To Blockchain or not to Blockchain: That is the question

!"#$%$&'()*#+*)#,*-"#$%$&'().*,&',*(/*,&0*120/,(#)*#3*,&0*()/2+')$0*')4*#,&0+*/0$,#+/*

Valentina Gatteschi[#], Fabrizio Lamberti[#], Claudio Demartini[#]
Chiara Pranteda[+], Víctor Santamaría[+]
[#] Politecnico di Torino, Dip. di Automatica e Informatica, C.so Duca degli Abruzzi 24, Torino, Italy
[+] Reale Group, Via Corte d'Appello, 11, 10122 Torino, Italy

*

5&#+,*'-/,+'$,

Blockchain technology is receiving an ever-increasing attention. In this work, we present pros and cons of this technology, by taking the point of view of (IT) professionals evaluating whether to embrace this technology or not for their business. Use cases selected from a particular domain represented by the insurance sector are analyzed, and several application guidelines that can be generalized and applied to other sectors are identified.

6078#+4/9*blockchain, bitcoin, cryptocurrency, smart contracts, insurance

:),+#42$,(#)*

A *blockchain* is a public ledger distributed over a network, recording transactions (messages sent from one network node to another) executed among network participants. Before insertion, each transaction is verified by network nodes according to a majority consensus mechanism. Recorded information cannot be changed/erased and, at whatever time, the history of each transaction can be recreated.

The blockchain is receiving an ever-increasing attention, with about $300 millions invested in 2016 (source: http://www.juniperresearch.com/press/press-releases/vc-blockchain-investments-approach-$300-millio-(2)). Early adopters consider it a breakthrough invention, which could change many everyday activities and business processes in different application domains (source: http://securities.bnpparibas.com//insights/bitcoin-and-blockchain-what-you.html). For instance, it could be used to record election votes, ensuring transparency in count operations. Similarly, given its transnational scope, it could be exploited to track tangible luxury items, intellectual property rights and so forth.

According to Gartner's hype cycle (source: http://prwire.com.au/pr/62010/gartner-blockchain-and-connected-home-are-almost-at-the-peak-of-the-hype-cycle), blockchain is currently reaching the peak of inflated expectations, meaning that the potential of this technology could have been overestimated. Companies could then find it difficult to objectively judge its pros and cons, and evaluate opportunities it could offer.

In this work we take the point of view of (IT) professionals having to decide whether their business could benefit from the adoption of this technology, and try to identify the information required for an effective choice. From this point of view, it will be also useful to consider whether their business needs to interact with new blockchain-enabled companies/ business models.

Although part of the discussion will be on generic business opportunities and technical aspects (see sidebar "How blockchain works"), we will then focus on a specific application domain, represented by the insurance sector. Motivations are twofold. First, based on the insurance hype cycle (source: http://insurancethoughtleadership.com/the-hype-cycle-of-insurance-disruption), blockchain technology is still in the initial part of the curve connecting technology trigger and peak of inflated expectations phases, showing that there is room for innovation. Second, insurance market characteristics (e.g., services offered, processes implemented, customers served, etc.) make blockchain adoption in this sector a particularly controversial matter, since it is not clear yet whether it could be worth of investments. Exploration has just started, with the creation of the first blockchain-centered insurance consortium, named B3i (http://www.coindesk.com/europe-insurance-blockchain-consortium) and participated by five big insurers and reinsurers.

Digital Object Identifier 10.1109/MITP.2017.265110355 1520-9202/$26.00 2017 IEEE

Despite the focus on a particular sector, observations made and conclusions drawn would be easy to generalize to obtain insights that could help professionals to deal with issues currently faced also in other application domains.

How blockchain works (SIDEBAR)

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

In order to better understand how blockchain works, the example illustrated in Figure 1 could be considered. 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. In order 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, thus 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 (i.e., it comes from her wallet) 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 occurred 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 so-called 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.

In order to add the newly created block to the blockchain, nodes start the mining process, a competition in which they have to solve a complex mathematical problem. The process, which is 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 as valid and it is added to the blockchain, making each node update its local copy (the winner could also receive a reward, e.g., in the form of a transaction fee). As a result of the mining process, John will see, in his wallet, that the amount sent by Alice has been received.

Figure 1. How transactions are recorded on the blockchain.

Digital Object Identifier 10.1109/MITP.2017.265110355 1520-9202/$26.00 2017 IEEE

The introduction of such a complex validation mechanism was meant to make nearly impossible for a node to control the majority of the network, since it would need an extremely high computational power to create a false block, solve the mathematical problem before other nodes, and reach the 51% of 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 imply modifying also the summary of the block containing it, and, as a consequence, of the blocks that follow.

!"#$%$&'()*0;#"2,(#)/*')4*<#,0),('"*'<<"($',(#)/*

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

As time passed, new application scenarios were identified for blockchain (Table 1 reports a comprehensive list of potential applications) and numerous prototypes, going far beyond money transfer [1], were developed (see sidebar "Existing blockchain-based applications/prototypes").

Three different evolution of the blockchain can be identified, named respectively Blockchain 1.0, 2.0 and 3.0 [2].

Blockchain 1.0 is strongly related to bitcoins and cryptocurrencies [3]. The blockchain "only" acts as the decentralized ledger recording cryptocurrency transactions. Users store their credentials in a digital *wallet*, and use them to transfer money. 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 (http://www.ethereum.org, a well-known alternative to Bitcoin providing a framework to easily create blockchain-based applications), Monero (http://getmonero.org, guaranteeing untraceability of transactions), and Ripple (http://ripple.com, enabling instant payments, especially for bank transfers).

If the focus of Blockchain 1.0 is money, Blockchain 2.0 is about registering, confirming and transferring contracts/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, currently under development for Bitcoin). Smart contracts are pieces of code, stored on the blockchain, 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, in case of testator's death a smart contract could automatically transfer assets to the beneficiary.

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 in the blockchain.

Applications of smart contracts are various: they could be exploited in blockchain-based crowdfunding campaigns to automatically trigger payments when the target is reached; they could automatize betting systems, allowing people to bet on events, using oracles to verify whether they occurred, and transferring money to winners; they could be used in conjunction with Internet of Things devices (IoT) [4], e.g., to automatically unlock intelligent hotel room locks after payment, etc.

Smart contracts could also 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 more restricted to finance and goods transactions, but embraces sectors like government, health, science, learning, etc.

Digital Object Identifier 10.1109/MITP.2017.265110355 1520-9202/$26.00 2017 IEEE

For government use, the blockchain can be used to record, in an immutable and publicly verifiable way, election votes, 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 thus 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, since people could publish their thoughts on the blockchain without having anyone deleting or changing them (even though new ways of censoring contents could be developed, e.g., by creating thousands of new posts hiding inconvenient ones).

The blockchain could also support freedom and help people improve their lives in other contexts, such as health and science. Here, it could be used to record genomic data (whose access, in many countries, is forbidden) and make them accessible to the owners. This information could help them change their life-style, e.g., if a predisposition to a given disease is found. Furthermore, researchers could gain access to a wide ledger of health data recorded during examinations/ treatments, or through personal activity trackers.

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

Finally, in the industrial context, blockchain could be integrated with Big Data technologies to create predictive-reactive systems, gathering and storing a huge amount of information to be later processed and making it actionable by combining the power of artificial intelligence and smart contracts.

Table 1. Blockchain applications, grouped based on assets exchanged (adapted from [2], [5], http://ledracapital.com/blog/2014/3/11/bitcoin-series-24-the-mega-master-blockchain-list)

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 registrations, 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 *	Proofs of insurance/ownership, notarized documents
Physical asset keys *	Digital keys for home/hotel rooms, rental/leased cars, lockers, mail boxes, IoT devices
Intangible assets *	Patents, trademarks, copyrights, reservations, domain names, digital rights (multimedia, books, etc.), proofs of authenticity/authorship, licenses, domain names, online identities
Other records*	Cultural/historical events, documentaries, (big) data (weather, temperatures, traffic, sports score)

Digital Object Identifier 10.1109/MITP.2017.265110355 1520-9202/$26.00 2017 IEEE

=>(/,()?*-"#$%$&'()@-'/04*'<<"($',(#)/A<+#,#,7<0/*B5:C=!DEF*

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

Personal data management

In general, applications in this area exploit a blockchain wallet to recognize the identity of a user. Their advantage is that the users could login with a unique identifier, instead of using traditional credentials (http://bitid.bitcoin.blue). In addition, the digital identity of users 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, e.g., to open bank accounts, undersign policies, etc. (http://kyc-chain.com).

Intellectual property

Such systems generally rely on the blockchain to store the hash of a document, together with its timestamp, in order 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/Betting

A number of financial companies are carrying out investments to include the blockchain in their applications and allow users to pay in cryptocurrencies. For instance, NASDAQ widely invested in blockchain technology with the aim to reduce costs in shares management, and created a partnership with Chain (http://chain.com) to develop a protocol for financial networks in order to store information on shares issued or exchanged. Several banks recently adopted Ripple to manage real-time international payments (http://ripple.com/insights/ripple-and-r3-team-up-with-12-banks-to-trial-xrp-for-cross-border-payments). Smart contracts are also largely used in online lotteries, since they could assure the winner that he or she will actually got the prize. Some examples are http://lastis.me and http://etherpot.github.io, or pyramid-like rewarding systems such as http://ethpyramid.tk. Other systems adopt a similar approach, but with the aim to collect people binary predictions about future occurrences (http://augur.net, http://gnosis.pm). If users' prediction is correct, they will receive a reward.

Software and internet

The blockchain could be used to record system logs, thus making impossible for attackers to delete/alter events history (http://www.reply.eu/en/content/securechain). Other applications encompass the use of the 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). In order to avoid storing duplicates, each time a new resource is uploaded, a comparison with its hash and the one of the already stored resources is performed. Domain names have been also stored on 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 reduce censorship by storing contents produced by the users (http://gist.github.com/metacoin/10dea79e15294950c8c3), or to reward producers based on readers' votes (http://thankscoin.org).

Government

The blockchain could be used for gathering, in a transparent and publicly verifiable way, citizens' votes (http://www.reply.eu/en/content/ballotchain). A vote could be represented as a small transfer of a cryptocurrency-equivalent from the voter's wallet to the candidate's one. In this way, votes could be casted on any device (computers, tablets, mobile phones or multimedia totems) still maintaining the guarantees of anonymity, uniqueness and unchangeability.

Digital Object Identifier 10.1109/MITP.2017.265110355 1520-9202/$26.00 2017 IEEE

Commerce and supply chain

This sector is among the ones receiving the greater attention and investments, since it could benefit from the possibility of using the blockchain as a mechanism to support the identification of counterfeit items. Applications range from the exchange of sport and music tickets (http://www.reply.eu/en/content/blockchain-ticketing-solution-cloudchain), to merchandise, products and subscriptions (http://angel.co/mypowers-1) as well as more costly goods, such as cars (http://www.reply.eu/en/content/thats-mine). In the luxury goods market, the blockchain has been used as a worldwide ledger of diamonds and their ownership (http://everledger.io), or to trace (and locate) goods along the supply chain (http://blockverify.io). Other applications use the blockchain to improve the supply chain. This is the case of http://eaterra.org, which aims at directly connecting food producers and consumers, or of http://www.provenance.org, which uses the blockchain to enable food traceability. Finally, ambitious projects such as http://profeth.org propose to use the blockchain and smart contracts to embed intelligence in the supply chain and to favor the match of goods and services offer and demand.

Services

Some initiatives proposed to include cryptocurrencies payments or blockchain-based storage of transactions in existing services. This is the case of http://lazooz.net, a blockchain-based Uber-like platform, or of http://askkato.com.au, a decentralized digital concierge service relying on smart contracts.

IoT

IoT 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 (http://www.reply.eu/en/content/blokcom, www.reply.eu/en/content/authentichain). Other prototypes (http://www.coindesk.com/ibm-reveals-proof-concept-blockchain-powered-internet-things) proposed scenarios where the blockchain could enable, e.g., intelligent washing machines to autonomously order detergent when needed, or ask for maintenance, in case of failures. Another innovative solution is http://slock.it, which proposes a blockchain-based renting room system based on intelligent lockers enabling access only to users with a valid reservation. Slock.it team is also involved in another project, named Blockcharge (http://youtube.com/watch?v=0A0LqJ9oYNg), which relies on blockchain to enable the sharing of electricity (e.g., to charge electric vehicles on the way). Finally, http://transactivegrid.net 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 part.

Healthcare

In the healthcare sector, blockchain-based solutions are used to collect vital data and location information and eventually send an alert in case of danger (http://github.com/mizutaka/DAERS). The advantage of relying on the blockchain is a guarantee that the system would not stop working.

D4;'),'?0/A4(/'4;'),'?0/*

By looking at Table 1, it can be observed that potential for blockchain application is enormous and heterogeneous. Notwithstanding, some experts claimed that blockchain technology is either overhyped (http://www.multichain.com/blog/2015/11/avoiding-pointless-blockchain-project), not mature yet (http://marmelab.com/blog/2016/06/14/blockchain-for-web-developers-the-truth.html), or applied to use cases that could be addressed with already-mastered technologies (http://identityassurance.blog.gov.uk/2016/08/15/does-digital-identity-need-blockchain-technology).

Those aiming 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, since advantages deriving from

Digital Object Identifier 10.1109/MITP.2017.265110355 1520-9202/$26.00 2017 IEEE

its adoption could vary from sector to sector, and from one use case to another. This technology presents also some drawbacks [6], which should be carefully evaluated before deciding to go with it.

Below, the main advantages and disadvantages of blockchain are summarized. Since potentialities have been shown already, advantages will be reviewed quickly, whereas disadvantages will be discussed more in details.

Advantages

- It implements a shared repository, maintained by peers: everyone could access data/view transactions. Moreover, being stored on nodes, it prevents data loss in case of unexpected events.
- It provides trust between parties: digital signature and validation ensure every node/user behave correctly, without the need of intermediaries.
- Everyone could potentially read/write on it: it could become a worldwide data repository, accessed by different actors.
- Everyone could read not only the final state of transactions, but also the history of passed states: transparency is guaranteed.
- It is immutable: data could not be erased/changed.
- It could run without a central authority and could not be controlled/censored/shut down.
- With smart contracts, activities could be automatized.

Disadvantages

- It is characterized by a high power consumption: a Bitcoin transaction could cost $6 when considering the energy consumed by network nodes (http://www.zdnet.com/article/lets-quit-the-blockchain-magic-talk).
- Mining, i.e., the act of adding new transactions to the blockchain, 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 just wasted resources. To increase probability to win, nodes could join mining pools and collaborate with other nodes, sharing revenues. A solution to reduce the amount of computing power needed could be to change the mining process from *proof-of-work* (see sidebar "How blockchain works") to *proof-of-stake*. In *proof-of-stake*, nodes can buy the opportunity to mine using some 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 occurred since its creation, about 105 Gb and 70 Gb for Bitcoin and Ethereum respectively, source: http://bitinfocharts.com) are stored on each network node. Performances are therefore not comparable with databases (yet).
- Adding information is slow: creating a Bitcoin block takes around 10-60 minutes (source: http://blockchain.info/charts/avg-confirmation-time). Ethereum requires 15 seconds, (source: http://etherscan.io/chart/blocktime), a smaller though still significant amount of time.
- Unchangeability and transparency of blockchain could harm users' privacy and reputation: every network node would store a copy of the blockchain, and 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 of 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/governance mechanism and need to be as robust as the blockchain itself, not to become the weakest part of the process.

Digital Object Identifier 10.1109/MITP.2017.265110355 1520-9202/$26.00 2017 IEEE

- Smart contracts could be buggy: given the fact that their code is publicly available and, once created, they become autonomous entities, they could be "candy for hackers" (http://marmelab.com/blog/2016/06/14/blockchain-for-web-developers-the-truth.html). Being 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 smart contract-based attack happened on Etherum on June 2016, when about $60 million were "stolen".

One of the most common critics raised to blockchain is that a high number of blockchain-based applications could be already implemented using existing technologies, such as (properly secured) centralized databases. Experts also identified the following key questions that people evaluating the adoption of blockchain technology should answer to find whether is the right solution to their needs (http://www.multichain.com/blog/2015/11/avoiding-pointless-blockchain-project).

- Is there the necessity to have a shared database?
- Is there the necessity to have multiple parties writing data?
- Are potential writers untrusted (i.e., should writers be prevented to modify others' previous entries)?
- Is disintermediation needed (i.e., is there the necessity to remove trusted intermediaries verifying/authenticating transactions)?
- Is there the necessity to see how transactions are linked to each other (i.e., having different actors independently write transactions concerning a single user)?

Should one or more questions above receive a negative answer, probably blockchain would just introduce a overhead without bringing true benefits.

D*<+'$,($'"*/,247*$'/0*,&0*()/2+')$0*/0$,#+*

The insurance sector recently showed a high interest for blockchain. Some large companies made significant investments to explore its potentialities for their business (http://www.cbinsights.com/blog/financial-services-corporate-blockchain-investments), while consultancy firms investigated its applicability to the insurance sector [7]–[9]. Envisioned applications are reported in the following.

Applications

Exploitation of smart contracts for improving customer experience (CX) and lowering operating costs: the self-executing ability of smart contracts could increase claim-processing speed (providing excellent experiences to clients receiving their money even before they claim it, since 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 case of persistence of adverse conditions, authorize the reimbursement.

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

Smart contracts could be used in combination with IoT, e.g., for home insurance, triggering automatic reimbursements in case of damages of roofs equipped with smart damp sensors (http://www.ft.com/cms/s/0/f2b0b2ee-9012-11e4-a0e5-00144feabdc0.html#axzz4DAQsiRry).

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

Digital Object Identifier 10.1109/MITP.2017.265110355 1520-9202/$26.00 2017 IEEE

Fraud prevention: a shared blockchain recording policies undersigned on a worldwide basis [7] together with data possibly coming from other domains (medical reports, police theft reports, etc.) can help identify frauds during claims processing.

Data entry/identity verification: blockchain-based identity verification systems could reduce customers' data entry overload while undersigning/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 ID documents and check them. In a more sophisticated scenario (assuming a wide adoption of the blockchain by different actors), additional information could be stored (health examinations, assets ownership, etc.), and gathered by smart contracts for automatic and precise premium computations (http://www.reply.com/en/content/insurechain).

Pay-per-use: smart contracts could enable pay-per-use insurance policies, relying on IoT for automatic undersignment. Travel insurance premiums could be collected only if customers' GPS coordinates (e.g., 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 http://inspeer.me, http://friendsurance.com and http://heyguevara.com appeared few years ago). Nonetheless, smart contracts could provide wide innovations in this field, since they could allow the creation of DAOs whose functioning rules are hard-coded. With DAOs, insurers groups would be able to manage themselves without the need of external control (http://dynamisapp.com, http://wekeep.io).

As shown, potential use cases are various, and involve different exploitations of the blockchain. To investigate potential benefits/drawbacks deriving from the application of the considered technology in each use case, we analyzed them and tried to provide an answer to the five questions above (findings are summarized in Table 2).

Answers to key questions

Exploitation of smart contracts for improving customer experience (CX) and lowering operating costs: here, data is collected from multiple actors/sources (mechanics, weather/flight services, sensors, etc.). The need for a shared database depends on the single application: for car repairs, a shared database is probably required, written by mechanics and checked by the company. However, we could assume that company and certified mechanics undersigned an agreement and, consequently, that there is trust between parties. Documents sent by uncertified mechanics would be manually processed. In other cases, the company could rely on external APIs to retrieve desired information from online services or sensors, and update its database accordingly. Disintermediation is a controversial matter since, in claims processing, insurance companies actually act as intermediaries reconciling policies data with damages evaluation. Furthermore, a significant number of claims probably could not be automatically processed, since they would still need to be evaluated by assessors before being settled. The need for disintermediation could arise when damages could be automatically evaluated (e.g., by means of IoT technologies) or when the customer does not trust the company. Nonetheless, regarding the latter point, at least in developed countries the behavior of insurance companies is defined by several regulations aimed to ensure trust. Hence, disintermediation would not be a sensible need. Finally, in some cases the necessity to retrieve all the transactions/events linked to a policy/person could arise (e.g., for customer relationship management). This operation, however, could already be performed with traditional systems.

Fraud prevention: here, a shared database, written by multiple parties (doctors, 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

Digital Object Identifier 10.1109/MITP.2017.265110355 1520-9202/$26.00 2017 IEEE

could be preferred. Consequently, it appears that this use case could benefit from blockchain. Nonetheless, some issues should be considered too: first, a critical mass would be required, since a high number of data inserted by different actors would be needed. Secondly, measures to ensure privacy of data should be adopted. Finally, since blockchain data could not be changed, error management systems should be devised.

Data entry/identity verification: similarly to fraud prevention, a shared ledger would be needed to record customers' documents, proofs of ownership, etc. by different writers, and link them to their digital identity. Writers should be prevented from modifying information previously inserted by others. As in fraud prevention, disintermediation could lower costs. Blockchain could be a good solution, enabling information writing/sharing, provided that issues above are properly addressed.

Pay-per-use: here, the blockchain could be used to certify if/when customers activated a policy. Multiple writers (company and customers) would write data on a shared database, and would need the guarantee that policies data could not be modified. Disintermediation seems a less relevant need, since only two actors are involved (customers and insurance companies) and since insurance companies already act as intermediaries. Similarly, companies already store in their repositories information concerning customers' previous transactions, making linked transactions not so paramount as other requirements. Hence, 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 also mentioned that, in numerous countries, trust between customer and insurance companies is already ensured by regulations, thus removing the need to rely on a trusted third party. However, since in the future blockchain technology will be increasingly advertised by mass media, having blockchain-based pay-per-use insurances could be a competitive advantage, which could increase further, should customers be allowed to pay in Bitcoins 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, e.g., for customers' identify verification/claims recording. Thus, relying on blockchain could be a good choice. Nonetheless, peer-to-peer insurances aim to remove intermediaries. Consequently, the diffusion of DAOs-based insurances could represent a significant threat to traditional businesses.

Table 2. Analysis of use cases (columns) w.r.t. questions (rows).

	Shared database	Multiple writers	Untrusted writers	Disintermediation	Linked transactions
Improving CX & lowering operating costs	+/-	+/-	+/-	+/-	+/-
Fraud prevention	+	+	+	+	+
Data entry/id. verification	+	+	+	+	+
Pay-per-use	+/-	+/-	+/-	-	-
Peer-to-peer	+	+	+	+	+

"+": positive answer
"-": negative answer
"+/-": both answers could apply, depending on the context

C(/$2//(#)*

From the analysis reported, it should be rather clear that not all the insurance use cases could benefit in the same way from the adoption of blockchain. Should insurance companies opt for adopting it, they could probably start by using it for easing data entry/customers 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, also banks (which already made important investments in blockchain) could be

Digital Object Identifier 10.1109/MITP.2017.265110355 1520-9202/$26.00 2017 IEEE

interested in developing/maintaining a shared ledger. Insurance companies/banks may rely on existing applications (e.g., http://kyc-chain.com), reducing initial investments.

Afterwards, efforts could be devoted to develop blockchain-based fraud prevention systems. This would be a long-term investment presenting high risks since, to succeed, it would require the involvement of numerous actors and the definition of standards to store information. Initially, insurance companies could store policies/claims linked to customers' digital identities on a worldwide basis, thus reducing information asymmetries in customers 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 (a cost could be charged for each undersigned policy). In this respect, market surveys [10] found that numerous customers still consider personal interaction with intermediaries important. Hence, the shift to peer-to-peer insurances is probably not imminent yet.

The exploitation of blockchain and smart contracts for lowering operating costs, improving CX and increasing transparency could be a key choice, should the company want to address new emerging markets (where a mechanism of trust is not fully established yet), or in micro-insurances contexts (not viable in the past, due to human-intensive administrative processes and unaffordable high fees for small payments, also enabled by the blockchain). Nonetheless, companies should consider that, in several cases, manual claims assessment/processing would still be needed.

Finally, in pay-per-use, the blockchain could provide a proof of policy undersignment. However, in this respect, interested investors should first verify which are the national rules for pay-per-use insurances, e.g., 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.

G#)$"2/(#)/*

Blockchain is a hot topic and has been considered by media as a breakthrough technology. In this paper, we provided some technical background to understand how this technology works, and underlined its advantages/disadvantages by also presenting a review of potential applications.

In particular, we took the point of view of a professional investigating whether blockchain could be worth of investment, and focused the field of research to insurance, a sector in which blockchain could either lay the foundations for new processes/services or represent a threat, due to its capability to remove (existing) intermediaries.

We analyzed possible use cases and answered key questions to identify whether a blockchain is actually needed or whether existing technologies will suffice. As a result, we found some areas where blockchain could bring huge benefits, changing also the way processes are implemented, and others where benefits could be less disruptive or where comparable outcomes could be achieved also with traditional systems.

Our aim was to show that, even though blockchain could 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 company's sector and business goals.

Even though a specific domain was considered, the analysis made could be easily extended to other scenarios sharing comparable use cases, thus helping professionals to make decisions also in different contexts/sectors.

Moreover, regardless of whether a professional will finally decide to adopt the blockchain or not, our feeling is that every minute spent to deal with the dilemma "*blockchain or not to blockchain?*" is a minute gone for exploring and understanding an amazing new technology, not because it is "cool", but because, as shown, it is an incredible business enabler.

*

Digital Object Identifier 10.1109/MITP.2017.265110355 1520-9202/$26.00 2017 IEEE

E030+0)$0/*

[1] G. Hurlburt, "Might the Blockchain Outlive Bitcoin?," *IT Professional*, vol. 18, no. 2, pp. 12–16, 2016.

[2] M. Swan, *Blockchain: Blueprint for a New Economy*. O'Reilly Media, 2015, pp. 1–152.

[3] F. Tschorsch and B. Scheuermann, "Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies," *IEEE Communications Surveys Tutorials*, vol. 18, no. 3, pp. 2084–2123, 2016.

[4] K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.

[5] M. Mainelli and M. Smith, "Sharing ledgers for sharing economies: an exploration of mutual distributed ledgers (aka blockchain technology)," *The Journal of Financial Perspectives*, vol. 3, no. 3, pp. 38–69, 2015.

[6] M. Peck, "The blockchain has a dark side," *IEEE Spectrum*, vol. 53, no. 6, pp. 12–13, 2016.

[7] A. Shelkovnikov, "Blockchain applications in insurance," *Deloitte Report*, pp. 1–2, 2016.

[8] J.-T. Lorenz, B. Münstermann, M. Higginson, P. B. Olesen, N. Bohlken, and V. Ricciardi, "Blockchain in insurance-opportunity or threat?," *McKinsey & Company Report*, pp. 1–9, 2016.

[9] S. Crawford and D. Piesse, "Blockchain technology as a platform for digitization - Implications for the insurance industry," *Ernst & Young Report*, pp. 1–16, 2016.

[10] Ernst & Young, "Voice of the customer - Time for insurers to rethink their relationships," *Ernst & Young Report*, pp. 1–36, 2012.

Digital Object Identifier 10.1109/MITP.2017.265110355 1520-9202/$26.00 2017 IEEE

D2,&#+*-(#/*

*

H'"0),()'*I',,0/$&(is a Postdoctoral Research Assistant at Politecnico di Torino. She received her M.S. degree in management engineering and the Ph.D. degree in computer engineering, from Politecnico di Torino, Italy, in 2008 and 2013, respectively. Her research interests are in the areas of semantic processing, intelligent systems, human-computer interaction. Contact her at valentina.gatteschi@polito.it.

*

J'-+(K(#*L'M-0+,((SM'14) is an Associate Professor at Politecnico di Torino, Italy. He received his M.S. and the Ph.D. degrees in computer engineering from Politecnico di Torino, Italy, in 2000 and 2005, respectively. His research interests are in the areas of computational intelligence, semantic processing, distributed computing, human-computer interaction, computer graphics, and visualization. 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 or via http://staff.polito.it/fabrizio.lamberti.

*

G"'24(#* C0M'+,()(* (SM'14) is a Full Professor at Politecnico di Torino, where he teaches information systems and innovation and product development. His research interests are in 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 or via http://staff.polito.it/claudio.demartini.

G&('+'*N+'),04' is a member of Reale Group's Innovation Team where she's actually making research in the area of the sharing economy. Graduated in Physics at the University of Turin in 1992, she has worked as Physics and Electronics Professor in high school for 6 years before being ingaged in Reale Mutua where she has worked in the IT department, until 2016, and in the commercial department until 2015. Contact her at chiara.pranteda@realemutua.it.

H0$,#+*5'),'M'+0' is Responsible for Technology & Digital Innovation at Reale ITES, a Reale Group company. He received a degree in Mathematics by Universidad Complutense de Madrid (1989) and has completed several executive master programs at IE Business School ("Digital Innovation & IT Governance", Madrid, 2015) and IDE -CESEM ("Information Systems Management", Madrid, 2004). His research interests are in the areas of technology/business innovation and innovation organization. Contact him at victor.santamaria@realeites.com.

Digital Object Identifier 10.1109/MITP.2017.265110355 1520-9202/$26.00 2017 IEEE