizzle, is there in using blockchain when the outcome is full attribution?

Others also blur the lines here, with Digital Science and Katalysis noting in a recent press release [15] that they will be exploring "practical solutions that leverage the distributed registry and smart contract elements of blockchain technologies" as they pertain to peer review systems. Ideas like this embed the requirement for accurate attribution, which is something blockchain seems to make more complicated. Some aspects of blockchain – ledgers, hashes,and secure transactions – might have be relevant, but

those aren't as sexy. They're the USB drives of computing, boring and reliable. They can exist without blockchain.

Attribution is one of the most important aspects of research and scholarship. Researchers and authors want their works and contributions attributed to them to bolster their names, to get more grant funding, and to advance their careers. Researchers need their works attributed to them to avoid problems with ethics committees, academic perceptions, and co-authors.

But not all attributions are public, yet they need to be visible to the right people at the right time. For example, the names of peer-reviewers, statistical reviewers, and technical reviewers need to be known, at least to the editors and certain staff. Blockchain's relevance to any of these roles is questionable. I can't see a journal running a pseudonym-filled, blockchain-enabled peer-reviewer network, because at some point – either privately or publicly – someone has to know who reviewed what. Some entity – an editor, a publisher – is responsible, and must be able to see down the chain.

So, what about cryptocurrencies? In an especially excited portion of the *Kitchen* interview I mentioned earlier, Joris van Rossum speculates that "a cryptocurrency for science could be developed" [16]. But, again, what are we talking about? What is a cryptocurrency, exactly?

It's an interesting question that is reaching the highest level of regulators in multiple nations and confederations, because what are being called "cryptocurrencies" may not be currencies at all. They may be more properly described as securities, as outlined in a recent *BusinessWeek* article entitled, "The Ancient History of Bitcoin" [17].

The authors of this article note that courts have found that what matters is the substance of a transaction, not its form. That is, whether people are transacting land, time, or tokens, the form of the transaction may be represented as a currency or a real estate transaction or something else, but if the substance is about having shares in the hopes that those shares increase in value, then the transaction is a security, like a stock or bond. For example, if you are selling shares in a plot of land on the premise that what grows on that land will yield profits you will distribute, you are selling a security, not real estate. Currencies are another matter entirely, and come in three broad flavors:

- *Fiat currency* has no intrinsic value, but rather value established by a backer, typically a government.
- *Commodity currency* is valuable because the commodity it's made of – gold, silver – has intrinsic value.
- *Representative currency* represents a share of value of a stockpile, so a gold note when the gold standard was in effect represented $10 of actual gold in a vault somewhere.

Bitcoin and its ilk are closest to a representative currency, but they fall short because what Bitcoin value represents isn't itself intrinsically valuable. Instead, what cryptocurrency owners seem to be purchasing are shares of a venture (coin mining and competition for the result) that the owners are betting will succeed – that is, people who buy Bitcoins and other cryptocurrencies are participating in a securities activities, holding equity in hopes that it increases in value before they sell it for actual fiat currency. In other words, buyers are essentially acquiring a piece of the Bitcoin business. Therefore, a cryptocurrency for science would have to have the characteristics of a security, shares of something that could be converted into currency by selling off said shares at a particular price at a particular time. And, as we've seen, these securities tend to be volatile.

If cryptocurrencies are defined as securities, then the path to regulation may be clearer. Jay Clayton, the US Securities and Exchange Commission (SEC) Chairman stated late last year, citing a Supreme Court case [18]:

Simply calling something a "currency" or a currency-based product does not mean that it is not a security.

So, there may not actually be a cryptocurrency yet, but rather cryptosecurities. By the way, 95%+ of regular fiat currencies are electronic already, so there's nothing fancy about e-money, and there hasn't been for decades.

Is blockchain relevant to scholarly communication? Possibly, but it's important to realize that it's far from plug-and-play, that legal issues aren't settled, and that depending on the use-case, it may not be the best technical solution if you're trying to balance ease-of-implementation, costs, security, compliance, and many other factors.

To borrow a phrase used earlier, the substance of an activity matters more than the form it takes.

Or, to quote Douglas Adams, "We are stuck with technology when what we really want is just stuff that works" [19].

About the Author

Kent R. Anderson is the CEO of RedLink. He is a past-President of the Society for Scholarly Publishing, the founder of "The Scholarly Kitchen", and has been Publisher for Science, the Journal of Bone & Joint Surgery, and Publishing Director for the New England Journal of Medicine. Anderson spoke at the NFAIS "Blockchain for Scholarly Publishing" conference, and some of this post made its way into his talk. Contact information: Email: kanderson@redlink.com; Twitter: @kanderson.

References

[1] Kent Anderson, Can blockchain withstand skepticism? An inquiry, *The Scholarly Kitchen* (2018), see: https://scholarlykitchen.sspnet.org/2018/04/05/can-blockchain-withstand-skepticism-an-inquiry/, reprinted with permission.

[2] P. Ford, Bitcoin is ridiculous; blockchain is dangerous, *Bloomberg Businessweek* (2018), see: https://www.bloomberg.com/news/features/2018-03-09/bitcoin-is-ridiculous-blockchain-is-dangerous-paul-ford, accessed September 23, 2018.

[3] See ARTiFACTS, at https://artifacts.ai/, accessed September 23, 2018.

[4] See Blockchain for Scholarly Publishing, an NFAIS conference held May 16–16, 2018 in Alexandria, VA, USA, program is available at: http://www.nfais.org/index.php?option=com_mc&view=mc&mcid=72&eventId=544203, accessed September 23, 2018. Kent Anderson was a presenter at this conference.

[5] A. Meadows, Everything you always wanted to know about blockchain (but were afraid to ask), *The Scholarly Kitchen* (2018), see: https://scholarlykitchen.sspnet.org/2018/04/03/everything-always-wanted-know-blockchain-afraid-ask/, accessed September 23, 2018.

[6] "The Byzantine Generals' Problem, https://en.wikipedia.org/wiki/Byzantine_fault_tolerance#Byzantine_Generals'_Problem, accessed September 23, 2018.

[7] J. Glave, The dawn of the infomediary, *Wired* (1999), see: https://www.wired.com/1999/02/the-dawn-of-the-infomediary/, accessed September 24, 2018.

[8] A. Narayanan, S. Barocas, V. Toubiana, H. Nissenbaum and D. Boneh, A critical look at decentralized personal data architectures, (2012), see: http://randomwalker.info/publications/critical-look-at-decentralization-v1.pdf, accessed September 23, 2018.

[9] A. Meadows, Everything you always wanted to know about blockchain (but were afraid to ask), *The Scholarly Kitchen* (2018), see: https://scholarlykitchen.sspnet.org/2018/04/03/everything-always-wanted-know-blockchain-afraid-ask/, accessed September 23, 2018.

[10] A. Meadows, Everything you always wanted to know about blockchain (but were afraid to ask), *The Scholarly Kitchen* (2018), see: https://scholarlykitchen.sspnet.org/2018/04/03/everything-always-wanted-know-blockchain-afraid-ask/#comment-74467, accessed September 23, 2018.

[11] G.E. Kelso, Cornell researchers: Bitcoin not as decentralized as assumed, *Bitcoin.com* (2018), see: https://news.bitcoin.com/cornell-researchers-bitcoin-not-as-decentralized-as-assumed/, accessed September 23, 2018.

[12] O. Kharif, Is your blockchain business doomed? (Europe's new data protection regulation could spell trouble for companies), *Bloomberg Businessweek* (2018), see: https://www.bloomberg.com/news/articles/2018-03-22/is-your-blockchain-business-doomed, accessed September 23, 2018.

[13] "Bitcoin Transactions Aren't as Anonymous as Everyone Hoped," by Emerging Technology from the arXiv, August 23, 2017, see: https://www.technologyreview.com/s/608716/bitcoin-transactions-arent-as-anonymous-as-everyone-hoped/, accessed September 23, 2018.

[14] A. Meadows, Everything you always wanted to know about blockchain (but were afraid to ask), *The Scholarly Kitchen* (2018), see: https://scholarlykitchen.sspnet.org/2018/04/03/everything-always-wanted-know-blockchain-afraid-ask/, accessed September 23, 2018.

[15] See: https://www.digital-science.com/press-releases/digital-science-and-katalysis-lead-initiative-to-explore-blockchain-technologies-for-peer-review/, accessed September 23, 2018.

[16] A. Meadows, Everything you always wanted to know about blockchain (but were afraid to ask), *The Scholarly Kitchen* (2018), see: https://scholarlykitchen.sspnet.org/2018/04/03/everything-always-wanted-know-blockchain-afraid-ask/, accessed September 23, 2018.

[17] P. Coy, M. Leising and O. Kharif, The ancient history of bitcoin, *Bloomberg Businessweek* (2018), See: https://www.bloomberg.com/news/articles/2018-03-29/the-ancient-history-of-bitcoin, accessed September 23, 2018.

[18] P. Coy, M. Leising and O. Kharif, et al., The ancient history of bitcoin, *Bloomberg Businessweek* (2018), see: https://www.bloomberg.com/news/articles/2018-03-29/the-ancient-history-of-bitcoin, accessed September 23, 2018.

[19] D. Adams, *The Salmon of Doubt: Hitchhiking the Galaxy One Last Time*. Ballantine Books, New York, 2003.