Journal of Parallel and Distributed Computing 138 (2020) 99–114

Contents lists available at ScienceDirect

J. Parallel Distrib. Comput.

journal homepage: www.elsevier.com/locate/jpdc

Blockchain 3.0 applications survey

Damiano Di Francesco Maesa [a,*], Paolo Mori [b]

[a] Department of Computer Science and Technology, University of Cambridge, United Kingdom
[b] Istituto di Informatica e Telematica, Consiglio Nazionale delle Ricerche, Pisa, Italy

ARTICLE INFO

Article history:
Received 7 December 2019
Received in revised form 23 December 2019
Accepted 27 December 2019
Available online 3 January 2020

Keywords:
Blockchain
DLT
Smart contracts
Distributed Applications

ABSTRACT

In this paper we survey a number of interesting applications of blockchain technology not related to cryptocurrencies. As a matter of fact, after an initial period of application to cryptocurrencies and to the financial world, blockchain technology has been successfully exploited in many other different scenarios, where its unique features allowed the definition of innovative and sometimes disruptive solutions. In particular, this paper takes into account the following application scenarios: end-to-end verifiable electronic voting, healthcare records management, identity management systems, access control systems, decentralized notary (with a focus on intellectual property protection) and supply chain management. For each of these, we firstly analyse the problem, the related requirements and the advantages the adoption of blockchain technology might bring. Then, we present a number of relevant solutions proposed in the literature both by academia and companies.

1. Introduction

Blockchain is an emerging technology which is having an ever increasing spread both in academia and business organizations. Blockchain technology was first proposed to support cryptocurrencies like Bitcoin, so cryptocurrency blockchains and related applications are often labelled as *Blockchain 1.0*. The main achievement of cryptocurrencies is the decentralization of value transfers between untrusted entities, but many other more complex applications can be built on top of this disruptive innovation. The introduction of smart contracts to realize *Decentralised applications* (Dapps), *Decentralised Autonomous Organizations* (DAOs), smart property, smart tokens, etcetera paved the way to automated financial applications based on cryptocurrencies. All these novel applications in the financial area made possible by the union of smart contracts with digital currencies are labelled *Blockchain 2.0*. However, blockchains are not limited to cryptocurrencies, which are just a possible implementation of the broader concept of *Distributed Ledger Technology* (DLT). As a matter of fact, distributed ledgers may contain arbitrary information, not necessarily related to money of finance. All applications of blockchain technology referable to the wider spectrum of non cryptocurrency-related distributed ledger uses are commonly referred as *Blockchain 3.0* applications. We do note that, even if such applications are conceptually independent from cryptocurrencies, they can still benefit from an integration with them, and in practice they are often deployed on a cryptocurrency based blockchain such as Bitcoin or Ethereum. Blockchain 3.0 means porting all the properties obtained by the blockchain trustless decentralization (such as immutability, transparency and no need for intermediaries) to other systems which are built on top of blockchain technology.

Due to the recent hype in blockchain technology, during the last years there have been new proposals for Blockchain 3.0 applications almost everyday, as every company feels the need for a blockchain based solution. The Google trend chart for the terms of the five top searched topics among the six presented in this paper (i.e. excluding Access Control systems) are shown in Fig. 3, to estimate the relative interest in each of them. So it is not surprising that blockchain technology made its way into the prestigious research and advisory firm Gartner report, *Top Trends in the Gartner Hype Cycle for Emerging Technologies, 2017* [111] as shown in Fig. 1. Despite that, the same firm considers most blockchain technologies still a long way from fulfilment, as shown in Fig. 2.

We should remind that the innovative properties of a blockchains are often gained at the expenses of scalability and resource costs. Consequently, only those scenarios where the advantages clearly outweigh the drawbacks will actually benefit of the disruptive possibilities of blockchain adoption.

1.1. Survey methodology

This paper surveys a number of application scenarios where the adoption of blockchain technology has been proposed,

* Correspondence to: Department of Computer Science and Technology, William Gates Building, 15 JJ Thomson Avenue, Cambridge, CB3 0FD, United Kingdom.
E-mail addresses: dd534@cam.ac.uk (D. Di Francesco Maesa), paolo.mori@iit.cnr.it (P. Mori).

https://doi.org/10.1016/j.jpdc.2019.12.019
0743-7315/

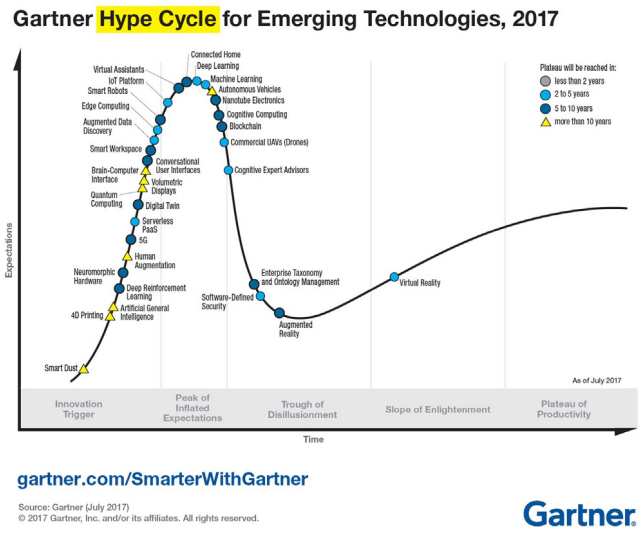

Fig. 1. Gartner Hype Cycle for Emerging Technologies, 2017. *Source:* [111].

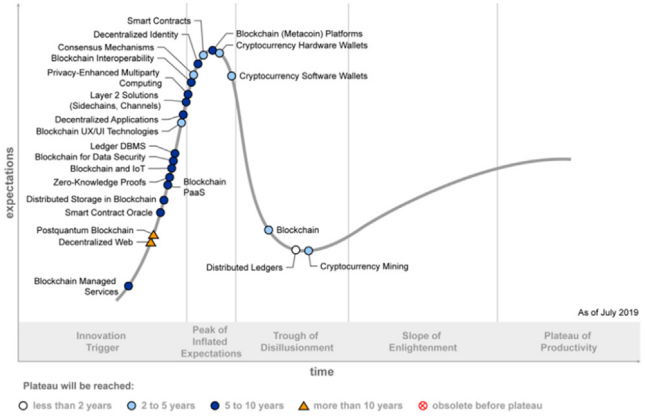

Fig. 2. Gartner Hype Cycle for Blockchain Technologies, 2019. *Source:* [46].

namely: electronic voting, healthcare records management, identity management, access control, decentralized notary and supply chains management. For each of these scenario we give a *Problem Definition*, we describe the relevant *Blockchain Based Proposals* and the main *Cases Studied*. We do note that the list of application scenarios we considered is not exhaustive. In fact the flexibility of blockchain technology makes it suitable for a vast range of applications. However, we believe that the application scenarios chosen are the most promising and studied ones that have not yet been analysed in depth in previous literature reviews. Detailed surveys which are exactly focused on the scenarios not presented in this work already exist in the literature. For example, among those scenarios we list cryptocurrencies [93,125], finance and insurance [84,105] and the Internet of Things [62,83,120]. Similarly, no previous review work (e.g. [19,37,44]) has studied the applications considered in this paper in the same depth.

Moreover, some further scenarios have not been addressed in this paper as well because, although we think that the adoption of blockchain technology could bring relevant benefits, there is still not a mature enough number of proposal in such fields. Among them we list: Energy Trading, Gift Cards, Loyalty Programs, Online Social Networks, Games and Recommendation Systems.

1.2. Paper structure

This paper is structured as follows: Section 2 presents a background concerning Distributed Ledgers and Blockchains, Sections 3–8 present the main applications of such technology to, respectively, end-to-end verifiable electronic voting, healthcare records management, identity management systems, access control systems, decentralized notary, intellectual property protection and supply chains management scenarios, Section 9 discusses the common advantages and drawbacks of blockchain usage in the previously listed application scenarios and, finally, Section 10 concludes the paper.

2. Background

2.1. Distributed ledger technology

A *distributed ledger* [115] (often referred as *DLT*, from Distributed Ledger Technology) is a decentralized repository of data managed and maintained by many participants, without necessity of assuming trust among each other. In general, the participants have the same rights and control over the repository, and communicate directly between themselves in a P2P fashion to propose and notify updates of such repository. Often such updates satisfy an append only rule to guarantee the data immutability property. There is no need for intermediaries nor for a centralized controller, since the participants employ a distributed consensus algorithm to reach a decision on the updates to be made to the repository.

Even if it is called *distributed* ledger it would be technically more precise to call it *decentralized* ledger. In fact, in computer science the term *distributed* is mainly used to indicate a network of autonomous entities communicating between themselves to reach a common goal, like a distributed ledger, but, in general, no coherence is assumed between the participants. Each node could be executing a completely different task while communicating its result as data for the other nodes. For example, a distributed system can be employed to coordinate a set of threads computing different algorithms. In a distributed ledger, instead, each (compliant) node is expected to follow the same protocol to reach the same result (each time a consensus is reached), i.e., each honest participant should end up with the same copy of the repository. In fact there is no unique agreed ledger, instead a copy of the same ledger is stored and maintained by each node, and the ledger held by the majority of the network (non necessarily a numerical majority) is considered as the correct one. Formally, it is more correct to say that the ledger is *replicated*, since a copy of it is stored by each participant and the same management operations are repeated by all of them locally.

2.2. Blockchain technology

Blockchain is just one possible technology to implement a distributed ledger. A blockchain implements a distributed ledger by grouping records (i.e., ledger state updates) into blocks that are made tamper resistant by adding a cryptographic signature of the block data. Usually, this is achieved by adding a cryptographic hash of the entire block content in the block header. The blocks are then chained together by back-linking each block to the predecessor in a tamper resistant way. Again, the most common way of achieving this is through cryptographic hash functions, by adding the hash of the previous block in the following block header. By making each block recursively dependent on both its content and the previous block in the chain, such block becomes dependent on the entire content of all the blocks before it, all the way to first block created (often called the *genesis* block). This

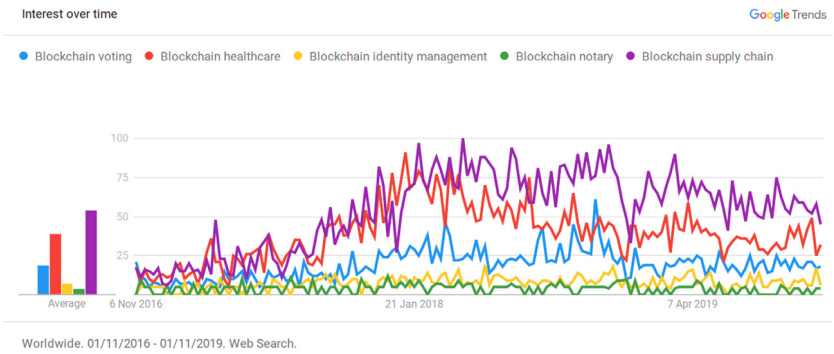

Fig. 3. Google trends [49] chart from 1st of November 2016 to 1st of November 2019 for the search terms *Blockchain voting* (blue), *Blockchain healthcare* (red), *Blockchain identity management* (yellow), *Blockchain notary* (green) and *Blockchain supply chain* (purple). (For interpretation of the references to colour in this figure legend, the reader is referred to the web version of this article.)

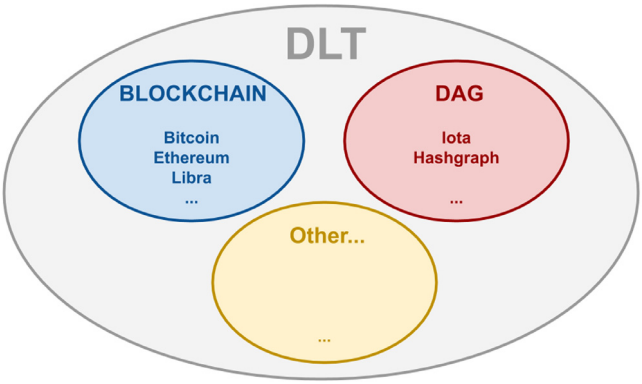

Fig. 4. Distributed ledger technology implementation proposals topology.

way it is not possible to modify any data inside a block without invalidating all the subsequent blocks [79].

Implementing a distributed ledger with a blockchain allows to build an immutable, distributed, always available, secure and publicly accessible repository of data [44]. Often, the records stored in each block are called *transactions* due to historical reasons [79]. In fact, blockchain technology was first introduced to support cryptocurrencies (by the Bitcoin cryptocurrency protocol [79]) and in such a scenario the blockchain is used as a public ledger to store transfers of value between entities, called transactions.

The main issues with blockchain implementation of distributed ledgers are scalability and efficiency [44]. A pure blockchain often uses expensive distributed consensus algorithms to guarantee an eventual consensus on the repository consistency in a trustless environment. But more efficient and simpler consensus algorithms are possible if we relax the trust assumptions in the system. In general, the more trust we place on entities and the more efficient the system gets, but often also more centralized. The different types of blockchains basically differ for the trust level associated with *write* and *read* operations. By write operation we mean the ability to update the ledger, i.e., write content on it, while by read operation we mean the ability to read the blockchain content. Blockchains are called public (resp. private) whether any trustless (resp. only trusted) entities can read. They are called permissionless (resp. permissioned) whether any trustless (resp. only trusted) entities can write [83].

A blockchain can contain any type of data in its records, also code. But storing and executing is not the same thing. Coupling executable code with blockchain technology allows for the so called *smart contracts* [122]. The term *contract* in the name can be misinterpreted, a smart contract is simply code containing arbitrary programming logic, not necessary a contract between entities. A smart contract supporting blockchain is a blockchain where the distributed consensus validates also the execution of the code contained in each block. Basically, each function call to the code repository stored in the blockchain is executed sequentially in the current block state, and the final state is updated accordingly [121]. Given a block, each participant can re-execute the function calls it contains and check if the results are correct, i.e., the same they obtained. Executing a smart contract in the blockchain guarantees it a set of new properties, like:

- *atomicity*, an operation runs entirely or fails without affecting the state;
- *synchronicity*, the code is executed in a synchronous way;
- *provenance*, the code can only be executed by traceable external calls;
- *availability*, the code and associated data is always available;
- *immutability*, the code cannot be changed or tampered with after deployment;
- *immortality*, the code and data can only be removed if it commits a self destruct operation.

We do remark that blockchain is just a possible implementation of a distributed ledger, not the only one. For example, distributed ledgers not implemented with blockchains are Radix [92], IOTA [57], Hedera Hasgraph [52] and R3 Corda [91], see Fig. 4.

3. Electronic voting

In this section we present the possible application of blockchain technology to *electronic voting* (or *e-voting*) systems. We remark that e-voting refers to a very specific application, i.e., we define electronic voting any type of voting system where votes are cast and tallied through electronic systems [3]. This is in general not the same as *distributed* or *digital voting*. While distributed voting is a general enough process to refer to a broad array of applications (for example leader election between autonomous agents), e-voting was born with the precise use case of human political elections in mind. In this framework, e-voting may apply to many different voting schemes, not only related to political elections (that may have different rules themselves depending on the country), but also, for instance, to stock holders voting on corporate decisions.

3.1. Problem definition

E-voting presents advantages and drawbacks compared to traditional voting systems. For example, a usually mentioned advantage is the greater turnout expected [113], especially for e-voting

systems allowing remote voting (i.e., the ability to vote without having to physically go to a designated voting booth). For voters, expressing their preferences through few clicks on a digital device without leaving their homes might save time and money, easing the election burden (both as time consumption and monetary cost) on the single user as well as on the entire society. It might make voting especially easier with voters with special needs or reduced mobility, as well as voters travelling abroad or busy working. This is even more true if the voting procedure is repeated often, like for direct democracy initiatives. One of the main disadvantages is the increase risk for election tampering, since by basing the voting system on electronic devices we expose it to hacks of such devices. Moreover the risk-reward trade-off of an attacker is higher, since the hack attempts require less resources and can be conducted on a much greater scale than traditional physical systems [80]. Furthermore, the proposed systems might look more complicated than traditional ones, for example if a system requires public key cryptography it usually entrusts the voter with the security of a private key, and most users may compromise their security by not protecting such secret information adequately. This also opens a new attack venue for an adversary that could try to steal such private information from the users.

E-voting requires the satisfaction of some precise properties derived from the original human use case, which mainly concern security, auditability and privacy and, when satisfied, allow a so called end-to-end (E2E) verifiable voting system [20]. By security and auditability we mean that it is not possible to tamper with a vote (i.e., changing the preference expressed by the voter) without the voting entity ability to notice that. Mainly the voter should be able to check that each vote was cast as intended, recorded as cast and tallied as recorded. Any outside observer should also be able to verify the election result (i.e., all and only allowed votes were considered and tallied correctly) without having been involved in the election. Furthermore we could desire that the voters should be able to prove to a third party authority that those checks failed (and so their votes were tampered with) without sharing any private information about their votes. By privacy we mean that each vote should be only known to the voter even while voting. A stronger voter privacy property called "coercion resistance" might also be required, which means that the voters could pretend to cooperate with a malicious entity while instead voting their own choice [61].

Usually E2E voting is achieved by creating a receipt for the voter representing their vote in an obfuscated way [80]. This receipt is used alongside some public data stored on a bulletin board, that, coupled with the private information of the receipt, should provide auditability. No information should be leaked from the bulletin board nor the receipt about each vote, the only source of information should be the result itself. Finally we note that no security assumptions (i.e., not to be malicious or faulty) are bestowed on the voter, the voting devices or the election authority, they are all considered untrusted by each other.

3.2. Blockchain based proposals

Curiously enough, the first proposal of an e-voting system is from Chaum in 1981 [20], the same author of the first digital currency scheme two years later [21].

Several proposals have emerged on how to implement an e-voting system on top of most popular blockchains available today. Of course the easier platform to achieve such goal is a Bitcoin-style cryptocurrency oriented blockchain. In the following we show the outline of a possible implementation of an e-voting system in such a scenario, based on real existing proposals. In general the voting process takes place in three conceptually separated steps: voters registration, vote casting and votes tallying.

At voter registration time, the system needs to enforce voter eligibility, i.e., it verifies that all and only entitled voters are allowed to cast a single vote. The general scenario includes a centralized trusted authority to recognize allowed voters. The simplest solution to achieve this is for voters to create a new address (i.e., cryptographic key pair) and advertise it to the authority. The authority can then send a token payment to the address from one of its publicly known addresses, or publish the voter address in an eligible voters public list. At the same time, each candidate advertises a set of addresses representing themselves (of course it is in the interest of the candidates not to advertise addresses they actually do not control). To cast a preference each voter sends their received voting token (or a freshly created token in case of eligibility list) to an address of the chosen candidate. The tally can then be done by simply counting all the tokens received by each candidate set of addresses.

This simple framework is not complex enough to guarantee E2E voting security, but is helpful to easily show advantages and drawbacks of using a public blockchain. First of all we note that using a public blockchain trivially protects the system from a malevolent election authority. Since the authority has no control neither at casting nor at tallying time it cannot tamper with the election. This can be weakened in systems relying on a permissioned blockchain, which still rely on a trusted entity to evaluate voter eligibility, but this is inevitable in traditional systems and still auditable in case of unduly denial of voting rights or fake voters forging. A voter can prove that they were not included in the eligible list or show that their address has not received any voting token (but at the price of disclosing which address belongs to it). The process should be of course secure enough to guarantee that the eligibility authority cannot fraudulently link voters with bogus addresses they control (for example by requiring an unforgeable voter confirmation step). On the other side an external observer can chose a set of addresses that voted and challenge the authority to show that those addresses really corresponded to rightful voters. Furthermore is important to note that it is needed to also employ obfuscation techniques to prevent a direct linking between voting address and voter identity in the eligibility authority table, otherwise the authority would be able to see what candidate each voter choose, breaking the fundamental vote secrecy property. Another important issue of such systems is that it allows for real time tallying, which is, is in general, a non desired property, since it can influence the election outcome, and, more seriously, it can leak vote private information if a precise enough timing analysis is possible.

If we compare this simple system with the general E2E voting approach described in the previous section we clearly see how blockchain technology is used as the bulletin board of the system. This is the main conclusion reached in [80]. Not only a blockchain satisfies all the properties required from a secure bulletin board but it also introduces new useful properties. As already stated, a public blockchain decentralizes the bulletin board management and control hence protecting the e-voting infrastructure from an untrusted central authority. This would also contribute to system robustness and availability since it would rely on the resilience of the underlying blockchain. On the other hand, voting would require to create transactions and so pay fees in a public blockchain. This could harm usability and vote accessibility.

Several proposal have been advanced to use the novel smart contract capabilities offered by recent blockchains. There is no common implementation to outline here but they all rely on the principle of delegating the aforementioned operations of voter authentication, votes casting and tallying to smart contracts. This allows to have smart ballots and smart tallying contracts, possibly able to enrich the system with new functionalities. We do remark that this introduces further problems of scalability depending

on the blockchain chosen. In fact, if the smart contracts are required to perform costly cryptographic operations they could become too slow and too costly in practice for an useable system supporting a high number of users. For example the *Open Vote Network* smart contract based implementation proposed in [74] could support at most sixty voters with the Ethereum block gas limit of 4 700 000 gas that was enforced when [74] was written.

We recall that, in Ethereum, every transaction has to pay a fee, proportional to its complexity, to be inserted in a block, in order to repay the miners of their effort. Every operation of a smart contract has a price, called *gas*, and the total gas of a transaction is the sum of all the gas of all the operations it contains. The gas limit of a block is the maximum amount of gas that can be spent to execute the transactions contained in that block.

Nowadays, the block gas limit has almost doubled (about 8 000 000 gas at the time of writing, i.e., block of Ethereum main chain at height 9 063 545). Because the cost of the transactions presented in [74] is linear in the number of voters this would mean that only elections of at most about 100 voters are in practice currently supported. Moreover, very high transactions fees should be offered to ensure that such demanding transactions (i.e., consuming alone a high percentage of the available block gas) would be executed in a timely fashion.

3.3. Cases studied

In the following we summarize the main proposals both commercial and academic that we found in the available literature (see Table 1). Do note that due to the novelty of blockchain technology almost all of the existing systems have been proposed in the last three years (i.e., since 2016). The most cited commercial proposal is BitCongress [9], even if the system seems to have been since discontinued. It used Bitcoin coloured tokens through Counterparty [25] to authenticate voters and cast votes, and Ethereum smart contracts to tally votes. Each voter was identified in the system with only one vote associated to them during their lifetime, unfortunately this prevents a voter from taking part in multiple elections at the same time. Another famous proposal was *FollowMyVote* [38,43] from a no-profit organization. The project is open source and based on BitShares [11], a fork of the Bitcoin protocol. The underlying not so popular blockchain makes it more vulnerable and less robust. The system allows for three different election types: Proportional Representation, Mixed Member and Majority. It still requires a central eligibility authority, with blind signatures to obtain voter identity obfuscation. Other proposals using Ethereum include *Procivis* [88], the aforementioned Open Vote Network implementation [74], *Democracy.earth* [28], and *Polys* [87] over a private Ethereum fork. Proposals to use a blockchain with traditional voting booth electronic devices are *VoteWatcher* [119] and *VoteBook*, [63]. Other projects include blockchain agnostic *Secure.vote* [96], commercial *Votem* [118] and *TIVI* [109], academic *VOLT* project, Spanish *AgoraVoting* over Bitcoin [1] and *Inno.vote* over the *BallotChain* blockchain [56]. Unfortunately all this projects have no E2E voting security formal proof.

Only a few formal academic proposals have been presented (e.g., *Remotegrity* [127]), we will show them in temporal order in the following. The first such proposal was [129], based on the scheme of a distributed lottery and using zero knowledge proofs [42] over the Bitcoin blockchain. Another work, [69], proposed an alternative approach using a trusted third party to manage the eligibility process. The proposal is applicable either to the Bitcoin blockchain or any permissioned blockchain and follows the same general scheme outlined before about voting schemes in Bitcoin. A similar proposal is shown in [26], using blind signatures alongside the Bitcoin protocol. A weakness of the proposal is the requirement for prepaid Bitcoin cards to be given to the voters. A similar scheme was used in [104], but based on Zerocoin to enhance voters privacy. Similar approach is used in [106], that uses Zcash instead to anonymize transactions. After the aforementioned proposal on Ethereum using smart contracts [74], in [7] the authors propose a new e-voting system based on a Shamir's secret sharing scheme built over multisignature PayToScriptHash scripts on the Bitcoin blockchain. They also present an enhancement of the CoinsShuffle [95] technique, called *CircleShuffle* to further decouple the inputs of a CoinShuffle transaction from each output. Finally another proposal on Bitcoin following the usual scheme was presented in [8]. Nevertheless it does not satisfy all the E2E secure properties and the authors suggestion to use a permissioned blockchain to alone solve the issue might not be enough.

Table 1
Blockchain voting systems.

Name	Link	Blockchain used
Open Vote Network	[74]	Ethereum
BitCongress	[9]	Bitcoin
FollowMyVote	[43]	Bitcoin fork
Procivis	[88]	Ethereum
Democracy.earth	[28]	Ethereum
Polys	[87]	Ethereum fork
Votem	[118]	Ethereum
AgoraVoting	[1]	Bitcoin
Inno.vote	[56]	BallotChain
Academic proposals	[7,26,69,129]	Bitcoin
Academic proposal	[104]	Zerocoin
Academic proposal	[106]	Zcash

3.4. A final remark

As we have seen in the previous sections, Blockchain technology in general already employs an idea of distributed *voting* (not properly e-voting) to achieve a consensus on the next block to be appended to the chain. Most distributed consensus algorithms proposed can be seen as distributed voting algorithms to chose a miner to add the next block to the chain. In those systems miners have different voting weight according to their commitment to the election. The commitment is expressed in different ways depending on the consensus algorithm chosen, for example with Proof of Work (PoW) [81] miners show commitment by dedicating computational power, while with Proof of Stake (PoS) [81] they show funds ownership. The main difference with respect to real voting systems is that the election of the miner is probabilistic, i.e., each "candidate" has a probability to win proportional to the number of votes he receives, but there is no certainty that the candidate with the most votes will win. Nevertheless on the long run the system will converge to reflect the voters will through the number of blocks mined by each candidate (even if this can be further complicated by the dynamic nature of miners that can freely enter and leave the system). This is why in practice the consensus algorithm has been used as a tool to vote on important decisions for existing blockchain protocols. For example the Bitcoin community has often employed this trick to decide on protocol upgrades. Miners are asked to cast a vote about the upgrade as data in their coinbase transaction. This allows to have an approximation of the mining community will once enough blocks have been mined. This approach feels natural for a cryptocurrency such as Bitcoin where a protocol upgrade could require a hard fork that might not be accepted by all the users and may cause a harmful split in the network. Casting votes in real blocks allow to check if the vast majority of miners really contributing to the network at the time do agree with the proposal.

4. Health care

4.1. Problem description

In the digital era more and more private information about ourselves is stored and managed electronically. Being related to an identified or identifiable living individual, that information are called *Personal Data*, and it needs to be properly protected from unauthorized accesses with adequate technical solutions, as stated by the General Data Protection Regulation (GDPR) EU 2016/679 [107]. One kind of personal data is health data: each medical examination produces valuable sensitive data belonging to the patient that needs to be properly shared with doctors, pharmacies, insurance companies or other healthcare scenario stakeholders but, at the same time, protected from other accesses. Nowadays, most national health systems are trying to collect all personal medical information related to the same patient in a unique electronic medical record, called Electronic Health Record (EHR). Such a record contains very sensible information produced during an entire lifetime, and yet it is often managed by medical institutions and practitioners not technically aware or equipped enough to guarantee the appropriate security levels. Moreover, most medical institutions store and create patients' medical records in different formats often not compatible not only among different nations, but sometimes even among different labs inside the same hospital. The need for a system to manage and store medical records in a secure way has led to a lot of proposals to use a blockchain.

4.2. Blockchain based proposals

Despite the many proposals, most of them follow a common general idea: a system storing medical personal records on a blockchain under the control of their owners. The cryptographic security (digital signatures, etc.) is leveraged to enforce that the users would be the only one in charge of their digital information, hence the only one able to grant access to their own records [59,126].

Storing the entire records on the blockchain would not be a good idea for two main reasons. First, it raises obvious privacy concerns since all data in the blockchain would be visible to all other users. Of course the data could be encrypted, but this could still not be enough from a legal point of view. Moreover, the public and immutable nature of the blockchain would mean that the encrypted data would remain forever visible on the chain. If a future technological advance would make the security mechanism used to protect that data no longer secure, then its content could be retroactively read. The second reason is that the record could become very big in size. The medical data contained inside the record is by its own nature space demanding, because it could comprehend a lot of images (for example from Magnetic Resonance Images) and because it keeps growing as the patient ages. The medical record of a lifetime would take a lot of memory to be stored. On the other hand, blockchain space is scarce due to its decentralized nature, and the entire blockchain with all its data should be replicated on each node, so each bit it contains consumes storage space for each node. It would also negatively impact the performance of the communication network, since big blocks to store a lot of new data would require a lot of bandwidth to be relayed among nodes, delaying new blocks discovery notifications and so potentially increasing natural forks probability (which are causes of wasted mining resources for the entire network). This means that it is in practice unfeasible and not desirable to store entire medical records on the blockchain. Luckily this is not necessary, and all the proposed systems work all the same by simply keeping on chain only pointers to where the records are actually and securely stored. This is the same approach proposed in [130] to manage personal data in general through a blockchain. In those systems, the blockchain acts only as a decentralized secure system where users can manage the access to their personal records [15,70,85]. The real data is stored off-chain in a traditional manner, of course with care to preserve the privacy of the content.

In such a system, users alone are in control of their own data by granting or denying access (e.g., to pharmacies or insurance companies) to it. Of course the users do not have to grant access to their entire medical record, but they can choose what data to share with each subject. At any time the users would be aware of who has access to which part of their own data, since they are the only ones able to grant such access. In such a system there would be no intermediaries and no need for trusted third parties. If this system is deployed on top of a blockchain with a native currency, such as Bitcoin or Ethereum, then the users could also be directly paid in exchange for grated accesses, for instance, if the user grants access to their data to a scientific organization for research purpose. Furthermore, since users are in charge of securing their own data, it would relieve both medical institutions and companies from this difficult and costly task. In turn, this would have an impact on the corresponding legal framework, since users are the ones giving consent for the use of their data each time they grant an access. At the same time, the notary nature of the blockchain (due to its immutability and timestamping it automatically constitutes an audit trail) would increase the system transparency and auditabilty. A patient, for example, could prove to have taken a certain test without disclosing personal information or relying on a third party. This would cut expenses for the patient and greatly shorten the time required compared to current systems. Furthermore, it could also help detect health care frauds. Finally, we note that cryptographically advanced solutions could be employed to allow use of the private data without actual data disclosure (e.g., homomorphic encryption computations [48]).

Another advantage of such a system would be the universality of the record format. The blockchain would act as an intermediary that all the different systems have to interact with, dictating a common language to exchange data. This could ease the lack of format interoperability problem often experienced nowadays with personal medical records [128]. The existence of a single point of access for medical information in a single format could also benefit health studies and research. Users could grant access to their medical data for aggregated medical studies, that would benefit from a huge patients base to analyse (potentially in an automated way, e.g., with big data techniques [67]). Users could then be directly rewarded for their participation by blockchain micropayments.

In practice we do not expect a single blockchain to manage the global population medical records, it would be more feasible to have different blockchains at different institutional levels (e.g., from national level to single medical institution level). All those blockchains could be federated to allow interoperability without the need for data replication between one another. We also do not expect all these blockchains to be public. A permissioned solution with medical institutions as nodes would seem like a natural implementation of the system [34]. Furthermore, employing blockchain technologies with smart contracts support would also enable more expressive systems.

4.3. Cases studied

One proposal using smart contracts (on the Ethereum network) is *MedRec* [36], one of the few working academic proof

Table 2
Blockchain healthcare systems.

Name	Link	Blockchain Used
MedRec	[36]	Ethereum
Estonia Healthcare	[53]	KSI Blockchain
Gem	[47]	Ethereum, Hyperledger,...
Hashed Health	[50]	Ethereum, Hyperledger,...
SimplyVital Health	[101]	Ethereum
Robomed Network	[94]	Ethereum
Healthcare Working Group	[51]	Hyperledger

of concept implementation available in the literature. The system follows the basic scheme outlined before, but also introduces an interesting twist. It introduces access to aggregated and anonymized data (useable for example for research) as mining reward to foster participation in the expensive mining process.

Very few proposals have also been presented to apply distributed ledger technology to epidemics relief. Of course blockchain technology through cryptocurrencies can already contribute by allowing direct micropayments to make fast donations. In [23] the author proposes to use a distributed ledger to monitor a disease and its spreading. The concept can be strengthened by coupling the idea with smart contracts capabilities to trigger automatic responses or alarms in case of preconditions concerning the monitoring of epidemics.

Outside of the academic world, many companies have tried to apply blockchain technology to the health care sector. Blockchain technology has even been used in practice to protect electronic medical records in a famous experiment by Estonia [5,53,75]. Among the commercial proposals joining blockchain technology with some aspect of health care we remember *Gem* [47], *Hashed Health* [50], *SimplyVital Health* [101], *PokitDot* [86], *Robomed Network* [94] and *Healthcare Working Group* of the Hyperledger project [51] (see Table 2).

5. Identity management systems

5.1. Problem definition

An identity management system is used to identify an entity (living individual or software) in a digital system and involves all data and means of authentication needed to recognize that entity. Basically, such a system labels each entity with an identifier (usually in a human friendly format, e.g., a meaningful string), it provides a way for the entity to authenticate (often by proving knowledge of some private information, e.g., a password, a PIN, a one-time-password, etc.) and stores its relevant identity information. Identity data can be as simple as name, age, date and place of birth, etcetera, for an electronic passport, or as complex as bank and credit data for a financial application.

Nowadays, identity management systems are mostly centralized and isolated from each other (see Fig. 5(a)). Consequently, users are forced to rely on a different central service to manage their identity data in each different domain. Besides being inefficient and cumbersome for users (forcing them to remember a lot of different private authentication information), this is also dangerous for users' privacy. Moreover, central identity management systems need to be trusted by users not only to not maliciously exploit such information, but also to effectively protect it from external attacks, considering also that big quantities of valuable data stored all together in a single place are attractive beacons for hackers. To improve user experience, federated identity systems have been proposed [108,110], where identity managers remain centralized for each domain but users can use the identity of a single domain to access all the federated ones. The identity portability between systems can extend beyond authentication also allowing for some identity data to be shared. Even if this solution eases the burden on users, it still gives them no control over their identity data that remain centralized for each domain as before.

A *user-centric* identity management system [17], instead, would solve privacy issues by putting the user in charge of their own identity data, not third parties. Basically a user-centric identity system is a federated system where the identity control is given to the user. Its natural implementation is to use a blockchain (or any other distributed ledger implementation) to obtain *self-sovereign* identity systems such as the ones presented in [108,110], where the identity management systems are agnostic of the underlying applications using them (see Fig. 5(b)).

5.2. Blockchain based proposals

The idea of a self-sovereign identity system based on blockchain is no different from the idea of blockchain based personal health record shown in Section 4. As a matter of fact, if we consider health data as identity information the systems are interchangeable. For example, in [18] a DLT based self-sovereign identity systems is described as allowing entities to create immutable *identity records* represented as *identity containers* able to *accept attributes or credentials from any number of organizations [...]. Each organization can decide whether to trust credentials in the container based on which organization verified or attested to them*. This is exactly the same concept behind blockchain based health records and, as such, they share most of the advantages. If we analyse the desired properties required by such a system stated in [108], we notice that they can be satisfied by a public blockchain based implementation:

- Control. *Users must control their identities.*
  Access. *Users must have access to their own data.*
  Consent. *Users must agree to the use of their identity.*
  A blockchain is censorship resistant, users not only are free to join independently from any third party, but are also the only ones controlling their own data, they can access and update it without intermediaries, and they alone decide to whom to grant access to it.
- Minimalization. *Disclosure of claims must be minimized.* This can be achieved by storing the identity data in a secure way to provide users privacy. Of course no private data should be stored in plain on a publicly accessible blockchain. As we have already explained for health records in Section 4, data can be stored in encrypted format on the blockchain, and advanced cryptographic techniques (e.g., zero knowledge proofs [42] or homomorphic encryption [48]) can be employed to verify some data properties without actually disclosing it (e.g., proving that a user is older than eighteen years old without exposing their age). However, it should be noted how such techniques usually introduce a cost or efficiency burden on the system (see [6] for an evaluation of existing proposals).
- Existence. *Users must have an independent existence.* This is clearly true in a blockchain, that is independent from the applications using it.
- Transparency. *Systems and algorithms must be transparent.* This is guaranteed by the decentralized, open source and non-proprietary nature of a public blockchain.
- Persistence. *Identities must be long-lived.* Identities and their data would last as long as the underlying blockchain is not abandoned. The use of an immutable blockchain however could lead to issues to guarantee the opposite of this principle that is sometimes required: the *right to be forgotten*. A blockchain based system wishing to grant this property should be designed accordingly.

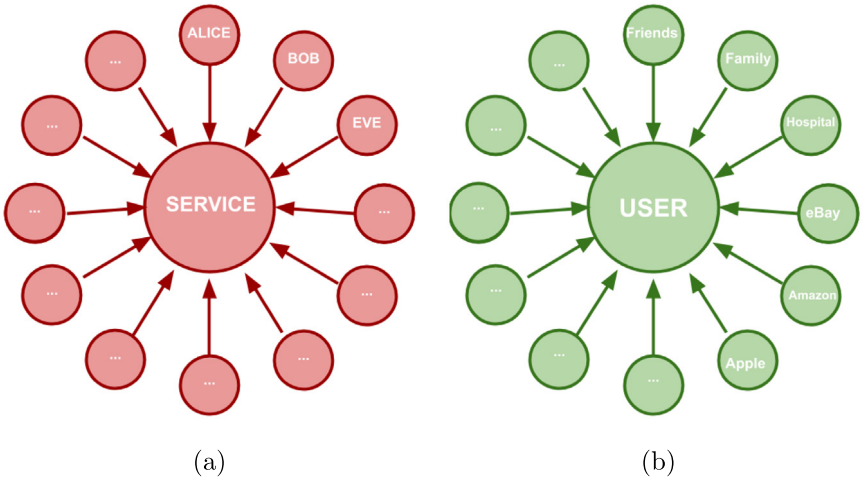

Fig. 5. Traditional centralized (a) and self-sovereign (b) identity management system schemes. Inspired by [4].

- Portability. *Information and services about identity must be transportable.* This is trivial using a blockchain that constitutes the only point of access for external services requests, provided that a well known standard representation of such information is adopted. Hence, each application would be able to exploit user information by accessing the blockchain. The user remains the only one in control of their identity independently from the systems exploiting it.
- Interoperability. *Identities should be as widely useable as possible.* This is related to the previous bullet and is granted by using a blockchain as single hub for external systems to interact with. As for the Portability property, a common standard representation is needed.
- Protection. *The rights of users must be protected.* Guaranteed by the security and decentralization of the cryptographic functions underlying blockchain technology.

As pointed out in [110], those properties are all expression of the three main properties usually required from an identity system:

- **Security**, the identity information must be kept secure
- **Controllability**, users must be in control of who can access their data
- **Portability**, the user must be able to use their identity data wherever they want and not be tied to a single provider

Besides the user direct control of their own data and the censorship resistant inclusiveness pointed out before, a decentralized blockchain could also lead to the practical advantage of reduced expenses. This is not only true for the users, also counting the potential costs of identity thefts and private data leaking of traditional centralized solutions, but also for the external services that would not have to store and protect any more private information. As a whole, private information would only be managed by the users, so there would not be the need to replicate it among the interested services with the related costs and privacy issues.

We also note how blockchain could in practice introduce novel issues for users, especially about the practicality of the system. For example, users would be alone in charge of the management of all the cryptographic keys protecting their identity information. In practice trusted escrow systems, possibly at a state level, could be necessary to recover lost keys or roll back mistakes made by users. For examples Id-cards issued by the government storing the corresponding keys could be employed, accepting the need for trust in the government issuing them.

5.3. Cases studied

Several proposals and actual blockchain based identity management services have emerged during recent years (see Table 3). In [35] the authors identify *uPort* [117], *Sovrin* [110] and *ShoCard* [100] as the three most representative proposals. uPort implements a self-sovereign identity system through smart contracts on the Ethereum blockchain [116]. As such, external services can interact through other smart contracts. The identifier of a user is the Ethereum address (called *unique uPort identifier*) of its main identity manager contract, and the connected identity data is not stored directly on the blockchain but rather through the hash of the actual data that is stored on IPFS [58]. Sovrin, instead, builds its self-sovereign identity system on a public but permissioned ad hoc blockchain [102]. The trusted miners, called *stewards*, are controlled by the non-profit *Sovrin Foundation* to ensure their honesty. Even if data can be stored on chain, it is advised to store it locally and disclose only to agreed parties through cryptographic side channels. Same as uPort, there exists a feature based on a list of trusted entities to recover an identity in case the corresponding secret key gets lost. Differently from the two previous examples, ShoCard is not used to build a self-sovereign identity system, instead, it relies on a centralized service that creates and stores user identities on a blockchain (based on Bitcoin [99]), alongside pre-existing identity certifications (e.g., driver's license). That information can later be linked and verified to prove entity identities. A user creates an initial transaction to start a new identity, and their identifier (called *ShoCardID*) is the hash of that transaction. Using that identifier as an anchor, additional identity information can be added to the user or verified. The need for a centralized service (the ShoCard server) makes the system actually centralized, since despite relying on a public blockchain it would be rendered unusable if the central server were to go down. ShoCard and the other systems with a similar paradigm (e.g., BitID [10] and IdchainZ [54]) are unable to provide a real self-sovereign identity system. More proposals and actual services related to identity systems employing blockchain technology at some extent can be found in [18] and [60].

6. Access control systems

6.1. Problem definition

Access control systems are aimed at regulating the accesses to valuable resources according to the security and privacy requirements defined by the related owners. In particular, resource

Table 3
Blockchain identity management systems.

Name	Link	Blockchain used
uPort	[117]	Ethereum
Sovrin	[102]	Custom permissioned blockchain
ShoCard	[100]	Bitcoin
BitID	[10]	Bitcoin
IdchainZ	[54]	ChainZy

owners typically choose an access control model suitable for the requirements of their environments (e.g., Role Based Access Control, Attribute Based Access Control, History Based Access Control, Usage Control, etc.) and then they express their security and privacy preferences by choosing a policy language for that model (e.g., Attribute Based ones like XACML [82], History Based ones like [73], etc.). To enforce such policies when subjects request to access the resources, the owners need to deploy proper Access Control systems implementing the models they chose.

A solution for resource owners is to deploy and run their own instances of such Access Control systems on their premises, but this requires them to deal with the configuration, deployment and management of these Access Control systems, thus implying a notable effort. To avoid this burden, an alternative solution for resource owners is to outsource the Access Control functionality to external systems or services which, obviously, must be operated by trusted third parties in order to be guaranteed of the enforcement of the requested policy thus avoiding unduly authorizations or denials of access. For example, some Access Control systems implemented as Cloud SaaS (Software as a Service) services have been proposed, such as OpenPMF SCaaS [68]. These services often use an open-platform API, in a way such that their users are not bounded to use a specific implementation, but they can exploit them to have a uniform management of policy enforcement for all the resources they own.

6.2. Blockchain based proposals

An alternative solution for outsourcing the Access Control process is to implement Access Control systems on top of blockchains. In fact, smart contract capabilities can be exploited to execute the whole (or some phases of the) policy evaluation process on the blockchain. In particular, the blockchain can be used to store Access Control policies, access requests (issued by the subjects who want to access the resources) and the related results (access permitted/access denied), as well as for executing the access decision process, i.e., to evaluate the relevant policies against the access requests [30]. An Access Control policy could be represented through a smart contract, created and stored on the blockchain by the resource owner [31]. Since the blockchain is an append only ledger, the policy, in smart contract form, will be stored on the blockchain forever but, for instance, it could be logically replaced by uploading on the blockchain a new one. Other data concerning the access decision process can be stored on the blockchain as well. For example, the Attribute Based Access Control model exploits attributes for representing relevant features of subjects, resources and environment. Those attributes could be managed by smart contracts as well, and the policy smart contracts could invoke them when they need the current values to carry on the decision process (as proposed in [29]).

A blockchain based Access Control system would inherit from blockchain technology some relevant advantages which ease auditability. In fact, both resource owners and subjects accessing resources are enabled to verify how the policy has been evaluated for each access request that has been performed thanks to the properties of transparency, immutability and permanent storage of a blockchain. This means that users can always browse the blockchain and control the access requests that have been performed on a given resource, the policy that has been enforced, the values of the attributes at that time, and the resulting access decisions returned as response to their access requests. Obviously, this could raise privacy issues that should be taken into account.

Table 4
Blockchain access control systems.

Proposal	Link	Blockchain used
ABAC policies management	[30]	Bitcoin
Smart Policies	[32]	Ethereum
External data protection	[130]	Bitcoin
SCARAB	[64]	cothority-ByzCoin
RBAC with smart contracts	[27]	Ethereum
IoT data	[97]	Bitcoin
BlendCAC	[124]	Ethereum
Privacy aware AC	[98]	Tangle

6.3. Cases studied

A complete blockchain based Access Control system implementing the Attribute Based Access Control model has been presented in [32]. This approach adopts XACML as policy language and exploits the Ethereum blockchain for implementing all the phases of the policy evaluation process. As a matter of fact, both the engine which evaluates the security policy against the current request and the managers of the attributes required for the policy evaluation are implemented as interoperating smart contracts and, consequently, are executed on the blockchain (i.e., by the miners). Only the policy writing and creation phase is performed off-chain, because the translation of the policies from XACML to Ethereum smart contracts would be too expensive to be executed on-chain. Another proposal is presented in [130], where the authors combine blockchain and off-chain storage to build a personal data management platform focused on privacy protection. However, the proposed approach is not a general Access Control system, but it simply controls the read operations on the data stored by the users. The authors of [64], instead, proposes a method to store secret data (i.e., encrypted data) on a blockchain, managed by a set of trustees that are in charge of controlling the access to such data. In this case, the blockchain is used as a tamper proof log of access requests and to guarantee operations atomicity. A Role Based Access Control system which uses smart contracts and blockchain technology as infrastructures to represent the trust and endorsement relationship essential to realize a challenge-response authentication protocol that verifies users ownership of roles has been proposed in [27]. Finally, in [97,98,124], and [2], the blockchain is used as Access Control tool for the Internet of Things (see Table 4).

7. Decentralized notary

7.1. Problem definition

The intuitive idea behind a notary is to have a trusted witness to the ownership or ratification of an agreement between mutually untrusted parties. In the digital space, often notary services are required to prove the existence and ownership of a given digital asset at a given time. A decentralized or distributed notary aims at achieving the level of trust of a trusted third party, without actually relying on any. This makes blockchain protocol particularly effective for such tasks. Blockchain was invented, in fact, to manage a decentralized ledger, i.e. a special case of decentralized notary where digital assets represent financial value.

7.2. Blockchain based proposals

The immutability and timestamping properties of a blockchain allow to store on it a piece of data at a certain time with the guarantee that it will not be modified in the future. This leads naturally to the idea of using the blockchain as a decentralized notary system. It means that users can submit any information to the blockchain, and then, through the distributed consensus, the miners community will add this information to a block at a certain time. Since it would then be unfeasible to modify such a block in the future (under blockchain security assumptions), it is possible to prove that at that time that piece of information existed and was not tampered with. If the information stored represents the cryptographic hash of an electronic document then it is possible to prove the document existed unmodified at that give time. This timed proof of existence is the main functionality of the so called *blockchain notary systems*. Sometimes this property is also called *proof of ownership* to stress the property of pre-image resistance of cryptographic hash functions, that implies that only someone actually owning the document could have computed the correct hash value stored on the blockchain. Moreover, if the hash value was submitted to the blockchain through a signed transaction, the signature can be used as further proof of ownership.

7.3. Cases studied

A traditional notary has to perform additional services (not including all the legally mandatory controls) like checking for parties identities and witnessing that they are the ones signing the document, confirming that the parties are aware of the content of the document and are willing to sign it, checking if a new agreement is in conflict with an existing previous commitment, etcetera. If a blockchain notary wants to completely cover a traditional notary role it needs a more complex infrastructure built around the blockchain to provide all those functionalities (like, for example, an identity management system). Nevertheless most blockchain notary systems available today only offer the aforementioned proof of existence. Some examples of such services are shown in Table 5.

We do note that such simple systems have some intrinsic limitations, for example the timestamp associated to the data (i.e., the timestamp of the block the data is contained in) is not accurate for two reasons. First, the block timestamp is not accurate (it is the tamperable local time of the miner who builds it), and it can vary by at most two hours from the expected one. This means that a subsequent block can have a lower time than its predecessor. By tampering with the block times, a malevolent miner powerful enough may successfully invalidate the system. Furthermore, the timestamp of the block only records the time when the transaction submitting the data is accepted, not when it was submitted. This means that the two times may differ greatly and race attacks might be possible. This would be an issue in those scenarios where the precise time when a transaction is submitted is crucial, such as in some supply chain tracking systems. A Blockchain only provides a (discrete) temporal ordering between transactions.

Time inaccuracy can be a deterrent also to a possible novel application of blockchain notary systems, e.g., machine to machine proof of existence, where the existence of a document needs to be produced and verified within minutes. Nevertheless, blockchain technology allows for proof of existence between automatic devices for three main reasons:

- it allows automatic recording and checks for content existence;
- it provides formal guarantees of security for the system without the need for trust between the parties;
- it greatly lowers the cost to record or check existence proofs.

The last point is especially important when coupled with automation. A traditional notary is orders of magnitude more expensive and slower than a blockchain based proof of existence system (hundred or thousands of dollars and days versus few cents and minutes). This opens the possibility for automatic devices to automatically record some information regularly in time. For example, the entire profile of a social network user could be recorded at regular snapshots in time to certify the content uploaded and activities carried on. Another field of application might be with IoT devices.

7.4. Application: Intellectual property

The real improvement over traditional systems comes when a notary system is deployed on top of a blockchain supporting smart contracts. A smart contract can not only record the proof of existence of certain data, but also define operations allowed on such data. This opens for entirely new possibilities. For example we can think of a smart notary system for the protection of intellectual property. In fact, blockchain based notary systems can prove the existence (and potentially ownership) of any digital content including music, videos, images and other user creative content (e.g., *Monegraph* that allows to record and trade digital assets on the Bitcoin blockchain [77]). Using smart contracts we could define rules for the fruition of the content, possibly coupled with a pricing of such operations (i.e., royalties) using the underlying cryptocurrency supported by the blockchain (if present). For example, we could deploy a smart contract that not only provides the proof of ownership for a certain new song, but also allows users to purchase the right to listen to such song, paying directly to the owner's address. Such a system would avoid all the intermediaries, allowing the owner to receive the full gain for their creations. Of course users may still have incentives to rely on third parties for advertisement, visibility, etcetera. More importantly setting up a smart contract is way cheaper than traditional means, so new users would have a very low entry cost to start offering their own creations. It also increases transparency, because the owner knows who is accessing their content, and users willing to access it have a clear and cheap entry point to ask the access permission (i.e., what is traditionally called a *license*). The company Ujo Music [114] is already offering such a service using the Ethereum blockchain. Its first proof of concept was deployed in 2015 publishing the song *Tiny Human* by Imogen Heap [55] through an Ethereum smart contract. Another similar service is *MUSE* [78] that instead of relying on an existent blockchain it builds its own.

8. Supply chain management

8.1. Problem definition

A supply chain is the chain of passages (physical or virtual relocation, transformation and exchange) that products or services undergo from raw material or natural resources (including human intellect) to a finished product for the end customer. The management of a supply chain is a complex task that requires to plan all the activities and logistics involved and it spans across many different companies and suppliers, all the way to the customers. Often the management of a supply chain has also to take into account standards and regulations (both from states and companies) that need to be satisfied between links in the chain. In general, there is little to no trust between different nodes in the chain, since trust is built between companies as they successfully work together over time, and this gets more and more difficult in a more open and fluid market. This means that a

Table 5
Blockchain notary systems.

Name	Link	Blockchain used
Blocksign	https://blocksign.com	Bitcoin
Bitcoin.com Notary	https://notary.bitcoin.com/	BitcoinCash
Acronis	https://www.acronis.com/en-us/business/blockchain-notary	Ethereum
Stampd	https://stampd.io/	Bitcoin, BitcoinCash, Ethereum or Dash
Stampery	https://stampery.com/	Bitcoin, Ethereum
Proof of Existence	https://proofofexistence.com/	Bitcoin
ProveBit	https://github.com/thereal1024/ProveBit	Bitcoin
Bitnotar	https://github.com/bitcoinaustria/bitnotar	Bitcoin
Bernstein	https://www.bernstein.io/	Bitcoin

paper trail needs to be produced and verified at each step to try to protect players from counterfeiting and keep the goods moving along the chain. This paper trail can also be required by third party inspectors to verify that no regulations have been infringed. Since the chain spans from raw material to end consumer it is often very long and stretched along different jurisdictions, rapidly becoming cumbersome and expensive to maintain, as well as prone to forgery and human error. It also may cause additional expenses to the parties involved to settle disputes or inadequate goods returns. This often means that in most scenarios the supply chain management costs have a significant impact on the final price of a traded good.

8.2. Blockchain based proposals

As we have seen in Section 7, a blockchain can be effectively used to provide a timestamped proof of existence of a digital asset to create a notary system. This same concept can be extended to a supply chain management system. By digitizing the physical goods, for example by associating them a unique tamper resistant code, and recording on the blockchain all the information associated with them (e.g., price, date, location, quality, certification, etcetera) as well as their passages between links in the supply chain, we can obtain a secure and transparent supply chain management system on top of a blockchain (see Fig. 6). Since all information stored on the blockchain is immutable, it becomes impossible (under blockchain security assumptions) to tamper with the system. The base idea is no different from the original intuition behind Bitcoin, as in Bitcoin the blockchain is used to track the history of each coin to prevent double spending. So in a blockchain based supply chain system it is used to track the history of digital traces of assets. The main advantages of such a system are the following.

- **Increased transparency**. Storing all the immutable information on a blockchain would increase the traceability of products and so enhance trust between parties involved as well as final consumers. Clearly, having an easy traceable chain of transformations of a good will help contrast counterfeits and frauds, as well as ensure intermediaries and external contractor suppliers compliance to corporate standards and regulations. The transparency of the entire process could also enhance the reputation and public image of virtuous companies.
- **Easier auditability**. Any third party having access to the traceable life of a good on the blockchain could check its correctness without need of a slow and costly inspection of an entire paper trail compiled in different formats. The end user itself could verify the origin of the materials used and each transformation step to buy accordingly.
- **Reduced management and verification costs**. Checking or maintaining the trace of a product on a blockchain is way less expensive than examining or creating a long paper trail, leading to huge cost reductions for the companies involved as well as independent auditors. Moreover, the security granted by the blockchain would reduce the need for many intermediaries as well as dispute resolutions, further lowering the companies expenses (and potentially the final price of a good for the consumer). Finally, the contrast to counterfeiting and grey market will further reduce honest parties losses. This is especially true for high value goods such as diamonds and pharmaceutical drugs.
- **Increased management and verification speed**. Events recorded on a blockchain can be created and audited in almost real time, speeding up both recording and verification operations. By adopting a blockchain as data recording standard cuts intermediaries and the process can be sped up as well. Furthermore, the process can be automatized through self enforcing smart contracts to speed up repetitive operations.

By lowering the initial costs and the importance of reputation for suppliers, a blockchain system could also help a more fluid and dynamic suppliers ecosystem. Paradoxically, even if a blockchain is in general more costly and inefficient than centralized solutions, in this scenario it would help to create a more competitive and agile environment.

8.3. Cases studied

In general, the property of increased and easier traceability would be beneficial for different sectors where product provenance is critical. For example, in the pharmaceutical industry it can be lives-saving to timely recognize the manufacturer of a faulty drug to fast isolate it. Another practical example is the food industry where it might be necessary to track down products to the farms or treatment plants that produced them in case of disease outbreaks or dangerous contamination or pollution. A pilot project to use blockchain technology to trace the pork industry in China was started by Walmart [24] in partnership with IBM (see Fig. 7), leveraging the Hyperledger blockchain [16]. IBM is not new to supply chain applications of blockchain technology built on top of Hyperledger, as it is also collaborating with Maersk, leader in the ocean shipping industry, on a similar project, mainly aimed at reducing the traditional paper trail costs that Maersk estimates to be as much as one fifth of the entire shipping costs [71].

But provenance is not only important to pinpoint producers of faulty products, it is also important in industries with the need to prove that goods are authentic or ethically produced or obtained (e.g., fair trade or organic certification in the food industry). A practical application is diamond tracking. For such valuable goods it is important to prove their authenticity and that they were not used to fund violence (the so called *blood diamonds*). Systems tracking diamonds on blockchain are already used alongside the traditional methods, for example, the De Beers Group of Companies, the world largest diamonds producer by

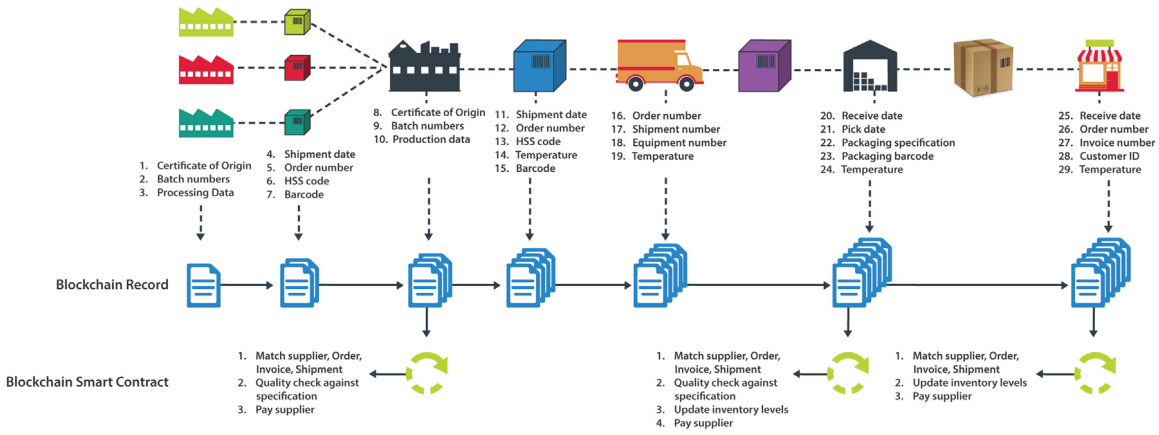

Fig. 6. Scheme of a generic blockchain based supply chain management system.
Source: [12].

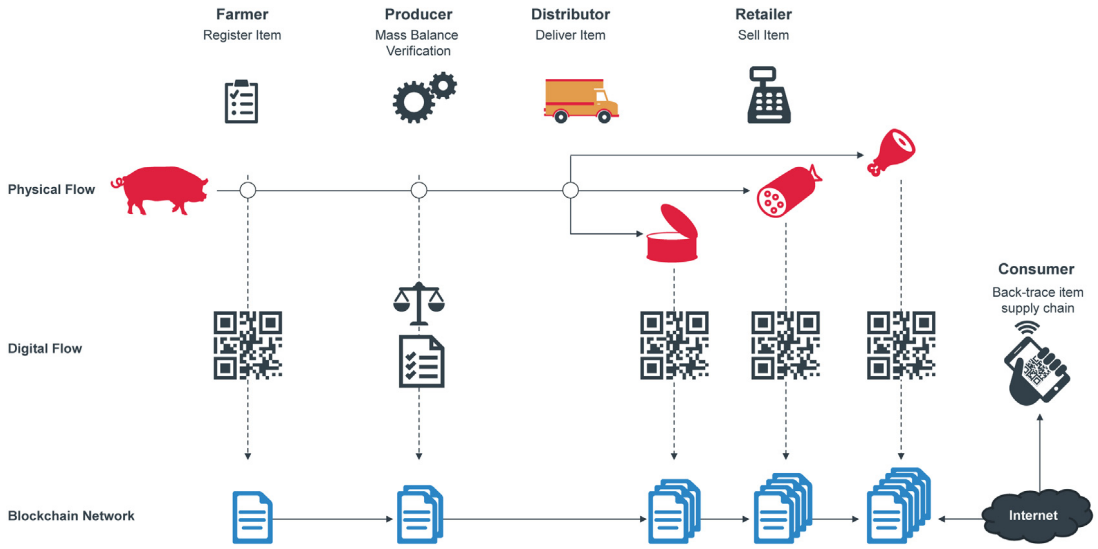

Fig. 7. Scheme of Walmart pork tracking in China using a blockchain based supply chain management system.
Source: [12].

value, developed a working prototype [33]. Another older initiative is *Everledger* [39] that is active since 2015 and allows to store arbitrary valuable goods but strongly advertises its adoption with diamonds [40]. *Provenance* [89] is another company offering general supply chain management based on the blockchain. Its pilot experiment was the tracking of tuna in Indonesia [90] to prevent human rights abuse of fishermen as well as illegal overfishing and other examples are *Blockverify* [13], *Sweetbridge* [103] and *Factom* [41].

We should now point out that often not all information should be kept publicly visible on the blockchain. In fact, that could cause confidential information leaking that could be used by competing companies to gain an unfair advantage. But transparency is not necessarily in conflict with privacy. As a matter of fact, we already saw that advanced cryptographic techniques can be used to guarantee that some properties are satisfied by the data without revealing the data itself [42,48]. For example, a supplier might publish private information about their inventory without showing the actual amount of each product. This way a buyer could know if the supplier has a certain good available without actually knowing how many units are available, so to avoid the leaking of private corporate information that a competitor could profit from. At the same time a farmer might keep their identity private to the customer while still proving that their products satisfy a certain standard (e.g fair trade). A company providing a blockchain based supply chain management system with a keen interest in privacy is *Chronicled* [22] that relies on zk-SNARK and is focused on applications involving the IoT.

Finally, we point out how integrating blockchain supply chain systems with smart contracts could potentially bring whole new possibilities, especially if paired with IoT. A traditional or blockchain based supply chain management system can be greatly strengthened when coupled with *smart labels*, i.e., labels of goods containing IoT sensors providing a data feed elaborated by smart contracts on the blockchain. If such sensors are built tamper resistant (for example employing hardware secure chips) then they can provide the smart contracts with a secure flow of data to monitor the goods along the supply chain, detecting counterfeiting attempts or exposure to critical conditions. A clear application would be the pharmaceutical supply chain, where smart sensors could monitor that delicate drugs are kept within the intended threshold of temperature, humidity, light exposure, etcetera. An example of a company providing a blockchain based supply chain management system oriented to such smart IoT devices is *Modum* [14,76], especially active in pharmaceutical monitoring and tracking. Of course the use of smart contracts

Table 6
Blockchain based supply Chain systems.

Name	Link	Blockchain used
IBM pilots	[24,71]	Hyperledger
Everledger	[39]	Hyperledger/Ethereum
Provenance	[89]	Ethereum
Blockverify	[13]	Bitcoin
Sweetbridge	[103]	Hyperledger
Factom	[41]	Custom Factom blockchain
Chronicled	[22]	Ethereum
Modum	[76]	Ethereum

and IoT devices in a supply chain scenario enables also real time analytics, that could be leveraged by machine learning predictive algorithms to adjust production accordingly. Monitoring in real time or predicting the goods manufactured would allow suppliers to better manage a dynamic production as well as reduce material waste and economical losses from unsold items. The benefits would not end with the end consumer buying the product, as the entire recycling and collection industry is part of the supply chain as well and would benefit from such innovations.

Even if the application of blockchain technology to supply chain management is mainly carried out by the interested companies and their relative pilot tests (summarized in Table 6), also some academic work has been presented in the last three years. In [45] the authors address the inefficiency of a public blockchain supporting a supply chain management system, proposing an alternative solution. In [112] blockchain is used to contrast counterfeit and stolen product tags, by building a supply chain scheme to transfer ownership of radio frequency identification tagged products, so that each node in the chain can check integrity and correct ownership of the tags before buying the corresponding product. A proof of concept implementation of the proposal, based on the Ethereum blockchain, is presented and evaluated. The authors of [66] present a survey of blockchain based supply chain management applications and discusses general potentialities and limitations. Similarly, the focus of [65] is on digital supply chain, i.e., electronic data exchange between business partners focused on Business to Business integration, that is traditionally heavily reliant on third party intermediaries. Through interviews to experts (mainly to Finnish entities) the authors highlight the main perceived advantages of the applicability of blockchain technologies to such a system. In [123] a federation of private blockchains connected through a public one is presented, that allows for complete exchange of private information between interested parties (through a private chain) while leaving the process monitorable (without access to private information) through the public one. Finally, [72] is an interesting work not directly connected to the supply chain management problem but still pertinent, since it highlights a different approach to reach a common goal: consumers information and building of trust. The authors point out the importance of reviews in current online commerce, while remembering that most review platforms are centralized entities able to malevolently forge reviews to mislead consumers. A much more secure blockchain based decentralized system to submit and read reviews is presented, and a proof of concept implementation on the Ethereum blockchain is shown and evaluated.

9. Discussion

Throughout the proposed applications of blockchain technology presented in this paper we can find a common thread. The main blockchain inherited property that all considered applications aim to leverage is transparency. Mainly a blockchain is used in its intended form of trusted repository of data publicly readable. This feature relies on the combination of immutability, tamper resistance and persistence a blockchain offers to the data stored inside. A related leveraged property is the ability for participants to prove a given claim, i.e. auditability. All such desired advantages derive from the defining ability of a blockchain to create trust among mutually untrusted entities, allowing participants to trust the common repository.

Such transparency features are not the only common advantage leveraged by all presented applications. A blockchain is also valued as a trusted common repository to allow interoperability between different applications and services. Ironically, a blockchain is used as trusted third party repository, despite being originally proposed as a way to remove third party intermediaries.

Another, apparently contradictory, benefit cited in all the applications considered is the ability to lower costs. In fact, a blockchain is usually more expensive, in terms of resources dedicated, compared to a traditional centralized system. However, a blockchain substitutes the need for trusted third party intermediaries. Hence, it allows to save on, usually expensive, overheads. This is especially evident in the supply chain or distributed notary applications, where traditional intermediaries can be especially expensive or cumbersome.

Finally, the last main common blockchain feature that empowers all the studied applications is the ability to run smart contracts. The capability of having predefined and agreed upon code running independently from the participants control, allow for really novel capabilities, not possible in a traditional system.

10. Conclusions

In this paper we have studied six novel and promising so called *Blockchain 3.0* applications: electronic voting, healthcare records management, identity management, decentralized notary, with a special focus about intellectual property protection, and supply chain management.

For each application we have first defined their problems that blockchain technology proposes to solve. We have then presented how such problems can be tackled in general by a blockchain adoption and we have reviewed for each application a set of proposals in the literature both from the academic community and industry sector.

The existence of such a large number of *Blockchain 3.0* applications shows that there is still a keen interest in blockchain technology, even after some years from its creation, and leaves us to hypothesize that this interest will grow further in the years to come.

Declaration of competing interest

No author associated with this paper has disclosed any potential or pertinent conflicts which may be perceived to have impending conflict with this work. For full disclosure statements refer to https://doi.org/10.1016/j.jpdc.2019.12.019.

CRediT authorship contribution statement

Damiano Di Francesco Maesa: Conceptualization, Data curation, Formal analysis, Funding acquisition, Investigation, Methodology, Project administration, Resources, Software, Supervision, Validation, Visualization, Writing - original draft, Writing - review & editing. **Paolo Mori:** Conceptualization, Data curation, Formal analysis, Funding acquisition, Investigation, Methodology, Project administration, Resources, Software, Supervision, Validation, Visualization, Writing - original draft, Writing - review & editing.

References

[1] AgoraVoting, 2019, http://agoravoting.org/#index. (Accessed 30 Nov 2019).
[2] G. Ali, N. Ahmad, Y. Cao, M. Asif, H. Cruickshank, Q.E. Ali, Blockchain based permission delegation and access control in internet of things (baci), Comput. Secur. (2019).
[3] S.T. Ali, J. Murray, An overview of end-to-end verifiable voting systems, in: Real-World Electronic Voting: Design, Analysis and Deployment, CRC Press, 2016, pp. 171–218.
[4] An internet for identity, 2019, http://www.windley.com/archives/2016/08/an_internet_for_identity.shtml. (Accessed 30 Nov 2019).
[5] S. Angraal, H.M. Krumholz, W.L. Schulz, Blockchain technology: applications in health care, Circ.: Cardiovasc. Qual. Outcomes 10 (9) (2017) e003800.
[6] K. Baghery, On the efficiency of privacy-preserving smart contract systems, in: International Conference on Cryptology in Africa, Springer, 2019, pp. 118–136.
[7] S. Bartolucci, P. Bernat, D. Joseph, Sharvot: secret share-based voting on the blockchain, 2018, arXiv preprint arXiv:1803.04861.
[8] S. Bistarelli, M. Mantilacci, P. Santancini, F. Santini, An end-to-end voting-system based on bitcoin, in: Proceedings of the Symposium on Applied Computing, ACM, 2017, pp. 1836–1841.
[9] Bitcongress whitepaper, 2019, https://bravenewcoin.com/assets/Whitepapers/BitCongressWhitepaper.pdf. (Accessed 30 Nov 2019).
[10] Bitid, 2019, https://github.com/bitid/bitid/blob/master/BIP_draft.md. (Accessed 30 Nov 2019).
[11] Bitshares, 2019, https://bitshares.org/. (Accessed 30 Nov 2019).
[12] Blockchains for supply chains – part I.I., 2019, http://resolvesp.com/blockchains-supply-chains-part-ii/. (Accessed 30 Nov 2019).
[13] Blockverify, 2019, http://www.blockverify.io/. (Accessed 30 Nov 2019).
[14] T. Bocek, B.B. Rodrigues, T. Strasser, B. Stiller, Blockchains everywhere-a use-case of blockchains in the pharma supply-chain, in: Integrated Network and Service Management, IM, 2017 IFIP/IEEE Symposium on, IEEE, 2017, pp. 772–777.
[15] C. Brodersen, B. Kalis, C. Leong, E. Mitchell, E. Pupo, A. Truscott, L. Accenture, Blockchain: securing a new health interoperability experience, Accenture LLP, 2016.
[16] C. Cachin, Architecture of the Hyperledger blockchain fabric, in: Workshop on Distributed Cryptocurrencies and Consensus Ledgers, 2016.
[17] K. Cameron, A User-Centric Identity Metasystem, 2008.
[18] Caribou Digital, Private-Sector Digital Identity in Emerging Markets Farnham, Surrey, Caribou Digital Publishing, United Kingdom, 2016.
[19] F. Casino, T.K. Dasaklis, C. Patsakis, A systematic literature review of blockchain-based applications: current status, classification and open issues, Telemat. Inform. 36 (2019) 55–81.
[20] D.L. Chaum, Untraceable electronic mail, return addresses, and digital pseudonyms, Commun. ACM 24 (2) (1981) 84–90.
[21] D. Chaum, Blind signatures for untraceable payments, in: Advances in Cryptology, Springer, 1983, pp. 199–203.
[22] Chronicled, 2019, https://chronicled.com/. (Accessed 30 Nov 2019).
[23] F.C. Coelho, Optimizing disease surveillance by reporting on the blockchain, 2018, bioRxiv 278473.
[24] Coindesk, walmart blockchain pilot aims to make China's pork market safer, 2019, https://www.coindesk.com/walmart-blockchain-pilot-china-pork-market/. (Accessed 30 Nov 2019).
[25] Counterparty, 2019, https://counterparty.io/. (Accessed 30 Nov 2019).
[26] J.P. Cruz, Y. Kaji, E-voting System Based on the Bitcoin Protocol and Blind Signatures, 2016.
[27] J.P. Cruz, Y. Kaji, N. Yanai, RBAC-SC: Role-based access control using smart contract, IEEE Access 6 (2018) 12240–12251.
[28] Democracy.earth, 2019, http://democracy.earth/. (Accessed 30 Nov 2019).
[29] D. Di Francesco Maesa, A. Lunardelli, P. Mori, L. Ricci, Exploiting blockchain technology for attribute management in access control systems, in: International Conference on the Economics of Grids, Clouds, Systems, and Services, Springer, 2019, pp. 3–14.
[30] D. Di Francesco Maesa, P. Mori, L. Ricci, Blockchain based access control, in: IFIP International Conference on Distributed Applications and Interoperable Systems, Springer, 2017, pp. 206–220.
[31] D. Di Francesco Maesa, P. Mori, L. Ricci, Blockchain based access control services, in: 2018 IEEE International Conference on Internet of Things, iThings, and IEEE Green Computing and Communications, GreenCom, and IEEE Cyber, Physical and Social Computing, CPSCom, and IEEE Smart Data, SmartData, IEEE, 2018, pp. 1379–1386.
[32] D. Di Francesco Maesa, P. Mori, L. Ricci, A blockchain based approach for the definition of auditable access control systems, Comput. Secur. 84 (2019) 93–119.
[33] Diamond blockchain initiative, 2019, https://www.diamondblockchaininitiative.com/. (Accessed 30 Nov 2019).
[34] A. Dubovitskaya, Z. Xu, S. Ryu, M. Schumacher, F. Wang, Secure and trustable electronic medical records sharing using blockchain, 2017, arXiv preprint arXiv:1709.06528.
[35] P. Dunphy, F.A. Petitcolas, A first look at identity management schemes on the blockchain, 2018, arXiv preprint arXiv:1801.03294.
[36] A. Ekblaw, A. Azaria, J.D. Halamka, A. Lippman, A case study for blockchain in healthcare:"medrec" prototype for electronic health records and medical research data, in: Proceedings of IEEE Open & Big Data Conference, vol. 13, 2016, p. 13.
[37] C. Elsden, A. Manohar, J. Briggs, M. Harding, C. Speed, J. Vines, Making sense of blockchain applications: A typology for HCI, in: Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems, ACM, 2018, p. 458.
[38] A.K. Ernest, The Key To Unlocking The Black Box: Why The World Needs A Transparent Voting DAC, Follow My Vote, 2014.
[39] Everledger, 2019, https://www.everledger.io/. (Accessed 30 Nov 2019).
[40] Everledger, diamonds, 2019, https://diamonds.everledger.io/. (Accessed 30 Nov 2019).
[41] Factom, 2019, https://www.factom.com/. (Accessed 30 Nov 2019).
[42] U. Feige, A. Fiat, A. Shamir, Zero-knowledge proofs of identity, J. Cryptol. 1 (2) (1988) 77–94.
[43] FollowMyVote, 2019, https://followmyvote.com/. (Accessed 30 Nov 2019).
[44] W. Gao, W.G. Hatcher, W. Yu, A survey of blockchain: techniques, applications, and challenges, in: 2018 27th International Conference on Computer Communication and Networks, ICCCN, IEEE, 2018, pp. 1–11.
[45] Z. Gao, L. Xu, L. Chen, X. Zhao, Y. Lu, W. Shi, Coc: A unified distributed ledger based supply chain management system, J. Comput. Sci. Tech. 33 (2) (2018) 237–248.
[46] Gartner, Hype cycle for blockchain technologies, 2019, https://www.gartner.com/en/newsroom/press-releases/2019-10-08-gartner-2019-hype-cycle-shows-most-blockchain-technologies-are-still-five-to-10-years-away-from-transformational-impact.
[47] Gem, 2019, https://gem.co/health/. (Accessed 30 Nov 2019).
[48] C. Gentry, A Fully Homomorphic Encryption Scheme, Stanford University, 2009.
[49] Google Trends, 2019, https://trends.google.com/trends/. (Accessed 30 Nov 2019).
[50] Hashed health, 2019, http://www.hashedhealth.com/. (Accessed 30 Nov 2019).
[51] Healthcare working group, 2019, https://www.hyperledger.org/industries/healthcare. (Accessed 30 Nov 2019).
[52] Hedera Hasgraph, 2019, https://www.hederahashgraph.com/. (Accessed 30 Nov 2019).
[53] T. Heston, A Case Study in Blockchain Healthcare Innovation, 2017.
[54] IdchainZ, 2019, http://idchainz.com/. (Accessed 30 Nov 2019).
[55] Imogen heap, thiny human, 2019, https://imogen2.surge.sh/#/imogen_heap/tiny_human/tiny_human. (Accessed 30 Nov 2019).
[56] Inno.Vote whitepaper, 2019, http://inno.vote/whitepaper/Inno.vote%20%E2%80%94%20Bringing%20Democracy%20to%20Elections.pdf. (Accessed 30 Nov 2019).
[57] Iota, 2019, https://iota.org/. (Accessed 30 Nov 2019).
[58] IPFS, 2019, https://ipfs.io/. (Accessed 30 Nov 2019).
[59] D. Ivan, Moving toward a blockchain-based method for the secure storage of patient records, in: ONC/NIST Use of Blockchain for Healthcare and Research Workshop, ONC/NIST, Gaithersburg, Maryland, United States, 2016.
[60] O. Jacobovitz, Blockchain for Identity Management, 2016.
[61] A. Juels, D. Catalano, M. Jakobsson, Coercion-resistant electronic elections, in: D. Chaum, M. Jakobsson, R.L. Rivest, P.Y.A. Ryan, J. Benaloh, M. Kutylowski, B. Adida (Eds.), Towards Trustworthy Elections: New Directions in Electronic Voting, Springer Berlin Heidelberg, Berlin, Heidelberg, 2010, pp. 37–63, http://dx.doi.org/10.1007/978-3-642-12980-3_2.
[62] M.A. Khan, K. Salah, IoT security: Review, blockchain solutions, and open challenges, Future Gener. Comput. Syst. 82 (2018) 395–411.
[63] K. Kirby, A. Masi, F. Maymi, Votebook. A proposal for a blockchain-based electronic voting system, The Economist, 2016.
[64] E. Kokoris-Kogias, E.C. Alp, S.D. Siby, N. Gailly, P. Jovanovic, L. Gasser, B. Ford, Hidden in Plain Sight: Storing and Managing Secrets on a Public Ledger, Tech. rep., 2018, Cryptology ePrint Archive: 209 https://eprint.iacr.org/2018/209.pdf.
[65] K. Korpela, J. Hallikas, T. Dahlberg, Digital supply chain transformation toward blockchain integration, in: Proceedings of the 50th Hawaii International Conference on System Sciences, 2017.
[66] N. Kshetri, 1 blockchain's roles in meeting key supply chain management objectives, Int. J. Inf. Manage. 39 (2018) 80–89.

[67] T.-T. Kuo, L. Ohno-Machado, Modelchain: Decentralized privacy-preserving healthcare predictive modeling framework on private blockchain networks, 2018, arXiv preprint arXiv:1802.01746.

[68] U. Lang, OpenPMF SCaaS: Authorization as a Service for Cloud & SOA Applications, in: Second International Conference on Cloud Computing, CloudCom 2010, 2010, pp. 634–643.

[69] K. Lee, J.I. James, T.G. Ejeta, H.J. Kim, Electronic voting service using block-chain, J. Digit. Forensics Secur. Law 11 (2) (2016) 123.

[70] L.A. Linn, M.B. Koo, Blockchain for health data and its potential use in health it and health care related research, in: ONC/NIST Use of Blockchain for Healthcare and Research Workshop, ONC/NIST, Gaithersburg, Maryland, United States, 2016.

[71] Maersk, Maersk and IBM to form joint venture applying blockchain to improve global trade and digitise supply chains, 2019, https://www.maersk.com/press/press-release-archive/maersk-and-ibm-to-form-joint-venture. (Accessed 30 Nov 2019).

[72] D. Martens, W. Maalej, Reviewchain: Untampered product reviews on the blockchain, 2018, arXiv preprint arXiv:1803.01661.

[73] F. Martinelli, P. Mori, Enhancing java security with history based access control, in: Foundations of Security Analysis and Design IV, FOSAD 2006/2007 Tutorial Lectures, in: Lecture Notes in Computer Science, vol. 4677, Springer, 2007, pp. 135–159.

[74] P. McCorry, S.F. Shahandashti, F. Hao, A smart contract for boardroom voting with maximum voter privacy, in: International Conference on Financial Cryptography and Data Security, Springer, 2017, pp. 357–375.

[75] M. Mettler, Blockchain technology in healthcare: the revolution starts here, in: e-Health Networking, Applications and Services, Healthcom, 2016 IEEE 18th International Conference on, IEEE, 2016, pp. 1–3.

[76] Modum, 2019, https://modum.io/. (Accessed 30 Nov 2019).

[77] Monegraph, 2019, https://monegraph.com/. (Accessed 30 Nov 2019).

[78] Muse, 2019, https://museblockchain.com/. (Accessed 30 Nov 2019).

[79] S. Nakamoto, Bitcoin: A Peer-To-Peer Electronic Cash System, 2008.

[80] Y. Nasser, C. Okoye, J. Clark, P.Y. Ryan, Blockchains and Voting: Somewhere Between Hype and a Panacea, 2018.

[81] T. Nguyen, K. Kim, A survey about consensus algorithms used in blockchain, J. Inf. Process. Syst. 14 (2018) 101–128, http://dx.doi.org/10.3745/JIPS.01.0024.

[82] OASIS, eXtensible Access Control Markup Language (XACML) Version 3.0, OASIS XACML TC, 2013.

[83] A. Panarello, N. Tapas, G. Merlino, F. Longo, A. Puliafito, Blockchain and IoT integration: A systematic survey, Sensors 18 (8) (2018) 2575.

[84] H. Peter, A. Moser, Blockchain-applications in banking & payment transactions: results of a survey, Eur. Financial Syst. (2017) 141.

[85] K. Peterson, R. Deeduvanu, P. Kanjamala, K. Boles, A blockchain-based approach to health information exchange networks, in: Proc. NIST Workshop Blockchain Healthcare, vol. 1, 2016, pp. 1–10.

[86] PokitDot, 2019, http://www.pokitdok.com/. (Accessed 30 Nov 2019).

[87] Polys, 2019, https://polys.me/. (Accessed 30 Nov 2019).

[88] Procivis and University of Zurich develop blockchain based e-voting solution – Procivis, 2019, http://procivis.ch/2017/09/26/procivis-and-university-of-zurich-develop-blockchain-based-e-voting-solution/. (Accessed 30 Nov 2019).

[89] Provenance, 2019, https://www.provenance.org. (Accessed 30 Nov 2019).

[90] Provenance, tracking tuna on the blockchain, 2019, https://www.provenance.org/tracking-tuna-on-the-blockchain. (Accessed 30 Nov 2019).

[91] R3 Corda, 2019, https://docs.corda.net/. (Accessed 30 Nov 2019).

[92] Radix, 2019, https://www.radixdlt.com/. (Accessed 30 Nov 2019).

[93] A.S. Robby Houben, Cryptocurrencies and Blockchain Legal Context and Implications for Financial Crime, Money Laundering and Tax Evasion, Tech. rep., STUDY Requested by the TAX3 committee, European Parliament, Policy Department for Economic, Scientific and Quality of Life Policies, 2018.

[94] Robomed network whitepaper, 2019, https://robomed.io/download/Robomed_whitepaper_eng_final.pdf. (Accessed 30 Nov 2019).

[95] T. Ruffing, P. Moreno-Sanchez, A. Kate, Coinshuffle: practical decentralized coin mixing for bitcoin, in: European Symposium on Research in Computer Security, Springer, 2014, pp. 345–364.

[96] Secure.vote, 2019, https://secure.vote/. (Accessed 30 Nov 2019).

[97] H. Shafagh, L. Burkhalter, A. Hithnawi, S. Duquennoy, Towards blockchain-based auditable storage and sharing of iot data, in: Proceedings of the 2017 on Cloud Computing Security Workshop, ACM, 2017, pp. 45–50.

[98] S. Shafeeq, M. Alam, A. Khan, Privacy aware decentralized access control system, Future Gener. Comput. Syst. 101 (2019) 420–433, http://dx.doi.org/10.1016/j.future.2019.06.025, URL http://www.sciencedirect.com/science/article/pii/S0167739X18332308.

[99] Shocard, 2019, https://shocard.com/how-it-works/. (Accessed 30 Nov 2019).

[100] Shocard whitepaper, 2019, https://shocard.com/wp-content/uploads/2016/11/travel-identity-of-the-future.pdf. (Accessed 30 Nov 2019).

[101] Simplyvital health, 2019, https://www.simplyvitalhealth.com/. (Accessed 30 Nov 2019).

[102] Sovrin, 2019, https://sovrin.org/. (Accessed 30 Nov 2019).

[103] Sweetbridge whitepaper, 2019, https://sweetbridge.com/public/docs/Sweetbridge-Whitepaper.pdf. (Accessed 30 Nov 2019).

[104] Y. Takabatake, D. Kotani, Y. Okabe, An anonymous distributed electronic voting system using Zerocoin, Institute of Electronics, Information and Communication Engineers, IEICE, 2016.

[105] A. Tapscott, D. Tapscott, How blockchain is changing finance, Harv. Bus. Rev. 1 (9) (2017) 2–5.

[106] P. Tarasov, H. Tewari, The future of e-voting, IADIS Int. J. Comput. Sci. Inf. Syst. 12 (2) (2017).

[107] The European Parliament and the Council of the European Union, regulation (EU) 2016/679 of the european parliament and of the council of 27 April 2016, Off. J. Eur. Union, 4.5.2016.

[108] The path to self-sovereign identity, 2019, http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html. (Accessed 30 Nov 2019).

[109] TIVI, 2019, https://tivi.io/. (Accessed 30 Nov 2019).

[110] A. Tobin, D. Reed, The Inevitable Rise of Self-Sovereign Identity, The Sovrin Foundation, 2016.

[111] Top trends in the Gartner hype cycle for emerging technologies, 2017, https://www.gartner.com/smarterwithgartner/top-trends-in-the-gartner-hype-cycle-for-emerging-technologies-2017/. (Accessed 30 Nov 2019).

[112] K. Toyoda, P.T. Mathiopoulos, I. Sasase, T. Ohtsuki, A novel blockchain-based product ownership management system (POMS) for anti-counterfeits in the post supply chain, IEEE Access (2017).

[113] A.H. Trechsel, V.V. Kucherenko, F. Silva, Potential and Challenges of e-Voting in the European Union, Tech. rep., 2016.

[114] Ujo music, 2019, https://ujomusic.com/. (Accessed 30 Nov 2019).

[115] S. Underwood, Blockchain beyond bitcoin, Commun. ACM 59 (11) (2016) 15–17.

[116] UPort, 2019, http://developer.uport.me/. (Accessed 30 Nov 2019).

[117] UPort whitepaper, 2019, http://blockchainlab.com/pdf/uPort_whitepaper_DRAFT20161020.pdf. (Accessed 30 Nov 2019).

[118] Votem, 2019, https://votem.com/. (Accessed 30 Nov 2019).

[119] Votewatcher, 2019, http://votewatcher.com/. (Accessed 30 Nov 2019).

[120] X. Wang, X. Zha, W. Ni, R.P. Liu, Y.J. Guo, X. Niu, K. Zheng, Survey on blockchain for Internet of Things, Comput. Commun. 136 (2019) 10–29, http://dx.doi.org/10.1016/j.comcom.2019.01.006, URL http://www.sciencedirect.com/science/article/pii/S0140366418306881.

[121] G. Wood, Ethereum: A Secure Decentralised Generalised Transaction Ledger, 2014, Ethereum Project Yellow Paper 151.

[122] A. Wright, P. De Filippi, Decentralized blockchain technology and the rise of lex cryptographia, 2015, Available at SSRN 2580664.

[123] H. Wu, Z. Li, B. King, Z. Ben Miled, J. Wassick, J. Tazelaar, A distributed ledger for supply chain physical distribution visibility, Information 8 (4) (2017) 137.

[124] R. Xu, Y. Chen, E. Blasch, G. Chen, Blendcac: a blockchain-enabled decentralized capability-based access control for IoTs, in: 2018 IEEE International Conference on Internet of Things, iThings, and IEEE Green Computing and Communications, GreenCom, and IEEE Cyber, Physical and Social Computing, CPSCom, and IEEE Smart Data, SmartData, 2018, pp. 1027–1034, http://dx.doi.org/10.1109/Cybermatics_2018.2018.00191.

[125] Y. Yuan, F. Wang, Blockchain and cryptocurrencies: model, techniques, and applications, IEEE Trans. Syst. Man Cybern. 48 (9) (2018) 1421–1428, http://dx.doi.org/10.1109/TSMC.2018.2854904.

[126] X. Yue, H. Wang, D. Jin, M. Li, W. Jiang, Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control, J. Med. Syst. 40 (10) (2016) 218.

[127] F. Zagórski, R.T. Carback, D. Chaum, J. Clark, A. Essex, P.L. Vora, Remotegrity: design and use of an end-to-end verifiable remote voting system, in: International Conference on Applied Cryptography and Network Security, Springer, 2013, pp. 441–457.

[128] P. Zhang, M.A. Walker, J. White, D.C. Schmidt, G. Lenz, Metrics for assessing blockchain-based healthcare decentralized apps, in: e-Health Networking, Applications and Services, Healthcom, 2017 IEEE 19th International Conference on, IEEE, 2017, pp. 1–4.

[129] Z. Zhao, T.-H. Chan, How to vote privately using bitcoin, in: International Conference on Information and Communications Security, Springer, 2015, pp. 82–96.

[130] G. Zyskind, O. Nathan, et al., Decentralizing privacy: using blockchain to protect personal data, in: Security and Privacy Workshops, SPW, 2015 IEEE, IEEE, 2015, pp. 180–184.

Damiano Di Francesco Maesa has received both his master degree (cum laude) and Ph.D. in computer science from the University of Pisa. He is specialized on Bitcoin cryptocurrency analysis and blockchain technology novel applications, on which subject he has published on conference proceedings and international journals. He has held several guest lectures and seminars to spread awareness in blockchain technology. He has been an academic guest at the "Research Group for Distributed Computing (DISCO)" at ETH Zürich and a Research Affiliate of the Italian National Research Institute (CNR). He currently is a Research Associate at the computer lab of the university of Cambridge.

Paolo Mori (M.Sc. 1998, Ph.D. 2003) is a researcher at ''Istituto di Informatica e Telematica'' of ''Consiglio Nazionale delle Ricerche'' of Italy. His main research interests involve trust, security and privacy in distributed systems, mobile devices, online social networks, and blockchains, focusing on access/usage control and trust in Cloud, mobile devices and Internet of Things. He usually serves in the Organization and Program Committees of international conference/workshops, such as the ''International Conference of Information System Security and Privacy'' (ICISSP). He is (co-)author of 100+ scientific papers published on international journals and conference/workshop proceedings. He is usually actively involved in research projects on information and communication security, such as the European Commission funded ''Confidential and Compliant Clouds'' (CoCo-Cloud) and ''Collaborative and Confidential Information Sharing and Analysis for Cyber Protection'' (C3ISP) and the EIT Digital High Impact Initiative ''Trusted Data Management with Service Ecosystem''.