Blockchain offers applications well beyond Bitcoin but faces its own limitations

Stephen Ornes, *Science Writer*

In 2008, Satoshi Nakamoto introduced the world to Bitcoin, a volatile digital currency that's untethered to any specific institution or country (1). (Satoshi Nakamoto was quickly revealed to be a pseudonym; the true identity of the inventor or inventors remains unknown.) In the years that followed, the value of Bitcoin has soared, plummeted, and soared again while giving rise to a raft of new cryptocurrencies of varying stability and legitimacy. Bitcoin and the others have their boosters and their detractors (see Opinion: Valuation, liquidity price, and stability of cryptocurrencies, https://www.pnas.org/content/115/6/1131).

But Bitcoin wasn't just revolutionary as a virtual currency innovation. It also introduced a novel way for investors and others to obtain, monitor, and trade that currency. Users record and secure financial transactions along with a timestamp using blockchain, a ledger system designed by Nakamoto that's unlike any traditional accounting system used before. A blockchain isn't stored on a central computer or controlled by a single boss; instead, it's distributed, which means every user on a blockchain network has a copy of the entire ledger. Information is also protected by a consensus algorithm—a computer program that enables the network to validate transactions.

Blockchain will forever be linked to cryptocurrencies, but researchers have begun to explore untapped applications for blockchain's secure ledger approach. Image credit: Shutterstock/laremenko Sergii.

Blockchain will forever be linked to cryptocurrencies, but many researchers have begun to explore untapped applications for blockchain's secure ledger approach. Its built-in mechanisms of trust and attribution make it appealing as a way to organize networks where people want to share information—a potentially big asset for tracking information in all sorts of science-related systems. Applications include forging new ways of managing distributed electrical grids, tracking regulated food and drugs, monitoring devices in the ever-growing "Internet of Things" (IoT), and perhaps even quickly and accurately documenting how new scientific findings emerge.

But blockchain itself is also susceptible to hype. Some proposed applications may not make sense. "Really, there are only two or three things blockchain gives you that other systems don't," says computer scientist David Mazières, codirector of the Center for Blockchain Research at Stanford University in Palo Alto, CA. Those include a way for two people to have a transaction, especially if they don't trust each other, and a tamper-proof record of the history of transactions. If a system doesn't need those components, he says, there's likely a better way to manage the information.

"One of the things I ask people is, how does your project take advantage of specific features of blockchain?" Mazières adds. "If you have a centrally trusted party, you don't need a blockchain." Although excited by recent advances in blockchain technologies, he says many projects don't require blockchain's unique attributes. "There are a lot of misguided efforts, as well."

Even suitable projects may need to tailor their approach; Bitcoin's blockchain version is an untenable model, skeptics emphasize. Its consensus algorithm is too cumbersome and energy intensive, it's relatively slow to add transactions, and it requires lots of data storage because every user must keep a copy of the entire ledger. Publicly available blockchains also present privacy problems. Hence, in certain settings blockchain may need to be tweaked to fit the security, energy, and user demands of networks beyond cryptocurrencies.

www.pnas.org/cgi/doi/10.1073/pnas.1914849116

The Brooklyn Microgrid uses a blockchain-based system to allow people to sell energy to their neighbors without the costs associated with a large, central power company. Image credit: Sasha Santiago of Storylabs I/O for Brooklyn Microgrid.

Most importantly, says electrical engineer Krishna Ratakonda at IBM, people need to have an incentive to participate. A blockchain that collects data from customers without offering anything in return likely won't attract many boosters. "These are the situations," says Ratakonda, "where things fall apart."

Keeping Track

A blockchain consists of a "block," data written as an alphanumeric code. This can only be added if the network approves and validates it. In the case of Bitcoin, this occurs via a "Proof of Work" algorithm. That means any blocks added to the chain must be encoded with the solution to a computational problem that's hard to crack but easy to verify (such as finding the prime factors of a big number). The entire network can validate the solution, verify the addition, and add the block to the chain with a timestamp. Bitcoin's power is its size: Any user can observe this solution, and information is protected by consensus.

Bitcoin users have an incentive to keep the network running because they have invested significant energy and resources into their participation. There's also a financial incentive. Users who solve these problems receive units of cryptocurrency. The Proof of Work requirement, meanwhile, discourages hacking because breaking into the blockchain entails investing time and energy to decode a single block but without any incentive or support from the network.

"Proof of Work was a good starting point to keep everyone honest," says Ratakonda. It was a concept that everyone could trust, even if they didn't trust each other, he notes. "That was really a necessity."

But Proof of Work does require serious computing power, leading computer scientists to seek alternative means of certifying trustworthiness. For example, the Brooklyn Microgrid, which lets consumers generate electricity through solar panels and other means and sell it to their neighbors, approves users individually and validates transactions instead of requiring Proof of Work.

Killer Apps

Already, both private and public entities are pursuing blockchain systems. Walmart has announced plans to work with IBM to develop a blockchain-based system that can track the distribution of lettuce to easily track the source of *Salmonella* contamination or other outbreaks (2). Some insurance companies are testing blockchain approaches to verify coverage of claims, cut down on fraud, and reduce day-to-day costs (3). Amazon offers a service for consumers to create and maintain blockchain networks using Hyperledger, a blockchain framework. And the US Food & Drug Administration has launched a pilot plan that uses blockchain to track prescribed drugs (4).

The uses are likely to multiply. Many online devices, part of a growing IoT, are notoriously insecure against hacks. That's in part, because hackers can find and exploit software weaknesses before the users can detect them or manufacturers can fix them. Blockchain may offer a fix. If its ledger is tamper-proof, it could reveal every transaction among smart devices, including unauthorized access by hackers. A smart lock could reveal who entered a house, and when, for example, and detect unauthorized entries. In 2017, a consortium of tech giants including Cisco and Bosch announced plans to explore new projects using blockchain to improve IoT security. "Blockchain is a near-perfect auditing instrument," says software engineer Konstantinos Christidis, who contributes to Hyperledger Fabric, a blockchain framework hosted by the Linux Foundation and used by IBM.

But although blockchain may detect intruders, it won't be able to stop them. And devices may be hacked in such a way that they're not flagged by a blockchain. Ratakonda points out that IoT networks already have robust ways to share data, and blockchain wouldn't necessarily offer any benefit in such cases. "If the existing ones are sufficient, why would you need a blockchain?"

Securing Virtual Communities

"Smart" electric grids already allow people with solar panels or wind turbines to sell energy to a power company. But some experts say blockchain-based systems could enable those people to sell energy directly to their neighbors without the costs associated with a large, central power company, as in the case of the Brooklyn Microgrid. Such a peer-to-peer approach could turn energy grids into local systems.

Starting in 2016, researcher Esther Mengelkamp at the Karlsruhe Institute of Technology in Germany began looking for ways to "create an energy community that is completely self-sufficient in terms of electricity, heat, and other kinds of energy," she says. Surveys showed that people were interested but that communities lacked the means to establish this kind system. So Mengelkamp started investigating blockchain-based set-ups, among the best systems with "smart" contracts, which can be used to automatically execute transactions when the buyers and sellers reach a certain price or demand (5).

"Until a few institutions buy into this concept, it's not going to kick off by itself. It has to get enough momentum that it becomes a meaningful thing."
—James Evans

Features such as smart contracts could also help address a pressing issue in biomedicine: monetizing personal data in a way that's fair to sellers and buyers alike while protecting privacy and ensuring transparency with regard to how that data used. "Everybody is talking about the value of data," says physicist and mathematician Alex Zhavoronkov at Hong Kong-based Insilico Medicine, a company that focuses on new drug discovery by combining artificial intelligence with blockchain. "But people are struggling to properly evaluate it. How much is your data worth?"

It could be worth a lot. Zhavoronkov sees blockchain as a powerful organizing force for health care and biomedical data. "I think it will eventually lead to a new data economics," he says.

Techniques such as high-throughput genetic sequencing are generating large datasets, presenting quandaries about how to collect, use, analyze, and control personal data. Zhavoronkov thinks private blockchains—in which patients have control over who can see and use blocks of information—offer an appealing organizing principle (6). Unlike public blockchains, these "permissioned" networks would only be visible to authorized users (although the networks would not be impervious to hacks).

Zhavoronkov has been working with a company called Longenesis in Hong Kong that develops private blockchain tools for hospitals and pharmaceutical companies to use with patients. "We treat data items as assets," says the company's CEO, Garri Zmudze. Their idea, says Zmudze, is to find a way for hospitals and other institutions to monetize patient data but do it in a way that's transparent to—and controlled by—patients who choose to participate. Guaranteeing the security and privacy of such a network, he says, will be a pivotal issue.

Users can check the blockchain ledger see who uses their data and when and what happened to it. Every doctor's visit, prescription, treatment plan, and exchange of information would be recorded on the ledger. If people consent to participate in a clinical trial, their consent—and the terms of that consent—would be recorded. Using smart contracts, they could automate that process.

Zmudze goes further, suggesting that the features of blockchain can reduce barriers to medical advances. If a pharmaceutical company in Norway wants to run an international study on men of a certain age and with a certain health condition, it can use blockchain to create a transaction with the information request, instead of having to recruit patients through collaborating institutions. And if patients agree to join, their consent is logged on the ledger.

Perhaps the biggest obstacle to this approach is security because blockchain ledgers reveal all transactions. Zmudze thinks that challenge is surmountable: A ledger would include transactions about the data but not the data itself. That way, that data could be deleted—without having to delete the entire blockchain. "The patient has the mechanism not only to control the data but also the mechanism to see the history," says Zmudze.

Who Did What, and When

At the University of Chicago's Knowledge Lab, sociologist James Evans has been mulling over ways that blockchain could revolutionize the scientific process itself.

A traditional published scientific article bundles a lot of information into a tidy, discrete package that often fails to accurately represent the work that went into it. "It's a very chunky system," Evans says. In the past four decades, the amount of effort that goes into producing a scientific paper has increased dramatically. A single biomedical article published now contains, on average, twice as many experiments as an article published in the late 1970s (7). "We're packing more and more stuff into these papers, and in some sense we're giving less detail," says Evans.

That detail could be important. Researchers typically don't share negative results, reports on failed experimental approaches, or outlines of experimental methods that worked but didn't support the researcher's hypothesis. "An awareness of experimental dead ends could help others avoid repeating the same mistakes,"

says Evans. And novel methods that didn't work for one experiment might be useful for another.

A blockchain network might help, Evans says. Blockchain could break down individual contributions to a scientific discovery. Instead of only looking to a published paper for its findings and experimental results, researchers could share new methods and techniques—and the potentially informative dead ends they hit along the way.

Mazières sees some advantages. Blockchain's tamper-proof timestamp could help researchers establish who did what and when and even help them stay on task. "It might be useful to basically have [researchers] commit to what they're doing or planned to do," he says.

Challenges Ahead

Blockchain is far from perfect. In addition to energy and computing demands, Ratakonda cites transparency as a big challenge. Some blockchain platforms, such as Hyperledger and Quorum, which was developed by JP Morgan Chase, are transparent to anyone. "These I would recommend," says Ratakonda. He worries about the proliferation of private blockchains in which not all users have access to the entire ledger.

But Ratakonda says privacy is "probably the key challenge" to implementing blockchain networks. A hacker who virtually masquerades as a patient, for example, might still be able to gain access to electronic health records—or decipher identities on a public network or get a person's private key and control his or her data. Blockchains encrypted with today's best cryptographic algorithms—and never updated—may still be vulnerable to future hackers.

And there are sometimes better, easier alternatives, as Mazières and other researchers point out. Smart contracts on their own, for example, don't justify using a blockchain. "A smart contract is just another word for a program," he says, and it's possible to build in these programs without using a blockchain. In many cases, blockchain may not be the appropriate technological solution to the problem. Case in point: The researchers behind the Landau Microgrid Project, which is still in use, ultimately decided not to use blockchain technology—opting instead for a different centralized system that still allows for peer-to-peer energy trading.

Even when blockchain offers potential advantages, institutional buy-in will be a big challenge. A prime example is a blockchain-based system that improves crediting and funding allocations among researchers. "Until a few institutions buy into this concept, it's not going to kick off by itself," says Evans. "It has to get enough momentum that it becomes a meaningful thing."

1 S. Nakamoto, Bitcoin: A peer-to-peer electronic cash system. https://www.bitcoin.com/bitcoin.pdf. Accessed 15 March 2019.
2 M. Smith, In wake of romaine *E. coli* scare, Walmart deploys blockchain to track leafy greens. https://news.walmart.com/2018/09/24/in-wake-of-romaine-e-coli-scare-walmart-deploys-blockchain-to-track-leafy-greens. Accessed 1 May 2019.
3 M. A. Henk, Blockchain: An insurance focus. http://us.milliman.com/insight/2016/Blockchain-An-insurance-focus. Accessed 28 March 2019.
4 US Food & Drug Administration, FDA takes new steps to adopt more modern technologies for improving the security of the drug supply chain through innovations that improve tracking and tracing of medicines. https://www.fda.gov/news-events/press-announcements/fda-takes-new-steps-adopt-more-modern-technologies-improving-security-drug-supply-chain-through. Accessed 1 May 2019.
5 E. Mengelkemp, Decentralizing energy systems through local energy markets: The LAMP-Project. http://mkwi2018.leuphana.de/wp-content/uploads/MKWI_90.pdf. Accessed 27 August 2019.
6 P. Mamoshina *et al.*, Converging blockchain and next-generation artificial intelligence technologies to decentralize and accelerate biomedical research and healthcare. *Oncotarget* **9**, 5665–5690 (2017).
7 A. Rzhetsky, J. G. Foster, I. T. Foster, J. A. Evans, Choosing experiments to accelerate collective discovery. *Proc. Natl. Acad. Sci. U.S.A.* **112**, 14569–14574 (2015).