DOI:10.1145/3225619

Hanna Halaburda

▸ Marshall Van Alstyne, Column Editor

Economic and Business Dimensions
Blockchain Revolution without the Blockchain?

Most of the suggested benefits of blockchain technologies do not come from elements unique to the blockchain.

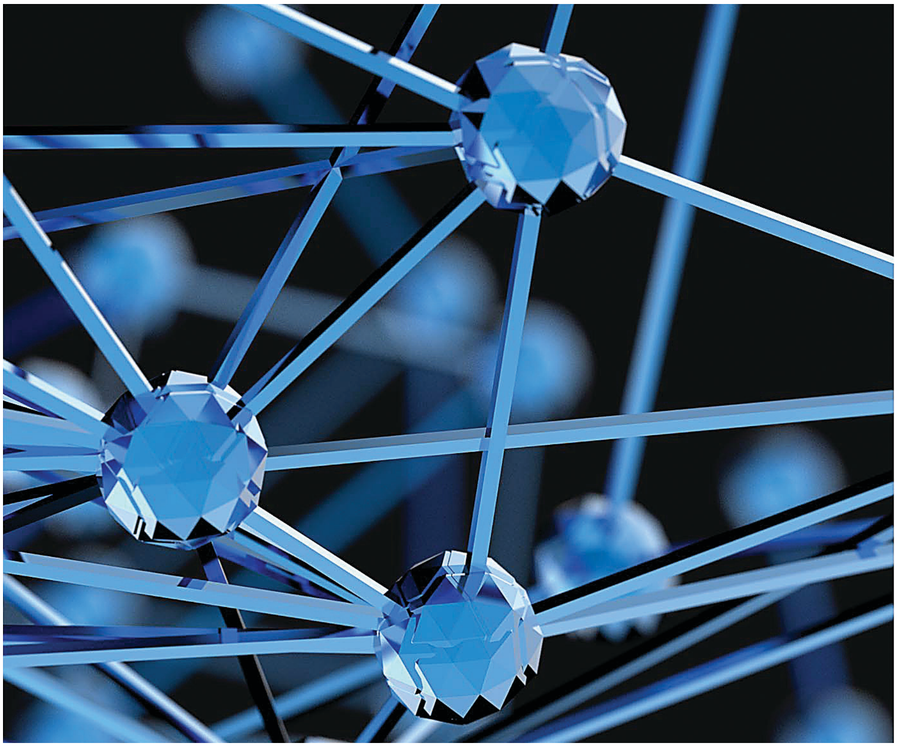

IMAGE BY ZAP2PHOTO

BLOCKCHAIN HAS ATTRACTED a lot of attention. Many are excited about this new technology based on a public, permissionless, distributed ledger that cryptographically assures immutability without a need for a trusted third party and allows for smart contracts. Large and small companies want to get on board, as they expect this technology will lower their costs by making transactions quicker, safer, transparent, and decentralized. However, the technology behind the blockchain is for the most part not well understood—there is no consensus on what benefits it may really bring, or on how it may fail.

A more careful look into the technology reveals that most of the proposed benefits of "blockchain technologies" do not really come from blockchain. Smart contracts, encryption, and distributed ledger are separate concepts. The three may be implemented together, but they do not need to be. Most of the proposed benefits come from encryption and smart contracts. But encryption and smart contracts do not need blockchain.

Confusion Around What Blockchain Actually Is

The growing excitement about blockchain technologies is perhaps best summarized in the increasingly popular slogan "blockchain revolution."The revolution is buoyed by a few forces, of which the most significant is the expectation of substantial cost savings.

The main sources of savings are supposed to come from increased security, faster transactions, and a shared ledger. However, the statements about the benefits of blockchain seem to confuse three different concepts: encryption; automated execution of transactions ("smart contracts"); and distributed ledger, a type of a distributed database. The three may be applied together, but they are separate tools, and not all of them are necessary in a blockchain system.

So, what is "blockchain"? While there is no one standard definition of blockchain, the most parsimonious and commonly used is "distributed ledger of transactions."[a] This is why the term "blockchain technologies" is often used interchangeably with the phrase "distributed ledger technologies."

Where Is the Confusion Coming From?

The source of confusion around blockchain can be traced to the origin of the term. "Blockchain" was introduced as a shorthand term for "chain of blocks of transactions," which was part of the Bitcoin system.[4] Later, "blockchain" became an independent term in media discussions of whether there are other uses for distributed ledgers of transactions beyond Bitcoin.

Bitcoin's system—a system operating without a trusted third party—has been quite successful since it started in 2009, in the sense there has been no fraud on its blockchain. For this reason, it is often said to be secure. Bitcoin's blockchain is also public (all transactions are visible), and permissionless (any computer may participate in validating transactions and adding them to the ledger).

Some pundits erroneously extrapolate that any blockchain will have these properties: distributed, secure, public, permissionless, and will operate without the need for a trusted third party. This extrapolation may come from a misconception that the Bitcoin's blockchain properties come solely from technology, while in reality they come from a combination of technology and an incentive system that accounts for the behavior of human participants. Yes, the Bitcoin system uses cryptographic tools. But the reason why the system is virtually immutable is because it is too costly to "rewrite the history."

Note that smart contracts are not a core property of the Bitcoin blockchain. The Bitcoin system has a rudimentary capability to create code that would allow for some transactions to be automatically executed. Ethereum expanded on this feature, introducing a blockchain with a main purpose to facilitate smart contracts (see http://www.ethereum.org.) Since the term "smart contracts" entered the mainstream media in the context of blockchain, this may have created a perception that smart contracts are native to blockchains. However, a code automatically executing a transaction can be implemented by a wide range of entities.[5]

Current applications of blockchain have gathered only limited appeal.

Therefore, smart contracts, encryption, and distributed ledger are separate concepts. They may be implemented together, but do not need to be. The term "blockchain" should not be used as a catch-all aggregation of these different terms.

Why Is It Important to Consider Smart Contracts, Encryption, and Distributed Ledger Separately?

The distinction matters for estimating costs and benefits, or even predicting the best uses of blockchain technologies. For example, smart contracts are computer programs that automatically implement the terms of an agreement between parties. One typically given example is that of a car lease: upon a missed payment, the car automatically locks and returns the control to the lender. Since execution of a smart contract does not involve a decision or an action of a human, it may increase speed as well as minimize the number of mistakes. Both would result in cost savings.

Some media outlets state that "through blockchain technology, smart contracts are now a reality."[3] However, smart contracts were a reality long before: an automated recurring payment that someone sets up with his or her bank or a limit order with a stock exchange are examples of smart contracts. Blockchain is not needed to gain the benefits from smart contracts, because smart contracts can be set up just as effectively on a centralized system.

Other significant cost savings may come from improved encryption, which results in increased security of the system. Currently, encryption is underutilized in business practice. Bitcoin's blockchain itself uses standard, well-established cryptography tools. But excitement about blockchain's safety turned more attention to the new developments in cryptography.

What Are the Benefits of Blockchain?

What about the benefits of a distributed ledger—the blockchain itself? A distributed ledger allows multiple parties in the system to add transactions to a shared ledger in a way that the changes are reflected consistently across all copies.[b] It brings benefits in places where reconciliation of contradictory ledgers is costly. At the same time, recording transactions on a shared ledger takes more time than on a centralized ledger, because of the reconciliation mechanisms (consensus mechanisms) that must be employed. Moreover, the need to store the ledger in multiple locations may significantly add to storage and computational costs. So far it has not been clearly demonstrated in which circumstances the benefits of employing a distributed ledger outweighs the cost of delays and duplicated storage.

Distributed ledgers are a special case of distributed databases. They have been known, and used, for three decades. But proponents of blockchain technologies expect more from the new technology than just distributed ledger. They expect that adopting blockchain could result in further cost savings due to disintermediation, as it does not require a trusted third party to be virtually immutable. Indeed, the core of Bitcoin's computer-scientific innovation was the security of a permissionless distributed ledger, so that there is no need for a trusted third party anywhere in the system.

[a] Note that "ledger of transactions" is different from "ledger of balances." The former keeps the history of transactions, as in the "chain of blocks of transactions." Using this definition, "Ledger of balances" would not be a blockchain.

[b] Technically, distributed databases also have other desirable properties, but this one seems to be the focus in the context of blockchain technologies and fintech.

However, these benefits may be difficult to realize in a blockchain without Bitcoin. It has proven to be a challenge to create a decentralized, permissionless, and safe blockchain to transfer assets other than the native cryptocurrency (for example, bitcoins).

The first major issue is the gateway problem: The information about the underlying assets must enter the blockchain in the first place. The second major challenge is ensuring immutability of the ledger without a native currency. In most of the currently proposed applications, both these issues have been addressed by creating closed, permissioned blockchains, which require some involvement of a trusted third party. This is because blockchain without bitcoins is no longer virtually immutable without a trusted third party. In many cases, the permissioned blockchains are the right tools for their purpose, but more often a centralized system would be more efficient and reliable.

Current applications of blockchain have gathered only limited appeal. Bitcoin's blockchain is the most successful, but even after a decade Bitcoin has been adopted as a payment method only for specific niches. Mainstream users often indicate existing payment systems, such as credit and debit cards, not only satisfy their needs, but also provide services above what Bitcoin delivers.[2]

There are ideas for other, non-currency applications of blockchain, such as real-estate ownership records, voting information, or identity verification. However, a careful look into these areas shows the problems there do not arise from the need for a distributed ledger of transactions.

Consider an example of the pilot program administered by the Cook County real-estate office.[1] When someone acquires property, they usually need to purchase title insurance in case someone else claims the ownership property over the seller. The Cook County office was wondering whether putting the real-estate ownership on a blockchain would resolve this uncertainty. However, the major cause of the title uncertainty is that when a property is sold, there is no obligation to report it to the county office (or elsewhere). It is enough to have a written sales contract as a proof. Moreover, the sales reported to the county office are manually entered into the system, which results in typing errors. Neither of these problems is solved by implementing a blockchain …

The Future of the Blockchain Revolution

I expect blockchain technologies will have a big impact on many industries, and that it will not be limited to finance. However, it may not happen in the way it is currently envisioned. Both the entrants and the incumbents are looking with interest at the properties of Bitcoin's blockchain and smart contracts. But as they realize the benefits of different elements of the system, it may turn out that while new encryption tools and automated execution of transactions (smart contracts) have large and clear benefits, distributed databases may have a more limited appeal. Most of all, we need to realize that outside of Bitcoin (or other cryptocurrencies) we do not have a technology that offers "permissionless distributed ledgers that cryptographically assure immutability without a need for trusted third parties."

The blockchain revolution may give us new tools and change the landscape of some industries. But since the benefits of encryption and smart contracts can be realized without a distributed ledger, the world after the blockchain revolution may well be a world without the blockchain.

References

1. Cook County Recorder of Deeds. Blockchain Pilot Program. Final Report. May 30, 2017; https://bit.ly/2IeWDUZ
2. Henry, C., Huynh, K., and Nicholls, G. Bitcoin awareness and usage in Canada. BoC Staff Working Paper 2017-56. (Dec. 2017); https://bit.ly/2IjbLMR
3. Lielacher, A. A cost-benefit analysis of using smart contracts in banking. BTCManager.com (Apr. 14, 2017); https://bit.ly/2IIQJel
4. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System, 2008; https://bit.ly/2IgFLx8
5. Szabo, N. Formalizing and securing relationship on public networks. *First Monday* (Sept. 1997); https://bit.ly/2IgFLx8

For more extensive discussion on the topic see "Blockchain Revolution without the Blockchain," BoC Staff Analytical Note 2018-5; https://bit.ly/2GhXhva

Hanna Halaburda (hhalaburda@gmail.com) is a Visiting Professor at NYU-Stern and a Senior Economist at the Bank of Canada.

The views expressed in this column are those of the author. No responsibility for them should be attributed to the Bank of Canada.

Calendar of Events

July 2–4
ITiCSE '18: Innovation and Technology in Computer Science Education,
Larnaka, Cyprus,
Sponsored: ACM/SIG,
Contact: Janet Read,
Email: jcread@uclan.ac.uk

July 7–8
CI 2018: Collective Intelligence 2018,
Zurich, Switzerland,
Sponsored: ACM/SIG,
Contact: Abraham Bernstein,
Email: bernstein@ifi.uzh.ch

July 8–11
UMAP '18: 26th Conference on User Modeling, Adaptation and Personalization,
Singapore,
Co-Sponsored: ACM/SIG,
Contact: Jie Zhang,
Email: zhangj@ntu.edu.sg

July 8–12
SIGIR '18: The 41st International ACM SIGIR Conference on Research and Development in Information Retrieval,
Ann Arbor, MI
Sponsored: ACM/SIG,
Contact: Kevyn Collins-Thompson,
Email: kevynct@umich.edu

July 9–12
HT '18: 29th Conference on Hypertext and Social Media,
Baltimore, MD,
Sponsored: ACM/SIG,
Contact: Dongwon Lee,
Email: dongwon@psu.edu

July 15–19
GECCO '18:
Genetic and Evolutionary Computation Conference,
Kyoto, Japan,
Sponsored: ACM/SIG,
Contact: Keiki Takadama,
Email: keiki@inf.uec.ac.jp

July 16–18
SPAA '18: 30th ACM Symposium on Parallelism in Algorithms and Architectures,
Vienna, Austria,
Co-Sponsored: ACM/SIG,
Contact: Christian Scheideler,
Email: scheidel@upb.de