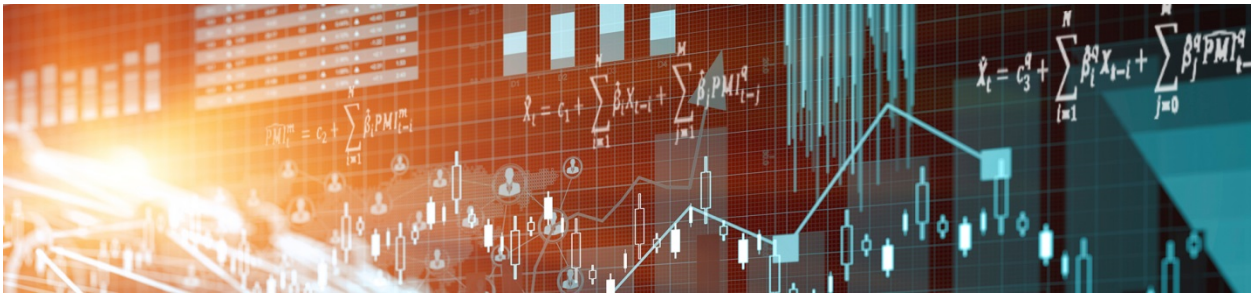
BANK OF CANADA
BANQUE DU CANADA

Staff Analytical Note/Note analytique du personnel 2018-5

Blockchain Revolution Without the Blockchain



by Hanna Halaburda

Currency Department
Bank of Canada
Ottawa, Ontario, Canada K1A 0G9
hhalaburda@bankofcanada.ca

Bank of Canada staff analytical notes are short articles that focus on topical issues relevant to the current economic and financial context, produced independently from the Bank's Governing Council. This work may support or challenge prevailing policy orthodoxy. Therefore, the views expressed in this note are solely those of the authors and may differ from official Bank of Canada views. No responsibility for them should be attributed to the Bank.

Abstract

The technology behind blockchain has attracted a lot of attention. However, this technology is for the most part not well understood. There is no consensus on what benefits it may bring or on how it may fail. A careful look into the technology finds that most of the proposed benefits of so-called blockchain technologies do not really come from elements unique to blockchain. Instead, they come from more conventional elements such as encryption and smart contracts. Moreover, even those applications that would benefit from a distributed system may benefit more from a distributed database designed differently than blockchain.

Bank topics: Digital currencies; Recent economic and financial developments; Service sector

JEL codes: D8, G2, O3, O33

Résumé

La technologie à la base de la chaîne de blocs suscite beaucoup d'intérêt. Or cette technologie, pour l'essentiel, n'est pas bien comprise. Il n'existe aucun consensus sur ses avantages ni sur ses défaillances possibles. Si on l'examine attentivement, on constate que la plupart des avantages escomptés ne découlent pas d'éléments propres à la chaîne de blocs, mais d'éléments plus traditionnels, comme le chiffrement et les contrats qui s'autoexécutent. De plus, même les applications qui profiteraient d'un réseau décentralisé pourraient bénéficier davantage d'une base de données partagée conçue différemment de la chaîne de blocs.

Sujets : Monnaies numériques; Évolution économique et financière récente; Secteur des services

Codes JEL : D8, G2, O3, O33

ISSN 2369-9639

© 2018 Bank of Canada

Blockchain—often called "the technology behind Bitcoin"—has attracted a lot of attention, perhaps somewhat comparable to that devoted to the Internet at the time of the dot-com boom. Many are excited about this new technology, supposedly 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, since they expect this technology to 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,[1] or on how it may fail.

Optimism in the face of novelty and uncertainty of a new technology is not a new phenomenon, but it does affect the economy, for example, through optimistic valuations of blockchain-referencing startups. This optimism also appears in estimates quoted by the media that indicate large cost savings but don't offer much detail about how those savings would occur.

A more careful look into the technology reveals that most of the proposed benefits of so-called blockchain technologies do not actually come from blockchain. What gets bundled up as blockchain technologies—smart contracts, encryption and a distributed ledger—are separate concepts. The three may be implemented together, but they do not need to be. We analyze them separately and argue that most of the proposed benefits come from encryption and smart contracts. But encryption and smart contracts do *not* need blockchain.

So, while the wave of excitement may facilitate adoption of new technology solutions, the landscape after the so-called blockchain revolution may include very few actual blockchain applications. Instead, the changes could focus on encryption and smart contracts.

Confusion around what blockchain actually is

The market's excitement about blockchain technologies is growing and is perhaps best summarized in the increasingly popular slogan "blockchain revolution." It is estimated that the blockchain market size

[1]For example, some pundits point to "privacy" while others to "transparency" as a benefit of blockchain.

will grow from US$210 million in 2016 to over US$2 billion by 2021.[2] Blockchain technologies are expected to change the way the financial industry, supply chains, government record-keeping and many other areas operate. The *Financial Times*[3] describes the technology as follows:

> Blockchain is an electronic ledger of transactions that are continuously maintained in blocks of records. What gets its developers, investors and fans so excited, however, is that ledgers are jointly held and run by all participants. It is meant to be cryptographically secured to prevent anyone being able to manipulate records, such as who voted for whom, or who owns a bank account.[4]

The revolution is supported by a few forces, the most significant of which is the expectation of substantial cost savings, as described in the following quotes from *Financial Times*:

> Blockchain is the electronic ledger originally built to underpin bitcoin markets. Promoters say it will lead to cheaper, more secure ways of settling all kinds of transactions.[5]

> The technology—an electronic ledger with records stored in "blocks"—aims to automate the complex networks of trust and verification on which modern finance sits, potentially cutting tens of billions of dollars of costs from the financial sector.[6]

The main sources of savings are supposed to come from increased security, faster transactions and a shared ledger.[7] Faster transactions on blockchain are often—but not exclusively—ascribed to smart contracts (i.e., automated execution of transactions). A shared ledger is supposed to contribute to cost savings because blockchain is assumed to operate without a trusted third party and therefore to eliminate intermediaries.

---

[2] As estimated by Markets and Markets, a market research company (https://www.marketsandmarkets.com/Market-Reports/blockchain-technology-market-90100890.html). Market size is measured by revenues from sale of blockchain-related solutions.

[3] It is worth noting that among all the media excitement, the *Financial Times'* voice is probably the most cautious in blockchain matters.

[4] J. Wild, "Blockchain believers hold fast to a utopian vision," *Financial Times*, January 27, 2017.

[5] G. Meyer and N. Hume, "Trafigura tests blockchain for settling US oil market deals," *Financial Times*, March 27, 2017.

[6] P. Stafford, "Blockchain consortium raises record $100m," *Financial Times,* May 23, 2017.

[7] Additional expected benefits include public data and time-stamping of transactions.

However, these assumptions about the benefits of blockchain seem to confuse at least three different concepts: (1) encryption, (2) smart contracts, and (3) 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 a "distributed ledger of transactions."[8] This is why the term "blockchain technologies" is often used interchangeably with "distributed ledger technologies." This parsimonious definition allows blockchains to have different attributes. Specifically, not every distributed ledger can be secure without a trusted third party[9] or needs to involve smart contracts. More importantly, encryption or smart contracts do not require a distributed ledger (i.e., blockchain) to be implemented.

Where is this confusion coming from?

Confusion around blockchain can be traced to the origin of the term. The term "blockchain" was introduced as shorthand for a "chain of blocks of transactions," which was part of the Bitcoin system. Therefore, in the Bitcoin context it meant a "distributed ledger of transactions." Later, "blockchain" became an independent term in media discussions of whether there are other uses for distributed ledgers of transactions beyond Bitcoin.

Since it started in 2009, the Bitcoin system, which operates without a trusted third party, has been successful in preventing fraud on its blockchain.[10] That is, Bitcoin's blockchain has proved to be for all practical purposes "immutable." 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).

---

[8] Note that a "ledger of transactions" is different from a "ledger of balances." The former keeps the history of transactions, as in the "chain of blocks of transactions." A ledger of balances wouldn't be a blockchain.

[9] Alternatively, one could insist on defining "blockchain" to be a distributed ledger that is secure without any trusted third party. That is a more restrictive definition that would exclude most currently proposed applications of blockchain technologies.

[10] While there have been thefts of large sums of bitcoins, e.g., on Mt.Gox, none of them occurred by falsifying the blockchain. The difference is akin to the difference between a bank robbery and counterfeiting in the realm of paper currency. While "bank robberies" have happened in the world of Bitcoin, the system has proven to be resistant to "counterfeiting."

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 an illusion that the Bitcoin's blockchain properties come solely from technology, while they actually come from a combination of technology and an incentive system that accounts for the behaviour of human participants. Yes, the Bitcoin system uses cryptographic tools: public-private key encryption, hashing algorithms. But the system is virtually immutable[11] because changing the blockchain's history is *too costly*.[12]

Bitcoin's blockchain has these properties because it is a part of the Bitcoin system. Other distributed systems may not be able to sustain these properties. This is because the Bitcoin system is much more than just the blockchain. The system also involves native cryptocurrency (bitcoins), mining and other elements. Changing the elements of the system, e.g., by removing the native cryptocurrency, or by changing the proof-of-work mechanism, affects the incentives of the participants and therefore may alter the properties of the distributed ledger that is supported by this modified system.

Note also that smart contracts are not a core property of the Bitcoin blockchain. The Bitcoin system allowed for additional comments along with the transactions, which provided rudimentary capability to create code that would allow for automatic execution of some transactions. Ethereum expanded on this feature, introducing a blockchain with the main purpose of facilitating smart contracts.[13] Mainstream media's use of the term "smart contracts" solely in the context of blockchain may have created the perception that smart contracts are native to blockchains. However, a code automatically executing a transaction can be implemented by a wide range of entities.

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.

[11] Bitcoin's blockchain is immutable with very high probability, but does not guarantee absolute immutability.
[12] The Bitcoin system makes adding a block to the blockchain artificially costly by making verification nodes compete to solve a cryptographic puzzle. This also makes changing blockchain's history prohibitively costly. Changing this feature, while leaving all the cryptography in place, could jeopardize the safety of a blockchain operating without a trusted third party.
[13] See www.ethereum.org.

Why is it important to consider smart contracts, encryption and distributed ledger separately?

The broadening of the meaning of "blockchain" to include smart contracts, encryption and distributed ledger could simply reflect the evolution of a term in a living language. However, precision matters for estimating costs and benefits, or even for predicting the best uses of blockchain technologies. Smart contracts, encryption and distributed ledger each bring different benefits. And since they can be implemented independently, an optimal solution for a particular application may include only some of these tools but not others. This may matter for the future of the blockchain revolution.

Smart contracts are computer programs that automatically implement the terms of an agreement between parties. One example typically given is that of a car lease: upon a missed payment, the car would automatically lock and control would return to the lender. Since execution of a smart contract does not involve a decision or an action by a human, it may be faster and minimize the number of mistakes. Both the increased speed and reduction in errors would result in cost savings.

The term "smart contracts," and the car example, come from Nick Szabo's 1997 article,[14] published 12 years before Bitcoin and its blockchain. Some media outlets state that "through blockchain technology, smart contracts are now a reality."[15] However, smart contracts were a reality long before. An automated recurring payment that someone sets up with a bank is an example of a smart contract. Blockchain is not needed to gain the benefits from smart contracts, because smart contracts can be set up on a centralized system—a bank's system or a platform dedicated to smart contracts used by individuals.

Encryption, which increases the security of a computer system, may also result in significant cost savings.[16] Currently, encryption is underutilized in business practice. For example, until recently public-

[14] N. Szabo, "Formalizing and Securing Relationships on Public Networks," *First Monday*, September 1997. Available at http://firstmonday.org/ojs/index.php/fm/article/view/548.

[15] See, e.g., A. Lielacher, "A Cost-Benefit Analysis of Using Smart Contracts in Banking," BTCManager.com, April 14, 2017. Available at https://btcmanager.com/a-cost-benefit-analysis-of-using-smart-contracts-in-banking/.

[16] The security of Bitcoin's blockchain comes from two sources: (i) encryption tools, such as public-private key, using hash functions, etc; and (ii) incentives induced by the mining scheme. We focus here on encryption. As we discuss later, the incentives induced by mining are difficult to sustain in blockchains without native cryptocurrency and without a trusted third party (or parties).

private key encryption was typically used to log into a business's information technology system, but once users were admitted into the system, there was some, but little protection.[17]

Excitement about blockchain turned more attention to new developments in cryptography. Bitcoin's blockchain uses standard, well-established cryptography tools (public-private key encryption, hash functions, etc.). But novel tools developed in recent years allow for much bolder uses. The premise is to create encryption systems that would protect the information—no matter where it is stored—rather than protect a specific computer.

Serious efforts in this direction have already been undertaken by industry heavyweights, as stated by R. Martin Chavez, the chief financial officer of Goldman Sachs:

> We focused on encryption and key management, worked on these issues with AWS and Google, and now we are in a new state. Our developers are indifferent as to whether a particular data compute load will happen out of Amazon and Google [cloud computing services] or whether they will happen in our own data centers. And we assume that all the computers are hostile; it doesn't matter whether they are at AWS or our own data centers.[18]

This essentially describes a paradigm shift in the approach to cyber security, and we should pay attention to it. Given the large sums currently spent in relation to fraud and hacking, this shift has potential for significant cost savings. A 2016 study of large companies estimated that cyber crime costs the average large US company US$17 million. The global average is US$9.5 million.[19] However, it is doubtful that we need blockchain to get the benefits of encryption and to trigger these cost savings.[20]

What are the benefits of blockchain?

The arguments above show how smart contracts and encryption can result in cost savings. But what about the benefits of distributed ledger, i.e., the blockchain itself?

---

[17] For example, often, information is encrypted on specific drives in companies' computer systems.

[18] R. M. Chavez, "Data, Computing, and Transformation in the Financial Industry," speech at the symposium "Data, Dollars and Algorithms: The Computational Economy," Harvard Institute for Applied Computational Science, January 19, 2017. Available at https://www.youtube.com/watch?v=VF6DrX9H0Ug .

[19] *2016 Cost of Cyber Crime Study & the Risk of Business Innovation*, Ponemon Institute Research Report, October 2016. The numbers are steadily increasing. In 2015 the average cost was US$15 million in the United States and US$8 million globally.

[20] The Goldman Sachs solutions described in the Chavez quote do not rely on blockchain.

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 its copies.[21] 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 need to be employed. Moreover, the need to store the copies of the ledger in multiple locations may significantly add to storage and computational costs. To date, it has not been clearly demonstrated in which circumstances the benefits of employing a distributed ledger outweighs the cost of delays and duplicated storage.

Moreover, with the experience of Bitcoin, proponents of blockchain technologies expect more from the new technology than just a distributed ledger. By looking at Bitcoin's blockchain and the fact that it has not suffered a breach since its inception, the pundits extrapolate that any blockchain by its nature offers added security benefits beyond encryption. They also expect that adopting blockchain would result in further cost savings due to disintermediation, since Bitcoin's blockchain 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.[22]

Distributed ledgers are a special type of distributed databases, which have been known and used for three decades. But while previous distributed databases were permissioned and required a third party to manage the permissions and help maintain the database, Bitcoin was the first that allowed for a *permissionless* distributed ledger.[23] So yes, Bitcoin's blockchain is virtually immutable without a need for a trusted third party.

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 secure blockchain to transfer assets other than a native cryptocurrency (for example, bitcoins for the Bitcoin blockchain).

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

[22] The security of the ledger is not guaranteed. However, the probability of a failure is pushed so low that the ledger is considered secure for all practical purposes. Nonetheless, there are factors that can affect this probability. Some are well known and discussed in the literature, such as the 51 per cent attack.

[23] There were earlier, less successful tries to establish permissionless ledgers, e.g., bit-gold.

The first major challenge is the gateway problem: the information about the underlying assets needs to enter the blockchain in the first place. For example, suppose we want to use a blockchain to record and transfer land-ownership titles. To initiate this process, a *gateway* needs to attest that a specific plot of land exists and to assign it to an initial owner. Whether the gateway is an individual, an institution or a consortium, it needs to be a trusted third party for subsequent users of the blockchain. Importantly, Bitcoin does not need a gateway. Since the Bitcoin currency is native to its blockchain, all bitcoins are created on the blockchain automatically and can then be transferred as per the Bitcoin protocol.[24]

The second major challenge is assuring immutability of the ledger without a native currency. It is important to remember that Bitcoin's virtual immutability comes not only from encryption but also from the incentives embedded in the system. What makes the ledger immutable is the fact that adding a block to the blockchain is costly. A network participant (say, a Bitcoin miner) needs to expend significant resources to win the tournament (to be the quickest to find a solution to a puzzle), which awards that participant the right to add a new block of transactions to the blockchain. This cost also makes rewriting the history of the blockchain expensive, resulting in virtual immutability. The network participants are rewarded for their costly work with bitcoins.[25] Without bitcoins (or other native cryptocurrency), the network participants need to be motivated by incentives from outside of the blockchain.

In most of the currently proposed applications, both challenges have been addressed by creating closed, permissioned blockchains. This is because a blockchain without bitcoins is no longer virtually immutable without a trusted third party. In many cases, permissioned blockchains are the right tools for their purpose. We need to recognize, however, that they depart from Bitcoin's innovation. They effectively go back to the traditional concept of distributed databases. Moreover, if *permissionless* is not the goal, then we need to consider whether a blockchain, i.e., a distributed ledger of transactions, is the optimal design choice for those permissioned distributed databases. Proof-of-work is a quite inefficient consensus mechanism, not only in terms of electricity, but also in terms of speed and resilience. And maintaining the entire history of transactions consumes more memory than, for example, keeping balances.

[24] Note also that while Bitcoin is decentralized in the sense that verification and settlement of transactions occurs in a decentralized way, the issuance of bitcoins is very much centralized and controlled by the algorithm.

[25] Recently, alternative consensus mechanisms have been proposed, such as proof-of-stake. So far, they do not offer immutability with as high probability as the proof-of-work as implemented in the Bitcoin system.

We accept these inefficiencies in Bitcoin's blockchain because they allow for a *permissionless* distributed database. As we see, blockchain applied outside of Bitcoin (or other native cryptocurrency) loses its desired properties. It is no longer permissionless and immutable without the need for trusted third parties. If we accept permissioned systems, the three decades of extensive research on distributed databases in computer science offer us more efficient solutions: better consensus mechanisms and memory storage strategies. Maybe they would do a better job than blockchain.

One of the indirect effects of the blockchain revolution may be the popularization of traditional distributed databases. Distributed databases have been a vibrant research field in computer science for decades. Before Bitcoin, however, commercial and popular interest was mostly limited to back-office operations of large Internet companies, such as Facebook. The blockchain revolution has brought distributed databases to the forefront and may result in wider adoption and new ideas for their use. However, the benefits of distributed databases may be limited to very specific applications. And even in the context of these applications, while valuable, it is not clear that distributed databases would bring substantial cost savings.

The future of the blockchain revolution

Blockchain technologies will likely have a significant impact on many industries, not just finance. However, this may not happen in the way envisioned.

Computation and communication technologies have decreased the cost of experimentation and digital entrepreneurship. This resulted in a proliferation of start-ups, creating competitive pressure and exposing inefficiencies in existing (legacy) systems. Both new and existing players are looking with interest at the properties of smart contracts and Bitcoin's blockchain. But as they realize the benefits of different aspects of the system, it may turn out that new encryption tools and smart contracts have large and clear benefits, while distributed ledgers may have a more limited appeal. And for many applications, the most suitable will be the traditional distributed database rather than one based on Bitcoin's blockchain.

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.