Blockchain Revolution without the Blockchain

Hanna Halaburda

Bank of Canada* & NYU–Stern

July 3, 2017

Blockchain — "the technology behind Bitcoin" — has attracted a lot of attention, perhaps somewhat comparably to that devoted to the Internet at the time of the dot-com boom. Many are excited about this new technology based on 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 that 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,[1] or on how it may fail. This 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-related startups. It also shows up in estimates quoted in the media that indicate large cost savings — without offering much detail about how those savings would occur.

As we show here, 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. We analyze them separately and argue that most of the proposed benefits come from encryption and smart contracts. But encryption and smart

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

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

contracts do not need blockchain.

So, while the wave of excitement may facilitate adoption of new IT 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 will grow from $210 million in 2016 to over $2 billion by 2021.[2] Blockchain technologies are expected to change the face of the financial industry, supply chains, government record-keeping, and many other areas. The revolution is buoyed by a few forces, of which the most significant is the expectation of substantial cost savings. It is exemplified by the following quotes from *Financial Times*[3] articles on blockchain:

> *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.*[4]
>
> *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.*[5]
>
> *The technology — an electronic ledger with records stored in "blocks" — aims to automate the complex networks of trust and verification on which modern fi-*

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

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

[4] "Trafigura tests blockchain for settling US oil market deals," by Gregory Meyer and Neil Hume, March 27, 2017.

[5] "Blockchain believers hold fast to a utopian vision," by Jane Wild, January 27, 2017.

nance 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. A shared ledger is supposed to contribute to cost savings because blockchain is expected to operate without a trusted third party, and therefore leads to elimination of intermediaries.

However, such statements about the benefits of blockchain seem to confuse at least three different concepts: (1) encryption; (2) automated execution of transactions ("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 "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?

The source of confusion around blockchain can be traced to the origin of the term. The term "blockchain" was introduced as a shorthand for "chain of blocks of transactions," which was part of the Bitcoin system. Therefore, in the Bitcoin context it meant a "distributed ledger

[6] "Blockchain consortium raises record $100m," by Phillip Stafford, May 23, 2017.

[7] There are also additional expected benefits, e.g., public data and time-stamping of transactions.

[8] 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." "Ledger of balances" wouldn't really 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.

of transactions." 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 that there has been no 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).

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 in reality they come from a combination of technology and an incentive system that accounts for the behavior of human participants. Yes, Bitcoin system uses cryptographic tools: public-private key encryption, hashing algorithms. But the reason why the system is virtually immutable[11] is because it is too costly to "rewrite the history."[12]

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. This gave rise to 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.[13] 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.

[10]While there have been thefts of large sums of bitcoins, e.g., Mt.Gox, none of them occurred by falsifying the blockchain. The difference is akin to the difference between 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."

[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. Exactly this cost also makes changing blockchain's history prohibitively costly. Changing this feature, while leaving all the cryptography in place, could jeopardize the safety of the blockchain in the absence of a trusted third party.

[13]See www.ethereum.org

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?

One could say that the broadening meaning of "blockchain" simply reflects the evolution of a term in a living language; that initially "blockchain" meant only a distributed ledger, but now the use of the term has evolved, and its meaning includes also smart contracts and encryption. However, precision matters for estimating costs and benefits, or even predicting the best uses of blockchain technologies. The three different aspects — 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.

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.

The term "smart contracts," and the car example, come from Nick Szabo's 1997 article, published 15 years before Bitcoin and the Bitcoin's blockchain. Some media outlets state that "through blockchain technology, smart contracts are now a reality".[14] However, smart contracts were a reality long before. An automated recurring payment that someone sets up with his or her 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 if the contracts are with the bank, or a platform dedicated to

[14]See, e.g., https://btcmanager.com/a-cost-benefit-analysis-of-using-smart-contracts-in-banking/

smart contracts that could be used by independent individuals.

Other significant cost savings may come from improved encryption, which results in increased security of the system. Currently, encryption is underutilized in business practice. For example, the public-private key encryption is typically used for the log-in process into a business's IT system, but once users are admitted into the system, there is some, but little protection. Often, information is encrypted on particular drives inside companies.

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

Serious efforts in this direction have been already undertaken by the industry's heavyweights, as stated by R.Martin Chavez, the CFO 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.*[15]

This essentially describes a paradigm shift in the approach to cyber security, and we should pay attention to it. Given large sums currently spent in relation to fraud and hacking, this shift has a potential for significant cost savings. A 2016 study on large companies estimated that cybercrime costs the average large American company $17 million. The global average is $9.5 million.[16] However, it is doubtful that we need blockchain to get the benefits of encryption and trigger the cost savings.[17]

[15] At Symposium "Data, Dollars and Algorithms" at Harvard University, January 19, 2017, available at https://www.youtube.com/watch?v=VF6DrX9H0Ug

[16] *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 in US was $15 million, and $8 million globally.

[17] Goldman Sachs? solutions described in Chavez's quote do not rely on blockchain.

What are the benefits of blockchain?

What about the benefits of a distributed ledger, i.e., 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.[18] 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 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.

But proponents of blockchain technologies expect more from the new technology than just distributed ledger. And these expectations come from the experience with Bitcoin. By looking at Bitcoin's blockchain and the fact that it has not suffered a breach since its inception, the pundits infer that blockchain by its nature offers added security benefits beyond encryption. Moreover, they also 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.[19]

Distributed ledgers are a special case of distributed databases. They have been known, and used, for three decades. But it was only Bitcoin that allowed for a permissionless distributed ledger, while distributed databases before were permissioned and required a third party to manage the permissions and help maintain the database.[20] 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

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

[19]Security of the ledger is not guaranteed. However, the probability of a failure is pushed so low that it is considered secured 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% attack.

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

safe blockchain to transfer assets other than the native cryptocurrency (say, bitcoins for the Bitcoin blockchain).

The first major issue 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 someone, a gateway, needs to attest that a particular 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 the subsequent users of the blockchain. Importantly, the gateway problem is not an issue for Bitcoin. 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.[21]

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 costly, and results in virtual immutability. The nodes are rewarded for their costly work with bitcoins.[22] Without bitcoins (or other native cryptocurrency), the nodes need to be motivated by incentives from outside of the blockchain.

In most of the currently proposed applications, both these issues have been addressed by creating closed, permissioned blockchains. 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. We need to recognize, however, that they depart from Bitcoin's innovation. They effectively go back to the traditional distributed

[21]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.

[22]Recently, there have been alternative consensus mechanisms proposed, like proof-of-stake. So far, they do not offer immutability with as high probability as the proof-of-work combined with adjustable puzzle difficulty, as it is implemented in the Bitcoin system.

databases. Moreover, if "permissionless" is not the goal, then we need to wonder whether a blockchain, i.e., distributed ledger of transactions, is the optimal 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 resiliency. And keeping the whole history of transactions is more memory consuming than, e.g., keeping balances.

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

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

The future of the blockchain revolution

I expect that 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.

What we see is that computation and communication technologies have decreased the cost of experimentation and digital entrepreneurship. This resulted in a proliferation of start-ups, which both create competitive pressure and expose inefficiencies of existing (legacy) systems. 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. 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.