To Blockchain or Not to Blockchain: That Is the Question

Valentina Gatteschi
Politecnico di Torino

Fabrizio Lamberti
Politecnico di Torino

Claudio Demartini
Politecnico di Torino

Chiara Pranteda
Reale Group

Víctor Santamaría
Reale Group

Blockchain has been considered a breakthrough technology—but does your company need it? In this article, the authors discuss the advantages and disadvantages of blockchain technology using examples from the insurance sector, which can be generalized and applied to other sectors.

A blockchain is a public ledger distributed over a network that records transactions (messages sent from one network node to another) executed among network participants. Each transaction is verified by network nodes according to a majority consensus mechanism before being added to the blockchain. Recorded information cannot be changed or erased and the history of each transaction can be re-created at any time.

Blockchain is receiving ever-increasing attention, with about $300 million invested in 2016. Early adopters consider it a breakthrough technology that could change many everyday activities and business processes in different application domains. For instance, it could be used to record election votes, ensuring transparency. Given its transnational scope, it could be used to track tangible luxury items, intellectual property rights, and so on.

According to Gartner's hype cycle, blockchain is currently reaching the "peak of inflated expectations," meaning that the potential of this technology could have been overestimated.[1] Companies could find it difficult to objectively judge its advantages and disadvantages, and to evaluate potential opportunities.

In this article, we take the point of view of IT professionals deciding whether their business could benefit from the adoption of blockchain, and try to identify the information required for an effective decision.

Although part of the discussion will be about generic business opportunities and technical aspects (see the "How Blockchain Works" sidebar), we will focus on a specific application domain—the insurance sector. Motivations for this are twofold. First, based on the insurance hype cycle,[2] blockchain technology is still in the initial part of the curve that connects "technology

Published by the IEEE Computer Society
1520-9202/18/$33.00 ©2018 IEEE

trigger" with "peak of inflated expectations," showing that there is room for innovation. Second, insurance market characteristics (services offered, processes implemented, customers served, and so on) make blockchain adoption a particularly controversial matter because it is not clear yet whether it will be worth the investment. Exploration has just started with the creation of B3i, the first blockchain-centered insurance consortium.[3]

Despite the focus on the insurance sector, our observations and conclusions will be easy to generalize and could help professionals deal with issues in other application domains.

SIDEBAR: HOW BLOCKCHAIN WORKS

Blockchain technology is sometimes represented as a long DNA chain, periodically increasing in size when information related to new transactions is added. Transactions are grouped in blocks (where the name "blockchain" comes from), which are sorted in a sequential way with each block linked to the previous one. The chain is maintained by a network of nodes, which verify the validity of transactions and add them to new blocks in a process called *mining*.

Blockchain technology is sometimes represented as a long DNA chain, periodically increasing in size when information related to new transactions is added.

To better understand how blockchain works, consider the example shown in Figure 1. Alice wants to transfer a given amount of cryptocurrency to John (cryptocurrency could be replaced by another asset with a digital counterpart). Cryptocurrency is stored in a digital wallet, which is identified by an address. To make the transfer, Alice specifies the desired amount to be transferred and the address of John's wallet. Then she broadcasts the transaction to the network. The transaction is digitally signed using secret information stored in the wallet, ensuring that it actually comes from Alice's wallet and that it cannot be altered by someone else.

Other network nodes check whether the transaction has been actually authorized by Alice by analyzing the digital signature. Then they verify if she is entitled to spend the money by computing her balance on a local copy of the blockchain (which stores all the transactions on the network, including transfers to and from her wallet). If the transfer can be made, the nodes insert the transaction in a new block.

The new block contains a list of all the transactions to be validated, and records in its header a summary of them (the *hash*, a mathematical function that maps a given set of data to a fixed-size sequence of symbols) as well as of the previous block header.

To add the newly created block to the blockchain, nodes start the mining process—a competition in which the nodes have to solve a complex mathematical problem. This process, referred to as *proof of work*, requires nodes to find a random value that, combined with the hash of transactions and of the previous block header, produces a given result. When a node identifies a possible solution, it broadcasts the result to the others nodes, which check it. If the majority of the nodes agree on the result, the block is considered valid and it is added to the blockchain, making each node update its local copy (the winner could also receive a reward; for example, in the form of a transaction fee). As a result of the mining process, John will see that the amount sent by Alice has been received in his wallet.

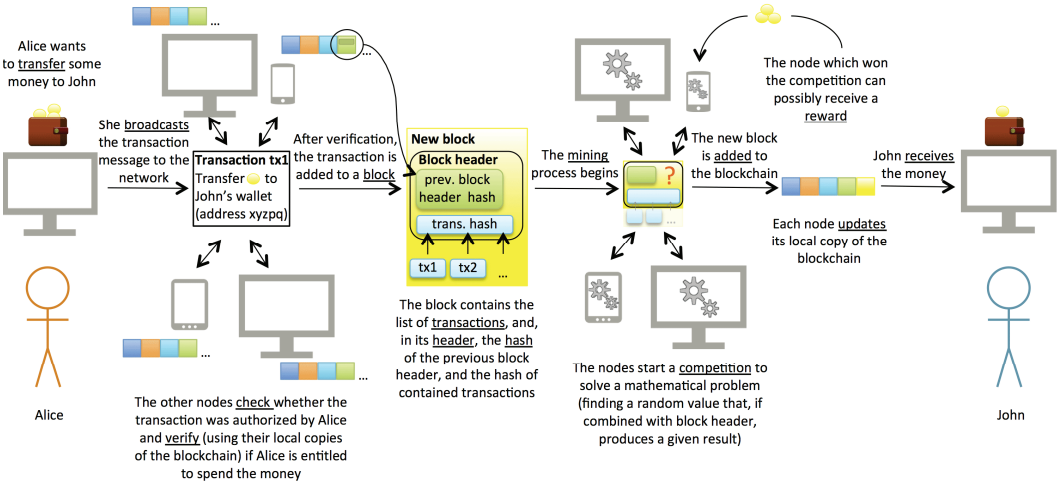

Figure 1. How blockchain transactions are recorded.

Such a complex validation mechanism makes it nearly impossible for a node to control the majority of the network, as it would require extremely high computational power to create a false block, solve the mathematical problem before other nodes, and reach the 51 percent consensus on the just-mined block. Moreover, the fact that each validated block contains a reference to the previous block (secured using cryptography methods) prevents malicious modifications to recorded transactions. In fact, changing a transaction would also imply modifying the summary of the block containing it and of the blocks that follow.

BLOCKCHAIN EVOLUTION AND POTENTIAL APPLICATIONS

Blockchain technology was conceived in 2008 to record Bitcoin (http://bitcoin.org) transactions in an immutable and publicly verifiable way. Bitcoin was the first prototype of cryptocurrency and was invented to enable money transfers between parties without relying on intermediaries.

As time passed, new application scenarios were identified (Table 1 includes a comprehensive list of potential applications) and numerous prototypes were developed, going far beyond money transfer[4] (see the "Existing Blockchain-Based Applications and Prototypes" sidebar).

Three different blockchain evolutions can be identified: Blockchain 1.0, 2.0, and 3.0.[5] Blockchain 1.0 is strongly related to Bitcoin and cryptocurrencies.[6] Since the birth of Bitcoin, more than 600 cryptocurrencies have been created (which usually act as exchange tokens for blockchain-based applications). The most famous ones (based on market capitalization data) are Ethereum (a well-known alternative to Bitcoin providing a framework to easily create blockchain-based applications; www.ethereum.org), Monero (guarantees untraceability of transactions; http://getmonero.org), and Ripple (enables instant payments, especially for bank transfers; http://ripple.com).

If the focus of Blockchain 1.0 is money, Blockchain 2.0 is about registering, confirming, and transferring contracts or properties. Application fields range from the use of blockchain as a decentralized copy of local databases (especially for public records and attestations) to more sophisticated applications.

The most relevant feature of Blockchain 2.0 is the integration with *smart contracts* (initially provided only by Ethereum and currently under development for Bitcoin). Smart contracts are pieces of code stored on the blockchain that are programmed to behave in a given manner when certain conditions are met. They can be executed automatically without control of a third party. For example, should a will be encoded in the blockchain, a smart contract could automatically transfer assets to the beneficiary in the case of the testator's death.

To gather information their activation conditions are based upon, smart contracts rely on oracles—off-chain services taking data from the real world and pushing them to the blockchain. Applications of smart contracts could be used in blockchain-based crowdfunding campaigns to automatically trigger payments when the goal is reached; they could automatize betting systems, allowing people to bet on events and transferring money to winners; or they could be used in conjunction with Internet of Things devices[7] to automatically unlock intelligent hotel room locks after payment.

In Blockchain 3.0, the application field is no longer restricted to finance and goods transactions, but embraces sectors like government, health, science, and education.

Smart contracts could enable the creation of new kinds of organizations, such as decentralized autonomous organizations (DAOs), by encoding the rules for making decisions and managing groups of people.

In Blockchain 3.0, the application field is no longer restricted to finance and goods transactions, but embraces sectors like government, health, science, education, and more.

For government use, blockchain can be used to record election votes in an immutable and publicly verifiable way, thus increasing transparency. It could also support personalized governance systems, where citizens pay only for services they actually use. Blockchain can also be used to publish a politician's program, providing everyone access to the program and allowing them to verify whether promises have been kept.

The immutability of blockchain could also become an advantage in countries where censorship is a praxis, as people could publish their thoughts on the blockchain without anyone deleting or changing the text (although new ways of censoring content could be developed; for example, by creating thousands of new posts to hide inconvenient ones).

Blockchain could also help people improve their lives in other contexts, such as health and science. It could be used to record genomic data (whose access is forbidden in many countries) and make this information accessible to the owners. This could help people change their lifestyle—for example, if a predisposition to a given disease is found. Furthermore, researchers could gain access to a wide ledger of health data recorded during examinations or treatments, or through personal activity trackers.

In the education domain, smart contracts could manage financial endowments; for example, enabling money transfers only when students have successfully passed a learning module's final exam. They could also record students' achievements, ensuring transparency in mobility contexts or in the job-seeking and hiring processes.

In the industrial context, blockchain could be integrated with big data technologies to create predictive-reactive systems, gathering and storing huge amounts of information to be processed later and making it actionable by combining the power of artificial intelligence and smart contracts.

Table 1. Blockchain applications. Groupings are based on assets exchanged.[5,8]

Type	Applications
General	Escrow transactions, bonded contracts, third-party arbitration, multiparty signature transactions
Financial transactions	Currencies, stocks, private/public equities, crowdfunds, bonds, mutual funds, derivatives, annuities, pensions, insurance policies, trading/spending records, microfinance, charity donations, air miles

Public records	Land/property titles, vehicle registration, business licenses, business ownership/incorporation/dissolution records, criminal/court/government records, marriage/birth/death certificates, voting IDs, health/safety inspections, shipping/satellite registries, building/gun permits, forensic evidence
Semi-public records	Degrees/certifications/learning outcomes/grades, human resources/medical/delivery records, genome data
Private records	IOUs, loans, contracts, bets, signatures, wills, trusts
Identification	Driver's licenses, identity cards, passports, voter registrations
Attestation	Proof of insurance/ownership, notarized documents
Physical asset keys	Digital keys for homes/hotel rooms, rental/leased cars, lockers, mail boxes, Internet of Things devices
Intangible assets	Patents, trademarks, copyrights, reservations, domain names, digital rights, proof of authenticity/authorship, licenses, domain names, online identities
Other records	Cultural/historical events, documentaries, data (weather, temperature, traffic, sports scores)

SIDEBAR: EXISTING BLOCKCHAIN-BASED APPLICATIONS AND PROTOTYPES

A number of blockchain-based applications already exist in different sectors and contexts. Some are still only a prototype, whereas others are available to the wider public. Here we provide an overview of solutions developed so far for each sector.

Personal data management. In general, applications in this area use a blockchain wallet to recognize a user's identity. Their advantage is that users could log in with a unique identifier, instead of using traditional credentials (http://bitid.bitcoin.blue). In addition, users' digital identity could be validated once by certified organizations and then used multiple times, freeing users from the need to share their IDs and personal information when they have to open bank accounts, undersign policies, and so on (https://kyc-chain.com).

Intellectual property. Such systems generally rely on blockchain to store the hash of a document, together with its timestamp, to prove its existence and authorship (http://proofofexistence.com; http://virtual-notary.org). Some platforms also allow authors to license their work (http://ascribe.io) and to receive automatic payments triggered by smart contracts when others access it (http://monegraph.com; http://ujomusic.com).

Finance, trading, and betting. A number of financial companies are carrying out investments to include blockchain in their applications and allow users to pay in cryptocurrencies. For instance,

NASDAQ widely invested in blockchain technology to reduce costs in shares management, and created a partnership with Chain (http://chain.com) to develop a protocol for financial networks to store information on shares issued or exchanged. Several banks recently adopted Ripple to manage real-time international payments.[9] Smart contracts are also largely used in online lotteries, as they could assure the winner that he or she will actually get the prize (http://lastis.me; http://etherpot.github.io). Other systems adopt a similar approach, but aim to collect people's binary predictions about future occurrences (http://augur.net; http://gnosis.pm). If a user's prediction is correct, they will receive a reward.

Software and the Internet. Blockchain could be used to record system logs, making it impossible for attackers to delete or alter events' histories (www.reply.com/en/content/securechain). Other applications encompass the use of blockchain for cloud storage. Generally, such applications record portions of files in a node's hard drive and automatically reward the node on the basis of loaned space (http://storj.io; http://ipfs.io; http://maidsafe.net). To avoid storing duplicates, each time a new resource is uploaded, a comparison with its hash and one of the already-stored resources is performed. Domain names have been also stored on the blockchain. Here, the objective is to replace DNS servers with a blockchain-based one, where users could automatically register a domain paying with cryptocurrencies (http://namecoin.org; http://blockstack.org). Other blockchain uses are related to reducing censorship by storing contents produced by users (http://gist.github.com/metacoin/10dea79e15294950c8c3), or to reward producers based on readers' votes (www.thankscoin.org).

Government. Blockchain could be used for gathering citizens' votes in a transparent and publicly verifiable way (www.reply.com/en/content/ballotchain). A vote could be represented as a small transfer of a cryptocurrency (or equivalent) from the voter's wallet to the candidate's one. In this way, votes could be cast on any device (computers, tablets, mobile phones, or multimedia totems) while guaranteeing anonymity, uniqueness, and immutability.

Blockchain could be used to record system logs, making it impossible for attackers to delete or alter events' histories.

Commerce and supply chain. This sector is among those receiving the greatest attention and investment, as it could benefit from using blockchain to support the identification of counterfeit items. Applications range from the exchange of sports and music tickets (www.reply.com/en/content/blockchain-ticketing-solution-cloudchain) to merchandise, products, and subscriptions, as well as more costly goods such as cars (www.reply.com/en/content/thats-mine). In the luxury goods market, blockchain has been used as a worldwide ledger for diamonds and their ownership (http://everledger.io), or to trace and locate goods along the supply chain (http://blockverify.io). Other applications use blockchain to improve the supply chain. This is the case with Provenance (www.provenance.org), which uses blockchain to enable food traceability. Finally, ambitious projects such as Profeth (http://profeth.org) propose to use blockchain and smart contracts to embed intelligence in the supply chain and allow direct exchange of goods and services without requiring a monetary system.

Services. Some initiatives propose to include cryptocurrency payments or blockchain-based storage of transactions in existing services. This is the case with La'Zooz (http://lazooz.org), a blockchain-based Uber-like platform.

Internet of Things. This is another promising field for blockchain technology. Here, blockchain has been used to support interoperability between devices, certifying that messages received by a device have been sent by a trusted one (www.reply.com/en/content/blokcom; www.reply.com/en/content/authentichain). Other prototypes have proposed scenarios where blockchain could enable intelligent washing machines to autonomously order detergent when needed or ask for maintenance in case of failures.[10] Another innovative solution is Slock.it (https://slock.it), which proposes a blockchain-based room-renting system that uses intelligent lockers that enable access only to those with a valid reservation. The Slock.it team is also involved in another project called Blockcharge, which relies on blockchain to enable electricity sharing (for example, to charge electric vehicles). Finally, Lo3Energy (https://lo3energy.com) proposes an application for

peer-to-peer home-produced energy trading, where households could sell generated electricity to neighbors without having to rely on a third party.

Healthcare. In the healthcare sector, blockchain-based solutions are used to collect vital data and location information and to send alerts in case of danger. The advantage of relying on blockchain technology is a guarantee that the system will not stop working.

ADVANTAGES AND DISADVANTAGES OF BLOCKCHAIN

Table 1 shows that the potential for blockchain applications is enormous and heterogeneous. However, some experts have claimed that blockchain technology is overhyped,[11] not mature yet,[12] or applied to use cases that could be addressed with already-mastered technologies.[13]

Those who wish to invest in this technology should point to unresolved problems and new needs, and be aware that blockchain is not the optimal solution a priori, as its advantages vary from sector to sector and from one use case to another. Blockchain also presents some drawbacks,[14] which should be carefully evaluated before deciding to adopt it.

Here, we summarize the main advantages and disadvantages of blockchain. Because we have already discussed blockchain's potential, we briefly review the advantages and discuss the disadvantages in more detail.

Advantages

- Implements a shared repository that is maintained by peers—everyone can access data and view transactions. Moreover, storing information on nodes prevents data loss in case of unexpected events.
- Provides trust between parties. Digital signature and validation ensure that every node and user behaves correctly, without needing intermediaries.
- Could become a worldwide data repository accessed by different actors. Everyone can potentially read/write on it.
- Transparency is guaranteed. Everyone could read not only the final state of transactions, but also the history of passed states.
- Immutability. Data cannot be erased or changed.
- Decentralization. It can run without a central authority and cannot be controlled, censored, or shut down.
- Automation. With smart contracts, activities could be automatized.

Disadvantages

- Characterized by high power consumption. A Bitcoin transaction could cost $6 when considering the energy consumed by network nodes.[15]
- Mining requires expensive hardware, and the majority of computing power is wasted. Mining blocks is a competition among nodes where only the quickest wins—the others are just wasting resources. To increase the probability of winning, nodes could join mining pools and collaborate with other nodes, sharing revenues. A solution to reduce the amount of necessary computing power could be to change the mining process from proof of work to *proof of stake*, where nodes can purchase the opportunity to mine using tokens, and mining power is proportional to the number of tokens owned. This way, mining would be less resource intensive but would be restricted to token holders.
- Data replication requires space. Local copies of the blockchain (hence, of all transactions that have occurred since its creation—about 105 Gbytes for Bitcoin and 70 Gbytes for Bitcoin and Ethereum; http://bitinfocharts.com) are stored on each network node. Performances are therefore not yet comparable with databases.

- Adding information is slow. Creating a Bitcoin block takes around 10 to 60 minutes (http://blockchain.info/charts/avg-confirmation-time). Ethereum requires 15 seconds, (http://etherscan.io/chart/blocktime), a smaller though still significant amount of time.
- Immutability and transparency could harm users' privacy and reputation. Every network node would store a copy of the blockchain and could possibly access its content.
- Smart contracts cannot rely on external APIs. Every node should be able to process previous transactions and end with the same result as the other nodes. That is, information must be immutable. Consequently, data required by a smart contract should be first injected in the blockchain. Oracles can enable this injection, but require a strong reputation system or governance mechanism and need to be as robust as the blockchain itself, not to become the weakest part of the process.
- Smart contracts can be buggy. Because their code is publicly available and they become autonomous entities once they are created, they could be "candy for hackers."[12] As they are stored on the blockchain, smart contracts cannot be modified. To remove code bugs, developers have to create new contracts and transfer all data and pointers from the old to the new ones. The most relevant case of a smart-contract-based attack happened on Ethereum in June 2016, when about $60 million was "stolen."

KEY QUESTIONS FOR BLOCKCHAIN USE

One of the most common criticisms of blockchain is that a high number of blockchain-based applications could be implemented using existing technologies, such as (properly secured) centralized databases. Experts have also identified the following key questions[11] that people evaluating the adoption of blockchain technology should answer to determine whether it is the right solution for them.

- Is it necessary to have a shared database?
- Is it necessary to have multiple parties writing data?
- Are potential writers untrusted (should writers be prevented from modifying others' previous entries)?
- Is disintermediation needed (is it necessary to remove trusted intermediaries verifying or authenticating transactions)?
- Is it necessary to see how transactions are linked to each other (should different actors independently write transactions concerning a single user)?

Should one or more of these questions receive a negative answer, blockchain technology would likely introduce overhead without bringing true benefits.

A PRACTICAL CASE STUDY: THE INSURANCE SECTOR

The insurance sector has recently showed high interest in blockchain. Some large companies have made significant investments to explore its potential for their business16 and consultancy firms have investigated its applicability to the insurance sector.[17–19]

Applications of Blockchain

Here we describe five envisioned applications for the insurance sector.

Using smart contracts to improve customer experience and lower operating costs

The self-executing ability of smart contracts could speed up claims processing (clients would receive their money even before they claim it because a smart contract could automatically trigger a reimbursement as soon as a given event occurs) and reduce human effort. For instance, car

insurance smart contracts could be programmed to transfer money only if customers repair the car at certified mechanics.

In farming insurance, where farmers undersign policies against the consequences of bad weather, smart contracts could read weather data feeds and, in the case of persistently adverse conditions, authorize the reimbursement.

Another example is delay insurance, where smart contracts could automatically refund travelers when their flight or train has been delayed (http://insureth.mkvd.net).

Smart contracts could be used in combination with the IoT for home insurance. For example, automatic reimbursements could be triggered in case of damage to a roof equipped with sensors.

An additional advantage of smart contracts is that they can make ambiguities possibly affecting traditional text-based contracts disappear, as all their clauses would be hard-coded. This can increase transparency and lower the frequency and impact of legal disputes.

Fraud prevention

Shared blockchain-recording policies undersigned on a worldwide basis[17] together with data possibly coming from other domains (medical reports, police reports, and so on) can help identify fraud during claims processing.

Data entry/identity verification

Blockchain-based identity verification systems could reduce customers' data-entry overload while undersigning or renewing policies. Customers should first undergo an identification process where their ID is checked by certified intermediaries and linked to their wallets. Then, smart contracts could automatically retrieve IDs and check them. In a more sophisticated scenario (assuming a wide adoption of blockchain by different actors), additional information could be stored (such as health examinations, asset ownership, and so on), and gathered by smart contracts for automatic and precise premium computations (www.reply.com/en/content/insurechain).

Pay-per-use insurance

Smart contracts could enable pay-per-use insurance policies, relying on the IoT for automatic undersigning. Travel insurance premiums could be collected only if customers' GPS coordinates (collected by their smartphone) confirm they are abroad. Similarly, car insurance premiums could be paid only when customers are driving.

Peer-to-peer insurance

Peer-to-peer insurance is not a new idea (services like insPeer, Friendsurance, and heyguevara.com appeared a few years ago). Nonetheless, smart contracts could provide innovation in this field because they could allow the creation of DAOs, whose functioning rules are hard-coded. With DAOs, insurer groups would be able to manage themselves.

Answers to the Key Questions

Here, we analyze each of the five application scenarios using the key questions listed previously to determine whether blockchain is needed (findings are summarized in Table 2).

Using smart contracts to improve customer experience and lower operating costs

Data is collected from multiple actors and sources. The need for a shared database depends on the single application: for car repairs, for example, a shared database written by mechanics and

checked by the company is probably required. However, we could assume that the company and certified mechanics undersigned an agreement and that there is trust between the parties. Documents sent by uncertified mechanics would be manually processed. In other cases, the company could rely on external APIs to retrieve the desired information from online services or sensors and update the database accordingly.

Disintermediation is a controversial matter—in claims processing, insurance companies actually act as intermediaries, reconciling policy data with damage evaluation. Furthermore, a significant number of claims probably could not be automatically processed because they would still need to be evaluated by assessors before being settled. The need for disintermediation could arise when damages could be automatically evaluated (for example, by means of IoT technologies) or when the customer does not trust the company. In developed countries, the behavior of insurance companies is defined by several regulations aimed at ensuring trust. Hence, disintermediation would not be a sensible need. In some cases, the necessity to retrieve all the transactions or events linked to a policy or person could arise (for example, for customer relationship management). This operation, however, could be performed through traditional systems.

Fraud prevention

A shared database written by multiple parties (such as doctors and police officers) could be helpful. Inserted data should not be modified by other parties and should be linked to the customer's digital identity. Even though trusted intermediaries could guarantee the truthfulness of recorded information, their presence will increase costs. Hence, disintermediation could be preferred. Consequently, it appears that this use case could benefit from blockchain. Nonetheless, some issues should be considered. First, a critical mass would be required because a great amount of data would be inserted by different actors. Secondly, measures to ensure data privacy should be adopted. Finally, because blockchain data cannot be changed, error management systems should be put in place.

Data entry/identity verification

Similar to fraud prevention, a shared ledger would be needed to record customers' documents, proof of ownership, and so on, and to link them to their digital identity. Writers should be prevented from modifying information previously inserted by others. As with fraud prevention, disintermediation could lower costs. Blockchain could be a good solution that enables information writing and sharing, provided that the previously mentioned issues are properly addressed.

Pay-per-use insurance

Blockchain could be used to certify if or when customers activated a policy. Multiple writers (the company and its customers) would write data on a shared database and would need the guarantee that policy data could not be modified. Disintermediation seems less relevant because only two actors are involved (customers and insurance companies) and because insurance companies already act as intermediaries. Similarly, companies already store information concerning customers' previous transactions, making linked transactions not as paramount as other requirements. It appears that in this use case, blockchain would not be as disruptive as in the previous two scenarios. To support this thesis, it should be mentioned that in numerous countries, trust between customers and insurance companies is already ensured by regulations, removing the need to rely on a trusted third party. However, because future blockchain technology will be increasingly advertised by mass media, having blockchain-based pay-per-use insurance could be a competitive advantage. This could increase further should customers be allowed to pay in Bitcoin or other cryptocurrencies.

Peer-to-peer insurance

This scenario requires disintermediation, and smart contracts could manage interactions between multiple untrusted parties writing a shared database. It would also benefit from linked transactions—for example, for customers' identity verification or claims recording. Thus, relying on blockchain could be a good choice. Nonetheless, peer-to-peer insurance aims to remove intermediaries. Consequently, the diffusion of DAO-based insurance could represent a significant threat to traditional businesses.

Table 2. Analysis of use cases with regard to the five key questions (+: positive answer, −: negative answer, +/−: both answers could apply, depending on the context).

	Shared database	Multiple writers	Untrusted writers	Disintermediation	Linked transactions
Improving customer experience and lowering operating costs	+/−	+/−	+/−	+/−	+/−
Fraud prevention	+	+	+	+	+
Data entry/identity verification	+	+	+	+	+
Pay-per-use insurance	+/−	+/−	+/−	−	−
Peer-to-peer insurance	+	+	+	+	+

DISCUSSION

Our analysis shows that some but not all insurance use cases could benefit from the adoption of blockchain. Should insurance companies adopt it, they could probably start by using it for easing data entry and customer identity verification. In fact, even though this scenario would require several actors inserting information in the blockchain, the number of involved parties would be lower than in other scenarios. Moreover, banks (which have already made important investments in blockchain) could be interested in developing or maintaining a shared ledger. Insurance companies and banks might rely on existing applications to reduce initial investments.

Afterward, efforts could be devoted to develop blockchain-based fraud-prevention systems. This would be a long-term high-risk investment because in order to succeed, it would require the involvement of numerous actors and the definition of standards to store information. Initially, insurance companies could store policies and claims linked to customers' digital identities on a worldwide basis, thus reducing information asymmetries in customer acquisition. Then, other actors could be gradually involved.

Companies could then invest in creating the blockchain-based infrastructure for peer-to-peer insurance, turning a potential threat into a business opportunity (for example, a cost could be charged for each undersigned policy). In this respect, market surveys found that numerous customers still consider personal interaction with intermediaries important.[20] So, the shift to peer-to-peer insurance is probably not imminent.

Using blockchain and smart contracts for lowering operating costs, improving customer experience, and increasing transparency could be a key choice should a company want to address new

emerging markets (where a mechanism of trust is not yet fully established), or in micro-insurance contexts (not viable in the past because of human-intensive administrative processes and high fees for small payments, also enabled by blockchain). Nonetheless, companies should consider that in several cases, manual claims assessment and processing would still be needed.

Finally, in pay-per-use insurance, blockchain could provide a proof of policy undersigning. However, in this respect, interested investors should first verify the national rules for pay-per-use insurance—for example, is a signed document required? If so, a change in national rules would be required. In addition, if the company is a trusted one, other mechanisms could be used to ensure that a policy has been undersigned.

CONCLUSION

While blockchain can bring innovation in many sectors—and despite the enthusiasm for this technology—it should not be considered as a "magic bullet." Rather, its adoption should be carefully evaluated depending on a company's sector and business goals.

Although we evaluated a specific domain, our analysis could easily be extended to other scenarios sharing comparable use cases, thus helping professionals make decisions in different contexts and sectors.

REFERENCES

1. "Gartner: Blockchain and Connected Home are Almost at the Peak of the Hype Cycle," *PR Wire*, blog, 2016; https://prwire.com.au/pr/62010/gartner-blockchain-and-connected-home-are-almost-at-the-peak-of-the-hype-cycle.
2. S. Gilbert, "The Hype Cycle of Insurance Disruption," *InsuranceThoughtLeadership.com*, blog, 2016; http://insurancethoughtleadership.com/the-hype-cycle-of-insurance-disruption.
3. S. Higgins, "European Insurance Firms Launch New Blockchain Consortium," *Coindesk*, blog, 2016; www.coindesk.com/europe-insurance-blockchain-consortium.
4. G. Hurlburt, "Might the Blockchain Outlive Bitcoin?," *IT Professional*, vol. 18, no. 2, 2016, pp. 12–16.
5. M. Swan, *Blockchain: Blueprint for a New Economy*, vol. 3, no. 3, O'Reilly Media, 2015, pp. 38–69.
6. F. Tschorsch and B. Scheuermann, "Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies," *IEEE Communications Surveys Tutorials*, vol. 18, no. 3, 2016, pp. 2084–2123.
7. K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," *IEEE Access*, report Deloitte Report, vol. 4, 2016, pp. 2292–2303.
8. M. Mainelli and M. Smith, "Sharing Ledgers for Sharing Economies: An Exploration of Mutual Distributed Ledgers (aka Blockchain Technology)," *J. Financial Perspectives*, report, vol. 3, no. 3, McKinsey & Company Report, 2015, pp. 38–69.
9. A. Jarrett, "Ripple and R3 Team Up with 12 Banks to Trial XRP for Cross-Border Payments," *Ripple*, blog, Ripple, 2016; https://ripple.com/insights/ripple-and-r3-team-up-with-12-banks-to-trial-xrp-for-cross-border-payments.
10. S. Higgins, "IBM Reveals Proof of Concept for Blockchain-Powered Internet of Things," *Coindesk*, blog, 2015; www.coindesk.com/ibm-reveals-proof-concept-blockchain-powered-internet-things.
11. G. Greenspan, "Avoiding the Pointless Blockchain Project," *MultiChain*, blog, 2015; www.multichain.com/blog/2015/11/avoiding-pointless-blockchain-project.
12. F. Zaninotto, "The Blockchain Explained to Web Developers, Part 3: The Truth," *Marmelab*, blog, 2016; https://marmelab.com/blog/2016/06/14/blockchain-for-web-developers-the-truth.html.
13. A. Cooper, "Does Digital Identity Need Blockchain Technology?," *Gov.UK Verify*, blog, 2016; https://identityassurance.blog.gov.uk/2016/08/15/does-digital-identity-need-blockchain-technology.

14. M. Peck, "The Blockchain Has a Dark Side," *IEEE Spectrum*, vol. 53, no. 6, 2016, pp. 12–13.
15. "Let's Quit the Blockchain Magic Talk," *ZDNet*, blog, 2016; www.zdnet.com/article/lets-quit-the-blockchain-magic-talk.
16. "The March of Financial Services Giants into Bitcoin and Blockchain Startups in One Chart," *CBInsights*, blog, 2017; www.cbinsights.com/research/financial-services-corporate-blockchain-investments.
17. A. Shelkovnikov, *Blockchain Applications in Insurance*, report, Deloitte, 2016; www2.deloitte.com/content/dam/Deloitte/ch/Documents/innovation/ch-en-innovation-deloitte-blockchain-app-in-insurance.pdf.
18. *Blockchain in Insurance—Opportunity or Threat?*, report, McKinsey & Company, 2016; www.mckinsey.com/industries/financial-services/our-insights/blockchain-in-insurance-opportunity-or-threat.
19. *Blockchain Technology as a Platform for Digitization—Implications for the Insurance Industry*, report, Ernst & Young, 2016; www.ey.com/Publication/vwLUAssets/EY-blockchain-technology-as-a-platform-for-digitization/$FILE/EY-blockchain-technology-as-a-platform-for-digitization.pdf.
20. *Voice of the Customer—Time for Insurers to Rethink their Relationships*, report, Ernst & Young, 2012; www.ey.com/Publication/vwLUAssets/Global_Consumer_Insurance_Survey_2012_-_The_Americas/$FILE/EY_GIR_AMERICAS_SML.pdf.

ABOUT THE AUTHORS

Valentina Gatteschi is a postdoctoral research assistant at Politecnico di Torino. Her research interests include semantic processing, intelligent systems, and human-computer interaction. Gatteschi received a PhD in computer engineering from Politecnico di Torino. Contact her at valentina.gatteschi@polito.it.

Fabrizio Lamberti is an associate professor at Politecnico di Torino. His research interests include computational intelligence, semantic processing, distributed computing, human-computer interaction, computer graphics, and visualization. Lamberti received a PhD in computer engineering from Politecnico di Torino. He serves as an Associate Editor for *IEEE Transactions on Emerging Topics in Computing* and for *IEEE Consumer Electronics Magazine*. Contact him at fabrizio.lamberti@polito.it.

Claudio Demartini is a full professor at Politecnico di Torino, where he teaches information systems and innovation and product development. His research interests include software engineering, architectures, intelligent systems, and education. He is the chair of the Control and Computer Engineering Department and a member of the Academic Senate of Politecnico di Torino. Contact him at claudio.demartini@polito.it.

Chiara Pranteda is a member of Reale Group's Innovation Team. She received a degree in physics from the University of Turin. Contact her at chiara.pranteda@realemutua.it.

Víctor Santamaría is responsible for Technology & Digital Innovation at Reale ITES, a Reale Group company. His research interests include technology and business innovation. Santamaría received a degree in mathematics from Universidad Complutense de Madrid and has completed several executive master programs at IE Business School in digital innovation and IT governance and in information systems management. Contact him at victor.santamaria@realeites.com.