Blockchaining the Cloud

Christine Miyachi
Xerox Corporation

During the rise of cloud computing, activist programmers created blockchain. Now it has the potential to transform the existing cloud applications.

When I was in business school, we studied how to solve problems creatively. One technique introduced was TRIZ,[1] which involves coming up with a contradictory solution. For example, if a faster engine produces too much heat, propose a faster engine that cools—and then figure out how to do it. Let's apply that to one of the thorniest problems in cloud computing—trust. A centralized authority is typically the basis of trust today, but that authority can be spoofed, or be untrustworthy themselves. If I were to use TRIZ, I would propose to create trust established by decentralized authority and assume that no one can be trusted. That solution already exists: blockchain.

Mike Gault, co-founder and CEO of Guardtime claims CIOs (Chief Information Officers) require that cloud suppliers provide "a secure supply chain and that they can verify every step in that supply chain in real-time; when things go wrong it is possible to figure out what went wrong and that there is someone who can be held accountable."[2] But he claims that not a single cloud provider can meet that demand. Blockchain has the promise to deliver, and there are many proposed applications to improve verification. This technology has the potential to revolutionize the financial and legal sectors as well as a wide variety of other industries.

In essence, blockchain will enable untrusted users to work together—to exchange currency, to make agreements, to validate personal records—without centralized authority. Centralized authorities—for example, banks—are expensive. But using blockchain is not free, and the energy and computing power create a transaction is also expensive. Also, security concerns still exist. In this column, I will explore blockchain applications that will alter cloud computing and some of the hazards of blockchain.

DEFINITIONS

In 2009, Satoshi Nakumoto[3] created Bitcoin, a digital currency and one of the first implementations of blockchain technology in response to the 2008 banking meltdown. A centralized authority had failed its users and bitcoin would rid the world of that authority. The technology was made possible by the wide use of cloud computing and underlying internet technologies. A blockchain is a "database encompassing a physical chain of fixed-length blocks that include 1 to N transactions, where each transaction added to a new block is validated and then inserted into the block. When the block is completed, it is added to the end of the existing chain of blocks. Moreover, the only two operations—as opposed to the classic CRUD (create, read, update, delete)—are add-transaction and view-transaction."[4] A thorough introduction to blockchain was written by Morgan E. Peck in *IEEE Spectrum*, which he titled "Blockchains:

Copublished by the IEEE CS and IEEE ComSoc
2325-6095/18/$33.00 USD ©2018 IEEE

How They Work and Why They'll Change the World: The technology behind Bitcoin could touch every transaction you ever make."[5] Blockchain is a distributed ledger and the transactions between parties in the ledger are recorded permanently and independently verified by a majority of verifiers. More than currencies, imagine contracts as a blockchain where the code to execute them is embedded. Blockchain may not be disruptive, but more a foundational technology. Karin R. Lakhani of Harvard Business School says, "It has the potential to create new foundations for our economic and social systems. But while the impact will be enormous, it will take decades for blockchain to seep into our economic and social infrastructure."[6]

WHAT MAKES BLOCKCHAIN SECURE

Since blocks don't change after being added, hackers have difficulty tampering with the chain. The entire blockchain is shared among networked computers called nodes. With each new transaction, each copy of the blockchain is updated. But before that transaction is added, it must be verified. In the case of Bitcoin, the verification determines if that entity has a Bitcoin to spend. Nodes called miners validate transactions. The validation involves hashing and cryptography that is explained well in the *IEEE Spectrum* article mentioned above. What makes it tamperproof is that the nodes in the network do the validation and the majority have to agree that the block is valid. One downside is that the cryptographic operations uses a lot of computing and therefore a lot of energy (see Figure 1). The blockchain is a list, and each block has a link to the previous block. If someone wants to change the block, that hash of that block will conflict with the current chain, and the miners will not validate it. The blockchain is difficult to change and therein lies its security.

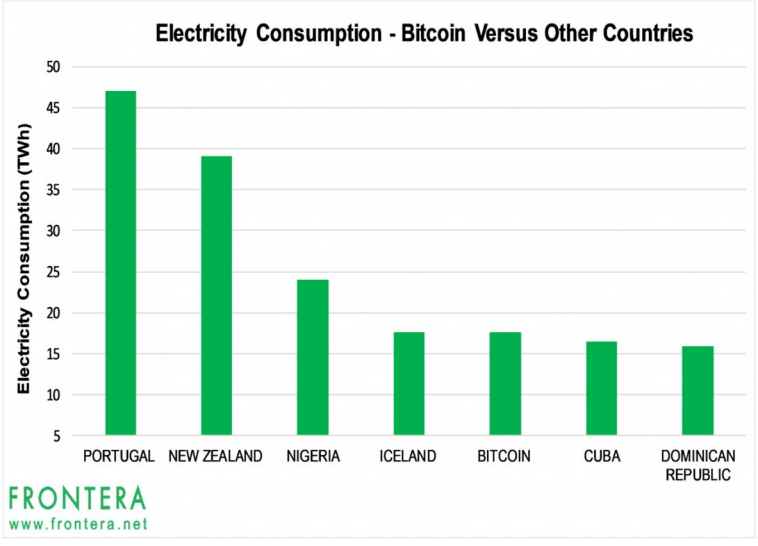

Figure 1. The energy consumption of all of today's Bitcoin processing is on the order of some smaller countries.[7]

THE DECENTRALIZATION OF THE INTERNET

The idea of decentralization was part of the introduction of the Internet. In 1996, John Perry Barlow created "A Declaration of the Independence of Cyberspace" where he made the plea for decentralization by saying to governments, "I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather."[8] While the Internet is still decentralized and governed by authorities like ICANN, a large amount of traffic passes through a few large corporations like Google, Amazon, Netflix and Facebook.[9]

Blockchain applications infused with this decentralization strategy are launching and institutions are rising to the challenge. The European Union put into effect a Payment Services Directive

(PSD2) in 2018.[10] Banks must now provide open programmable interfaces to third parties to manage customer finances. Blockchain is poised to take advantage of these APIs and provide secure transactions and eventually reduce the services of banks and the fees they charge.

With institutions getting more involved with blockchain, the decentralization that the Satoshi Nakamoto group envisioned may not occur. Vili Lehdonvirta, a professor at the University of Oxford, disagrees that blockchain will transform the economy and he calls this "the blockchain paradox."[11] His main point is that while blockchain can enforce rules, we need people to make the rules. Using Bitcoin as an example, he claims that the development team made the initial rules for Bitcoin. He says, "Humans are still very much in charge of setting the rules that the network enforces." Even with his insights, the blockchain was near the top of the hype cycle in 2017 (see Figure 2). The number of applications now available using blockchain has risen dramatically.

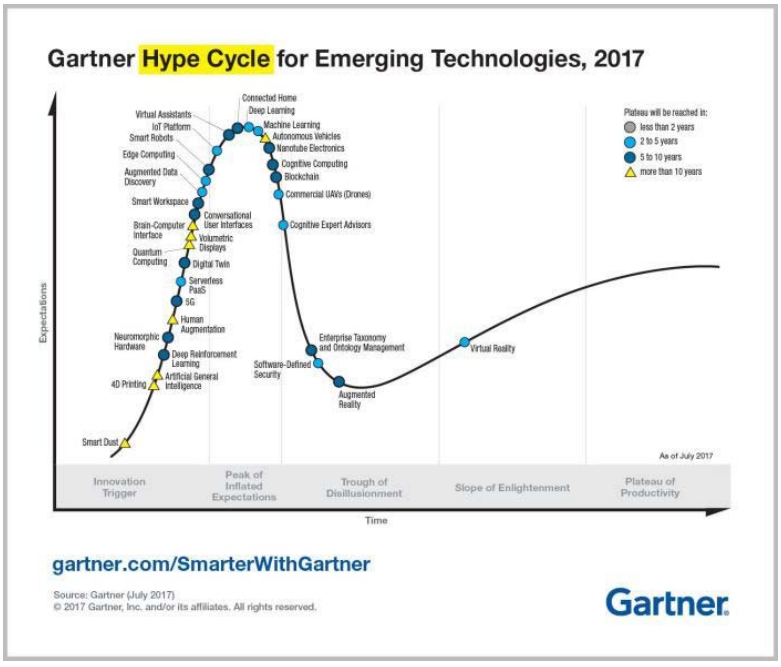

Figure 2. Blockchain was just over the top of the hype cycle in 2017.[12]

APPLICATIONS

Many of the large internet applications mine user data for profit. In the sharing economy, Uber and Airbnb take owner (cars or living quarters) information and match that information to customers who want to get a ride or rent an apartment. The value contributed is not equally distributed back to users as these companies take a share for their service. Just as with banks, a portion of the profits is captured by the intermediary. If people can store their identity on a blockchain, it is possible to reduce the role of this intermediary. La Zooz[13] is an identity management system based on blockchain—it is an open-source decentralized collaborative transportation system. Systems like this promote good behavior because you can't delete accounts and reregister because entries in the blockchain never get deleted. Your identity is verified but can be completely anonymous.

For secure identity, Onename[14] is a startup that allows you to create an ID using Bitcoin and they promise this ID can be used to log into websites without a need for a password. The Onename webapp is built on Blockstack. Blockstack is a decentralized naming and storage system. It's a replacement for traditional internet services like DNS, public-key infrastructure (PKI), and cloud storage and promotes an open internet by putting the users in control.

Real estate titles can be securely recorded and verified and not easily stolen. Many of the transactions of real estate rely on centralized authorities. Factcom[15] is a company dedicated to using blockchain for secure document management in real estate (and other industries), and they remove the dependence on these centralized authorities. Factcom believes "in keeping private data private and securing the world's wealth because privacy and possession of property are basic human rights."

Smart contracts, based on blockchain, are digital contracts that execute automatically and will provide a new business model for legal firms. The contracts are executed digitally and automatically and are irreversible. Lawyers will have to be programmers as well as understand the legal aspects of contracts and mediation. Smart contracts are self-enforcing and execute when a contract is broken or terminate when the terms of the contract complete.

Decentralized file storage based on blockchain promises to reduce costs associated with centralized file storage systems like DropBox or Google Drive. Storj[16] is a file system that rents out storage and bandwidth without using a centralized system. They claim to have the same performance and reliability as a centralized system, at a lower price, but at this time they are not accepting more users until they develop their next generation of software. Interplanetary File System (IPFS)[17] is another decentralized storage system using peer-to-peer methods. Like many of these blockchain applications, it is an open-source project.

Think about decentralized organizations that could work democratically and collaboratively—a company called backfeed.cc[18] provides a framework to do that. They say "Imagine Facebook owned by its users, decentralized transportation networks independent of Uber, markets dominated by open-source communities, where contributors are also shareholders and where the value created is redistributed both fairly and transparently." They promise that backfeed has the infrastructure to do that. Imagine solving the world's most difficult scientific problems by allowing anyone to post a solution and then rating that solution—Matryx.ai[19] provides a framework to perform this service. In the company's whitepaper they explain, "Matryx is composed of a bounty system and a marketplace for digital assets to be bought, sold, and remixed into new assets. Bounties are placed on solutions to specific problems. Submissions to bounty tournaments enter the collection of assets and are available to other users. In this way, collaborators are incentivized to build, distribute, and expand upon each other's work in the pursuit of valuable goals. Matryx reduces friction of collaboration between strangers by providing a common framework and concrete goals."

Blockchain even enables an application that may change the cloud itself. A decentralized cloud platform is available that guarantees privacy. Enigma[20] allows private data to be stored, shared, and analyzed but does not allow the data itself to be fully revealed. They say, "Blockchains without privacy are useless. Smart contracts without privacy are useless. If these technologies cannot work without privacy, then new privacy technologies are the truly useful innovations." And they promise to deliver new solutions to create that privacy.

NO PERFECT SOLUTION

The applications mentioned above have not all been fully implemented and thus are not completely proven. Initial Coin Offerings (ICOs, a blockchain alternative to Initial Public Offerings [IPOs] have had some difficult failures).[21] For many of these applications to work, governments and other institutions will need to go through some revolutionary changes and provide regulatory support. These are the intermediaries—just the type blockchain purports to remove. The blockchain paradox is that this technology needs governance and once the governance is there, blockchain is no long decentralized.

There are also ways to attack a blockchain. One way is an "eclipse attack." Nodes that have copies of the blockchain must communicate and this communication channel can be fooled. Also, a "selfish miner" could fool other nodes into wasting time-solving already-solved blocks. The failures are typically where the blockchain connects to other systems such as "hot wallets" that store the private keys used for the cryptography. There are solutions to these problems but a more difficult issue with bugs. If the blockchain code itself has a bug, the knowledge of this bug could be

used to attack. This is what happened in 2016 when a crowdsourced venture capital platform called The DAO (decentralized autonomous organization) based on the Ethereum blockchain opened for business. Soon after starting, an engineer found a bug in the code, and The DAO was hacked, with hackers stealing 60 million dollars in cryptocurrency.[22]

Private blockchains may be a solution to some of the security issues. The participants would be screened and there would be an immutable log of the participation. Private blockchains can also limit the miners to be trusted sources. Private blockchains are not as widely decentralized but could provide more secure operations. Using private blockchains may make the adoption of this technology more palatable to existing institutions such as governments and banks.

CONCLUSION

Blockchain is a technology that could be applied to solve some cloud security problems. The applications claim to give control back to individuals. But even though the internet is still considered decentralized, large organizations control much of the traffic. The same centralizing could happen with blockchain. Research out of Cornell University found that four miners did 53 percent of the bitcoin mining work in a week and similarly, three Ethereum miners did 61 percent of the work.[23] While the blockchain itself appears to solve some security issues, its widespread use is just starting. Governance will be necessary for blockchain applications to work within current systems. Misuse will always be looming. John Kenneth Galbraith said, "A constant in the history of money is that every remedy is reliably a source of new abuse."[24] And yet it doesn't keep us from reaching for that perfect remedy.

REFERENCES

1. "TRIZ," *Wikipedia*, Wikimedia Foundation, 3 July 2018; https://en.wikipedia.org/wiki/TRIZ.
2. M. Gault, "BlockCloud: Re-Inventing Cloud with Blockchains," *guardtime*, blog; https://guardtime.com/blog/blockcloud-re-inventing-cloud-with-blockchains.
3. "Satoshi Nakamoto," *Wikipedia*, Wikimedia Foundation, 13 July 2018; https://en.wikipedia.org/wiki/Satoshi_Nakamoto.
4. J.J. Bambara et al., *Blockchain: A Practical Guide to Developing Business, Law, and Technology Solutions*, McGraw-Hill Education, 2018.
5. M.E. Peck, "Blockchains: How They Work and Why They'll Change the World," *IEEE Spectrum*, 28 September 2017; https://spectrum.ieee.org/computing/networks/blockchains-how-they-work-and-why-theyll-change-the-world.
6. M. Iansiti and K.R. Lakhani, "The Truth About Blockchain," *Harvard Business Review*, 6 March 2018; https://hbr.org/2017/01/the-truth-about-blockchain.
7. S. Bubna, "Bitcoin Mining Now Consumes As Much Electricity As Iceland," *Frontera*, 17 October 2017; https://frontera.net/news/global-macro/bitcoin-mining-now-consumes-as-much-electricity-as-iceland/.
8. J.P. Barlow, "A Declaration of the Independence of Cyberspace," *Electronic Frontier Foundation*, 8 February 1996; https://www.eff.org/cyberspace-independence.
9. J. Brogan, "A Cheat Sheet Guide to Who Controls the Internet," *Slate*, 1 November 2016; http://www.slate.com/articles/technology/future_tense/2016/11/a_cheat_sheet_guide_to_who_controls_the_internet.html.
10. "Payment Services Directive," *Wikipedia*, Wikimedia Foundation, 3 July 2018; https://en.wikipedia.org/wiki/Payment_Services_Directive.
11. V. Lehdonvirta, "The Blockchain Paradox: Why Distributed Ledger Technologies May Do Little to Transform the Economy," Oxford Internet Institute, 21 November 2016; https://www.oii.ox.ac.uk/blog/the-blockchain-paradox-why-distributed-ledger-technologies-may-do-little-to-transform-the-economy/.
12. F. Van De Ven, "Blockchain, Gartner's Hype Cycle and a local Mexican coin called Túmin: is the age of disillusionment approaching?," *Medium*, 28 February 2018;

https://medium.com/@frankvandeven/blockchain-gartners-hype-cycle-and-a-local-mexican-coin-called-t%C3%BAmin-is-the-age-of-c3f77de9cc6d.
13. *La'Zooz*; http://lazooz.org/.
14. *Onename*; https://onename.com/.
15. *Factom — Making the World's Systems Honest*; https://www.factom.com/.
16. *Decentralized Cloud Storage - Storj*; https://storj.io/.
17. "InterPlanetary File System," *Wikipedia*, Wikimedia Foundation; https://en.wikipedia.org/wiki/InterPlanetary_File_System.
18. *Spreading Consensus*; http://backfeed.cc/.
19. *Matryx — Tackle Science's Greatest Challenges with VR and Blockchain-Based Collaboration*, Nanome; https://matryx.ai/.
20. *Project Overview ‹ Enigma – MIT Media Lab*, MIT Media Lab; https://www.media.mit.edu/projects/enigma/overview/.
21. G. Lewis-Kraus, "Inside the Crypto World's Biggest Scandal," *Wired*, 19 June 2018; https://www.wired.com/story/tezos-blockchain-love-story-horror-story/.
22. "The DAO (Organization)," *Wikipedia*, Wikimedia Foundation, 20 July 2018; https://en.wikipedia.org/wiki/The_DAO_(organization).
23. M. Orcutt, "How Secure Is Blockchain Really?," *MIT Technology Review*, 25 April 2018; https://www.technologyreview.com/s/610836/how-secure-is-blockchain-really/.
24. "John Kenneth Galbraith," *Wikiquote*, Wikimedia Foundation; https://en.wikiquote.org/wiki/John_Kenneth_Galbraith.

ABOUT THE AUTHOR

Christine Miyachi is a systems engineer at Xerox Corporation and holds several patents. She works on Xerox's Extensible Interface Platform, which enables developers to create applications that work with Xerox devices by using standard web-based tools. Miyachi has two MIT degrees: an MS in technology and policy/electrical engineering and computer science and an MS in system design and management. Contact her at cmiyachi@alum.mit.edu.