future internet

MDPI

Article

Blockchain and Smart Contracts for Insurance: Is the Technology Mature Enough?

Valentina Gatteschi [1,*], Fabrizio Lamberti [1], Claudio Demartini [1], Chiara Pranteda [2] and Víctor Santamaría [3]

[1] Politecnico di Torino, Dipartimento di Automatica e Informatica, Corso Duca degli Abruzzi 24, 10129 Torino, Italy; fabrizio.lamberti@polito.it (F.L.), claudio.demartini@polito.it (C.D.)
[2] Reale Group Innovation Team, Via Corte d'Appello 11, 10129 Torino, Italy; chiara.pranteda@realemutua.it
[3] Reale Group Innovation Team, Príncipe de Vergara, 125, 28002 Madrid, Spain; victor.santamaria@realeites.com
* Correspondence: valentina.gatteschi@polito.it

Received: 30 December 2017; Accepted: 14 February 2018; Published: 20 February 2018

Abstract: Blockchain is receiving increasing attention from academy and industry, since it is considered a breakthrough technology that could bring huge benefits to many different sectors. In 2017, Gartner positioned blockchain close to the peak of inflated expectations, acknowledging the enthusiasm for this technology that is now largely discussed by media. In this scenario, the risk to adopt it in the wake of enthusiasm, without objectively judging its actual added value is rather high. Insurance is one the sectors that, among others, started to carefully investigate the possibilities of blockchain. For this specific sector, however, the hype cycle shows that the technology is still in the innovation trigger phase, meaning that the spectrum of possible applications has not been fully explored yet. Insurers, as with many other companies not necessarily active only in the financial sector, are currently requested to make a hard decision, that is, whether to adopt blockchain or not, and they will only know if they were right in 3–5 years. The objective of this paper is to support actors involved in this decision process by illustrating what a blockchain is, analyzing its advantages and disadvantages, as well as discussing several use cases taken from the insurance sector, which could easily be extended to other domains.

Keywords: blockchain; bitcoin; insurance; smart contracts

1. Introduction

A blockchain is a distributed ledger maintained by network nodes, recording transactions executed between nodes (i.e., messages sent from one node to another). Information inserted in the blockchain is public, and cannot be modified or erased [1]. Smart contracts are self-executing contracts (generally saved on a blockchain) whose terms are directly written into lines of code [2].

Recently, blockchain and its relations with smart contracts has received increasing attention from media, which started to address it as "The next big thing" [3], "The new black", "The philosopher's stone" [4] or "The new Graal" [5]. In [6], blockchain has been compared to inventions such as the steam or combustion engine, since it is potentially able to bring benefits to a variety of everyday activities and business processes.

According to Gartner's hype cycle, blockchain is at the peak of inflated expectations, where the enthusiasm is at the highest level possible [7]. Nonetheless, concerns started to be expressed as well about a massive adoption of blockchain [5,8–13]. The common denominator in the above concerns is that technology is considered, on the one hand, to be not fully mature yet [5,9] and, on the other hand,

to be overhyped [8], since its application often produces outcomes that could be achieved using well-mastered alternatives [10].

The risk is that one is so much in love with this technology that it becomes impossible for one to objectively judge its true benefits. As stressed by Adam Cooper, a technical architect of the Bank of England, "[With blockchain] the focus as always should be on fulfilling user needs, not on implementing technologies simply because they are clever or interesting." [11].

The insurance sector, as with many others, started to investigate the application of blockchain technology through considerable investments from both big and small companies [14,15], investigations from consultancy firms [4,16,17], and the creation, in 2016, of the B3i, the first blockchain-centered insurance consortium [18].

The hype cycle for the insurance sector [19], however, depicts blockchain technology at the beginning of the curve connecting the technology trigger phase with the peak of inflated expectation, meaning that this technology has not been fully explored yet in this particular sector. Hence, the questions that insurance companies are asking themselves right now are "Are there clear use cases exploiting blockchain technology and smart contracts in the insurance sector?", "In case we want to adopt a blockchain, what is the most suitable blockchain architecture for our needs?" and, more in general, "Is blockchain technology mature enough for insurance?". It has been estimated that they will need to wait about 3 to 5 years to see whether they made the right choice today by deciding to invest or not in blockchain for their business [20].

The objective of this paper is to help companies operating in the insurance sector to answer the above questions by providing an overview of blockchain- (and smart contracts-) based use cases in such specific sector, and by highlighting strengths, weaknesses, opportunities and threats for this technology. The authors decided to focus on insurance because, in this sector, blockchain technology could have a relevant impact on a variety of processes and application scenarios. Notwithstanding, it is worth observing that, despite the focus on the particular domain the authors are operating into, many of the examples provided and considerations made throughout the paper could be helpful for a number of other companies, not necessarily from the financial domain. In fact, the aim is to stimulate reflections and discussions on this topic, leaving to the reader the final judgment on the actual benefits that could come from the adoption of the considered technology in a specific scenario.

The paper is organized as follows: Section 2 provides an overview of the blockchain technology, by presenting its key concepts. Section 3 discusses several use cases from the insurance sector, by mentioning prototype solutions available so far. Discussion is complemented by Section 4, which reports a SWOT analysis performed on a wider context to broaden the scope of the analysis beyond the insurance domain. Finally, conclusions are drawn in Section 5.

2. How Blockchain Works

The blockchain (literally, a "chain of blocks") made its first appearance in the research scenario in 2008, in the frame of the Bitcoin initiative [21,22]. The objective was to transfer online payments from one party to another, without relying on intermediaries. In this context, the blockchain was acting as the underlying ledger recording Bitcoin transfers and guaranteeing, by means of cryptographic operations, the authentication and non-repudiation of payments.

Even though Bitcoin is, by far, the most famous cryptocurrency, it is not alone. In fact, since 2008, more than 1300 cryptocurrencies have been created [23], which are being used as exchange tokens in many different blockchain-based applications.

The core concepts behind the blockchain technology are reported in the following.

- Transactions: each cryptocurrency transfer from one subject to another is represented as a transaction from A to B. Cryptocurrency is neither a physical nor a software object, but the result of incoming and outgoing transactions. For this reason, the blockchain keeps track of all the transactions occurred from its birth.
- Blocks: transactions are grouped in blocks. Each block collects all the transactions occurring in a given timeframe and keeps a reference to the preceding block (that is where the concept of "chain" comes from).

- Nodes: instead of being stored in a centralized database, the blockchain is spread over network computers (the "nodes"), each containing a local copy of the entire blockchain.
- Majority consensus: since a central authority is missing, decisions on the network are made according to a majority consensus. Each node modifies its local copy of the blockchain to make it mirror the status of the majority of the network nodes.
- Mining: nodes could either passively store a copy of the blockchain, or actively take part to the maintenance of the blockchain, in the so-called "mining" process. During mining, nodes check previous transactions to verify whether a subject is entitled to spend a given amount of cryptocurrency and, each time a block has to be added to the chain, solve a complex computational-intensive mathematical problem. This problem was specifically designed to limit the possibility for a malicious entity to manipulate the blockchain by falsifying transactions. The probability of attacks is extremely low, since adding a new (malicious) block or modify a previously added block to the chain would require control of the majority of the network nodes (to make them agree with the modification).
- Wallet: people transfer cryptocurrency using wallets. Cryptocurrency cannot be stored on a physical memory; rather, it is the result of previous transactions. Hence, the wallet only stores credentials (a complex, unchangeable combination of automatically assigned numbers and letters), which enable blockchain users to transfer cryptocurrencies they own. Each wallet is associated to one (or more) unique addresses. Should a user want to send a given amount of cryptocurrency to a peer, he/she would have to specify the recipient's address and the desired amount, and use his/her credentials to validate the transaction. This aspect is particularly important, since in case of credentials loss, the cryptocurrency owned by the user would not "disappear", but the user would be no more able to spend it. Moreover, the fact that the user validates the transaction with his/her credentials certifies that he/she was the actual initiator of the transaction.

In order to better understand how the blockchain works, it could be worth considering the example shown in Figure 1. In the depicted scenario, Alice wants to send some amount of cryptocurrency from her wallet (with address "x1z") to Arthur's wallet (with address "v4y").

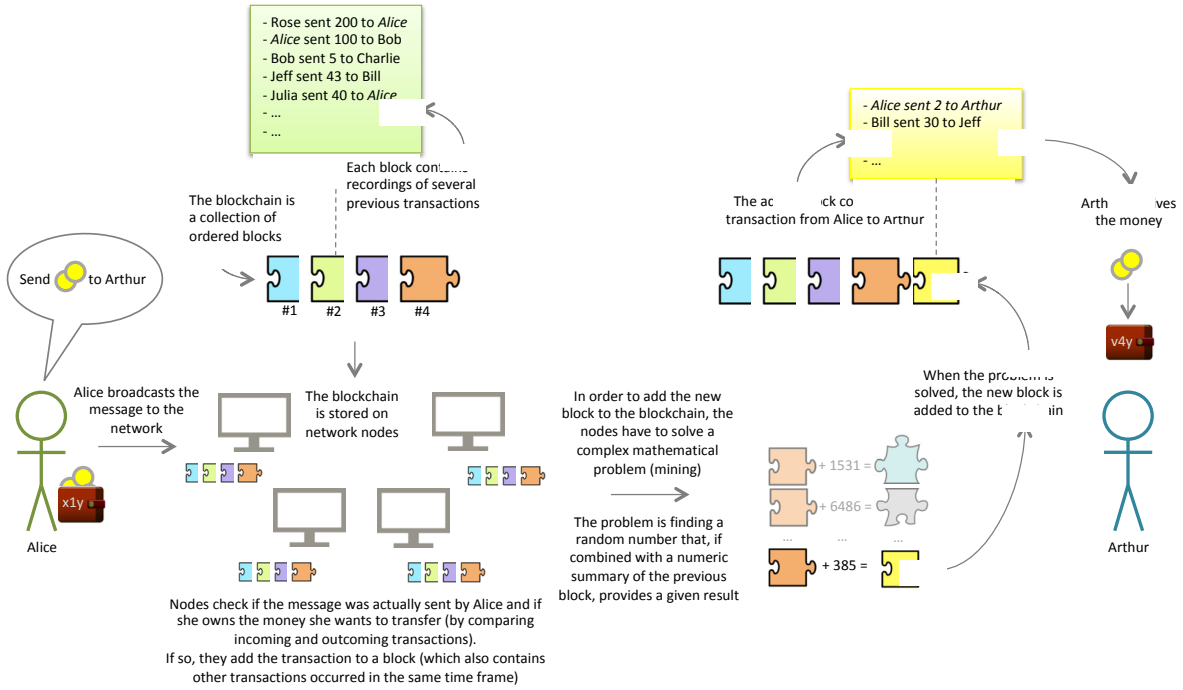

Figure 1. Performing transactions on the blockchain.

Alice makes a statement in which she specifies the amount to be transferred as well as the recipient of the transfer, and validates this message with her credentials (for sake of readiness, the

image reports users' names instead of their addresses). Then, she broadcasts the message to the network. Network nodes verify if the message's sender was actually Alice (by verifying if the message was correctly validated using her credentials), and check if she possesses the amount to be transferred. In order to perform this check, they use their local copy of the blockchain and analyze incoming and outgoing transactions from Alice's wallet address that are stored in previous blocks. If the message sent by Alice is valid and she is entitled to spend the money, they add Alice's transaction, together with other transactions occurring in the same time frame, to a block. In order to add the block to the blockchain, they then start solving a complex mathematical problem, where they have to find a random number that, combined with a numeric summary of the previous block, provides a given result. During this (mining) process, the fastest node receives a monetary reward. When a valid result is found, the new block is added to the blockchain. As a result, Arthur receives the money.

The above example should have allowed the reader to get better acquainted with the main characteristics of the blockchain, which make it a disruptive technology:

- Decentralized validation: the validation of transactions is performed by network nodes without the need of intermediaries;
- Data redundancy: each network node has a local copy of the blockchain, which prevents data losses;
- Data immutability: data stored in the blockchain could not be modified or deleted;
- Trust: cryptography enables trust between parties, since a transaction that has been validated using user's credentials cannot be repudiated;
- Transparency: everyone could read the blockchain and the transactions stored in it.

Though the example in Figure 1 refers to a transfer of cryptocurrency, application possibilities of the blockchain are not limited to monetary assets, but could encompass a wide variety of use cases.

Among the early application scenarios that were explored for the blockchain, it is worth recalling the notarial context. In fact, since the blockchain is immutable and publicly available, researchers suggested using it for storing public records and attestations [1]. Another domain where the blockchain has been recognized to be able to bring significant benefits is intellectual property protection. In this context, blockchain technology could be used to prove/certify the existence of a document at a given time [24]. In contexts where, e.g., freedom of thought is threatened, blockchain technology could be used to store information in order to avoid censorship [25]: in fact, everyone can write information on the blockchain and read it.

As time has passed, researchers have realized that the blockchain could also be used to store other kinds of assets, including pieces of code. It was the birth of "smart contracts", i.e., small programs stored in the blockchain and programmed to autonomously behave in a given manner when some conditions are met.

The idea of a smart contract has been known since the 90s [26], but it was only with the blockchain technology—and, in particular, with the Ethereum blockchain (probably the most famous blockchain after Bitcoin)—that smart contracts were able to unleash their full potential [27].

With a smart contract, a person could, for instance, encode his/her will in the blockchain in the form of a set of rules. In case of death, the smart contract could then automatically transfer the testator's money or other kind of assets to the beneficiary. The testator may also provide additional constraints, such as enabling the transfer only when the beneficiary reaches the age of majority, when he/she obtains a diploma, etc.

Since smart contracts' conditions are based on data stored in the blockchain, they need to rely on external services, which take data from the "real" world (e.g., from death records) and push them to the blockchain (or vice versa). These services are referred to as "oracles" [28]. By considering the testator's example, an oracle could inspect death records to identify whether the person passed away. If so, it could write this information on the blockchain (e.g., by changing the value of a Boolean variable indicating whether the person is alive or not). The smart contract, then, would trigger a conditional statement (based on the value of the variable), and execute the block of code initiating the money transfer.

Based on the type of information collected and on the interaction with the external world, oracles have been grouped into "software"/"hardware" oracles, and "inbound"/"outbound" oracles [29]. Software oracles are in charge of extracting information mainly from Web sources, whereas hardware oracles are meant to extract information from the physical world (e.g., through sensors). Inbound oracles insert information in the blockchain, whereas outbound oracles allow smart contracts to send information to the external world (e.g., letting hotels' intelligent lockers unlock themselves as soon as a person pays for a night).

Oracles have a huge responsibility in the correct execution of smart contracts, as the insertion of wrong information could trigger a money transfer without possibility of refund. Thus, there are companies that have developed oracles that certify the authenticity of extracted data for a small cost [28]. In some cases, it could be worth relying on more than one oracle, e.g., by considering a situation as "happened" if 3 out of 5 oracles confirm it [30].

Recently, an even more complex application of smart contracts and oracles was proposed, which is associated to the concept of Decentralized Autonomous Organization, or DAOs [31]. In this context, smart contracts are used to encode rules to govern an organization, e.g., how decisions are taken, the weight of each member's vote, etc. The advantage is that no external party is required to verify that the organization is properly managed, and underlying rules can be verified by the wider public, ensuring transparency and trust.

From the architectural point of view, it is worth remarking that there exist different types of blockchains, which differ in terms of read/write permissions. "Public blockchains" (such as the Bitcoin blockchain) are blockchains that could be readable and potentially writable by everyone. "Private blockchains" are blockchains that could be written only by organization members. Read permissions can be either restricted to the organization, or made public. In "consortium blockchains", a set of selected nodes belonging to different institutions control validation, and the blockchain is used to share information among participant institutions. Public blockchains are particularly useful when no central entity is available to verify a transaction, and full decentralization is needed. Private and consortium blockchains provide some advantages, such as lower validation costs and shorter validation times (given the fact that, because of the smaller number of nodes, the mathematical problem can be simplified), reduced risk of attacks (since nodes that validate transactions are known) and increased privacy (as read permissions could be granted only to selected nodes). Furthermore, in case of errors or bugs in smart contracts, private and consortium blockchains could extraordinarily modify or revert previous transactions.

The choice of the type of blockchain to adopt should be based on the amount of decentralization required, and on time/cost constraints [8,32]. Eventually, some hybrid solutions, exploiting cross-chain exchange layers between public and private blockchains, could be exploited [33], e.g., by using a private blockchain for a company's backend activities and a public blockchain for receiving/sending money from/to customers. Finally, it must be underlined that, when selecting the blockchain to use, one should pay attention to avoiding decentralization for the sake of itself. In fact, a number of companies' processes are currently managed in a successful way using relational databases, and the switch to a (private) blockchain could not be worth the effort [8,32]. With respect to private blockchains versus centralized databases, experts argue that "the biggest advantages of private blockchains in comparison to centralized databases are cryptographic auditing and known identities. Nobody can tamper with the data, and mistakes can be traced back" [34]. Others suggest that a blockchain could be a solution more suitable than a database only in case a company "plans to start privately and evolve into a regular public blockchain for public cross-verification as demand/volume grows" [34].

3. Blockchain Applications in Insurance: Selected Use Cases

As illustrated in the previous section, advantages of blockchain are various. A number of enthusiasts already proposed using this technology in various sectors and contexts, including:

- Government [35], to record in a transparent way citizens' votes, or politicians' programs (for verifying if promises made have been kept) or to enable autonomous governance systems [36];

- Intellectual property [24], to certify the proof of existence and authorship of a document;
- Internet [25], to reduce censorships, by exploiting the immutability of data stored in the blockchain;
- Finance [37], to transfer money between parties without having to rely on banks;
- Commerce [38], to record goods' characteristics as well as their ownership, especially for luxury goods, thus reducing the market of counterfeit/stolen items;
- Internet of Things (IoT) [39–41], e.g., by exploiting smart contracts to automatically process data coming from sensors, in order to let intelligent machines interact with each other [42] and autonomously take actions when specific situations occur;
- Education [43], to store information on qualifications acquired by learners, e.g., to reduce job application frauds; in this context, multiple actors (e.g., universities, training institutions, etc.) could write qualifications achieved by a person on the blockchain; human resources staff could then easily obtain information about when and where a given competency was obtained.

A rather comprehensive overview of applications developed in each of the above sectors can be found in [32,44]. What should be evident from the above list is that benefits deriving from the adoption of blockchain technology are not limited to a single sector/scenario. Moreover, even within a given sector, blockchain can have different impacts considering the various stakeholders operating in it, their business models, their needs, etc.

In the following, the attention will be specifically devoted to the insurance sector, where the use of blockchain could positively affect different internal processes (from customer acquisition and management, to frauds prevention, etc.) and could even allow companies to reach new markets [4,16,17,32]. In particular, a selection of use cases that could potentially benefit from blockchain technology will be introduced. For some use cases, prototype implementations have already been developed. In other cases, the use of blockchain has been only analyzed from a theoretical point of view. For each use case, advantages, disadvantages and impact on the insurance domain will be discussed.

3.1. Improvement of Customer Experience and Reduction of Operating Costs

In this use case, blockchain and smart contracts could be exploited to increase the speed of claim processing as well as to reduce the costs (and mistakes) associated with the manual processing of claims. From this perspective, a smart contract could encode the rules for enabling the transfer of refund from the company to the insured.

A simple application could consist of triggering an automatic transfer of refund only if the customer repairs the car at a certified mechanic, with the mechanic sending a transaction to the smart contract to prove its identity.

More complex use cases could also involve oracles to gather information from the real world. To make an example, in crop insurance an oracle could periodically check weather data and push this information in the blockchain. A smart contract could then read these data, and trigger a payment in case of persistence of bad weather.

These problems have been dealt with, for instance, in the prototype presented in [45]. In this case, the focus is on travel insurances, and the idea is to exploit a smart contract developed on the Ethereum blockchain for automatically refunding travelers if their flight/train was delayed.

Another interesting use case, which could widely benefit from the increasing diffusion of sensors, is the exploitation of smart contracts in combination with IoT. For instance, homes could be equipped with sensors that can directly notify a smart contract of a damage (e.g., damp sensors could be used to monitor damages on the roof) [46]. Similarly, smart appliances could automatically monitor their state, and initiate a claim or directly contact the repairer for a quicker assistance when needed.

Solutions such as the ones envisioned above bring benefits to different actors: to the insurance company, which could reduce the amount of resources normally devoted to claim processing, but also to customers, who would receive money even before having become aware of the damage.

Another advantage would come from the fact that everyone could inspect the smart contract. That is, the customer undersigning a policy would get a clear idea of its contractual conditions (even though, at the moment, he/she should master some programming skills in order to understand the smart contract code). Consequently, it would become easier for him/her to compare policies. Furthermore, the choice of a policy would no more based only on how much he/she trusts a given company (since trust would be implicitly guaranteed by the smart contract), but on objective data.

Despite these advantages, it must be said that the scenario above could be adopted only for a limited number of policies. In fact, the majority of claims processed by insurance companies still need to be evaluated by an external expert before being settled. In case of manual processing, however, the customer experience could still be improved by managing payments in cryptocurrencies, whose transfer would be quicker than with traditional methods (several seconds or minutes depending on the blockchain used).

From the architectural point of view, probably the most suitable choice is to adopt a combination of private and public blockchains. The private blockchain could be used to record policies and claims data, whereas the public blockchain could be used to trigger the refund in terms of tradable cryptocurrencies (such as Ethers or Bitcoins). The private blockchain could be maintained by trusted company's computers/nodes characterized by lower mining costs with regard to those of public blockchains. The public blockchain would be maintained by the wider public, through the mining incentives presented in Section 2. Alternatively, the company could decide to exploit only a public blockchain. This choice could be successful in case the company needs to improve its own reputation and obtain customers' trust (as the process would be fully decentralized), but would imply higher transaction costs.

3.2. Data Entry/Identity Verification

The cryptographic mechanism underlying the blockchain could be used to reduce the overhead related to manual data entry and verification of new customers [47].

With the blockchain, customers would be identified by a unique address (e.g., the one linked to their wallet). The first time they use a service, a certified intermediary would verify their identity and link it to their address. From that time on, every time they undersign a policy, they would no more need to provide an identification document; rather, they would only need to use their credentials.

Benefits of this use case could be seen again in a reduced time and cost to gather/provide information.

Nonetheless, this use case also has some relevant drawbacks the company should be aware of. A first drawback is related to the possible loss/steal of credentials. As said, since the blockchain works without intermediaries, no one could reset users' credentials. A solution could be to rely on external services, which could store credentials and return them to the users in case of loss. However, using such services would mean providing someone else access to one's sensitive information. Another drawback is linked to the fact that the current legal regulations should be modified to include blockchain-based identification, and some governments could refuse to approve this type of identification, e.g., due to mistrust in the technology.

From the architectural point of view, companies deciding to exploit blockchain-based Know Your Customer (KYC) could rely on external services running on public blockchains. In fact, some KYC services recently appeared, offering some prototypes based on existing blockchains. One example is Civic [48] (based on the Bitcoin blockchain) and KYC Legal [49] (exploiting the Ethereum blockchain). Such companies already built a network of validators, which receive a reward for each performed validation and charge small fees to companies requiring their services.

3.3. Premium Computation/Risk Assessment/Frauds Prevention

In this scenario, the blockchain is used to let multiple certified intermediaries record information related to a person (by linking them to his/her address).

Such intermediaries could be insurance companies (e.g., to record previous claims), police officers (e.g., to store criminal acts), medical staffs (e.g., to record a person's injuries and treatments),

or even smart wearable devices (which could inject in the blockchain data about one's physical activity).

A smart contract could read all the information linked to a person and automatically compute the premium and perform risk assessment, based on his/her physical health, driving behaviors, etc. [50].

Another application scenario is represented by fraud prevention. In this scenario, a smart contract could analyze collected data and identify frauds during claim processing (e.g., by crossing data related to a person's previous claims).

A scenario such as the one depicted in the above examples, however, could be difficultly realized in the short term. In fact, it implies that each person possesses a unique blockchain address (as presented in Section 3.2), and requires the active involvement of different actors (insurance companies, police officers, medical staff, etc.) as the quality of the results would be a consequence of the quality and quantity of data stored in the blockchain. Privacy is another relevant issue (especially for what it concerns medical records). In this view, in the construction of such a system, a thorough attention should be devoted to let only selected actors link information extracted from the blockchain to a person's identity. Furthermore, particular care should be devoted to the definition of common standards to record the information, in order to enable interoperability.

The most suitable architecture for this use case is a consortium blockchain. The blockchain would be maintained by selected nodes of the consortium, e.g., belonging to the different actors involved. The limited number of trusted nodes would increase security and privacy. Furthermore, the blockchain would keep track of the sender of each transaction. Finally, being controlled by a small number of nodes, mechanisms to revert blockchain state in case of transactions erroneously made (e.g., a driving infraction notified to the wrong person) could be devised.

3.4. Pay-Per-Use/Micro-Insurance

Smart contracts- and blockchain-based payments could enable new revenue sources, such as micro- and pay-per-use insurances. Though in the past micro-insurances were threatened by administrative costs, the exploitation of smart contracts could enable quick and cheap policy undersignment and management (even on mobile devices) [51]. Similarly, pay-per-use insurances could become a praxis, possibly in combination with IoT solutions for automatic undersignment. For instance, GPS data could be used to automatically collect, e.g., a travel premium only if the customer is abroad, a car premium only when the car is moving, etc. Pay-per-use mechanisms could be exploited in services such as Uber or Airbnb, e.g., activating the service when a customer is picked up or hosted.

With respect to the other use cases described in the paper, from the point of view of actors and technology to be involved, this is probably one of the quickest and easiest to be realized (because of the limited number of involved actors, and because the feasibility of prototypal solutions has already been demonstrated [51]). Moreover, from the point of view of the insurance company, introducing blockchain-based pay-per-use insurances (which could be even paid by using cryptocurrencies) could bring a competitive advantage, especially attracting young, technology enthusiasts.

Concerning architectural choices, companies aiming at addressing pay-per-use insurance could rely on a public blockchain. In this way, a smart contract could collect money from customers (e.g., Ethers or Bitcoins), keep them until a given date and transfer them to the insurance company if no damage occurs. Being on a public blockchain, everyone could inspect the smart contract code, increasing trust between parties.

3.5. Peer-to-Peer Insurance

Several peer-to-peer insurances already exist [52–54], though it must be said that, at present, they are not "real" peer-to-peer models, as they have a traditional insurance model or risk carrier behind them, supporting the heavy part of the insurance business.

In this context, smart contracts could represent an important innovation, as they would enable the creation of DAOs, where self-insured groups' functioning rules could be hard-coded.

A prototype solution named DYNAMIS and based on the Ethereum blockchain has already been implemented [55]. This solution aims to provide supplemental unemployment insurance for a community of self-managed people in terms of underwriting and claims acceptance and processing.

Even though in peer-to-peer insurance the blockchain could really become the key technology, from the insurance company's perspective it must be underlined that the objective of peer-to-peer insurance is the removal of intermediaries (i.e., the insurance companies themselves). Hence, a wise choice insurance companies could make here is to recognize this risk, and turn it from a threat into a business opportunity, e.g., by providing the infrastructure for peer-to-peer insurance.

From the architectural point of view, since this scenario requires a high amount of decentralization, a public blockchain would be more suited.

It should be underlined, however, that the adoption of peer-to-peer insurance models by the wider public is not imminent yet. In fact, apart from a small amount of technology enthusiasts who aim at reducing insurance costs, a high number of customers still considers the interaction with intermediaries important and worth of extra costs [56].

4. A SWOT Analysis

The above discussion should have provided the reader with a broad overview of potential applications of blockchain technology in the insurance sector. As seen, advantages appear to be numerous. Nonetheless, only a few prototypes exist so far, and it has been estimated that blockchain-based applications will be available to the wider public only in 10–15 years [5].

Starting from the considerations drawn in Section 3, in the following a SWOT analysis summarizing advantages and disadvantages of this technology is provided (Table 1). The objective here is to abstract from the specific domain considered, i.e., insurance, and to perform an analysis, which could potentially be helpful in a variety of contexts/sectors.

The strengths of blockchain technology are mainly related to the technological aspects presented in Section 2. By removing intermediaries, the cost of money transfers can be lowered (e.g., bank commissions cease to exist). Transfers can also be made faster, as cryptocurrencies are directly moved from a wallet's address to another without intermediate steps (as it usually occurs, e.g., in overseas bank transfers). Smart contracts provide a high degree of automation. Transparency is guaranteed as well, as the blockchain could be accessed worldwide. In addition, since everyone could potentially write on the ledger, the blockchain could become the repository of a huge amount of information, which could be used for data analytics in different sectors (not necessarily related to insurance and finance, such as medicine, education, etc.). The underlying cryptographic mechanism guarantees that data are not modified and that transactions could not be repudiated. Finally, the replication of the blockchain on each network node ensures that the blockchain would survive to unexpected events.

The most relevant weaknesses are related to scalability, energy consumption and performance.

In fact, at present, the number of transactions that could be handled per second is extremely low when compared to traditional systems (mainly because of the computational power required to validate new blocks). If, at the present time, blockchain-based transactions are quicker than traditional bank transfers (on average they require few seconds to several minutes, instead of 1–2 days), for instant payments and for other kinds of applications, performance should not be adequate to needs. In this respect, it is worth outlining that some blockchain platforms are changing the process of validating blocks, reducing the complexity of the mathematical problem to be solved and restricting the possibility to perform mining only to a subset of trusted nodes. Apart from time, space is also an issue, since data are replicated on each network node. To make an example, the Bitcoin blockchain requires more than 170 GB of storage on each network node [57]. In addition, the amount of energy consumed by network nodes, and the cost of the hardware required to validate new blocks is extremely high, estimated around 6$ per transaction [58] (though it must be underlined that several initiatives to limit the amount of consumed energy are currently under development [59]).

Table 1. SWOT analysis of the adoption of blockchain.

	Positive	Negative
Internal	**Strengths** - Fast and low-cost money transfers - No need for intermediaries - Automation (by means of smart contracts) - Accessible worldwide - Transparency - Platform for data analytics - No data loss/modification/falsification - Non-repudiation	**Weaknesses** - Scalability - Low performance - Energy consumption - Reduced users' privacy - Autonomous code is "candy for hackers" - Need to rely to external oracles - No intermediary to contact in case of loss of users' credentials - Volatility of cryptocurrencies - Still in an early stage (no "winning" blockchain, need of programming skills to read code, blockchain concepts difficult to be mastered) - Same results achieved with well-mastered technologies
External	**Opportunities** - Competitive advantage (if efforts to reduce/hide the complexity behind blockchain are successful, or in case of diffusion of IoT) - Possibility to address new markets (e.g., supporting car and house sharing, disk storage rental, etc.) - Availability of a huge amount of heterogeneous data, pushed in the blockchain by different actors	**Threats** - Could be perceived as unsecure/unreliable - Low adoption from external actors means lack of information - Governments could consider blockchain and smart contracts "dangerous" - Medium-long term investment - Not suitable for all existing processes - Customers would still consider personal interaction important

The fact that, once information is encoded in the blockchain, it is immutable and accessible by everyone is another weakness, and could harm users' privacy. To make an example, everyone could check the amount of money owned by a person, by analyzing his/her incoming transactions. Should other types of information be stored in the blockchain (e.g., medical records), this issue would become even more relevant. To cope with privacy issues, some solutions to anonymize payments/transactions have been proposed [60–63].

The immutability and self-execution of code could be another weakness for blockchain, since smart contracts could become "candy for hackers" [9]. In fact, hackers could exploit bugs in smart contracts to steal money, as it recently happened on the Ethereum network, where, in the most famous attack of this kind, around $60 million were "stolen" in June 2016. Even assuming that smart contracts are free of bugs, some applications would still need external oracles to inject information in the blockchain. The weakest point, in this case, would become the oracle. As said, the consequences of injecting in the blockchain wrong information could be partially mitigated by relying on more than one oracle, each getting information from different sources.

Apart from technical aspects discussed above, other weaknesses affect blockchain usability. First of all, the impossibility to receive assistance in case of credentials loss (even though this weakness could be partially removed by relying on trusted services, as explained in Section 3). Another aspect is cryptocurrencies volatility, which could become a limitation to the adoption of blockchain-based payments. In fact, given the fact that cryptocurrencies are subject of speculation and considering that

technology is not fully mature yet (and bugs frequently appear), value of cryptocurrencies show huge fluctuations.

Another weakness is related to the fact that development tools are still in an early stage, and standards for developing blockchain-based applications have not been defined yet.

Finally, it is worth remarking that, in some cases, blockchain would not be the most suitable technology to use, as existing, well-mastered alternatives would enable the achievement of comparable results [64].

Opportunities are mainly related to whether the market would embrace the technology or not.

At the present time, interacting with the blockchain requires some technical skills (e.g., mastering the concept of blocks, installing a wallet, etc.). Several efforts are currently carried out in order to reduce/hide the complexity behind the technology (e.g., the development of browser plugins which let users easily inspect the ledger [65], the creation of user-friendly wallets [66], etc.). Should the above initiatives be successful, companies providing blockchain-based applications and services (and, in the insurance market, companies offering blockchain-based policies) could have a competitive advantage. This advantage would become larger in case of an increasing diffusion of IoT, as smart contracts could be coded to autonomously make decisions based on data acquired by sensors [39–41].

Another opportunity is related to the possibility to address new markets and create new types of services, mainly by leveraging DAOs and low transactions fees. Blockchain could be successfully used to support the sharing economy, from car and house sharing [67] to disk storage rental [68] (and, in an insurance scenario, to support micro, on-demand and peer-to-peer insurances).

Finally, should a high number of actors write data on the blockchain, innumerable new applications could appear. As a matter of example, a person's previous medical history could be easily retrieved by doctors in case of urgency; blockchain could become a repository of medical data which could be used by research scientists; blockchain-based supply chains could be more efficient as data could be shared nearly instantaneously among heterogeneous involved actors; in an insurance scenario, data could be used for frauds prevention, policies personalization, etc. Nonetheless, the type and impact of these applications would be a function of the amount and quality of information recorded.

Threats are linked to different external causes. First of all, there is still a risk that the market distrusts this technology, perceiving it as unsecure or unreliable, due to bugs, cryptocurrencies volatility, etc.

Other actors could think that it is too complicated, and the adoption rate on a worldwide basis could be low. As a countermeasure, such actors should receive a suitable training to be made aware of the advantages of this technology. Alternatively, efforts could be carried out to hide the underlying complexity.

Particular attention should be paid to legal regulations, which could threaten the adoption of blockchain. For instance, the regulation of the use and jurisdiction of smart contracts is still under debate. To make some examples, there could be situations in which the outcome of a smart contract would not be considered as legal by a court under existing laws (e.g., a smart contract regulating transactions of illegal goods) [69]. Similarly, there could be situations where hackers exploit smart contracts bugs to steal money. Some governments could consider blockchain and smart contracts too "dangerous", thus resulting in a limitation of the adoption on a larger scale.

Concerning practical aspects, blockchain-based applications are a medium- to long-term investment, and they could not be suited for integration in all the existing processes. In fact, as previously discussed for the insurance sector, some claims would still need to be manually processed, as not all the damages could be evaluated by sensors.

Finally, should blockchain technology become a praxis, it could impact on companies' relationship with their customers. First of all, some customers could refuse to adopt it, as they might still consider the personal interaction important. Similarly, companies that invested in human capital to offer a good customer service could lose market share, as the competition could be moved from the quality of service provided, to its price.

5. Conclusions

Blockchain is receiving an ever-growing attention from research and industry, and is considered a breakthrough technology. The increasing enthusiasm reported in the media, however, could bias an objective evaluation about whether to invest or not in this technology. The risk is that a company decides to embrace blockchain technology because it is fascinating, without reflecting on whether it is mature enough for an adoption in everyday activities, and by a wider public.

To help companies reduce the risk of chasing decentralization for the sake of itself just because blockchain is now under the spotlight, in this paper we presented an overview of potential applications and use cases of blockchain and smart contracts in the insurance sector. We also drafted a more general SWOT analysis of blockchain, which could be potentially applied to a variety of other sectors.

We decided to focus on insurance because this is a sector where blockchain has not been fully explored yet and in which blockchain could have a relevant impact on several processes and application scenarios. Hence, use cases in this sector could be helpful in identifying advantages and disadvantages of the technology itself.

The considerations made throughout the paper helped us answer the key questions reported in the introduction.

Concerning question 1, "Are there clear use cases exploiting blockchain technology and smart contracts in the insurance sector?", at the present time a number of use cases and prototype solutions have been devised in this sector. In particular, blockchain and smart contracts could be successfully used to speed up claims processing and reduce operating costs. In this scenario, a smart contract could trigger reimbursements based on data acquired from physical sensors (e.g., damp sensors installed on roofs) or from the Web (e.g., weather or flights delay data). In another scenario, data entry/identity verification, the blockchain could be used as the infrastructure to verify a person's identity. People's identities could be linked to a blockchain address; then, each time a person needs to be verified (e.g., to open a bank account), he/she could send a signed transaction from his/her address, by proving he/she is the address' owner. In the context of premium computation/risk assessment/frauds prevention, the blockchain could act as a shared ledger recording a person's previous history (previous claims, committed infractions, medical history, etc.). Insurance companies could rely on these data to identify frauds, or to automatically compute the premium of a policy. In the scenario of pay-per-use/micro-insurance, blockchain and smart contracts could be used to automatically activate/deactivate policies and covers, based on data collected by sensors. Finally, in the last identified scenario, i.e., peer-to-peer insurance, blockchain and smart contracts could be the key technologies to enable a shift to a full decentralization, e.g., supporting the automatic management of self-insured groups' funds.

Concerning question 2, "In case we want to adopt a blockchain, what is the most suitable blockchain architecture for our needs?", as presented in Section 3, the architectural solutions should be chosen based on the company's decentralization needs. In general, for the backend a private blockchain may be sufficient. Private blockchains have been frequently demonized, since using an instrument originally born to foster decentralization in a fully centralized environment may seem a contradiction. Nonetheless, they have the advantage of keeping track of the sender of a transaction and of all the previous occurred transactions, reducing the risk of data tampering. Furthermore, together with smart contracts, they could be used to increase the automatization of existing tasks. In case multiple institutions need to access data, a consortium blockchain may be preferable. This blockchain could be maintained by nodes belonging to the different institutions of the consortium, and could be used as a shared ledger. Finally, public blockchains could be useful to manage (automatic) payments with existing cryptocurrencies, or when there is the need to provide trust (using an unmodifiable ledger) between parties.

Concerning question 3, "Is blockchain technology mature enough for insurance?", while we believe that blockchain is a tremendous invention that could have an impact similar to the World Wide Web in the 90s, we also think that this technology still needs several improvements before becoming mainstream. The reasons behind this statement are various: first of all, a current limitation

of existing (public) blockchains is scalability. In fact, the number of transactions per second is low, and the network frequently suffers congestions. In a pay-per-use insurance scenario, these facts would translate into long waiting times before the desired policy cover is actually activated (and, what if an accident occurs while the transaction activating a cover was waiting for validation?).

Second, a winning blockchain is still missing. That means that a company could develop an application exploiting a given blockchain, and discover after few years that the chosen blockchain is no longer supported by the wider network. Using a public blockchain supported by few nodes could increase the risk of attacks (as few nodes could control the majority of the network).

Third, the interaction with the blockchain is still complex for the "average user". Mastering the concepts of wallet, transaction, mining, etc. requires some technical background. At the same time, Bitcoin has frequently been associated with a pyramid scheme or a fraud. As a consequence, there is still a lot of misinformation on blockchain, and people could still prefer "traditional" applications rather than decentralized ones. Furthermore, cryptocurrency volatility (which sometimes is driven by media news) could scare the potential users of decentralized applications.

Finally, the resources and best practices to develop a free-of-bugs smart contract are still insufficient. Smart contracts frequently experience attacks, in some cases with disastrous consequences [70]. This aspect could especially threaten peer-to-peer insurances, which would widely rely on smart contracts for their governance.

For the above reasons, we do not expect blockchain-based insurance applications to appear in the very near future.

It must be said, though, that the blockchain community is devoting great efforts to improving the above weaknesses. Regarding scalability, Lightning Network (for Bitcoin) [71] and Raiden Network (for Ethereum) [72] are currently under development. Both solutions are investigating how to mix online and offline transactions, in order to reduce mining costs and time. Concerning easing the interaction with the blockchain, some applications that let users easily interact with blockchain-based applications using their browsers or mobile phones are currently under development [65,66]. Concerning smart contracts security, bug bounties programs are more and more frequent, and a wide community of blockchain white hat hackers is currently being created [73].

Once the above initiatives are successful, blockchain technology could be gradually inserted in everyday lives. In the meantime, insurance companies are strongly suggested to start investigating it, by acquiring the required competencies, and by creating some prototype solutions. Such prototypes could be useful to evaluate how existing processes would be influenced and to what extent this technology would be accepted by the staff or by customers.

What is clear already is that blockchain is bringing a radical transformation to the way we act and think, and we all should be prepared for this change.

Author Contributions: The paper was prepared by all the five authors, which were involved in a study of Blockchain technology in the Insurance Sector. All the authors equally contributed to the manuscript. Valentina Gatteschi focused on technical aspects related to Blockchain and on State of Art approaches and applications, under the guidance of Prof. Fabrizio Lamberti and Prof. Claudio Demartini, who also provided assistance while shaping and revising the paper. Chiara Pranteda and Víctor Santamaría provided their knowledge of the Insurance Sector and helped developing the discussion on Insurance-related use cases as well as revising the paper.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Swan, M. *Blockchain: Blueprint for a New Economy*; O'Reilly Media: Newton, MA, USA, 2015.
2. Szabo, N. Smart Contracts: Formalizing and Securing Relationships on Public Networks. First Monday, vol 2, no.9, 1997. Available online: http://firstmonday.org/article/view/548/469 (accessed on 19 February 2018).
3. Ayvazyan, A. Blockchain—The Next Big Thing. Available online: https://www.catalysts.cc/en/big-data/blockchain-the-next-big-thing/ (accessed on 29 December 2017).
4. Ramada, M. For insurers #blockchain is the new black. Available online: http://blog.willis.com/2016/12/for-insurers-blockchain-is-the-new-black/ (accessed on 29 December 2017).

5. Duvivier, P.J. Is the blockchain the new graal of the financial sector? Available online: https://www.linkedin.com/pulse/blockchain-new-graal-financial-sector-pierre-jean-duvivier (accessed on 29 December 2017).
6. Palychata, J. Bitcoin: What you didn't know but always wanted to ask. Available online: http://securities.bnpparibas.com/quintessence/hot-topics/beyond/bitcoin-and-blockchain-what-you.html (accessed on 30 June 2016).
7. Panetta, K. Top Trends in the Gartner Hype Cycle for Emerging Technologies, 2017. Available online: https://www.gartner.com/smarterwithgartner/top-trends-in-the-gartner-hype-cycle-for-emerging-technologies-2017/ (accessed on 29 December 2017).
8. Greenspan, G. Avoiding the pointless blockchain project—How to determine if you've found a real blockchain use case. Available online: http://www.multichain.com/blog/2015/11/avoiding-pointless-blockchain-project/ (accessed on 29 December 2017).
9. Zaninotto, F. The Blockchain Explained to Web Developers, Part 3: The Truth. Available online: http://marmelab.com/blog/2016/06/14/blockchain-for-web-developers-the-truth.html (accessed on 29 December 2017).
10. Panetta, K. Top 10 Mistakes in Enterprise Blockchain Projects. Available online: http://www.gartner.com/smarterwithgartner/top-10-mistakes-in-enterprise-blockchain-projects/ (accessed on 29 December 2017).
11. Cooper, A. Does digital identity need blockchain technology? Available online: https://identityassurance.blog.gov.uk/2016/08/15/does-digital-identity-need-blockchain-technology/ (accessed on 29 December 2017).
12. Peck, M. The blockchain has a dark side. *IEEE Spectr.* **2016**, *53*, 12–13, doi:10.1109/MSPEC.2016.7473136.
13. Romano, D.; Schmid, G. Beyond Bitcoin: A Critical Look at Blockchain-Based Systems. *Cryptography* **2017**, *1*, 15.
14. Higgins, S. Insurance Giant Allianz France Exploring Blockchain Potential. Available online: http://www.coindesk.com/allianz-france-exploring-use-cases-with-blockchain-startup/ (accessed on 30 June 2016).
15. Insurance Times Newsdesk. AXA leads $55m investment in blockchain. Available online: http://www.insurancetimes.co.uk/axa-leads-55m-investment-in-blockchain/1417270.article (accessed on 29 June 2016).
16. Shelkovnikov, A. *Blockchain Applications in Insurance*; Deloitte Report; Deloitte LLP: London, UK, 2016; pp. 1–2.
17. Lorenz, J.-T.; Münstermann, B.; Higginson, M.; Olesen, P.B.; Bohlken, N.; Ricciardi, V. *Blockchain in Insurance-Opportunity or Threat?*; McKinsey & Company Report; McKinsey & Company: New York, NY, USA, 2016; pp. 1–9.
18. Higgins, S. European Insurance Firms Launch New Blockchain Consortium. Available online: http://www.coindesk.com/europe-insurance-blockchain-consortium/ (accessed on 29 December 2017).
19. Gilbert, S. The Hype Cycle of Insurance Disruption. Available online: http://insurancethoughtleadership.com/the-hype-cycle-of-insurance-disruption/ (accessed on 29 December 2017).
20. McKinsey&Company. Blockchain Technology in the Insurance Sector. In Proceedings of the Quarterly Meeting of the Federal Advisory Committee on Insurance (FACI), McKinsey & Company: New York, NY, USA, 2017.
21. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System; 2008, Available online: https://bitcoin.org/bitcoin.pdf (accessed on 19 February 2018).
22. Lischke, M.; Fabian, B. Analyzing the bitcoin network: The first four years. *Future Internet* **2016**, *8*, 7.
23. CoinMarketCap. Available online: https://coinmarketcap.com/ (accessed on 30 December 2017).
24. de la Rosa, J.L.; Gibovic, D.; Torres, V.; Maicher, L.; Miralles, F.; El-Fakdi, A.; Bikfalvi, A. On Intellectual Property in Online Open Innovation for SME by means of Blockchain and Smart Contracts. In Proceedings of the 3rd Annual World Open Innovation Conference WOIC, Barcelona, Spain, 15–16 December, 2016.
25. Lee, D. Arachneum: Blockchain meets Distributed Web. *arXiv* **2016**, arXiv:1609.02789.
26. Szabo, N. Smart Contracts. Available online: https://archive.is/zQ1p8, 1994. (accessed on 19 February 2018).

27. Ethereum Team. Ethereum White Paper—A Next-Generation Smart Contract and Decentralized Application Platform. Available online: https://github.com/ethereum/wiki/wiki/White-Paper (accessed on 29 December 2017).
28. Oraclize. Available online: http://www.oraclize.it/ (accessed on 30 December 2017).
29. Dourlens, J. Oracles: Bringing data to the blockchain. 9 October 2017, Available online: https://ethereumdev.io/oracles-getting-data-inside-blockchain/ (accessed on 29 December 2017).
30. Blockchain Hub. Oracles. Available online: https://blockchainhub.net/blockchain-oracles/ (accessed on 29 December 2017).
31. Jentzsch, C. Decentralized autonomous organization to automate governance. Available online: https://download. slock. it/public/DAO/WhitePaper. pdf (accessed on 23 June 2016).
32. Lamberti, F.; Gatteschi, V.; Demartini, C.; Pranteda, C.; Santamaria, V. Blockchain or not blockchain, that is the question of the insurance and other sectors. *IT Prof.* **2017**, doi:10.1109/MITP.2017.265110355.
33. Buterin, V. On Public and Private Blockchains. Available online: https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/ (accessed on 29 December 2017).
34. O'Connell, J. What Are the Use Cases for Private Blockchains? The Experts Weigh In. Available online: https://bitcoinmagazine.com/articles/what-are-the-use-cases-for-private-blockchains-the-experts-weigh-in-1466440884/ (accessed on 26 January 2018).
35. Ølnes, S. Beyond bitcoin enabling smart government using blockchain technology. In Proceedings of the International Conference on Electronic Government and the Information Systems Perspective, Porto, Portugal, 5–8 September, 2016; pp. 253–264.
36. Huckle, S.; White, M. Socialism and the blockchain. *Future Internet* **2016**, *8*, 49.
37. Treleaven, P.; Brown, R.G.; Yang, D. Blockchain Technology in Finance. *Computer* **2017**, *50*, 14–17.
38. Kim, H.M.; Laskowski, M. Towards an Ontology-Driven Blockchain Design for Supply Chain Provenance; SSRN: Rochester, NY, USA, 2016.
39. Christidis, K.; Devetsikiotis, M. Blockchains and Smart Contracts for the Internet of Things. *IEEE Access* **2016**, *4*, 2292–2303.
40. Conoscenti, M.; Vetrò, A.; De Martin, J.C. Blockchain for the Internet of Things: A Systematic Literature Review. In Proceedings of the 2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA), Agadir, Morocco, 29 November–2 December 2016; pp. 1–6.
41. Liu, X.; Zhao, M.; Li, S.; Zhang, F.; Trappe, W. A Security Framework for the Internet of Things in the Future Internet Architecture. *Future Internet* **2017**, *9*, 27.
42. Hong, Z.; Wang, Z.; Cai, W.; Leung, V. Blockchain-Empowered Fair Computational Resource Sharing System in the D2D Network. *Future Internet* **2017**, *9*, 85.
43. Sharples, M.; Domingue, J. The blockchain and kudos: A distributed system for educational record, reputation and reward. In Proceedings of the European Conference on Technology Enhanced Learning, Lyon, France, 13–16 September, 2016; pp. 490–496.
44. Peck, M.E. Blockchains: How they work and why they'll change the world. *IEEE Spectr.* **2017**, *54*, 26–35.
45. Bertani, T.; Butkute, K.; Canessa, F. Smart Flight Insurance—InsurETH. Available online: http://mkvd.s3.amazonaws.com/apps/InsurEth.pdf (accessed on 29 December 2017).
46. Davies, S. Bitcoin: Possible bane of the diamond thief. Available online: http://www.ft.com/cms/s/0/f2b0b2ee-9012-11e4-a0e5-00144feabdc0.html#axzz4DAQsiRry (accessed on 30 June 2016).
47. KYC-CHAIN. KYC-CHAIN Web Page. Available online: http://kyc-chain.com/# (accessed on 29 December 2017).
48. Civic. Available online: https://tokensale.civic.com/CivicTokenSaleWhitePaper.pdf (accessed on 29 January 2018).
49. KYC Legal. Available online: https://kyc.legal/WhitePaper-ENG.pdf (accessed on 29 January 2018).
50. Reply. Insurechain Available online: http://www.reply.com/en/content/insurechain (accessed on 29 December 2017).
51. Lamberti, F.; Gatteschi, V.; Demartini, C.; Pelissier, M.; Gómez, A.; Victor, S. On-demand Blockchain-based car insurance using smart contracts and sensors. *IEEE Consum. Electron. Mag.* 1–6.
52. de Broglie, L.; Mury, E.; Corbeaux, L. insPeer. Available online: http://www.inspeer.me/ (accessed on 29 December 2017).
53. Kunde, T.; Herfurth, S.; Meyer-Plath, J. Friendsurance: The P2P Insurance Concept. Available online: http://www.friendsurance.com/ (accessed on 29 December 2017).

54. Guevara. Guevara Web page. Available online: https://heyguevara.com/ (accessed on 29 December 2017).
55. Davis, J. Peer to Peer Insurance on an Ethereum Blockchain. Available online: http://www.dynamisapp.com/whitepaper.pdf (accessed on 29 December 2017).
56. Ernst & Young. Voice of the Customer—Time for Insurers to Rethink Their Relationships: Ernst & Young Report; Ernst & Young: London, UK, 2012; pp. 1–36.
57. Bitinfocharts. Cryptocurrency statistics. Available online: https://bitinfocharts.com/ (accessed on 29 December 2017).
58. Stilgherrian. Let's quit the blockchain magic talk. Available online: http://www.zdnet.com/article/lets-quit-the-blockchain-magic-talk/ (accessed on 29 December 2017).
59. Cocco, L.; Pinna, A.; Marchesi, M. Banking on Blockchain: Costs Savings Thanks to the Blockchain Technology. *Future Internet* **2017**, *9*, 25.
60. van Saberhagen, N. CryptoNote v 2.0. Available online: https://cryptonote.org/whitepaper.pdf (accessed on 29 December 2017).
61. Ben-Sasson, E.; Chiesa, A.; Garman, C.; Green, M.; Miers, I.; Tromer, E.; Virza, M. Zerocash: Decentralized Anonymous Payments from Bitcoin. Available online: http://zerocash-project.org/media/pdf/zerocash-extended-20140518.pdf (accessed on 29 December 2017).
62. Peck, M. A blockchain currency that beats bitcoin on privacy [News]. *IEEE Spectr.* **2016**, *53*, 11–13.
63. Ober, M.; Katzenbeisser, S.; Hamacher, K. Structure and anonymity of the bitcoin transaction graph. *Future Internet* **2013**, *5*, 237–250.
64. Peck, M.E. Blockchain world-Do you need a blockchain? This chart will tell you if the technology can solve your problem. *IEEE Spectr.* **2017**, *54*, 38–60.
65. MetaMask. Available online: https://metamask.io/ (accessed on 29 December 2017).
66. Status—a mobile Ethereum OS. Available online: https://status.im/ (accessed on 29 December 2017).
67. La'Zooz. Available online: http://lazooz.org/ (accessed on 28 September 2017).
68. STORJ. Available online: https://storj.io/ (accessed on 30 December 2017).
69. Raskin, M. The Law and Legality of Smart Contracts. Available online: https://ssrn.com/abstract=2959166 (accessed on 22 September 2016).
70. Atzei, N.; Bartoletti, M.; Cimoli, T. A survey of attacks on Ethereum smart contracts (SoK). In In Proceedings of the International Conference on Principles of Security and Trust, Uppsala, Sweden, 24–25 April 2017; pp. 164–186.
71. Lightning Network. Available online: https://lightning.network/ (accessed on 19 February 2018).
72. Raiden Network. Available online: https://raiden.network/ (accessed on 19 February 2018).
73. HACKEN. Tokenized bug bounty marketplace driven by white hats. Available online: https://hacken.io (accessed on 19 February 2018).