Blockchain: opportunities and challenges in the educational context

Victor Garcia-Font

Abstract A blockchain is a new technology that provides a distributed append-only ledger, which basically it means that it is almost unfeasible to modify or delete data once recorded. Furthermore, blockchains are maintained and governed by multiple nodes, which decide the state of the system following a consensus protocol. In this way, blockchains not only avoid single points of failure, but also create transparent systems that cannot be tampered or manipulated by a reduced group of entities with admin rights (unlike centralized systems). Attracted by these benefits, in the recent years many projects from many different sectors are proposing to use a blockchain to improve existing services or to deploy new business cases that require the consensus, the involvement and/or the cooperation of several actors. This chapter explores prominent proposals related to education and academia. In this context, trends are moving towards: financial applications, administrative efficiency, certification, immutable public registry, reputation systems, and identity systems and privacy. Moreover, this chapter also takes into account the problems associated with blockchains and discusses the main difficulties and challenges that proposals embracing this technology will have to address.

Key words: blockchain; cryptocurrencies, decentralization; education;

1 Introduction

In 2009, with the release of Bitcoin (Nakamoto 2008), not only the cryptocurrencies emerged as a new form of decentralized money, but also their underlying technology,

Victor Garcia-Font
Internet Interdisciplinary Institute (IN3)
Universitat Oberta de Catalunya (UOC)
CYBERCAT-Center for Cybersecurity Research of Catalonia
e-mail: vgarciafo@uoc.edu

the blockchain, became the basis of many other applications that enable the creation of collaborative business models that were not possible until then. The blockchain has been designed as an append-only ledger, where data can be easily read and appended, but where it is very hard to delete or modify any recorded information. These design principles make the blockchain a highly secure system containing traceable records that are considered to be immutable. Currently, these features and the different governance models of blockchain platforms are showing that it is possible to manage and control highly valuable digital assets, such as cryptocurrencies, in a collaborative manner involving multiple stakeholders with conflicting interests, removing middlemen and institutional silos.

Nevertheless, some projects have suffered from certain weaknesses of the blockchain (e.g. low throughput, high transaction fees) and the inconveniences of this collaborative way of managing a system (e.g. disagreements among the stakeholders involved in a project (Hertig 2018)). In order to mitigate the main drawbacks of blockchain technology and also to find alternative governance and consensus models that can be more suitable for different business cases, many variants from the original Bitcoin blockchain have been proposed. In fact, in the recent years, the blockchain ecosystem has evolved and has become highly complex. Many blockchain platforms have sprung up offering the promising features of this technology in many different flavours. At the same time, this complexity has mislead many projects to embrace blockchain technology in contexts where its benefits are dubious, or where other alternatives could have been more adequate to achieve similar results with less burdens.

Taking all the above into account, the purpose of this chapter is twofold. Firstly, this chapter is intended to be introductory to the blockchain. Thus, Section 2 explains the principles of this technology to non-technical readers. Secondly, this chapter focuses on the educational context. In this way, Section 3 points out current opportunities of blockchain in education and explores how this technology can enable new use cases and contribute to improve certain areas in this field. Then, Section 4 discusses the main difficulties and challenges in this scenario. Finally, Section 5 concludes the chapter.

2 Background

This section contains the necessary background for non-technical readers to be able to understand the basics of blockchain technology. First, an introduction to the blockchain is given in Section 2.1, and second, Section 2.2 describes the types of blockchain platforms.

2.1 Blockchain

In early 2009, the release of Bitcoin marked the beginning for a new form of money: cryptocurrencies. Although the main ideas behind this technology were already published some time ago, such as HashChash (Back 2002), B-money (Dai 1998), smart contracts (Szabo 1997) or in (Haber & Stornetta 1990), the publication of the Bitcoin software meant the first real implementation of a decentralized digital currency. Furthermore, this new technology goes far beyond a new payment system, and its core, the blockchain, enables the creation of decentralized applications that remove intermediaries, empower final users, and make possible new use cases and services that were not feasible until then.

The functioning of Bitcoin and the blockchain was first proposed in 2008 in the paper "Bitcoin: a peer-to-peer electronic cash system" (Nakamoto 2008) published by an anonymous author under the pseudonym Satoshi Nakamoto. Basically, Bitcoin, and in general any blockchain system, requires two main components: a software client installed in the user's equipment and a Peer-to-Peer (P2P) network that maintains the blockchain.

Regarding the software client, it is a computer program, known as wallet, that enables users to manage transactions that record data in the blockchain. In cryptocurrencies, these transactions are responsible of transfering funds. The basic mechanism enabling transactions is asymmetric cryptography. Briefly, a user creates a key-pair, which includes a public key, that can be disclosed, and a private key, that has to be kept secret. Using cryptographic protocols, the user can employ his or her private key to digitally sign a message. Then, anybody can use the public key to verify that the message was signed by the private key belonging to that key-pair. Similar to using a bank account number, in cryptocurrencies, users can store funds in an address, which is a value derived from the public key. Then, they can use the private key associated to that public key to digitally sign a transaction to move the funds to another address. In this way, a wallet is responsible of generating and storing the key-pairs, creating and digitally signing transactions, and, finally, interacting with the peer-to-peer network to deliver the transactions.

Regarding the peer-to-peer network, it is formed by nodes that have mainly the following functions: receiving and forwarding transactions and blocks, verifying that transactions and blocks are correct and follow a certain specification (e.g. in the Bitcoin protocol a transaction that is not properly signed is not valid, and a block over a certain size is not valid either), storing a copy of the blockchain, and generating new blocks. Nodes can have different responsibilities, being the nodes that generate new blocks a cornerstone of the network, because they are in charge of deciding the state of the system by recording the transactions received from the users. The following paragraphs give more details about how these nodes generate new blocks and maintain the blockchain.

In this type of system, transactions are from time to time packed in blocks, which are then appended to a data structure, forming in this way a sequential chain of blocks: the blockchain. Figure 1 includes a graphical representation of some blocks in a blockchain such as Bitcoin. The blockchain can be considered a kind of append-

only ledger, where data can only be added and it can never be deleted or modified. Hence, in order to modify a balance of a variable, it is necessary to create a new transaction referring to that variable, instead of directly modifying its value as it would be done in traditional databases or in a spreadsheet. Hence, the primary role of the blockchain is to record all transactions that are considered as accepted in the history of a service.

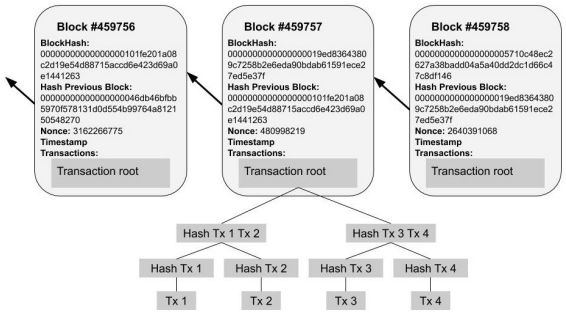

Fig. 1 Graphical representation of some blocks of the Bitcoin blockchain.

The nodes in charge of packing the transactions in new blocks are called miners and the process of generating the new blocks is called mining. This process starts when the miners receive transactions of the users forwarded from other nodes of the network. Each miner might receive different transactions or in a different order depending on the connectivity among nodes. Then, the miners verify that the transactions follow the Bitcoin protocol and select a subset of the valid transactions to be included in a new block. These transactions are included in the block using a tree data structure, as Figure 1 shows, known as Merkle tree (Merkle 1980). This type of structure allows nodes to quickly find if a transaction is included or not in a block.

Once the tree is generated, the miner creates a block header including the root of the tree, a timestamp, a reference to the hash of the previous published block and a field called Nonce, explained in more detail below. As Figure 1 shows, the links in the blockchain are the concatenation of block headers through the reference to the hash of the previous published block.

Regarding the Nonce, this field has no meaning by itself, and it can probably be ignored by anybody that only examines the content of the block, but it is not interested in verifying if it has been generated correctly. Actually, the Nonce is a tool that miners use to easily modify the block until the block follows a certain specification required by the Bitcoin protocol. In fact, finding an appropriate value for this field is what constitutes the primary effort of the miner during the mining process. In order to understand the importance of that field, first, it is important to highlight that a main goal of mining is to create a competition among the miners to select the node that publishes the next new block in the blockchain. This competition is carried out using a hash function, which is a non-invertible function that takes some data as input, and it generates a fixed-size short digest as output. With this

type of function, the output cannot be predicted analyzing the input data without executing the function. In blockchain, a hash of the block header is computed as a kind of block identifier and, according to the Bitcoin protocol, this identifier has to be lower than a certain value. This means that when a miner computes the hash value of a block header, if this value is not lower than the threshold, then the miner has to somehow change the block header in order to recompute the hash. Instead of changing the transactions in the block or some other field that would require a long computation, the miners use the Nonce field to try different values until they find a block that fulfills the protocol requirements, like trying to randomly find the missing piece of a puzzle. In this way, miners compete to be the first one to create an appropriate block. Once a miner can create a new block, it disseminates it through the network and all the nodes can start working in generating a block that follows the recently published block. Due to the effort required in finding a proper Nonce, this process is known as Proof-of-Work (PoW). In fact, this task requires investing a large amount of energetic resources, and in order to incentivize participation and competition, a reward in bitcoins is given in every published block. On average, in the Bitcoin network, a new block gets published every 10 minutes.

Additionally, the PoW is used to securize the blockchain. As it can be seen in Figure 1, the previous hash value is what links the blocks. In this way, once a block is published, any attempt to change any field included in the block would be easily spotted, because in order to go unnoticed, it would be also necessary to recompute the block hash, which would require a change of the pointer to this value in the next block. At the same time, this would change the next block hash, triggering changes like that in all the following blocks.

It is worth noting that with a data structure such as a blockchain, there is no principal node that decides which blocks are correct or which is the current state of the system. Conversely, each node participating on the network takes these decisions on its own. Thus, it is on the interest of all the participants to follow a common protocol and, for instance, it is on the interest of each miner to generate valid blocks that are not rejected by the other nodes. In fact, the blockchain was the first practical implementation on a large Internet-scale to achieve consensus on the state of a system, where participants do not need to know each other and, therefore, do not trust each other. Currently, other variants of this technology have been proposed that do not follow a sequential chain of blocks structure and that use alternative protocols to PoW. For these reasons, in a more general way, this type of protocols are called consensus protocols and this type of platforms are called distributed ledger technologies (DLT). Although not all DLT are a sequential chain of blocks, in this document, we use the terms blockchain and DLT indistinctly.

Furthermore, DLT can be used in many different use cases besides cryptocurrencies. In order to execute the program logic, DLT use what it is called smart contracts (Szabo 1997), which are a type of computer program that execute some actions defined beforehand when certain conditions are met. Combining smart contracts and blockchain enables parties that do not trust each other to automatically execute programs that record the result of the execution into a blockchain. Thus, without any intermediary, parties can automatically transfer cryptocurrency funds or

digital assets, or modify the state of certain system variables according to the input parameters of the smart contracts.

In this way, cryptocurrencies can be considered payment systems enabled by asymmetric cryptography, smart contracts and a blockchain. As an example, a standard smart contract for these systems consists of transferring a certain amount of cryptocurrency to a recipient able to submit a digital signature performed with a private key associated to an address recorded in the smart contract.

Another type of smart contract is described in (Hyperledger 2017), where the system uses a blockchain to track seafood provenance. In this use case, transactions record every time that fish are sold or traded. Furthermore, besides recording the parties involved in the transactions, some supply chain mechanisms also propose to use Internet-of-Things (IoT) devices to leave evidence of important variables about the trade. For instance, in the seafood supply chain example, sensors can be used to ensure that temperature in fish containers has not gone beyond a threshold during transportation.

In summary, DLT can be considered a technology that integrates the following basic components:

- An append-only data model capturing the state of the system.
- Smart contracts as a programming tool to change the state of the system.
- A consensus protocol to agree on the accepted transactions and their order.

2.2 Types of blockchain

The features mentioned up to this point in general refer to Bitcoin and, more generally, blockchain technology using PoW as consensus protocol. Nonetheless, the blockchain space is nowadays broad, and not only many other coins have been created, but also many projects propose to use blockchain in different environments besides cryptocurrencies. Depending on the context, certain blockchain features are more important than others and, therefore, researchers have designed some blockchain variants to overcome the drawbacks of Bitcoin and its consensus protocol. For example, Bitcoin aims to be public with traceable transactions. This means that the blockchain is accessible by anyone on the Internet, and the transactions show the address of the sender and the recipient. In this way, anyone can explore the blockchain and build a graph including the payment history of Bitcoin. On the other hand, other cryptocurrencies, such as Monero[1] and Zcash[2], provide less transparent systems, implementing mechanisms to enhance privacy and to hide the senders and the recipients of the transactions.

In this way, several mechanisms can be used in different ways to adapt certain characteristics of the blockchain to the needs of the different projects. Some of the proposals have even designed new consensus protocols that change fundamental

[1] Monero. `https://www.getmonero.org/`

[2] Zcash. `https://z.cash/`

principles of the original blockchain in order to give the responsibility of generating and validating new blocks only to a reduced set of nodes, which is to detriment of decentralization. Nevertheless, by granting different permissions to the nodes that want to participate in a blockchain, the promoters of these platforms can keep the control of the blockchain and can achieve better performance.

Decentralization and the fact that anybody can participate in the consensus protocol are principal characteristics of most cryptocurrencies. However, some use cases have proven that closed systems with permissions can also be useful in many other contexts. Thus, in the blockchain space there is a major classification of blockchain platforms according to the permissions required to participate in the consensus protocol. In this way, these technologies are normally classified between permissionless and permissioned blockchains. More details on these two types are provided below.

2.2.1 Permissionless blockchains

Bitcoin blockchain is of the permissionless type. This means that special rights are not needed to participate in the mining process. Thus, any interested party can install a software compatible with the Bitcoin protocol, connect to the network and start competing with the other nodes to generate new blocks. Moreover, no permission is needed to record transactions in the blockchain. The only requirements are to follow the Bitcoin protocol and to control some bitcoins in order to pay the transaction fees. Additionally, anybody can download the Bitcoin blockchain, read it and trace the recorded transactions. Therefore, this is a public permissionless blockchain. In fact, public permissionless blockchains are common in cryptocurrencies, because cryptocurrencies aim at being fully transparent systems in order to show that users are treated equally and according to the predefined rules.

It is worth noting that in these blockchain systems it is necessary to give an incentive to the miners for their work. Mining is a resource intensive process and, therefore, some compensation is indispensable to attract miners that compete with each other and, in this way, create a fully decentralized system. For this reason, permissionless blockchains are normally associated with a cryptocurrency, because the cryptocurrency is used to incentivise miners. Generally, miners get two types of incentives when they generate a new block. Firstly, they receive a predefined reward for the block and, secondly, they can collect the fees paid by the users for each transaction.

In this way, public permissionless blockchains can be extremely decentralized systems that open up a lot of possibilities. Nevertheless, blockchains of this type have certain disadvantages compared to other systems, such as centralized databases, that make them often still not ready to be an actual game changer. Basically, the main problems of these blockchains are velocity and scalability.

Regarding velocity, as previously stated, the Bitcoin blockchain creates a new block every 10 minutes on average. Therefore, in order to see newly published information after a block has been published, users have to wait 10 minutes on average. Moreover, not all new transactions can always be included in the following

block and, therefore, the waiting period can be longer. Additionally, for security reasons, transactions should not be considered fully valid until the block where they are published does not have 6 or more subsequent blocks. This means that, since each block is published every 10 minutes, then, in the best case scenario, users have to wait at least one hour. Although these facts are particular of the Bitcoin network, other permissionless blockchain technologies suffer similar problems. For instance, as it can be seen in Etherscan[3], the block time in the Ethereum network generally stays below 20 seconds, but this is still some orders of magnitude higher than the almost instantaneous performance of conventional databases.

Furthermore, the block time has also consequences on scalability and throughput. It is common that blockchain protocols define a maximum block size. This, combined with the block time, considerably limits the amount of transactions that can get published per second. Systems like Bitcoin or Ethereum cannot even handle 30 transactions per second, which is a really low amount compared to the ten thousand transactions per second that the Visa network can handle in peak times (Swan 2015).

Another concern with permissionless blockchains is the great amount of resources consumed in the PoW. As explained above, miners compete to be the fastest creating valid new blocks in order to get the rewards. This has led participants to spend high amounts of energy using highly powerful hardware in mining activities. In fact, it is estimated that the Bitcoin network consumes an amount of power approximately equivalent to a country like Ireland (G.F. 2018). Besides, it is common to use equipment specially designed for mining cryptocurrencies, which has to be replaced after few months because it becomes obsolete.

Finally, the facts explained in this section are common in many permissionless blockchains, mainly the ones based on PoW, such as Bitcoin and Ethereum. In order to address some of the disadvantages of PoW, for example to not require so much energy or to decrease block time, some alternatives have been proposed, among others: Proof-of-Stake (PoS), Delegated Proof-of-Stake (DPoS), Proof-of-Importance (PoI) or Proof-of-Burn (PoB). Nonetheless, these consensus protocols are still not ripe enough or they do not offer the same level of decentralization than PoW. More details about consensus protocols for permissionless blockchains can be found in (Cachin & Vukolić 2017).

2.2.2 Permissioned blockchains

Permissioned blockchains have been proposed for contexts where openness and full transparency are not a requirement, or even undesirable, such as in enterprise environments. Actually, identity management is an important aspect in this type of blockchain. Only certain entities have special permissions to validate and generate new blocks, to take decisions regarding the protocol, and even to participate in transactions or view the recorded data and the state of the system.

---

[3] Etherscan. Ethereum Average Block Time Chart. `https://etherscan.io/chart/blocktime`

Typically, permissioned blockchains are used in enterprise environments, where the information in the blockchain can be of interest and can even be recorded by many different entities related to a business, however the management of the platform can be left to few powerful stakeholders in a consortium (e.g. different governmental institutions, companies from the same holding, important stakeholders in a sector). For instance, (Hyperledger 2017) shows how to improve seafood provenance using a permissioned blockchain. In this example, every seafood transaction between different parties can be automatically recorded in the blockchain using smart contracts. In this way, with a permissioned blockchain, on the one hand, the different stakeholders regulating and controlling the seafood sector could be the only entities capable of validating and including transactions in the blocks, and also governing the protocol of the platform. These entities could also grant permissions to a more numerous group of people and companies in this sector (e.g. fishermen, restaurants) in order to participate in the system creating the transactions when fish get caught or traded. On the other hand, the information about seafood provenance gets immutably recorded and can be used in case of disputes or it can be made public to consumers.

Another outstanding use case of permissioned blockchains is in situations where transactions can be viewed or created by anybody, but just a reduced set of trusted entities can act as miners and have rights to take decisions concerning the protocol. This is the case of some cryptocurrencies like Ripple[4], which offers a cryptocurrency that can be used by the general public in a platform managed by a few trusted stakeholders.

This type of blockchain is clearly less revolutionary than permissionless blockchains. Actually, permissioned blockchains are considered by many just a shared database (Koens & Poll 2018). Nevertheless, due to the more restrictive conditions to write new blocks, the consensus protocols in this type of blockchains can substantially differ from PoW and, therefore, overcome some of the limitations of permissionless blockchains. For instance, in permissioned blockchains it is not necessary to incentivize competition among miners with cryptocurrency rewards. Conversely, entities participating in the consensus protocol should be self-interested in running a full blockchain node in order to gain some control over the system, for example, to not have to totally entrust the platform to a single entity from the consortium. In this case, consensus protocols for this type of blockchains can accept thousands of transactions per second, can be faster and require less energy than PoW. These are clear advantages enabled by the fact that nodes do not have to compete among each other to generate the next block, but rather cooperate in validating that all the participating nodes are correctly following the protocol, and if not, excluding the misbehaving ones. Some popular consensus protocols used in permissioned blockchains are: Simplified Byzantine Fault Tolerance (SBFT), Redundant Byzantine Fault Tolerance (RBFT) and Proof-of-Elapsed-Time (PoET). More details about consensus protocols for permissioned blockchains can be found in (Cachin & Vukolić 2017).

[4] Ripple. `https://ripple.com/`

In addition, privacy is another appealing feature of permissioned blockchains. In a permissionless blockchain, data are forwarded to all the nodes that connect to the P2P network. In many cases, such as in Bitcoin, data are not even encrypted and transactions are easily traceable by third parties. In other cases, such as Monero[5] or Zcash[6], blockchains use cryptographic protocols to obfuscate transaction data and prevent extracting information from the transaction graph. Nonetheless, although data are encrypted, and therefore not directly accessible by the mining nodes, the fact that information are by design distributed to all the nodes already raises certain concerns. For instance, bugs in cryptographic protocols can eventually lead to information disclosure. Furthermore, law concerning data protection is usually written taking into account traditional centralized information systems and it is not clear what should be the data treatment in highly decentralized systems such as a permissionless blockchain.

3 Applications of blockchain in educational contexts

As seen so far, blockchain is a promising technology that can change the way some industries work and can enable new business cases. In an educational context, many projects propose to use blockchain tackling several different problems. This section reviews current proposals in this domain and classifies the projects in six different categories according to the specific purposes of each project. These categories are: financial applications, administrative efficiency, certification, immutable public registry, reputation systems, and identity systems and privacy. Sections below provide further details about these categories.

3.1 Finantial applications

Cryptocurrencies have been the first application of blockchain and it is a typical use case in many scenarios. The usage of cryptocurrencies goes beyond simple payment systems. In fact, cryptocurrencies are a useful tool to easily provide rewards to users and create incentive-based systems.

In (Swan 2015), the author gathers several use cases of blockchain that can foster new economical models. Regarding learning, the author presents a use case based on smart literacy contracts. This type of smart contract is a kind of learning activity that has a reward attached after completion. The author argues that this can provide new forms of financial aid similar to microlending, but based on personal development instead of directly based on currency. In this way, donors can finance educational activities in bitcoins or in a specific coin created for this purpose (e.g. Learncoin).

---

[5] Monero. `https://www.getmonero.org/`

[6] Zcash. `https://z.cash/`

Other authors propose to use cryptocurrencies to stimulate collaboration in academic environments and, at the same time, reduce educational costs for students with financial difficulties. For instance, in (Devine 2015) the author delineates how education institutions can create blockchain tokens transferable to the students that assist professors in academic activities. The institution then have to accept the tokens back as a discount to reduce the cost of certain campus services or tuition fees.

In (Swan 2015), the author also includes other usages of cryptocurrencies meant to improve research and publication procedures. The author presents the idea of creating blockchain based journals and to use a Journalcoin to reward any party involved in the publishing process, such as authors, peer reviewers, editors, service providers, etc. Besides, in this context cryptocurrencies can be used as tokens in order to create a reputation-based system (see Section 3.5 for further details about reputation systems). Using a blockchain system, scientific publishing can become more transparent and, unlike current review mechanisms, rewards can be sent to the different contributors according to their work. The author also outlines some ideas on how to use other tokens, such as ExperimentalResultscoin or Researchcoin, to stimulate reproducible research or to purchase paper reading rights avoiding the middleman.

At the same time, cryptocurrencies can be used to boost participation of the general public in research activities. For instance, Storm (StormX.io 2017) is a platform designed to create microtasks with a gamification approach (i.e. applying game principles to increase engagement). After resolving a task, the resolver earns rewards in cryptocurrency. This can be indeed useful for many research projects, for example to find participants for surveys or to tag images to later test new machine learning models. Also, several cryptocurrency-based platforms have been proposed to trade computational resources, where users can lend their processing power (Golem.network 2017) or their storage space (Vorick & Champine 2014) in exchange for coins. A software platform with similar goals, but directly focussed on science, is Berkeley Open Infrastructure for Network Computing (BOINC) (Anderson 2004). Participants can install BOINC in their computers and contribute with their resources to scientific projects, such as SETI@Home[7] or Einstein@Home[8]. Gridcoin (Gridcoin Foundation 2018) has been created in order to give incentives to the participants using BOINC.

Finally, it is worth mentioning that although there are lots of proposals to create new coins to incentivize collaboration around specific use cases, there are not many empirical experiments or conclusive studies proving the feasibility of these proposals and, therefore, they should be treated with caution.

[7] SETI@Home. `https://setiathome.berkeley.edu/`

[8] Einstein@Home. `https://einsteinathome.org/`

3.2 Administrative efficiency

A common goal for many blockchain projects from different domains is to reduce paper-based workflows, decrease administrative costs and increase the efficiency in routinary procedures involving multiple parties.

The blockchain is a technology that enables creating a tamper-proof ledger shared by various stakeholders that can have competing interests and, therefore, that do not trust each other as the only source of information. In this way, the different stakeholders can use blockchain systems to create records in a secure and trustable manner. Furthermore, combining blockchain with smart contracts allows reliably automatizing many processes involving several of the stakeholders. In this way, data recorded by the smart contracts can be traced, making the parties accountable and creating a highly transparent system that can easily be verified by third parties. This can not only speedup administrative procedures, eliminate deduplicated data and information silos, but also help resolve possible conflicts among the parties. Obviously, privacy preserving techniques have to be considered to not reveal any sensitive information in these cases. Besides, since the information flowing in these systems generally concerns only a set of institutions and not the general public, then private and permissioned blockchains are commonly proposed in these situations to have a higher control over the governance of the systems and the data.

Currently, good examples of this usage of blockchain can be seen in the supply-chain and logistics. A remarkable initiative is Everledger[9], which claims to use rich forensics to identify diamonds and other gems and then, record in a blockchain any important detail about these assets in order to offer proof of origin for the precious stones. In the freight sector, Maersk and IBM (Haswell & Storgaard 2017) propose to use blockchain in order to offer a transparent way to know the location and other relevant features of cargo. The system interconnects numerous stakeholders involved in the transportation of goods, breaking some data silos and creating a common platform that has to eliminate some manual and paper-based procedures, saving in bureaucratic costs and accelerating administrative and operational actions. Although projects in this field are still very young and none has yet displaced completely existing systems, the need of common platforms with these characteristics are clear in logistics and, therefore, blockchain projects in this sector are advancing towards clear goals.

On the other hand, in the field of education, proposals in this regard are less clear and more immature. Nevertheless, the need to ease data exchange among academic institutions is strong and it is not a minor matter. Nowadays, mobility programs are in high demand, and society urges stronger interaction between industry and academia, which results in internships and training programs provided by third parties, but validated by high education institutions, which register them in the students transcripts. Mobility programs, internships and so on involve many different administrative procedures that are currently settled manually. Besides, these generally imply sharing large amounts of data among the different institutions involved in the agreements,

[9] Everledger. `https://www.everledger.io/`

such as academic achievements, transcripts or letters of commitment. Currently, these procedures are slow, cumbersome and entangle lots of paperwork. On this regard, Erasmus without papers (Jahnke 2017) is an initiative by the European University Foundation partnering together with several universities. This initiative aims at creating an European network to electronically exchange student data, eliminating paper-based workflow and, in this way, reducing bureaucratic procedures and administrative costs. The initiative proposes to deploy a platform on top of the current information technology infrastructure in order to enhance interoperability and ease information exchange. Although this platform is still at its infancy, the project plans to deploy a decentralized P2P network, open to any trustworthy stakeholder involved in student mobility. Moreover, the project also aims at creating several data standards for all the steps in the procedures involved in students mobility. According to this project, it is not possible to identify a unified flow of data among institutions. Nonetheless, it is possible to identify information that is commonly required to be exchanged related to mobility, such as: personal data, study rights, course contents, learning agreements, learning agreement amendments, transcript of records, grade distribution, inter-institutional agreements, student nomination, and information on start and end date of mobility.

3.3 Certification

Currently, academic certificates and diplomas are normally issued on paper. Although these certificates generally have anti-counterfeiting features, it is still possible to forge them, specially when being shared as a copy or a scan of the original document. Furthermore, the built-in mechanisms that prevent forging the documents are expensive, which makes them not suitable for course certificates of minor importance. Additionally, verifying paper-based certificates involves many times contacting the issuing institution, which is time-consuming and, therefore, expensive. Sometimes the verification is even not possible if the institution that has issued the certificate no longer exists.

For these reasons, creating digital academic certificates that could easily be shared with potential employers and other third parties has been a hot topic for many years. Although technology to enable this has long been there, such as Public Key Infrastructure (PKI), Certificate Authority (CA) and Timestamping Authority (TSA), the existence of certain related problems have prevented replacing paper by digital diplomas. These technologies could be administered either by the same academic institutions that issue the certificates or by trusted third parties. In the first case, there would be security concerns on the way each institution deploys and administers the certificate tools or, at least, there would be asymmetries among institutions. In both cases, the validity of the certificates would be strongly bounded to the issuers or the third parties running the certificate and timestamping infrastructures. The demise of an institution would inevitably have negative consequences to the reliability of its certificates. It is worth noting that academic certificates may have

a longer lifespan than their issuers or a PKI (taking this into account is especially important for titles issued by small schools). On the other hand, using a blockchain as an independent timestamping authority provides a reliable timestamping source (so, possible collusions among issuers and TSA are avoided), it prevents problems related to the demise of organizations running key services, and it also makes the system more resilient to cyber attacks, removing single points of failure. Furthermore, using a blockchain, the responsibility of managing the digital diplomas can be transferred to their holders, in this way releasing the academic institutions of the responsibility of storing personal data in centralized repositories, which can become targets of cyber attacks and ease massive data leaks.

One of the principal projects that enables publishing academic certificates on the blockchain is Blockcerts[10]. This is an open source project (Blockcerts 2019) started by the MIT's Media Lab and Learning Machine proposing a standard for creating, issuing, viewing and verifying blockchain-based certificates. Two main goals of this project are: enabling all participants to use self-sovereign identities (more details about decentralized identities in Section 3.6) and to control certificates themselves, and avoiding having to trust in any third party for any purposes. Therefore, Blockcerts has been designed to not require well known organizations to attest the identity neither of the issuer of the certificates nor the recipients. In this way, the identity of the participants cannot be directly proven using Blockcerts. Participants are represented by their public keys, and it is in their interest (or not) to demonstrate the ownership of the keys. Furthermore, by enabling recipients to control their own certificates, then central repositories to store all these data become optional. Systems with these characteristics are specially adequate for people with difficulties to prove their identity with official documentation, such as asylum seekers. Also, the fact that they do not depend on official repositories makes this type of diploma censor resistant.

From a technical point of view, Blockcerts basically proposes that an issuer signs a digital file (containing the information to certify) using his/her private key. Then, the signature is appended to the certificate. Afterwards, a hash of the certificate (including the issuer's signature) is published in a blockchain record along with the date and the recipient's address. In this way, the certificate is protected against tampering and any interested party having the issuer's and the recipient's public keys can easily verify who issued the certificate and to whom. Finally, the recipient can store the certificate in his/her Blockcerts wallet. The wallet, similar to the cryptocurrencies wallet, is used to store private information related to certificates, such as the certificate document and the private key that is associated with the public key included in the certificate.

Lifelong learning passport (Gräther et al. 2018) goes one step further than Blockcerts and proposes a machine verifiable certificate system based on Ethereum to administer digital diplomas managed using an identity hierarchy that can cope with basic needs of the academic certification system in a holistic way. On the top of the hierarchy, the authors propose to have accreditation authorities, which are responsi-

[10] Blockcerts. `https://www.blockcerts.org/`

ble to authorize education institutions to issue diplomas. Then, in the second level of the hierarchy there are the certificate authorities. These are the ones in the name of whom the diplomas are being issued (i.e. universities, schools, etc.). Finally, in the third level there are the certifiers, who are the ones indeed certifying the diploma in the name of the certificate authority. For example, certifiers can be employees of the certificate authorities. This project is a first approach to create a blockchain-based platform to handle academic titles taking into account the needs of the academic system on a global perspective. Nevertheless, this type of systems have still a long way to go. The complexity of the academic system regarding certificates goes far beyond issuers and accreditation authorities. For example, including information about the academic personnel in the platform linked to the university certificates would enhance the value of the titles of prestigious institutions with highly qualified professors that hold accreditations issued by quality agencies.

At the same time, many of the initiatives to publish certificates on the blockchain have the goal of changing the way a typical Curriculum Vitae (CV) is being presented to employers. In this regard, this initiatives generally aim at making machine verifiable CVs that become more dynamic, where job seekers can give more importance to minor achievements, such as short summer courses. With paper-based certificates, including this type of achievement on the CV generally means that employers have to trust candidates on the veracity of the included information, because verifying such achievements is too costly. However, besides designing technological solutions for this use case, in order to have an efficient and effective mechanism to issue and share these achievements, it is important to agree on certain data structures to represent them and make them easily interoperable. In this way, Open Badges[11] is a project working on a specification in order to standardize the way people can create an ever-evolving set of badges crediting for small merits. In (Tolbatov et al. 2018) the authors discuss the sustainability of the current learning models centralized on brick-and-mortar higher education institutions. In the paper, the authors debate on the adequacy of blockchain technology to hold education data in a way that the students gain the control over their data in order to create a portfolio where they can show, in a verifiable manner, any type of accomplishment, including university degrees, contributions to projects, micro-accreditations, or any other result from a new distributed learning reality.

3.4 Immutable public registry

Transparency and immutability are two important properties of blockchain systems. In this way, any data recorded in a blockchain can be publicly accessible (in public blockchains), records include an approximate publication timestamp, and users have strong guarantees that the information has not been altered. All these can be used to create proof of existence. By recording the hash of a document in a blockchain,

[11] Open Badges. `https://openbadges.org/`

then it is possible to prove that the person that recorded this information had a copy of the document when the hash value was recorded. Furthermore, the content of the document can be kept private and it just has to be disclosed in dispute situation. In this case, the owner of the document can easily prove that the recorded value in the blockchain corresponds to the hash value of the document. In this way, intellectual property can be protected in a confidential manner.

In education, this type of immutable public registries can be used to enforce copyright and detect plagiarism. For example, Po.et[12] is a decentralized and permissionless protocol built on top of Bitcoin and IPFS (Benet 2014) with which authors of academic content can have a prove that their work was published in a certain date. Many other applications of this kind have been presented in the blockchain space in order to eliminate middlemen like notaries and other kinds of public registries[13][14][15].

3.5 Reputation systems

Section 3.3 gathers some proposals to easily share achievements with which people can show their merits, and which are obvious ways to show the reputation of a person. Even though some of the proposals are focussed on sharing minor achievements, which enable dynamic portfolios, this is sometimes not enough because it cannot include non certifiable merits, such as the level of student satisfaction. Moreover, comparing certifications is sometimes difficult, subjective and not very machine-friendly. Therefore, some projects aim at going beyond certificates and propose to associate reputation scores to individuals. Actually, reputation systems (i.e. systems where users are associated with some type of metric or review about their behavior, involvement, etc.) are already being used in many online applications, like in vendor/buyer reviews in barter apps. Although these systems are practical to have a good user experience and avoid some scams, in general, they have the limitation of being strictly attached to a single application. This means that in every new system, users need to have a minimum interaction with the application in order to increase their reputation over the average. Furthermore, the way to compute the reputation measure and how reputation data are being administered normally depends on a single entity, which can raise some doubts on the rules to treat the reviews and the reputation data. For example, in issues regarding fraudulent reviews (Kinstler 2018).

Currently, in academia there are already certain reputation measures linked to scientific productivity, such as H-index or number of citations. Although these are widely accepted, they have similar problems to the reputation systems mentioned above. For instance, there are different ways to compute these metrics, which results

[12] Po.et. `https://www.po.et/`

[13] Stampd. `https://stampd.io/`

[14] Stampery. `https://stampery.com/`

[15] ProofOfExistence. `https://proofofexistence.com/`

in different systems offering different values for the same metrics (e.g. Scopus[16], ISI Web of Knowledge[17], Google Scholar[18]). Besides, these are very specific scientific metrics and do not take into consideration other aspects of research or teaching, like student satisfaction. In order to avoid the problems related to having a single authority administering the reputation platform and also to open the system to different applications of the educational and academic community, some projects propose to build the reputation platforms on top of a blockchain. In this regard, the authors of (Sharples & Domingue 2016) propose a blockchain reputation system for academia, where reputation becomes a transferable value. In order to boost their system, the authors propose to first give some reputation credit (named Kudos) to people and institutions according to certain classic metrics like university rankings, H-index and so on. Once an initial distribution of Kudos is done, these can be transferred among users. In this way, students could be rewarded with Kudos after completing tasks and passing exams. Also academic personnel could be rewarded in Kudos beyond scientific productivity. A system like this also allows to reward an author that has anonymously published interesting content online without the need of revealing the identity of the author. Another reputation system based on the blockchain is (Dennis & Owen 2016). In this case the authors are not only focused on academia and propose a system with a general reputation score. Actually, the proposed system puts the responsibility to compute the reputation score on the clients. In this way, a client can be programmed to compute reputation in a different way than another one, giving different weights to different variables or taking into account the type of transactions in the blockchain or how and by whom they have been registered.

Indeed these systems offer different capabilities than traditional ways of measuring reputation. They can give a general measure of reputation which is perfectly valid in certain situations. Besides, fine-grained systems are imaginable where reputation could be analyzed by area of expertise or where the measure would use dynamic mechanisms that could take into account different weights according the reputation of the awarding sources, the importance of the awarded situation, etc. However, some doubts arise by the fact that transferrable reputation opens the door to economically tradable reputation.

3.6 Identity systems and privacy

One of the most prominent research fields in blockchain is related to identity management. Nowadays, the most common authentication system still requires the usage of a user and a password. This has several drawbacks, for example user security depends on the proper implementation of the authentication mechanisms in each

[16] Scopus. `https://www.scopus.com`

[17] ISI Web of Knowledge. `https://www.webofknowledge.com/`

[18] Google Scholar. `https://scholar.google.com`

service; users tend to reuse passwords in different platforms; common user identifiers (or deducible identifiers) used in different services can be used to correlate information across sites; etc. Blockchain can help reducing some of these risks, enhancing security and privacy, decentralizing the storage of identifiers, and leaving aside traditional user/password login systems.

In this regard, the World Wide Web Consortium (W3C) is working on a new standard to use Decentralized Identifiers (DID) (Credentials Community Group 2018). DID are globally unique identifiers that can be directly created by their owners, not depending in this way on a central service, as with cryptocurrency wallets. The owners can associate public/private key-pairs to each DID that can be used for private communication and also to establish different identifiers not only for each different service, but also for different communications within the same application. The project Hyperledger Indy[19] is a well-known initiative in this regard. Furthermore, the usage of blockchain has relaunched the concept of self-sovereign identity, that aims to provide a system with which people are able to create and maintain themselves a digital identity, avoiding the need of a trusted entity issuing and storing this private information. A couple of relevant initiatives are Sovrin[20], based on Hyperledger Indy, and uPort[21], based on Ethereum. In the field of education, the characteristics of decentralized identity systems can be beneficial in many use cases. For example, StudyBits[22] is a project that proposes the usage of self-sovereign identities to issue educational certificates on the blockchain respecting privacy and anonymity. Also, as mentioned before, one of the goals of Blockcerts is to enable all participants to use self-sovereign identities. In fact, this system does not provide any built-in identity mechanism. Thus, decentralized identity seems a natural system for these use cases. Furthermore, academic identity has to go beyond borders and be prepared to acknowledge and credit achievements to people and institutions from different backgrounds, which can include conflict areas. Hence, open and censor resistant mechanisms must be borne in mind.

At the same time, as it has been mentioned before, the blockchain can enable systems that help preserving privacy. Similarly to the aforementioned Open Badges, the W3C is working on verifiable claims and credentials[23]. According to (Andrieu et al. 2017), "a verifiable claim is a qualification, achievement, quality, or piece of information about an entity's background such as a name, government ID, payment provider, home address, or university degree. Such a claim describes a quality or qualities, property or properties of an entity which establish its existence and uniqueness". The purpose of the working group is to define a specification to provide a standard to manage and exchange the claims and credentials on the web in a way that can be automatically verified by a machine and ensuring that are cryptographically secure and that preserve privacy. This specification combined with cryptographic

[19] Hyperledger Indy. https://www.hyperledger.org/projects/hyperledger-indy

[20] Sovrin. https://sovrin.org/

[21] uPort. https://www.uport.me/

[22] StudyBits. https://www.bcined.com/studybits.html

[23] Verifiable Claims Working Group. https://www.w3.org/2017/vc/WG/

methods, such as zero-knowledge proofs, can enable ways to attest some characteristic about a person, revealing a minimum amount of information. This goal is aligned with a minimal disclosure approach required by regulations such as the General Data Protection Regulation (GDPR). A typical example for this is to generate a claim stating that a person is over 21 years old. This claim can then be used to acquire alcoholic beverages without revealing the date of birth nor the real age of the holder.

In the context of education, verifiable claims and credentials can be useful in several cases, for example: to attest academic achievements without having to disclose the complete transcript of records, to prove eligibility for a scholarship without having to reveal certain personal details (e.g. low income), to give proof of identity in online courses, to prove achievements without revealing the real identity (e.g. showing a verifiable claim in an anonymous forum attesting a certification in order to emphasize the holder's posts). Other interesting use cases for verifiable claims can be found in (Andrieu et al. 2017).

4 Discussion

First thing that should be taken into account before deciding the type of blockchain that suits best a certain project is to evaluate whether a blockchain is even necessary or there are other technological solutions that can fit the same purpose without the drawbacks that entail using a blockchain. In the literature there are many articles, such as (Yaga et al. 2018) by National Institute of Standards and Technology (NIST) or (Hyperledger 2018) by Hyperledger giving guidelines to assess decision makers on whether a blockchain may be a convenient technology for their systems and if so, the most convenient type of blockchain to use. From this type of papers, (Koens & Poll 2018) is especially relevant, because the authors make a comprehensive analysis of 30 existing desisional schemes proposed in other articles, and they propose a detailed decision flow diagram that not only assists on whether to use or not a blockchain, but also it points out the best possible technologies to use instead of blockchain considering the different situations specified in their flow diagram. These alternatives are: not using any database, a central database, a shared central database, a distributed database, a distributed ledger, currently no solutions available, or a blockchain.

Furthermore, as shown in Section 3.3, sometimes the blockchain is proposed to replace other mechanisms like PKI or TSA. As we have seen, Blockcerts[24] justifies this in order to not depend on third parties and to have independent timestamping services, taking into account that the certificates issued with Blockcerts may last longer than the issuing institutions.

At the same time, besides evaluating possible alternatives to a blockchain, educational projects that decide to finally include a blockchain in their architecture have to bear in mind that blockchain is still relatively new and immature and, therefore, they

[24] Blockcerts. `https://www.blockcerts.org/`

may have to face and overcome certain obstacles. Bellow, we list the main difficulties and challenges that have been encountered so far in the blockchain space that are also applicable in the educational context:

Transactions are not recorded immediately, specially in permissionless blockchains, which tend to be slow. Blockchains are very different to conventional databases in this sense. In a conventional database, programmers are used to commit large volumes of data almost instantaneously. In contrast, when a transaction is sent to the blockchain platform, it can take some time until a node in charge of committing the information can include the transaction in a block. Even if the transaction can get included in the following block, this can already take some time (e.g. around 10 minutes in average between blocks in Bitcoin[25] and around 15 seconds in Ethereum[26]).

The **blockchain is not suitable to store large volumes of data**. Blockchain data are shared among the nodes of the network and, therefore, it is important to economize the volume of information that is sent in the transactions. Actually, in permissionless blockchains, transaction fees are computed according to their size. Therefore, in order to record large amounts of data, normally, a hash value is computed from the data and then, the hash value is recorded in the blockchain and the actual data are recorded in other storage systems, such as IPFS (Benet 2014).

The **low throughput** (i.e. maximum number of transactions per second) of permissionless blockchains can be a problem for systems that have to record many individual transactions. In Bitcoin, the throughput has been estimated to be around 7 transactions per second (Croman et al. 2016) (currently, this has slightly increased due to the deployment of SegWit (Lombrozo et al. 2018), which proposed a new way to include the transactions in the block and establish their maximum size). Anyway, as mentioned above, this is far from the ten thousand transactions per second that can be handled by the Visa network (Swan 2015). Although Bitcoin has one of the lowest throughputs of the blockchain space, other permissionless platforms have similar numbers. In order to overcome this problem, some projects create a Merkle tree of hashes from data that require immutability and then, only the root of the tree is recorded in the blockchain, reducing the number of transactions and also saving in transaction fees.

Scalability is a well known problem by the blockchain and cryptocurrencies community (Croman et al. 2016). The scalability issues arise when the usage of a system gets increased massively in a certain dimension. For example, exponentially increasing the number of users of the system or the number of transactions. Bitcoin has proven to be a secure and useful system to digitally transfer value. Nevertheless, in its current state, Bitcoin is able to handle only a reasonably low number of transactions. As mentioned above, it is far from being able to support amounts of transactions similar to a typical credit card system. Hence, currently permissionless blockchains cannot cope with high loads of concurrent users and transactions.

---

[25] Bitcoin block time historical chart. `https://bitinfocharts.com/comparison/bitcoin-confirmationtime.html`

[26] Ethereum average block time chart. `https://etherscan.io/chart/blocktime`

Experiencing **long delays in transaction commitment** in high activity periods is a consequence of the low throughput and the scalability problems of permissionless blockchains. When there are many more received transactions than the amount that the blocks can handle, then the transactions have to wait to be included in the blocks. For instance, on the 12 of November 2017 the median time required to include new transactions in a mined block in Bitcoin was 27 minutes[27].

High transaction fees have to be paid in high demand periods. When many more transactions are received than can be included in the blocks, then miners can be picky and select the transactions with the highest fees. On the 22th of December 2017 bitcoin transaction fees reached an average of 55 USD[28]. In any case, projects using permissionless blockchains need to acquire cryptocurrencies in order to create transactions and, therefore, they should have a strategy contemplating any possible situation as a consequence of the volatility in cryptocurrency prices.

Privacy requirements can become an actual challenge in highly transparent and traceable systems, especially when these systems are immutable and, therefore, rollbacks to erase mistakes leading to a privacy leak are not possible. A general rule is to not record any personal information in the blockchain, even if the data are encrypted. Blockchain data may be publicly available for decades and it should be taken into account that flaws may be eventually discovered in cryptographic algorithms or the key used to encrypt may be not long enough to be considered secure in the future. Thus, when personal data are involved in a transaction, normally a hash value of the data is recorded in the blockchain and the personal data are stored outside of the blockchain. Nonetheless, it should be considered what the consequences are of somebody being able to establish a link between the recorded hash value and the real information. This is particularly important in those initiatives transferring the responsibility of managing the personal data to the users, where these may not be aware of the consequences of sharing their personal information with third parties.

Governance disagreements. Blockchains are platforms administered by many different parties. This implies that changes on the protocol, and even software updates to repair bugs, have to be accepted by a great majority of the stakeholders. Conflicting interests among these can result in lockout situations. For instance, in 2017 in the Bitcoin community, various groups of interest had different positions regarding how to address scalability problems in this cryptocurrency. These differences created a conflict that lasted several months and Bitcoin ended up divided in two different cryptocurrencies (Bitcoin and Bitcoin Cash[29]) applying two different solutions.

Unexpected flaws in blockchain platforms can jeopardize basic features of systems built on top. For example, the authors of (Miller et al. 2017) have empirically proven that it is possible to link several transactions in Monero[30], a cryptocurrency where anonymity and non-linkability are its main characteristics. This is just an ex-

[27] Median confirmation time. `https://blockchain.info/charts/median-confirmation-time`

[28] Bitcoin Avg. Transaction Fee historical chart. `https://bitinfocharts.com/comparison/bitcoin-transactionfees.html`

[29] Bitcoin Cash. `https://www.bitcoincash.org`

[30] Monero. `https://getmonero.org/`

ample that blockchain technology is still immature and no project should blindly rely on it. Naturally, programing flaws and bugs are common in all the systems. However, immutability, transparency and governance disagreements can have a higher impact in these cases than in centralized systems. Besides, it should be considered that possible future findings can become a threat to some element in the blockchain. For instance, quantum computing could break some cryptographic mechanisms (Proos & Zalka 2003).

Attacks against blockchains. Although blockchains are considered highly secure, there are several studies reporting vulnerabilities of these systems (Conti et al. 2017). In this sense, due to their open nature, public permissionless blockchains are being more studied than private permissioned blockchains. Hence, in the future, unexpected discovered vulnerabilities should not surprise users relying on the permissioned and close nature of the latter.

Usability is nowadays a principal concern among blockchain programmers. Currently, cryptocurrencies are the main application of the blockchain. Although using these new payment systems is not difficult, it represents indeed an insurmountable hurdle for some people. Educational platforms using blockchain technology should learn from this and create application interfaces specially designed taking into account the needs and the capabilities of their users.

Interoperability between blockchain platforms is currently a challenge and, therefore, interacting with digital assets recorded in different blockchains, or transferring assets from one blockchain to another one is still difficult.

Regulation and law have to be taken into account by any project using blockchain technology. The blockchain is a disruptive technology that represents new ways of interacting with the digital world and enables new business cases that may still not be clear in regulatory documents. In other cases, users may not be aware of the legal implications of certain actions. For example, it is specially important to follow GDPR when using personal data; or to take into account the monetary value of cryptocurrencies, pay the necessary taxes and follow anti money laundry regulations.

Obviously, most of the problems and drawbacks mentioned in this section do not only affect educational projects, but in general any project adding a blockchain in its architecture. Furthermore, Section 3 has shown that many different types of applications can be built in this context, which makes it difficult to limit the list of drawbacks to just common issues for all educational initiatives. Nevertheless, the educational community has not been the first one to join the blockchain hype and, therefore, it can learn from the mistakes previously done by researchers and practitioners from other disciplines. For example, one of the first use cases of blockchain was in payments. The first applications were not design with user-friendly interfaces, which caused many people to not go on board and it even caused economic losses due to mistakes when transferring or storing cryptocurrencies (Frauenfelder 2017). Sometime later, not only users and developers of payment systems, but also of other types of applications realized that public blockchains had scalability problems. A single game called CryptoKitties was responsible for causing important congestion problems to the Ethereum network (BBC 2017). Moreover, as previously seen, transaction fees can increase a lot during high usage periods, which can disrupt many business cases

based on public blockchains. These are just some examples to show to the educational community, where blockchain adoption is still low, that besides the potential benefits of this technology, the blockchain means a change of paradigm that can also cause many inconveniences and unexpected problems. Therefore, before including a blockchain in any education project, it is necessary to analyze that the blockchain is the best alternative in each case, and there are no more conventional and more mature technologies to achieve the same results.

5 Conclusions

Blockchain is a new technology considered by many as a game changer, because it provides a highly secure append-only ledger, which is distributed and governed by multiple parties.

In this chapter, we have seen that, in the context of education, blockchain has many applications that are just springing up these recent years. Basically, the proposals cover six different areas: financial applications, administrative efficiency, certification, immutable public registry, reputation systems, and identity systems and privacy.

The proposals use blockchain with different goals. The financial applications and the reputation systems use cryptocurrencies to have secure means to transfer economic value or status tokens. Applications aiming to improve administrative efficiency propose to use a blockchain in order to have a system where commonly share certain information, which could reduce paperwork and, in this way, cutdown costs. Projects regarding certification and immutable public registries use the blockchain as boards where information can be made public as well as untamperable. Finally, the blockchain enables the creation of self-sovereign identities, which can return the control of the data to their owners and help deploying censorship-resistant systems where merits and claims can be shared in a private manner.

Nonetheless, blockchains are still new and immature. Therefore, they still have certain technical problems that can become a challenge or represent an insuperable difficulty for many projects. For instance, permissionless blockchains have a low throughput and they are still not scalable. These can result in long delays in transaction commitment and high fees in certain periods of congestion. Compared to conventional databases, blockchains are slow and they are not meant to store large volumes of data. Besides, systems built on top of a blockchain have to be aware of the new attack vectors introduced by this technology. Finally, it is also important to take into account other issues regarding usability, interoperability, the governance models, the implications on privacy of such transparent and traceable systems, and other legal and regulatory matters.

Acknowledgements This work was supported by the Spanish Government, in part under Grant RTI2018-095094-B-C22 "CONSENT", and in part under Grant TIN2014-57364-C2-2-R "SMARTGLACIS."

References

Anderson, D. P. (2004), BOINC: A system for public-resource computing and storage, *in* 'IEEE/ACM International Workshop on Grid Computing', pp. 4–10.

Andrieu, J., Lee, S. & Otto, N. (2017), 'Verifiable Claims Use Cases. In: World Wide Web Consortium'.
URL: *https://www.w3.org/TR/verifiable-claims-use-cases/*

Back, A. (2002), 'Hashcash-a denial of service counter-measure'.
URL: *ftp://sunsite.icm.edu.pl/site/replay.old/programs/hashcash/hashcash.pdf*

BBC (2017), 'CryptoKitties craze slows down transactions on Ethereum'.
URL: *https://www.bbc.com/news/technology-42237162*

Benet, J. (2014), 'IPFS-content addressed, versioned, p2p file system'.
URL: *https://github.com/ipfs/papers/raw/master/ipfs-cap2pfs/ipfs-p2p-file-system.pdf*

Blockcerts (2019), 'Blockchain certificates: Blockcerts'.
URL: *https://github.com/blockchain-certificates*

Cachin, C. & Vukolić, M. (2017), 'Blockchain consensus protocols in the wild'.

Conti, M., Lal, C. & Ruj, S. (2017), 'A survey on security and privacy issues of bitcoin'.

Credentials Community Group (2018), 'A Primer for Decentralized Identifiers'.
URL: *https://w3c-ccg.github.io/did-primer/*

Croman, K., Decker, C., Eyal, I., Gencer, A., Juels, A., Kosba, A., Miller, A., Saxena, P., Shi, E. & Sirer, E. (2016), On scaling decentralized blockchains, *in* 'International Conference on Financial Cryptography and Data Security', pp. 106–125.

Dai, W. (1998), 'B-money'.
URL: *http://www.weidai.com/bmoney.txt*

Dennis, R. & Owen, G. (2016), Rep on the block: A next generation reputation system based on the blockchain, *in* 'International Conference for Internet Technology and Secured Transactions (ICITST)', Infonomics Society, pp. 131–138.

Devine, P. (2015), 'Blockchain learning: can crypto-currency methods be appropriated to enhance online learning?'.

Frauenfelder, M. (2017), ''I forgot my PIN': An epic tale of losing $30,000 in bitcoin'.
URL: *https://www.wired.com/story/i-forgot-my-pin-an-epic-tale-of-losing-dollar30000-in-bitcoin/*

G.F. (2018), 'Why bitcoin uses so much energy'.
URL: *https://www.economist.com/the-economist-explains/2018/07/09/why-bitcoin-uses-so-much-energy*

Golem.network (2017), 'Golem: The Golem Project'.
URL: *https://golem.network/crowdfunding/Golemwhitepaper.pdf*

Gräther, W., Schütte, J. & Kolvenbach, S. (2018), Blockchain for Education: Lifelong Learning Passport, *in* 'Proceedings of the 1st ERCIM Blockchain Workshop 2018, Reports of the European Society for Socially Embedded Technologies', pp. 1–8.

Gridcoin Foundation (2018), 'Gridcoin white paper'.
URL: *https://gridcoin.us/assets/img/whitepaper.pdf*

Haber, S. & Stornetta, W. S. (1990), How to time-stamp a digital document, *in* 'Conference on the Theory and Application of Cryptography', Springer, pp. 437–455.

Haswell, H. & Storgaard, M. (2017), 'Maersk and IBM Unveil First Industry-Wide Cross-Border Supply Chain Solution on Blockchain'.
URL: *https://www-03.ibm.com/press/us/en/pressrelease/51712.wss*

Hertig, A. (2018), 'A Fight Is Breaking Out Over Bitcoin Cash - And It Just Might Split the Code'.
URL: *https://www.coindesk.com/a-fight-is-breaking-out-over-bitcoin-cash-and-it-just-might-split-the-code*

Hyperledger (2017), 'Hyperledger: Seafood Supply Chain Traceability.'.
URL: *https://sawtooth.hyperledger.org/examples/seafood.html*

Hyperledger (2018), 'Hyperledger: Lessons Learned from Hyperledger Fabric PoC Projects'.
URL: *https://www.hyperledger.org/blog/2018/04/19/lessons-learned-from-hyperledger-fabric-poc-projects*

Jahnke, S. (2017), 'Erasmus Without Paper'.
URL: *https://www.erasmuswithoutpaper.eu/sites/default/files/pages/EWP\%20desk\%20research\%20final\%20version.pdf*

Kinstler, L. (2018), 'How TripAdvisor changed travel'.
URL: *https://www.theguardian.com/news/2018/aug/17/how-tripadvisor-changed-travel*

Koens, T. & Poll, E. (2018), What Blockchain Alternative Do You Need?, *in* 'Data Privacy Management, Cryptocurrencies and Blockchain Technology', Springer, pp. 113—-129.

Lombrozo, E., Lau, J. & Wuille, P. (2018), 'Segregated Witness (Consensus layer)'.
URL: *https://github.com/bitcoin/bips/blob/master/bip-0141.mediawiki*

Merkle, R. C. (1980), Protocols for Public Key Cryptosystems, *in* 'Symposium on Security and Privacy', IEEE Computer Society, pp. 122–134.

Miller, A., Möser, M., Lee, K. & Narayanan, A. (2017), 'An empirical analysis of linkability in the Monero blockchain'.

Nakamoto, S. (2008), 'Bitcoin: A Peer-to-Peer Electronic Cash System'.
URL: *https://bitcoin.org/bitcoin.pdf*

Proos, J. & Zalka, C. (2003), 'Shor's discrete logarithm quantum algorithm for elliptic curves', *Quantum Information & Computation* **3**(4), 317–344.

Sharples, M. & Domingue, J. (2016), The Blockchain and Kudos: A Distributed System for Educational Record, Reputation and Reward, *in* 'European Conference on Technology Enhanced Learning', Vol. 9891, Springer, pp. 490–496.

StormX.io (2017), 'StormX: Storm Token. Gamified micro-task platform.'.
URL: *https://s3.amazonaws.com/cakecodes/pdf/storm_web/STORM_*

Token_White_Paper_Market_Research_Network_Development_vFINAL_.pdf

Swan, M. (2015), *Blockchain: Blueprint for a new economy*, O'Reilly Media.

Szabo, N. (1997), 'Formalizing and securing relationships on public networks', *First Monday* **2**(9).

Tolbatov, A., Ahadzhanova, S., Viunenko, A. & Tolbatov, V. (2018), 'Using blockchain technology for e-learning', *Measuring and Computing Devices in Technological Processes* pp. 110–113.

Vorick, D. & Champine, L. (2014), 'Sia: Simple Decentralized Storage'.
URL: *https://sia.tech/sia.pdf*

Yaga, D., Mell, P., Roby, N. & Scarfone, K. (2018), 'NISTIR 8202 (DRAFT), Blockchain Technology Overview'.
URL: *https://csrc.nist.gov/publications/detail/nistir/8202/draft*

Glossary

Bitcoin was the first implemented blockchain platform and the first cryptocurrency. 1–8, 10, 16, 20, 21

Certificate Authority is an entity that issues digital certificates. 13, 31

Ethereum is a blockchain platform providing Turing-complete smart contracts. 8, 14, 18, 20, 22

General Data Protection Regulation is an European Union regulation on data protection. 19, 31

National Institute of Standards and Technology is an agency of the United States to promote standards and innovation. 19, 31

Peer-to-Peer is a type of computer network, where nodes act both as a server and as a client. 3, 31

Public Key Infrastructure is a system to create, manage, distribute and revoke digital certificates. 13, 31

Timestamping Authority is an entity that provides a secure timestamp as a service. 13, 31

World Wide Web Consortium is a standards organizations for the Internet Web. 18, 31

Index

Acronyms

BOINC Berkeley Open Infrastructure for Network Computing. 11

CA Certificate Authority. 13, *Glossary:* Certificate Authority
CV Curriculum Vitae. 15

DID Decentralized Identifiers. 18

GDPR General Data Protection Regulation. 19, 22, *Glossary:* General Data Protection Regulation

NIST National Institute of Standards and Technology. 19, *Glossary:* National Institute of Standards and Technology

P2P Peer-to-Peer. 3, 10, 13, *Glossary:* Peer-to-Peer
PKI Public Key Infrastructure. 13, 14, 19, *Glossary:* Public Key Infrastructure

TSA Timestamping Authority. 13, 14, 19, *Glossary:* Timestamping Authority

W3C World Wide Web Consortium. 18, *Glossary:* World Wide Web Consortium