sustainability

MDPI

Article

Blockchain Technology: Redefining Trust for Digital Certificates

Guendalina Capece *, Nathan Levialdi Ghiron and Francesco Pasquale

Department of Business Engineering, University of Rome "Tor Vergata", Via del Politecnico 1, 00133 Rome, Italy; levialdi@dii.uniroma2.it (N.L.G.); pasquale@mat.uniroma2.it (F.P.)

* Correspondence: capece@dii.uniroma2.it

Received: 23 September 2020; Accepted: 8 October 2020; Published: 28 October 2020

Abstract: University certificates can have a significant impact on people's lives: they can help people get the job they want or allow companies to decide whether a candidate for a job has the appropriate skills. Despite their important social role, current systems for certifying academic achievements are slow, complicated, expensive, and vulnerable to forgery. In the education field, the Blockcerts project, an open source project launched by MIT and Learning Machine in 2016, seems to have the potential to become a new standard for issuing certificates using the Blockchain technology as a platform. It enables students to quickly and easily get a verifiable, tamper-proof version of their diploma. Additionally, the infrastructure provides permanence, convenience, and a level of security appropriate to the importance of the record, guaranteeing the legitimacy of the diploma. The University of Rome "Tor Vergata" started a pilot program in 2018 adopting the Blockcerts framework to issue digital diplomas. In this paper, we describe the whole process from a technical perspective and analyze the impact that a broad adoption of the Blockcerts standard might have, as compared to the current way of issuing diplomas at the University of "Tor Vergata". Our aim is that our work might contribute to building momentum for the application of the Blockchain technology to digital certificates and stimulate further discussion with other institutions to fully exploit the potential of the technology.

Keywords: Blockchain technology; digital certificate; digital innovation; trust; credentials; Blockcerts; education

1. Introduction

A certificate is an official document attesting a fact and, broadly speaking, the term is often used with different meanings: guarantee, proof, authorization, authentication, verification, credentials, accreditation, testimonial, warrant, license, voucher, diploma, and more. For the purpose of this paper, we call "certificate" any certification of achievement or membership. We can safely claim that some certificates are more important than others; this is especially true for those certificates that can influence people's choices. In particular, university degrees and professional certificates granted as an award for the completion of an educational program can help people get the job they want or allow companies to decide whether a candidate for a job has the appropriate skills.

Current systems for certifying academic achievements are slow, complicated, expensive, and exposed to counterfeiting. It is worth noting that, despite the currently widespread availability of decentralized online learning opportunities, there is no digital and standardized way to track and manage these accomplishments. As a result, the creation and adoption of a secure and decentralized digital certificate infrastructure based on the Blockchain technology have the potential to bring several advantages. First, they would enable students to quickly and easily get a verifiable, tamper-proof version of their diploma that they can share with employers, schools, family, and friends. Second,

the Blockchain technology would guarantee, essentially for free, permanence, convenience, and a level of security appropriate to the importance of the student record.

1.1. BlockCerts at MIT

A remarkable initiative based on Blockchain for certification is the "Blockcerts" project by Learning Machine (https://www.learningmachine.com/) and the Medialab (https://learn.media.mit.edu/) at the Massachusetts Institute of Technology (MIT) [1], which takes the shape of a platform and standards that enable institutions to implement Blockchain in educational programs (http://www.blockcerts.org/guide/).

In 2015, Philipp Schmidt [2], the director of learning innovation at the MIT Media Lab, became interested in finding a "more modular credentialing environment, where you would get some kind of recognition for lots of things you did throughout your life". Therefore, he began issuing internal, non-academic digital certificates to his team. Soon, Learning Machine (a Cambridge, Massachusetts, based software development company) and Schmidt's team at the Media Lab discovered they had a mutual interest in developing secure official records and began to collaborate. Throughout 2016, using Schmidt's team's prototypes, they developed an open-source toolkit called Blockcerts, which any developer or school can use to issue and verify blockchain-based educational credentials.

By summer 2017, as part of a pilot program, a cohort of 111 graduates, with 43 choosing to take part, became the first to have the option to receive their diplomas on their smartphones via an app, in addition to the traditional format. The pilot resulted from a partnership between the MIT Registrar's Office and Learning Machine. The app is called Blockcerts Wallet, and it enables students to quickly and easily get a verifiable, tamper-proof version of their diploma that they can share with employers, schools, family, and friends. To ensure the security of the diploma, the pilot utilizes the same Blockchain technology that powers the digital currency Bitcoin. It also integrates with MIT's identity provider, Touchstone. While digital credentials are not new, the MIT pilot has been pioneering, because it gives students autonomy over their own records. Indeed, from the beginning, one of the primary motivations of this project has been to empower students to be the curators of their own credentials and be able to share them in a secure way with whomever they choose. Another important motivation was that this format of official records can exist even if the institution ceases to exist, and people can own and use their official records forever.

The software Learning Machine developed uses the Bitcoin Blockchain, and even though recently there has been a proliferation of new types of blockchains, the Bitcoin one remained the gold standard for Learning Machine's purposes, because it prioritizes security over other qualities like speed, cost, or ease of use. Indeed, their purpose was to make official records that need to last a lifetime and work anywhere in the world.

Learning Machine also recognized there was a missing link in the system, despite the potential of Blockchain technology to make official, recipient-owned credentials a reality. In order for the information to be encrypted, the user also needs to obtain a public and private key—a set of unique numerical identifiers that represent them. This issue is a giant barrier, because asking students to generate publicprivate key pairs for the Bitcoin Blockchain is not easily comprehensible for the majority of them.

Blockcerts Wallet intended to solve this problem. After the student downloads the app, it generates the public–private key pair and sends the public key to MIT, where it is written into the digital record. Next, a one-way hash (a string of numbers that can be used for verification later) is added to the Blockchain. The diploma information itself does not go onto the Blockchain, just the timestamped transaction indicating that MIT created the digital record. Finally, MIT emails the digital diploma (a JavaScript Object Notation file, or JSON) with the student's public key inscribed into it. As the mobile app on the student's phone has his unique private key, the student can prove ownership of the diploma.

The utilization of this technology means that students can quickly share their virtual certificates with potential employers without involving an intermediary. Third parties can verify the legitimacy of the diploma by pasting the URL of the certificate into an MIT-hosted portal.

This portal can instantly verify the legitimacy of the certificate, negating the notarization step often required in the verification of paper certificates. Indeed, this generation of digital natives expects to share records in an easy way, but before Blockcerts, there was not a technology to support this need.

1.2. Blockchain over Bitcoin

Once the technology is consolidated, the obvious question is whether it should be applicable in other contexts equally complex and crucial, such as education. Indeed, although the technology of Blockchain is notably linked to Bitcoin, in the past two years, its utilization is extending.

Today all the business players—from banks to insurance companies, manufacturing companies, and the media—are taking an interest in Blockchain technology, and there are 579 projects (started or only announced) internationally registered from January 2016 to today, of which 46 are being tested or operative. These are the numbers of the Blockchain Observatory and Distributed Ledger of the School of Management of the Polytechnic of Milan [3].

There are also ongoing studies that challenge the sustainability of bitcoin, considering the environmental impacts, social issues, and economic aspects of the block-chain based infrastructure [4,5].

Moreover, despite the failure to identify clear business models and the absence of a globally defined standard, the blockchain is booming: the trials initiated or in the "proof of concept" phase in 2017 grew by 73% compared to the previous year, while the announcements, which often do not lead to concrete results, were 273% more. The vast majority of projects, equal to 59% of those surveyed to date, have been developed in the financial sector, but from 2017 we note a gradual expansion of the application areas that also affect government activity (9%), logistics (7.2%), utilities (3.9%), agrifood (3%), insurance (2.7%), health care (2.4%), air transport (2.4%), the media (1.8%), and telecommunications (1.2%). The blockchain today is mainly used for processes in payment systems (94 projects), tracking and supply chain (67), data and document management (64), and the capital market (51).

One of the most promising sectors is education. Blockchains are designed to be immutable. Once a block is written into a Blockchain, it cannot be changed. The trusted nature of Blockchain is one of its great potentials to be exploited: data on the Blockchain is legitimate, having been validated by multiple participants in the network. The main element influencing the possible successful proliferation and utilization of such credentials is that people can trust that they are immutable and easily verifiable. Trust indeed plays a key role in many social and economic interactions involving uncertainty and dependency [6–8] and, therefore, in educational credentials. Trust needs verification and the verification phase of credentials is indeed the most expensive activity in terms of time and therefore money. This is the aspect to leverage and to which to sensitize people involved in the process. Starting from these assumptions, we aim to explore this possibility: issue diploma certificates, record this "fact" in the Blockchain, and verify their existence in a tamper-proof way. This process enables us to save time and to simplify verification processes and, as a consequence, to save money and concentrate our efforts to make other processes more efficient.

1.3. Literature Review

The Blockchain is polarizing high scientific and media attention, while provoking enthusiasm about its potential uses and role in driving the decentralization of society [9] and freedom from central authorities. Much attention has been devoted to the positive or disruptive changes that the broad adoption of this technology will bring to our societies. Despite all this consideration, little literature has been dedicated to the challenges it may pose, apart from the technological ones. Beck and Muller-Bloch [10] stated that the advent of Blockchain can be compared to the invention of the Internet, showing the potential for radical transformations within a number of industries. Although, according to Yermack [11], a first analogical example of this technology was given by Haber and

Stornetta's work [12], which proposed a distributed ledger published in public media (e.g., newspapers) for time-stamping the creation of intellectual property, Nakamoto's paper in 2008 [13] established the basis of modern blockchain-based cryptocurrency innovation. Nakamoto's effort was the first to provide a trusted non-territorial digital currency, not depending on centralized and financial institutions, as affirmed by Catalini and Gans [14]. In fact, the majority of research was conducted in the Bitcoin environment, considering that Bitcoin is currently the most commonly used and important technology using Blockchain, with the largest user base. A decade after Nakamoto's white paper, the Blockchain technology has moved beyond cryptocurrencies, but still little is known about its promised disruptive potential that goes beyond IT [10]. Indeed, it is surprising that the number of solutions using Blockchain other than Bitcoin is still small. In 80% of the selected papers, the research was conducted in the Bitcoin environment. Only 20% focus on other applications using Blockchain technology. Security was the one of the major research topics in Blockchain and Bitcoin, relating to challenges and limitations such as trends and impacts of security incidents; 51% focused on attacks, data malleability problems, and authentication and cryptography issues. Although several solutions to address these issues have been presented, many of them are just brief suggestions, lacking concrete evaluation of their effectiveness. Furthermore, the applications of this technology are almost foreseen in every human field, and in this light, the possible utilizations of Blockchain have attracted high expectations. The literature review undertaken underlined that much attention must be given to those aspects that, to date, could be identified as the most uncertain or problematic in relation to Blockchain, its features (i.e., a distributed ledger, consensus, and smart contracts), and its applications on a large scale (trust, law and regulation, decentralized government, and governance), because Blockchain promises to deeply transform them and the correlated institutions, and because its potential applications are much broader than currency [15] and well beyond financial services [16].

According to the aim of our paper to redefine trust for digital certificates, we undertook a literature review focusing on trust. The distrust suffered by institutions today, and the birth of a technology that allows the creation of autonomous networks, poses thoughtful challenges to be faced to achieve an unprejudiced, inclusive, and sustainable society. In every human transaction, trust must be in place. In fact, trust is not a behavior (e.g., cooperation), or a choice (e.g., taking a risk), but a primary psychological condition that can cause or result from such actions [8]. Moreover, it is not transitive [17]. Distributed ledger technology allows participants to trust the outcome of a system without trusting the individual participants, which is a precondition for economic efficiency and prosperity [18–20]. The Blockchain has often been described as a trust-less system, a trust machine, and it can constitute the foundation for genuinely trust-free economy [21]. Introduced by Greiner and Wang [22], the notion of trust-free systems proposes to utilize Blockchain technology's "capability to automatically create an immutable, consensually agreed, and publicly available record of past transactions that is governed by the whole system to mitigate trust issues in peer-to-peer systems" [23]. Within the Blockchain, this happens with the so-called "consensus": it means that participants in a network have confidence that their ledgers are both accurate and consistent [17]. The distributed consensus protocol ensures the data integrity of the transactions [24]. The ledger is based on cryptographic techniques (the hash function and the digital signature) [25], combined with game theory [13], capable of solving the so-called double-spending problem and the Byzantine generals problem. Although there were theoretical solutions given in a 1982 paper by Lamport et al. [26], Nakamoto's implementation of Blockchain technology was the first to provide de facto Byzantine-fault-tolerant consensus [27]. Basically, the combination of security and transparency is what makes the Blockchain a trust-free technology [28]. Rachel Botsman, one of the pioneers of collaborative consumption, suggested that "the distribution of trust among people, accelerated by blockchain technology, will fundamentally transform the way trust is built" [23]. Therefore, the central question is not how to regulate blockchains, but how blockchains regulate [17]. Technologies can operate as a kind of law, regulating the behavior of their users [29]. The set-up of the Blockchain allows actors to trust the technology, which dispenses with the need to trust involved actors [30]. According to some researchers, with the Blockchain, a new form of

algorithmic trust is created, distinguished from the more traditional typology of trust that was initially only between human agents [31], representing "a shift from trusting people to trusting math" [32,33]. At the bare minimum, trust must be placed in the underlying cryptography [34], allowing all the operation by everyone [35]. This transparency is what it seems enough to claim the unnecessity of trust and correlated institutions. As mentioned above, trust is about expectations and vulnerability of the parties. The Blockchain ensures that expectations are not disappointed and vulnerability is reduced or removed through immutability and consensus.

2. The Blockchain Paradigm and the Bitcoin System

The Bitcoin Blockchain [13] is an open, decentralized public ledger for transaction records. In this section, we briefly introduce the technology and summarize its main features relevant to the digital certificates' application. We refer the reader interested in a complete description to [32,36].

In the "Bitcoin economy", a fixed number of new bitcoins are minted every ten minutes on average. Informally speaking, bitcoins are always tied to bitcoin addresses (since the time they are minted), and they can be transferred from one address to another by means of transactions. Anyone can generate new addresses, receive some amount of bitcoins, and send them to other addresses. In principle, anyone is also allowed to participate in the "race" for generating new bitcoins. There is no "authority" regulating the minting process (mining in the language of Bitcoin) and no "bank" managing transactions. All this is possible due to an effective combination of a few classical cryptographic concepts (namely, cryptographic hash functions [37] and digital signature schemes [38]) with the flexibility of peer-to-peer networks [39].

All nodes participating in the Bitcoin system are connected toward an unstructured peer-to-peer network running on top of the Internet: every time the Bitcoin software is executed on a computer (or smartphone, tablet, or any other device with the appropriate computational and connectivity capabilities), that computer becomes a node of the network, i.e., the software connects to a small set of other nodes running the same software and those nodes become its neighbors. Neighbors bring the new node up-to-speed on the current state of the system and constantly keep exchanging small packets of information with it. When a node receives a packet from one of its neighbors, it has all the information needed to verify the validity of the packet; if the packet turns out valid, the node forwards it to all its other neighbors that in turn will check the validity and forward the packet to their own neighbors. In this way, each newly-generated valid packet reaches all the nodes of the network, within two seconds or so. The information contained in the packets exchanged by the nodes of the Bitcoin network is, in most cases, either a transaction or a block.

To simplify, we can say that a transaction is made by (one or more) input addresses, output addresses, digital signatures, and some room for a small optional message. The transaction reassigns to the output addresses the bitcoins currently assigned to the input addresses. In order to be valid, the digital signatures must be completed with the private keys associated to the input addresses. As mentioned in the previous paragraph, a valid transaction sent by a node of the network reaches all the nodes within a few seconds. At this stage, the transaction is still considered "unconfirmed", even though all the nodes are already aware of the transfer of bitcoins from the input addresses to the output addresses, and they would not consider valid any other transaction with the same input addresses. The transaction becomes "confirmed" when a miner includes it in the next valid block.

Miners are nodes of the network that, in addition to the operations performed by any other node, use their computational power to try to generate the next valid block of the ledger. If they succeed, they get as a reward the newly minted bitcoins that come with it plus the transaction fees that come with any transaction they include in the block. In order to understand the details of this process, some preliminary technical notions about cryptographic hash functions are needed. However, for the purpose of this paper, it is enough to note that, in order to be considered valid, a block has to contain a link to the previous valid block, a timestamp, a digital fingerprint of the set of transactions included in the block, and a nonce, i.e., a number satisfying some properties. Finding such a nonce is a matter

of brute-force search, and the chances that a specific miner finds one are directly proportional to the computational power the miner uses for that purpose. When a miner finds such a nonce for its own block, the miner sends the block to all nodes via the peer-to-peer network; each node can independently verify that the block is actually valid, and all miners will start considering that one as the last valid block to link. The sequence of blocks, each one linked to the previous one, up to the genesis block mined by Satoshi Nakamoto in January 2009, forms the Blockchain.

The Blockchain is growing, by design, at an average rate of one new block every ten minutes. Everyone can run a node of the Bitcoin network and keep a copy of all the blocks and all the transactions included in them since the genesis block. Moreover, anyone can send a transaction to the other nodes, and if the transaction is valid, it will be included in one of the next block by the miners. When the block including the transaction is followed by a small number of new blocks, that transaction can be safely considered "permanently stored" in the Blockchain. By suitably using the small room for a message allowed in Bitcoin transactions, one can thus use the Blockchain as a publicly-accessible, write-only, and timestamped storage medium. This is what makes it an effective platform for digital certificates, as we will see in the next sections.

3. The Diploma Certificate Process "as is" at University of Rome "Tor Vergata"

The issuing of a Diploma is a delicate process, because it has to take into account a lot of information that is not so difficult to modify. Moreover, the verification process of the achievement of a certain academic qualification is even more delicate and more easily editable.

The process is also expensive in terms of resources and time and therefore money.

At the University of Rome "Tor Vergata", a student that needs the diploma certificate to be shared and utilized for his necessities has two possibilities to request a copy:

- He or his delegate can go personally to the Student Secretariat desk and, after demonstrating his identity with personal documents and a matriculation number, request the graduation certificate that the Secretariat can issue and deliver directly to the student.
- If the student cannot go personally to the Student Secretariat and none of his delegates can do so, the student can send the certificate request by email. For the verification of the identity of the student, the competent offices require some credentials already held by the University, such as the email address and telephone number that the student used during the university period and the scanned copies of two identity documents. After having carried out the necessary checks to verify the student's credentials and the effective possession of the qualification, the competent offices proceed with the issuing of the certificate required with the appropriate seals and signatures in italics, important for recognition and validation. The certificate in an electronic format is sent via a certified email (Posta Elettronica Cartificata—PEC) to the student.
- If the email address and the mobile number are different from those used by the student during the university period, the University will check the documents and the actual possession of the degree. If the process is successful, the competent offices proceed with the issuing of the authenticated certificate requested with the appropriate seals and signatures in italics, important for recognition and validation. The certificate in an electronic format is sent via certified email (PEC) to the student.

The procedure is different when a third party requires to the University if a student is really in possession of a specific qualification:

- If the request is made by another Public Administration through PEC, the University, after the due verification of the actual possession of the qualification by the student, always through PEC, confirms or denies the title.
- If the request comes from a company (Italian or foreign), the University is not required to provide information on the degree obtained by the student [40]. The request must be made by the student who, once the degree certificate is obtained, can then make the necessary use.

Abroad, there are companies that operate as the interface between the company that requires the verification of the certificate and the University. If the certificate of graduation is present in the request sent by email, the University will give a positive or negative response once the necessary checks have been made. If the certificate to be verified is not attached to the email, the student must request a copy of the degree certificate, and the University will proceed as previously illustrated.

The process was powered by Adonis Community Edition, and therefore we have been able to estimate its cost. At the University of Rome "Tor Vergata", the verification process of a certificate diploma is about 3.48 Euros per certificate. The time lapse between the receipt of the request and the sending of the reply is on average 3 days. Considering an average number of graduates per year equals 5400, the total cost of this activity is about 18,792 Euros, which is not insignificant, even though in a University financial statement it could be negligible. In fact, our goal is not mere economic savings, but the efficiency and scalability of the process that would affect not only the process itself, but also other processes that could gain more time and resources. Fifteen minutes for every certificate is about 81,000 min, corresponding to 1350 h or 36.5 weeks of work.

Using the Bitcoin Blockchain technology, the University can record in one single transaction an entire graduation session. Indeed, while it is possible to issue one certificate with one Bitcoin transaction, it is far more efficient to use one Bitcoin transaction to issue a batch of certificates. The issuer builds a Merkle tree of certificate hashes and registers the Merkle root as one field in the Bitcoin transaction. Suppose the batch contains n certificates, and certificate *i* contains recipient *i*'s information. The issuer hashes each certificate and combines them into a Merkle tree.

A Bitcoin transaction is determined by the size of the transaction and the transaction fee. Blockcerts transaction sizes are static and small—they add a single fixed-size output on top of a standard single-input, single-output transaction. This is true no matter the number of certificates in a batch. Therefore, the cost to issue a batch of Blockcerts is largely influenced by the transaction fee, which is a fee paid to miners to ensure timely mining of transactions. The recommended fee changes over time; current recommended values can be obtained from the "To get in next block" section of Recommended Bitcoin Network Transaction Fees (https://bitcoinexchangerate.org/fees).

In the Blockcerts project, the transaction fee is configurable. The default value (0.0006 bitcoins, approximately five euros at the current BTC/EURO exchange rate) guarantees that the transaction with the Merkle root of the certificates is very likely to be inserted in the next mined block. This setting can be overridden in the source file to reduce the cost.

After this single operation on the Blockchain, students are immediately masters of their credentials without further interactions with the university or institute that delivered the diploma or certificate.

4. The Digital Diploma at University of Rome "Tor Vergata"

By winter 2018, the University of Rome "Tor Vergata", and in particular a team of the Department of Enterprise Engineering, began to become familiar with the MIT project and to study and apply the open source programs made available by MIT and Learning Machine.

Many of the most remarkable challenges we encountered were technical in nature, because the Blockchain is a relatively new technology and its complexity and the fact that we were not the creators of the idea played an important role in becoming familiar with and starting to use it. Moreover, although we were in agreement with the concept of making students masters of their credentials and the positive economic return and efficiency of the process for the University, the immutable nature of such credentials makes it even more important to carefully consider the long-term effects of this technology. That is why we have taken small experimental steps, tested our system, and continue to make technical proofs.

The Blockcerts project source code (available at https://github.com/blockchain-certificates) consists of 26 repositories at the time of writing, and the software is currently under active development by the community. While most of the available software is already production-level code, several choices and customizations are required in order to start issuing and distributing Blockcerts-compatible certificates.

In our deployment at the University of Rome "Tor Vergata", we decided to run a Bitcoin full-node to generate the transactions containing the hashes of the certificates and to spread them to the Bitcoin network. On top of the Bitcoin full-node, we selected three main tools from the Blockcerts toolbox: cert-tools, cert-issuer, and cert-viewer.

- Cert-tools details how to make a digital certificate, describing the data standard for digital certificates, essentially a JSON file with the necessary fields needed for cert-issuer code to place it on the Blockchain. The schema is as close to the Mozilla Open Badges specifications as possible. In order to generate the certificates, "cert-tools" configuration files need to be populated with several pieces of information (e.g., the Bitcoin address identifying the issuing institution) and integrated with the system containing the students' data.
- Cert-issuer takes the JSON certificate, creates the hash of the certificate, and issues a certificate by broadcasting a Bitcoin transaction from the issuing institution's address to a recipient's address on the Bitcoin Blockchain with the hash embedded. In order to generate valid Bitcoin transactions, cert-issuer needs access to the private key associated to the Bitcoin address of the issuing institution. Moreover, it needs to be configured to interact with the Bitcoin full-node that spreads the transactions to the Bitcoin network and allows them to be included in the Blockchain.
- Cert-viewer is used to display and verify these certificates after they have been issued. The viewer code also provides the ability for users to request certificates and to generate a new Bitcoin identity. The Blockcerts wallet can also be used to display and verify the certificates.

By summer 2018, we had used and customized the above tools to issue some dummy certificates to test the overall procedure and to check their compliance with the Blockcerts wallet and the Blockcerts Universal Verifier (www.blockcerts.org).

We started our experimental pilot program with the 2018 Autumn/2019 Winter graduation sessions in the Department of Enterprise Engineering. In order to comply with the new EU General Data Protection Regulation (GDPR) [40], we decided to ask students participating in the pilot program to sign a statement agreement in which the procedure of the creation of digital certificates was explained and a primer of the principles behind Blockcerts was given. Indeed, parties wanting to use a public Blockchain to record off-chain assets face the problem related to real-world laws [16,41].

The subset of students selected for the pilot program were glad to participate to our innovative initiative, as like all the native digital people, they criticized the lack of such an instrument despite the proliferation of digital apps and online learning possibilities. We will test the procedure at larger scale in the future; in light of our pilot program, we see no obstacles to extending it to all the graduating students of the University of Rome "Tor Vergata".

Another interesting evolution of the Blockchain certificate at the University of Rome "Tor Vergata" is to record the full academic carrier of the students on the Blockchain. This operation could give students an even greater independence and mastery of their credentials and could simplify the University procedures when dealing with the restarting of a course of study or transfer to another course of study or another University. This procedure will also be a further development of all was done initially by MIT and Learning Machine.

5. Discussion

During the last two years, blockchain-based projects have become a hot topic. It is likely that much of the rhetoric has been overstated, and the same is true for some of the criticism.

It would be a mistake to think that we are dealing with a technology of immediate application, or that changes can be implemented easily, because the Blockchain is a very novel and complex technology. We are rather in an initial exploratory period. The Blockchain is not the solution that will fix everything that is wrong with today's credentials. However, it does offer some possibilities for improving the system we have today, and that is the reason why it is so interesting and challenging to explore [42].

The fervor with which some sectors have been pursuing Blockchain projects has raised alarm for the consequences that a literal application of this technology could have. At this time, speaking of the consequences of the possible implementations means to move into the field of speculation as much as the literature that is promoting it.

Blockchain is a disruptive technology that, after a few years of implementation as the basis of digital currency, is showing itself to be an open resource with possibilities in different fields. The key to the interest in this technology lies in its ability to move from a system of centralized data logging to a distributed system that ensures no alteration of the information and the maintenance of privacy. The real revolution of Blockchain is that redefines "trust" as "high-trust computing", as you no longer need to trust anyone but an algorithm. It brings reliability, transparency, and security to all manner of data exchanges: financial transactions, contractual and legal agreements, changes of ownership, and certifications.

The Blockchain represents an unprecedented opportunity for the enterprise and the public sector.

Every institution capable of exploiting these technologies will have a chance to radically streamline and enhance existing processes, create entirely new business models, and develop innovative products and services for a new generation of consumers. However, this is not a vision of a utopian, tech-enabled future: the technological capabilities are available today to keep an unalterable record of every exchange, removing the need for trusted, third-party intermediaries in digital transactions. The consequence are faster processes, real-time transaction visibility, and reduced costs across every industrial, social, and economic sector. Gartner estimates that Blockchain could create US$176 billion of value-added revenue by 2025, revolutionizing the supply chain, enabling new business models, and disrupting existing ones.

Blockchain technology can also play an important role in securing information repositories and being a complementary aspect of information governance. Indeed, a lot of the literature focus has been placed on big data analytics for decision-making, however further research is needed about the security and clearance permissions in private settings, as noted by Mikalef et al. [43,44]. Blockchain can help in filling this gap, showing other potential applications and uses of this technology. Furthermore, the collaborative nature of big data analytics with Blockchain technology is a useful and significant topic to be deepened in future research.

As MIT and Learning Machine have been working on their project of Blockchain certificates, one of the most asked questions was why they choose Bitcoin Blockchain and not other ones, such as Ethereum. The answer was that when MIT started the project, Ethereum was still only a the beginning of an idea, whereas Bitcoin has been the most tested and consistent Blockchain to rely on. In addition, the relatively robust self-interest of miners, and the financial investment made into Bitcoin (and Bitcoin-related companies), make it likely that it will be utilized for a good while longer.

We followed the MIT idea; however, our solution is not locked to one particular Blockchain: it would be easy to also start publishing our credentials to other blockchains, but for most of what we want to do in the first phase of experimentation, the functionality of the Bitcoin Blockchain continues to be sufficient. That is not to say that we are not curious about the potential of smart contracts, and we are discussing the potential of Ethereum-based side-chains to reduce transaction cost and expand functionality [45,46]. We are also interested in the evolution of Certificate Transparency (https://www.certificate-transparency.org/)—an Internet security standard and open-source framework for monitoring and auditing digital certificates—and we believe that a lot has been done with trust in digital certificates, but a lot more can be done and in a different manner. This is the reason why the University of Rome "Tor Vergata" aims at continuing its studies of digital certificates, trying to contribute to the exploitation of an Internet security standard and open-source framework for monitoring and auditing digital certificates. Blockchain is undoubtedly transformative. In fact, much of its impact has yet to be explored, even on a theoretical level.

Author Contributions: G.C. wrote the paper and coordinated the various aspects of the project dealing with the different offices and people involved. N.L.G. supported the team and secured the availability of the critical

University's resources. F.P. managed the tools and the infrastructure to issue experimental Blockcerts certificates and wrote Section 2. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Acknowledgments: The authors would like to thank Lorenzo Catucci of the Calculation Center for his precious help and willingness to put at our disposal the technical resources needed for our experimental proofs. The authors would also like to thank Domenico Genovese and Ettore Angelucci for their precious help in understanding the "as is" process of issuing a diploma certificate at the University of Rome "Tor Vergata". The authors would like to thank Arnaldo Morace Pinelli and his collaborators Ilaria Foggia and Luca Tubaro for their help in the delicate process of the drafting of the student statement agreement. The authors thank Luca Berloco for his precious help, mainly in the initial phase of the project.

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

References

1. Schmidt, J.P. Blockcerts—An Open Infrastructure for Academic Credentials on the Blockchain. MIT Media Lab Learning Initiative. 2016. Available online: https://medium.com/mit-media-lab/blockcerts-an-open-infrastructure-for-academic-credentials-on-the-blockchain-899a6b880b2f (accessed on 20 October 2020).
2. Schmidt, J.P. Certificates, Reputation, and the Blockchain. MIT Media Lab, 2015. Available online: https://medium.com/mit-media-lab/certificates-reputation-and-the-blockchain-aee03622426f (accessed on 20 October 2020).
3. School of Management of the Polytechnic of Milan—Blockchain Observatory & Distributed Ledger. Blockchain in Italia e nel mondo: Verso l'Internet of Value. 2019. Available online: https://www.osservatori.net/it_it/osservatori/comunicati-stampa/blockchain-italia-internet-of-value (accessed on 20 October 2020).
4. Giungato, P.; Rana, R.; Tarabella, A.; Tricase, C. Current trends in sustainability of bitcoins and related blockchain technology. *Sustainability* **2017**, *9*, 2214. [CrossRef]
5. Vranken, H. Sustainability of bitcoin and blockchains. *Curr. Opin. Environ. Sustain.* **2017**, *28*, 1–9. [CrossRef]
6. Deutsch, M. Trust and suspicion. *J. Confl. Resolut.* **1958**, *2*, 265–279. [CrossRef]
7. Kini, A.; Choobineh, J. Trust in electronic commerce: Definition and theoretical considerations. In Proceedings of the 31st Annual Hawaii International Conference on System Sciences, Los Alamitos, CA, USA, 9 January 1998; IEEE Computer Society Press: New York, NY, USA, 1998; Volume 4, pp. 51–61.
8. Rousseau, D.; Sitkin, S.; Burt, R.; Camerer, C. Not So Different After All: A Cross-discipline View of Trust. *Acad. Manag. Rev.* **1998**, *23*, 393–404. [CrossRef]
9. Gupta, V. The Promise of Blockchain Is a World Without Middlemen. *Harv. Bus. Rev.* **2017**. Available online: https://hbr.org/2017/03/the-promise-of-blockchain-is-a-world-without-middlemen (accessed on 20 October 2020).
10. Beck, R.; Müller-Bloch, C. Blockchain as Radical Innovation: A Framework for Engaging with Distributed Ledgers. In Proceedings of the 50th Hawaii International Conference on System Sciences; 2017. Available online: https://www.researchgate.net/publication/312166392_Blockchain_as_Radical_Innovation_A_Framework_for_Engaging_with_Distributed_Ledgers_as_Incumbent_Organization (accessed on 20 October 2020).
11. Yermack, D. Corporate governance and blockchains. *Rev. Financ.* **2017**, *21*, 7–31. [CrossRef]
12. Haber, S.; Stornetta, W.S. How to time-stamp a digital document. *J. Cryptol.* **1991**, *3*, 99–111. [CrossRef]
13. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. Available online: https://bitcoin.org/bitcoin.pdf (accessed on 20 October 2020).
14. Catalini, C.; Gans, J.S. Some Simple Economics of the Blockchain. Rotman School of Management Working Paper No. 2874598, 2017; MIT Sloan Research Paper No. 5191-16. Available online: https://ssrn.com/abstract=2874598 or http://dx.doi.org/10.2139/ssrn.2874598 (accessed on 20 October 2020).
15. Allen, D. Discovering and Developing the Blockchain Cryptoeconomy. 2017. Available online: https://ssrn.com/abstract=2815255 or http://dx.doi.org/10.2139/ssrn.2815255 (accessed on 20 October 2020).
16. Tapscott, D.; Tapscott, A. The Blockchain Revolution and Higher Education. *Educ. Rev.* **2017**, *52*, 11–24. Available online: https://er.educause.edu/articles/2017/3/the-blockchain-revolution-and-higher-education (accessed on 20 October 2020).
17. Werbach, K. Trust, But Verify: Why the Blockchain Needs the Law. *Berkeley Technol. Law J.* **2018**, *33*, 487. Available online: https://ssrn.com/abstract=2844409 (accessed on 20 October 2020). [CrossRef]

18. North, D. *Institutions, Institutional Change, and Economic Performance*; Cambridge University Press: Cambridge, UK, 1990.
19. Nooteboom, B. *Trust: Forms, Foundations, Functions, Failures and Figures*; Edward Elgar: Cheltenham, UK, 2002.
20. Davidson, S.; De Filippi, P.; Potts, J. Economics of Blockchain. 2016. Available online: https://ssrn.com/abstract=2744751 or http://dx.doi.org/10.2139/ssrn.2744751 (accessed on 20 October 2020).
21. Glaser, F. Pervasive Decentralisation of Digital Infrastructures: A Framework for Blockchain Enabled System and Use Case Analysis. In Proceedings of the 50th Hawaii International Conference on System Sciences (HICSS-50), Waikoloa Village, Hawaii, 4 January 2017; Available online: https://ssrn.com/abstract=3052165 (accessed on 20 October 2020).
22. Greiner, M.; Wang, H. Trust-free Systems—A New Research and Design Direction to Handle Trust-Issues in P2P Systems: The Case of Bitcoin. In Proceedings of the 21st Americas Conference on Information Systems, AMCIS, San Juan, PR, USA, 13–15 August 2015.
23. Hawlitschek, F.; Notheisen, B.; Teubner, T. The limits of trust-free systems: A literature review on blockchain technology and trust in the sharing economy. *Electron. Commer. Res. Appl.* **2018**, *29*, 50–63. [CrossRef]
24. Ølnes, S.; Ubacht, J.; Janssen, M. Blockchain in government: Benefits and implications of distributed ledger technology for information sharing. *Gov. Inf. Q.* **2017**, *34*, 355–364. Available online: https://doi.org/10.1016/j.giq.2017.09.007 (accessed on 20 October 2020). [CrossRef]
25. Ishmaev, G. Blockchain Technology as an Institution of Property. *Metaphilosophy* **2017**, *48*, 666–686. [CrossRef]
26. Lamport, L.; Shostak, R.; Pease, M. The Byzantine Generals Problem. *ACM Trans. Program. Lang. Syst.* **1982**, *4*, 382–401. [CrossRef]
27. Huckle, S.; White, M. Socialism and the blockchain. *Future Internet* **2016**, *8*, 49. [CrossRef]
28. Beck, R.; Stenum Czepluch, J.; Lollike, N.; Malone, S. Blockchain–The Gateway to Trust-Free Cryptographic Transactions. 2016. Research Papers 153. Available online: http://aisel.aisnet.org/ecis2016_rp/153 (accessed on 20 October 2020).
29. Werbach, K.; Cornell, N. Contracts Ex Machina. *Duke Law J.* **2017**, *67*, 313. Available online: https://ssrn.com/abstract=2936294 (accessed on 20 October 2020).
30. Finck, M. Blockchain Regulation. *Ger. Law J.* **2018**, *19*, 665–692. Available online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3014641 (accessed on 20 October 2020). [CrossRef]
31. Swan, M.; De Filippi, P. Toward a philosophy of blockchain: A Symposium: Introduction. *Metaphilosophy* **2017**, *48*, 603–619. Available online: https://ssrn.com/abstract=3097477 (accessed on 20 October 2020). [CrossRef]
32. Antonopoulos, A.M. *Mastering Bitcoin: Programming the Open Blockchain*; O'Reilly Media, Inc.: Sebastopol, CA, USA, 2017.
33. Atzori, M. Blockchain Technology and Decentralized Governance: Is the State Still Necessary? 2015. Available online: https://ssrn.com/abstract=2709713 or http://dx.doi.org/10.2139/ssrn.2709713 (accessed on 20 October 2020).
34. Hileman, G.; Rauchs, M. Global Blockchain Benchmarking Study. 2017. Available online: https://ssrn.com/abstract=3040224 or http://dx.doi.org/10.2139/ssrn.3040224 (accessed on 20 October 2020).
35. Wright, A.; De Filippi, P. Decentralized Blockchain Technology and the Rise of Lex Cryptographia. 2015. Available online: https://ssrn.com/abstract=2580664 or http://dx.doi.org/10.2139/ssrn.2580664 (accessed on 20 October 2020).
36. Narayanan, A.; Bonneau, J.; Felten, E.; Miller, A.; Goldfeder, S. *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*; Princeton University Press: Princeton, NJ, USA, 2016.
37. Damgård, I.B. Collision free hash functions and public key signature schemes. In *Advances in Cryptology—EUROCRYPT' 87*; Springer: Berlin/Heidelberg, Germany, 1988; Volume 304, pp. 203–216.
38. Diffie, W.; Hellman, M. New directions in cryptography. *IEEE Trans. Inf. Theory* **1976**, *22*, 644–654.
39. Barkai, D. *Peer-to-Peer Computing: Technologies for Sharing and Collaborating on the Net*; Intel Press: Santa Clara, CA, USA, 2001.
40. European Parliament and the Council. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation)". 2016. Available online: https://eur-lex.europa.eu/eli/reg/2016/679/oj (accessed on 20 October 2020).

41. McArthur, D. Will Blockchains Revolutionize Education? *Educ. Rev.* **2019**. Available online: https://er.educause.edu/articles/2018/5/will-blockchains-revolutionize-education (accessed on 20 October 2020).
42. Nazaré, J.; Duffy, K.H.; Schmidt, J.P. What We Learned from Designing an Academic Certificates System on the Blockchain. *Medium* **2016**. Available online: https://library.educause.edu/resources/2016/6/what-we-learned-from-designing-an-academic-certificates-system-on-the-blockchain (accessed on 20 October 2020).
43. Mikalef, P.; Boura, M.; Lekakos, G.; Krogstie, J. Big data analytics and firm performance: Findings from a mixed-method approach. *J. Bus. Res.* **2019**, *98*, 261–276. Available online: https://www.sciencedirect.com/science/article/pii/S014829631930061X or https://doi.org/10.1016/j.jbusres.2019.01.044 (accessed on 20 October 2020).
44. Mikalef, P.; Boura, M.; Lekakos, G.; Krogstie, J. The Role of Information Governance in Big Data Analytics driven Innovation. *Inf. Manag.* **2020**, *57*, 103361. Available online: https://www.sciencedirect.com/science/article/pii/S0378720620302998 (accessed on 20 October 2020). [CrossRef]
45. Kolvenbach, S.; Ruland, R.; Gräther, W.; Prinz, W. Blockchain 4 education. In Proceedings of the 16th European Conference on Computer-Supported Cooperative Work-Panels, Posters and Demos, Nancy, France, 4–8 June 2018; European Society for Socially Embedded Technologies (EUSSET): Siegen, Germany, 2018.
46. Gräther, W.; Kolvenbach, S.; Ruland, R.; Schütte, J.; Torres, C.; Wendland, F. Blockchain for education: Lifelong learning passport. In Proceedings of the 1st ERCIM Blockchain Workshop 2018, Amsterdam, The Netherlands, 8–9 May 2018; European Society for Socially Embedded Technologies (EUSSET): Siegen, Germany, 2018.