Blockchain: Hype or Hope for Government Agencies?

Federal IT leaders debate the utility of blockchain.

[Kevin McCaney](#)

Wed, 10/31/2018 - 00:00

Iaremenko/iStock

The blockchain debate is getting a little heated.

In one corner you have people like NYU economist Nouriel Roubini, who in written testimony told a Senate hearing this month that, "Blockchain is the most over-hyped technology ever," calling it the "[the mother of all scams](#) and (now busted) bubbles."

In the other, you have people like Health and Human Services Department Acquisition Chief Jose Arrieta, who a day later told a government tech symposium

that Federal IT officials who aren't on board the blockchain train "are very close to being irrelevant."

So which is it?

Federal and other government agencies are exploring the prospects of using blockchain for financial transactions, supply-chain tracking and other uses. It's even been proposed as a way to ensure secure voting in elections and protect the electrical grid. But the debate over its validity continues.

Roubini, a heavyweight in economics circles who was among the few who predicted the 2008 economic crisis (and was dubbed "Dr. Doom" after making the prediction in 2006), isn't alone among critics of the technology, some of whom say that its promise won't hold up in practice.

But blockchain has plenty of proponents, too. Wal-Mart is working with IBM on using a blockchain system to secure the supply chain for fresh produce against illnesses such as E. coli. The financial sector is using the technology for a variety of functions, from identity management and smart contracts to securing cross-border payments. The CEOs of several major banks have said they expect global banking to ride on blockchain in about five years.

Arietta also has fellow believers in government and the military. A member of the Naval Innovation Advisory Council wrote last year that blockchain could "revolutionize Naval Additive Manufacturing, finance and logistics, and that's only scratching the surface."

Blockchain Basics

Blockchain is a digital ledger system best known for undergirding the volatile world of cryptocurrencies like Bitcoin, but the technology's transparency and security has drawn interest from a lot of other areas, including government.

In a blockchain, every party involved has access to each transaction—recorded in blocks, or data sets, that are generally, but not exclusively, about 1 MB in size. Each party maintains its own database, identical to the other parties,' and is able to see and verify it directly, without third-party involvement. With each transaction, all copies are updated simultaneously and permanently, and every transaction is visible to everyone else associated with that blockchain, as Marco Iansiti and Karim

R. Lakhani explain in a detailed rundown of blockchain in the [Harvard Business Review.](#) Transactions entered into the database can't be changed, because each block in the chain is linked to every other block. (You can see where the name comes from). It also can be programmed to trigger transactions automatically.

Blockchain has incurred a bit of guilt by association because of some high-profile [hacks of Bitcoin](#) and [other cryptocurrencies](#), but Iansiti and Lakhani point out that the weaknesses in those hacks were with the cryptocurrency users rather than any vulnerabilities in blockchain. But there are other [criticisms of blockchain](#): it's complicated and difficult to use, and therefore unlikely to see widespread adoption, and it could to increase transaction costs (though others project it will reduce them). Some have pointed out that there's really [no clear definition of blockchain](#), with exceptions to just about every rule, making it hard to implement widely.

Cautiously Opportunistic

Concerns about the technology's viability aside, government agencies are at least dipping their toes in the water. HHS is [exploring using blockchain](#) in several areas, including sharing medical images, tracking records, and [acquisition](#). The Department of Homeland Security is [testing blockchain](#) for keeping counterfeit goods out of the supply chain. The Department of State is working with Coca-Cola on a pilot to create a blockchain worker registry to [combat forced labor](#) around the globe. The Department of Treasury has started a [proof-of-concept pilot](#) for managing its IT assets.

Bloomberg Government reported earlier this year that Federal agencies had awarded about [$8.4 million in blockchain contracts](#). A recent report by market analyst IDC highlighted eight [examples of blockchain use](#) in government and points to areas most likely to see use: among them smart contracts, asset management and land registry in the short term, and possibly electronic voting and refugee identification in the long term.

And while not buying into the technology wholesale, agencies are taking a hard look. In the 2018 National Defense Authorization Act, Congress ordered the Department of Defense to conduct a [comprehensive study](#) of blockchain. The National Institute of Standards and Technology this month released NIST [Internal Report 8202](#), an overview of blockchain that it says will lay the groundwork for a series of more comprehensive examinations of the technology.

Despite some occasionally flammable rhetoric on both sides, agencies need to keep in mind that blockchain is a developing technology. Iansiti and R. Lakhani compare it to TCP/IP in the early days of the Internet—open, distributed and shared, but still in need of development. They note that blockchain isn't so much a disruptive technology as a foundational one, and suggest that it will likely take decades before it can become an integral part of the economic and social infrastructure, if it does at all.

"The process of adoption will be gradual and steady, not sudden, as waves of technological and institutional change gain momentum," they write.

[View printer friendly version](#)
[blockchain](#)
[cybersecurity](#)
[IT modernization](#)