Universities cannot afford to buy in to blockchain mania (opinion)

Submitted by Jonathan A. Poritz on September 12, 2018 - 3:00am

One week ago, Inside Higher Ed and "Inside Digital Learning" published the essay "What Every College Leader Should Know About Blockchain," by Daniel Pianko, managing director of the investment firm University Ventures.

One of the first commenters on the article, DavidT, complained, "I still don't know what blockchain is."

Let's calm DavidT's demons by describing some of the key features of this much-admired technology. Unfortunately, with understanding comes sadness: there is really is no there there. In higher ed, for example, it doesn't really make any sense to use blockchains to store credentials, as Pianko mentions the University of Nicosia is doing. Similarly with most (all?) other proposed blockchain applications.

There are indeed many job openings for employees with blockchain skills, as Pianko pointed out. But it would be a mistake to conclude that we in higher education should build programs to satisfy the need for these workers. If investment firms in the Netherlands in the early 1630s had put pressure on the University of Leiden (founded about 50 years before) to produce more skilled tulip agronomists, it would have been a great mistake to accede to that pressure. Yes, there was a lot of financial churn going on in tulip markets, but it would have been foolish for an institution with long-term intentions to get caught in that mess.

So what is a blockchain, really?

Suppose a group of parties on the internet wishes to build up over time a sequence of blocks of data, satisfying some nice properties:

- immutability: once a block is accepted by the participants, it cannot be changed -- history does not change;
- consensus: all honest participants should agree as to what are the valid blocks.

One use of such a structure would be as a shared ledger of transactions of data, possibly of various kinds, between the parties. Immutability would prevent a misbehaving party from altering a past transaction that they now regret having performed. Meanwhile, consensus keeps all parties synchronized as to what is the current state of all of the exchanged data.

With a specialized consensus algorithm, the ledger could contain records about all valid transactions with quantities of some new token, where "valid" means that tokens move only when the particular individuals who own them authorize those movements -- this is a cryptocurrency, like Bitcoin, Etherium or Dogecoin.

Transactions here can be associated with particular individuals, or tokens "owned" and their authorized movements validated, by use of a beautiful bit of modern cryptography called a digital signature. In order to make such signatures, each party needs first to generate a pair of keys (like passwords): a public key that they show to everyone and a private key whose secrecy they must jealously guard. A digital signature on an electronic document is then a bit of additional data attached to the document, which can only be produced by the owner of a particular private key, but in a way that can be verified by anyone else working with the corresponding public key.

This mechanism is the means by which participants have some identity -- as the owner of a particular key pair -- in such shared ledgers. Sometimes it is considered advantageous that it is hard to associate a particular public key owner with a particular person or entity in the real world (this is the only extent to which Bitcoin is anonymous, in fact), while in other cases it would be good to have a robust way of making such a relationship, which would then be known as a public key infrastructure, or PKI.

It is actually quite easy to build a structure as just described, so long as all participants trust one central authority -- called a trusted third party, or TTP. In that case, the parties could submit transactions to the TTP, which would make sure they were consistent with past behavior and publish a block, signed with its universally trusted public key. This is what a central bank does, in essence, by controlling the money supply and supervising their national banking system.

Computer scientists wary of central control instead designed various ways to achieve immutability and consensus without any trusted third party; only then do we call the resulting shared public ledger a blockchain.

For example, the Bitcoin blockchain rewards participants for doing a very large amount of entirely meaningless work in order to produce valid blocks of transactions that everyone on the network will recognize -- this strategy is called proof of work. It enables the consensus algorithm to avoid conflicts even without a TTP, but at the cost of providing an incentive for the global Bitcoin network to consume about as much electricity as the nation of Austria at the time of this writing.

Implications for Higher Ed

So what is going on in Nicosia? For the credentials from the University of Nicosia, which are apparently on some blockchain, to carry any weight with the public, the university's public key would have to be recognized and trusted as
being associated with that real-world entity: there would have to be at least that much of a PKI in place. Why then
doesn't the university simply sign digital copies of its diplomas, or of the finer-grained credentials Pianko mentions, and
give them to graduates?

The graduates could email these signed electronic documents to potential employers, for example, who would be able
to verify them using that bit of PKI.

Similar problems occur in proposed applications of blockchains across many domains, where a trustworthy PKI is hard
to build, and if one did exist, it would enable far simpler solutions than a blockchain.

Notice also that in Nicosia it was not at all necessary that the public ledger of credentials be produced without a TTP.
They themselves, or the Cypriot Ministry of Education, are the authorities whom the public should trust regarding their
credentials.

In the U.S., a university's accrediting agency, or the state or federal Department of Education, would be an appropriate
TTP.

Those who proselytize for blockchain applications want to imply that consensus without a TTP is always better -- "single
point of failure" is the phrase often used to describe the problem with depending on specific authorities in the current
arrangement. But in many circumstances it is in fact entirely appropriate to want an adult in the room.

For example, suppose the dream of cryptocurrency enthusiasts had been realized before 2007, and we had all been
using Bitcoin rather than the good old fiat dollar. In that case, the U.S. Federal Reserve would not have been able to use
so-called quantitative easing and we might well have had a second Great Depression rather than first Great Recession.
I'm not a fan of monetary policies that advantage hedge fund managers, but neither do I like the prospect of
Hoovervilles springing up again.

Most of the blockchain-trained graduates Pianko wants us to produce would work in the area now called "Fintech." But
it is important to realize that the enthusiasm of the financial services industries for blockchains and cryptocurrencies is
not a techno-utopian vision: it is a neoliberal utopia where the government is excluded from power over the financial
system by the very code on which its technology runs. Do we want to offer up our graduates and our faculty's
scholarship to serve that purpose?

I used to be optimistic about the eventual outcome of the blockchain bubble. I thought it would soon pop, leaving us all
a little poorer (except for a few of the more charismatic charlatans, who would be much richer), but we would at least
all be forced to understand public key cryptography and the value of a good PKI.

As time goes on, though, I am getting more pessimistic: I fear putting more of our economy -- and even our educational
systems -- "on the blockchain" hardwires an extremist neoliberal worldview into the very code of our society. And, of
course, code is law.
Universities cannot afford to buy in to blockchain mania

---

Jonathan A. Poritz is an associate professor in the department of mathematics and physics and interim director and data analyst at the Center for Teaching and Learning at Colorado State University-Pueblo.

---


Links:
[2] https://digiconomist.net/bitcoinenergy-consumption
[5] https://www.poritz.net/jonathan/