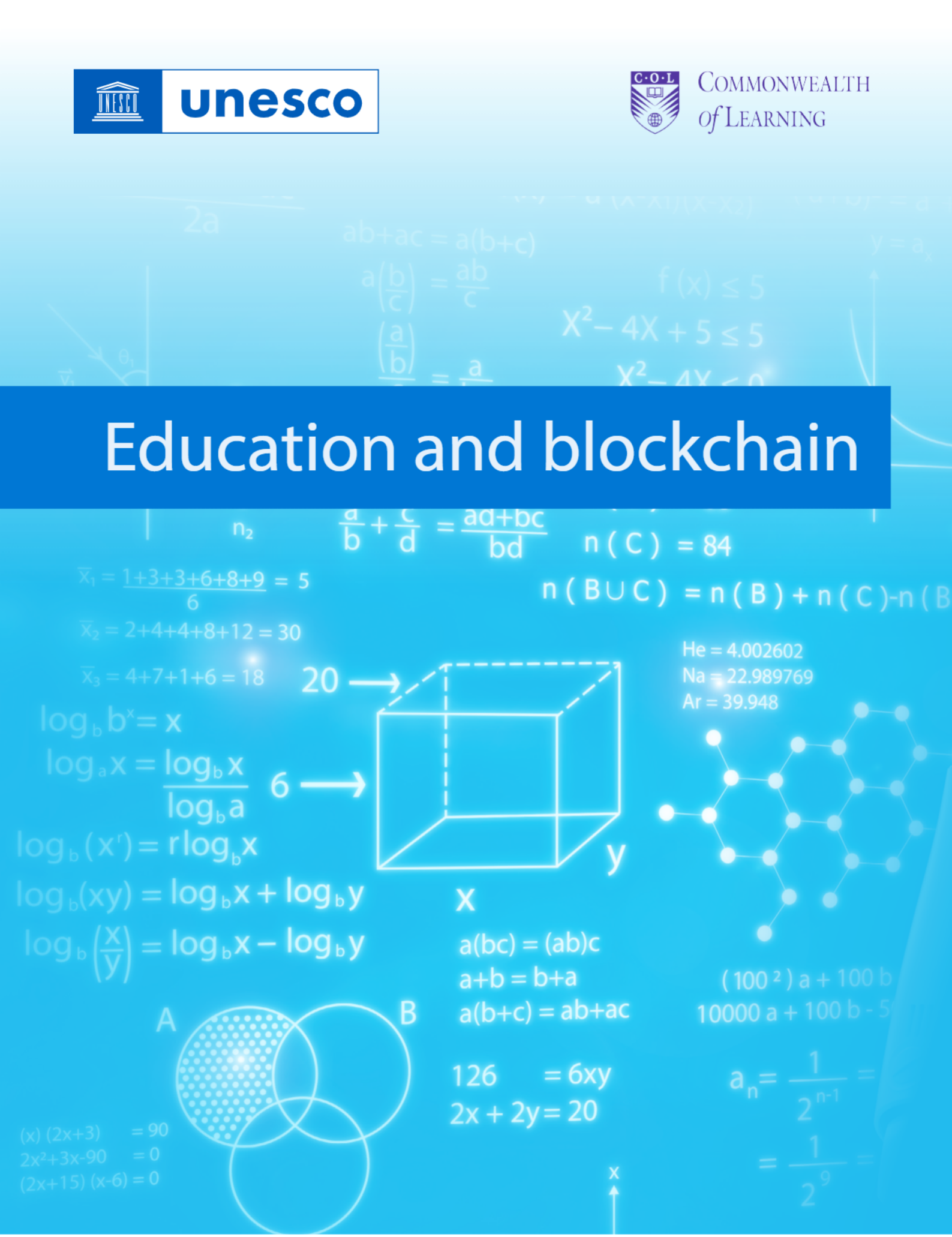
unesco

Commonwealth of Learning

Education and blockchain



Education 2030

UNESCO – a global leader in education

Education is UNESCO's top priority because it is a basic human right and the foundation for peace and sustainable development. UNESCO is the United Nations' specialized agency for education, providing global and regional leadership to drive progress, strengthening the resilience and capacity of national systems to serve all learners. UNESCO also leads efforts to respond to contemporary global challenges through transformative learning, with special focus on gender equality and Africa across all actions.

The Global Education 2030 Agenda

UNESCO, as the United Nations' specialized agency for education, is entrusted to lead and coordinate the Education 2030 Agenda, which is part of a global movement to eradicate poverty through 17 Sustainable Development Goals by 2030. Education, essential to achieve all of these goals, has its own dedicated Goal 4, which aims to ***"ensure inclusive and equitable quality education and promote lifelong learning opportunities for all."*** The Education 2030 Framework for Action provides guidance for the implementation of this ambitious goal and commitments.

unesco
United Nations
Educational, Scientific
and Cultural Organization

Education 2030

Published in 2022 by the United Nations Educational, Scientific and Cultural Organization
7, place de Fontenoy, 75352 Paris 07 SP, France
and Commonwealth of Learning
4710 Kingsway, Suite 2500, Burnaby, V5H 4M2, British Colombia, Canada

ISBN 978-92-3-100565-7

Coordinators: Venkataraman Balaji and Fengchun Miao
Authors: Alex Grech, Venkataraman Balaji and Fengchun Miao

Cover design: Ania Grygorczuk
Cover credit: iStock
Illustrations (pp. 3, 9, 26 and 36): iStock, adapted under standard licence issued to COL
All other icons and illustrations created by COL

Designed by the Commonwealth of Learning

Printed in Canada and France

SHORT SUMMARY

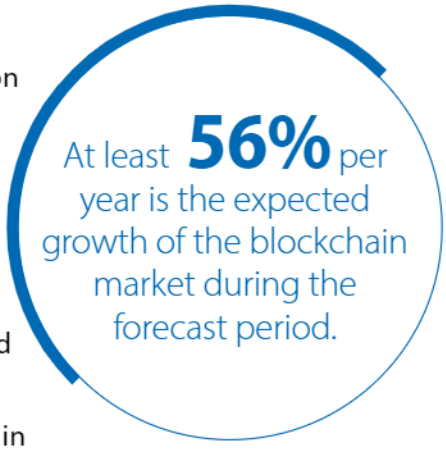
Blockchain - a potential game changer in education

Blockchain is a shared, decentralized and secure ledger technology to record and store digital transactions of almost any digital assets including digital identities, medical and educational records, birth and marriage certificates, skill credentials and digital contracts.

Promising initiatives with blockchain demonstrate that it is already possible to deploy the technology to cover credentialing and certification in both formal and non-formal learning settings. This publication demonstrates and assesses the emerging practices of applying blockchain technologies in education.

Primarily targeting policy-makers, the publication is divided into four parts.

- Part 1 engages with a set of essential knowledge on blockchain technologies presented as questions and answers.
- Part 2 focuses on issues related to the emerging practices associated with the use of blockchain within an education context, highlighting the use of blockchain for digital certificates, credentials, intellectual data management, smart contracts and performance-based payments.
- Part 3 explores the applicability of the technology in a set of use case scenarios, including the notarization of intellectual property rights and educational funding.
- Part 4 iterates the humanistic principles to steer the use of blockchain in education to safeguard human rights, inclusion, equality, gender equality and the sustainability of the environment and ecosystems.



This publication also sheds light on the implications of blockchain technologies for gender equality while drawing attention to the negative impact of the use of blockchain, especially on the environment and ecosystems.

unesco

"Since wars begin in the minds of men and women, it is in the minds of men and women that the defences of peace must be constructed."

unesco

Commonwealth of Learning

Education and blockchain

Foreword

The advent of COVID-19 has provided ample evidence for the need to build the resilience of institutions, systems and processes in the education sector. The increase in natural disasters has also had an impact on education, as data systems in disaster-affected areas have been damaged, irreversibly in some cases. In a context where the risk of climate-induced disasters is increasing, countries will need to treat incorporating data resilience in education as a fundamental aspect of disaster planning. It will be also help national efforts to achieve SDG 4. Blockchain technology can be a key asset in this respect.

Blockchain is an infrastructure for identity verification, which is one of the most relevant functions of this emerging technology in education. When a digital identity verification system can persist irrespective of the nature and extent of external changes, verifying the ownership of digital assets becomes easier. Certificates of attainment are increasingly issued in the digital realm. Micro credentials are one example. They can be linked to a core system of identity verification, namely blockchain, and authenticated more easily across institutional and national boundaries. Such an approach can also be useful in promoting transnational movement of qualifications.

The Commonwealth of Learning (COL) has been a pioneer in promoting a transnational qualifications framework (TQF) through the Virtual University for the Small States of the Commonwealth, a long-running programme involving thirty-two countries, many of which are facing a climate emergency. Policy-makers who work in the realm of TQF have expressed the need for an infrastructure that facilitates the mobility of qualifications. COL thus became interested in exploring the applications of blockchain. Since 2018, COL has offered a series of activities to improve awareness of the opportunities that blockchain can offer to leaders in education – for example, its MOOC on the use of blockchain in education. This was supplemented by a series of webinars and online workshops on blockchain for leaders of educational institutions and senior officials from Member countries in eastern and southern Africa. The present publication is a continuation of COL's effort to familiarize key stakeholders with the potential and benefits of blockchain in education.

COL promotes learning for sustainable development through the use of appropriate technologies and its role as both an enabler for building robust and resilient education systems and a catalyst for innovations. This publication helps fulfil both those roles. In collaborating with UNESCO in bringing out this publication, COL recognizes the importance of using all the appropriate technological tools to help Member States accelerate their progress towards achieving SDG 4 while paying due to attention to developing innovations to minimize the carbon footprint of education and ensure inclusion. For COL, innovations must begin by addressing the needs of the last person in the queue.

It gives me great pleasure to commend this publication, which addresses some of the above-mentioned priorities, as well as the current limitations and emerging solutions offered by blockchain technology.

Professor Asha Kanwar
President and CEO
Commonwealth of Learning

Foreword

In the rapidly evolving landscape of digital innovation, the use of blockchain – a shared, decentralized and distributed ledger technology to store transactions – is still at the exploratory stages in education. Yet, over the past two decades, the international student mobility has tripled to 6 million and is set to double in the next decade. The increasing number of students studying outside of their home countries, combined with the sharp growth of online cross-border learning due to COVID-19 pandemic and diversifying lifelong learning pathways, has triggered the need for portable, secure and verifiable digital credentials. The affordance of blockchain technologies carries unique potential to respond to this profound need.

Blockchain technology has already proven successful at verifying digital records, simplifying procedures to facilitate mobility, and reducing fraud through transparent and tamper-resistant records of certificates. Furthermore, as just cited, this technology allows users to have portable, secure and verifiable digital credentials, and to prove their identities to third parties while protecting their ownership of digital assets, which is one of the key functions of the metaverse. As the world moves towards the age of Web 3.0, blockchain is arguably the crypto key to the metaverse.

It is therefore imperative for education policy-makers to understand the uses and implications of blockchain and put measures in place to harness its potential for the common good. However, due to the novelty and hidden nature of the technology, most policy-makers in education systems do not have a full understanding of blockchain. This publication aims to fill this gap. It begins with an introduction to foundational principles and concepts of blockchain, followed by an examination of various implications of the technology for certificates, credentialing, management of intellectual property protection and digital identities. It reviews the current uses of blockchain in education, while recognizing a number of challenges stemming from the protection of data privacy, costs, scalability and especially the tremendous carbon footprint and energy consumption of blockchain systems and computing infrastructures. It articulates humanistic principles to guide policy-makers to ensure that the use of blockchain in education will protect human rights and data privacy, and reduce the negative impact on the environment and ecosystems.

The present publication, produced under our fruitful partnership with the Commonwealth of Learning (COL), enriches UNESCO's growing 'portfolio' on digital learning and complements three earlier ones: *Guidelines on the Development of Open Educational Resources Policies*, *AI and Education: Guidance for Policy-makers*, and *Guidelines for ICT in Education Policies and Masterplans*. It is my hope that this publication will inspire UNESCO Member States to look into blockchain, an under-used technology supporting the next generation of mainstream digital infrastructure, and ensure that its potential will be fully harnessed for the achievement of SDG 4 and the forging of a new social contract in education that puts human rights at its centre.

Stefania Giannini
UNESCO Assistant Director-General for Education

Acknowledgements

This publication on blockchain and education has been developed jointly by UNESCO and the Commonwealth of Learning, and draws on the experience of leading experts and organizations in the field of blockchain and education.

Fengchun Miao, Chief of the Unit for Technology and Artificial Intelligence in Education of the Future of Learning and Innovation Team, and Venkataraman Balaji, Vice President of the Commonwealth of Learning, conceptualized the framework of the publication and served as its co-authors, along with Alex Grech, from the University of Malta and Director of the 3CL Foundation.

Lesley Cameron provided editorial advice and contributed to improving the coherence among difference sections. Editorial advice from Dave Jackson is acknowledged.

Special thanks are extended to Lluís Ariño, Vanja Gutovic, Keith Holmes, Mitja Jermol and Wesley Teter for peer-reviewing the publication and providing critical input.

In addition, thanks go to Rebecca Ferrie for research on the references and to Glen Hertelendy for coordinating the production of the publication.

Contents

Figures

Tables

Boxes

Abbreviations

AML	Anti-Money Laundering
CA	Certification Authority
CCA	Crypto Climate Accord
CASC	Certificate Authority Security Council
CEF	Connecting Europe Facility
CGI	Consultants to Government & Industries
CIO	Chief Information Officer
DAO	Distributed Autonomous Organization
dApp	Decentralized Application
DHS	Department of Homeland Security
DLT	Distributed Ledger Technologies
DNS	Domain Name Servers
DSDP	Digital Student Data Portability
DSI	Digital Service Infrastructure
EBP	European Blockchain Partnership
EBSI	European Blockchain Services Infrastructure
ECIU	European Consortium of Innovative Universities
ECTS	European Credit Transfer System
eKYC	Electronic Know Your Customer
ENIC	European Network of Information Centres in the European Region
EQAR	European Quality Assurance Register
EQUIS	European Quality Improvement System
FUN	France Université Numérique
GDPR	General Data Protection Regulation
HTTP	HyperText Transfer Protocol
ICO	Initial Coin Offering
ICT	Information and Communication Technology

IEEE	Institute of Electrical and Electronics Engineers
IP	Intellectual Property
KYC	Know Your Customer
LDCs	Least Developed Countries
LLDCs	Landlocked Developing Countries
MCAST	Malta College for Arts, Sciences & Technologies
MIT	Massachusetts Institute of Technology
MOOC	Massive Open Online Course
NARIC	National Academic Recognition Information Centre in the European Region
NCFHE	National Commission for Further and Higher Education
NFT	Non-Fungible Token
NGO	Non-Governmental Organization
OBI	Open Badges Initiative
OER	Open Educational Resources
P2P	Peer-to-Peer
PKI	Public Key Infrastructure
SIDS	Small and Island Developing States
SME	Small-to-Medium Enterprise
SSI	Self-Sovereign Identity
TVET	Technical and Vocational Education and Training
UNIC	University of Nicosia
WFP	World Food Programme
WIPO	World Intellectual Property Organization

Executive summary

Blockchain is a ground-breaking technology whose affordances and limitations are only just being understood.

Blockchain is the underlying technology powering cryptocurrencies. Beyond its financial applications, its potential has come to the fore in other sectors, including trade and supply chains, creative industries, and public and third sectors. As a tamper-resistant and time-stamped database, blockchain technology can allow individuals, companies, public organizations, and other entities to validate transactions and update records in a synchronized, transparent and decentralized way. Instead of relying on intermediaries or third parties, trust between parties is based on the rules or consensus mechanisms everyone follows to verify, validate and add transactions to a blockchain.

Blockchain is a digital verification infrastructure that solves the problem of how to verify digital identity, one of the building blocks of all digital services.

The need to verify digital identities has driven investment in increasingly large centralized databases of personal identity information. These databases are not only expensive to develop and maintain but also extremely vulnerable to security breaches, fraud and identity theft, despite the best safeguards being in place. Regulations introduced to address issues related to user privacy, such as the General Data Protection Regulation (GDPR) in Europe, still fail to provide the requisite assurances of self-sovereign identity for the end user. Social and public norms largely dictate that an individual's identity can only be validated by third parties. In a similar vein, individuals do not necessarily 'own' their own data, and ownership of such data tends to be entrusted to third parties, who in turn may transact with it on the individual's behalf. Recent history has exposed the weaknesses of the current technological infrastructure, forcing many change-resistant organizations to spring into action and enhance their own (internal and external) digitalization processes.

Shortcomings in centralized digital repositories can be mitigated when digital credentials are mapped on a blockchain.

Blockchain is arguably the most significant innovation in the digital identity space in that it allows users to easily prove their identities to third parties and protect their ownership of digital assets. These affordances are particularly important in the education context, where remote studying and working are increasingly the norm and students and employees continue to require valid digital credentials along their lifelong learning pathway.

Although there are different types of blockchains with distinct functionalities and architecture, using a blockchain to notarize digital credentials can allow for:

- Self-sovereignty: Users can identify themselves while simultaneously maintaining control over the storage, management and sharing of their personal data. Users can verify claims and transactions without having to go through multiple intermediaries.
- Trust: The technical infrastructure provides the requisite confidence to facilitate transactions such as payments or the issuing of certificates.

- Transparency and provenance: Users can conduct transactions in the knowledge that each party has the capability to enter into that transaction.
- Immutability: Records can be written and stored permanently, without the possibility of modification.
- Disintermediation: There is no need for a central controlling authority to manage transactions, retain records and verify identity and credentials. Parties may collaborate and transact directly with each other without the need for mediating third parties.
- Governance: Existing governance can be deployed over the ledger to provide and guarantee the entitlement of issuers on issuing time.

Beyond the credentialing of learning, there are other areas in the education sector where blockchain technology can be applied.

These include the notarization of intellectual property rights; educational funding; performance-based pay and microcredit; the payment of tuition fees and scholarship grants; confidential student information; the management of student identity within educational ecosystems; the creation of a decentralized educational Web; and further evolution of learning-focused decentralized apps.

Blockchain does not follow a 'one-size-fits-all' model.

The potential opportunities offered by deploying blockchain technology are strongly related to context, culture, application, sector, and policy and socio-economic issues. It is notable that most innovative blockchain applications in the education sector have occurred in small, controlled contexts, with ready access to decision-makers who were aware of existing or foreseeable problems in their operations and then considered blockchain as a possible solution. Piloting and experimentation sandboxes are needed to bring together a variety of stakeholders from universities, research centres, industry, small-to-medium enterprises (SMEs), start-ups and, in all contexts, government.

Contemporary applications of distributed ledger technologies are at an inflection point, with the momentum shifting from research and pilot projects to the building of practical applications. Enthusiasm for the potential of any evolving technology such as blockchain must be tempered with recognition of its maturity, shortcomings and risks.

The analogy that blockchain technology is a hammer looking for a nail continues to resonate, even if the education sector seems to be an obvious nail. Concerns remain about its status as a not-yet-fully-mature technology, and specifically about its performance and scalability, energy consumption, integration with legacy infrastructures and interoperability. Popular concerns about the potential for collusion between participants, the management of public/private keys and the protection of personal, sensitive or confidential data similarly need to be addressed by technology advocates to demonstrate its tangible benefits over the use of conventional, tried-and-tested and less complex technologies. This is particularly true among digital enterprise organizations, and especially in more traditional enterprises that are still working on how to incorporate digital technologies into their existing operations and protocols.

The implementation of blockchain-based solutions calls for an interdisciplinary and comprehensive approach.

Capacity-building, knowledge-sharing and small-to-medium-scale piloting projects are likely to be decisive factors in facilitating the adoption of blockchain technology. Although blockchain has long been identified as an opportunity for driving much-needed change in the core processes of the education sector, use cases to date have been limited in scope and execution, with blockchain advocates and education policy-makers seemingly at odds about fundamental issues such as governance, self-sovereignty, interoperability, choice of blockchain platforms and overall trust in standards and the integrity of the infrastructure.

Initiatives in the education sector continue to be affected by the need for consensus among stakeholders with seemingly divergent agendas and capacities.

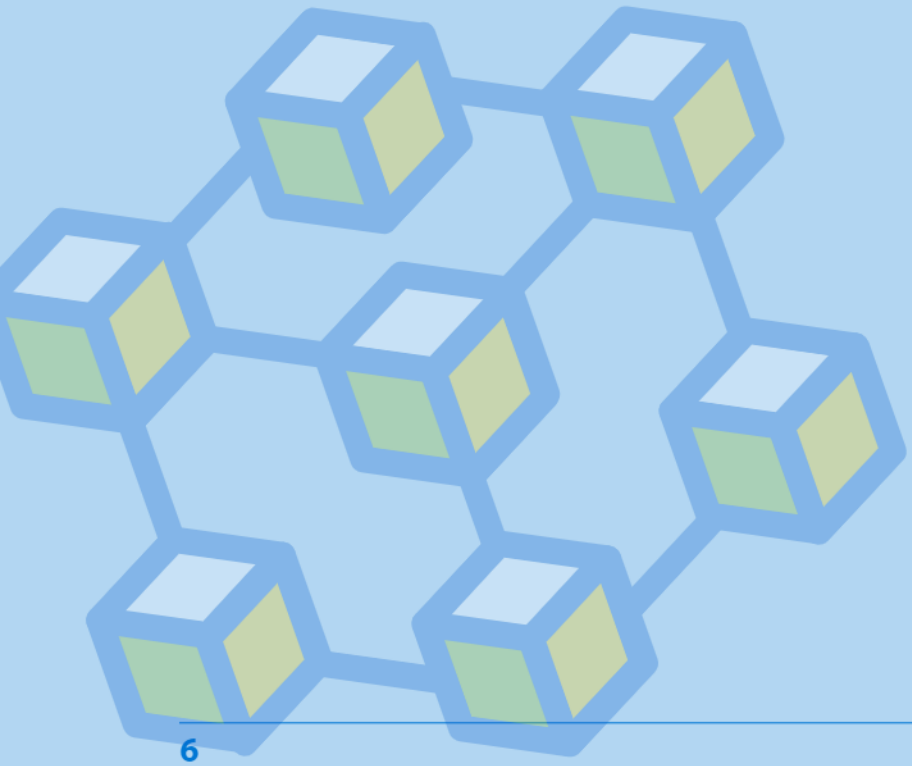
There is a need for more direct exchanges between academics, policy-makers, chief information officers (CIOs) and blockchain evangelists if the technology is to overcome resistance in the education sector, which is inherently cautious and slow to respond to seemingly disruptive technological forces. The role of education strategists and business process people in this process is critical. In the same way that the Internet reinvented communication and affected social behaviour, the hope remains that blockchain can address the current lacunae in transactions, contracts and trust – the underpinnings of business, government and society – and the education sector in particular.

Part 1

Foundation principles and concepts

Part1: Foundation principles and concepts

Since its emergence over a decade ago, blockchain has been positioned as a technology with the potential to transform society and change the way humans transact and interact (Hasselgren et al., 2020; Nascimento et al., 2019). Yet leaders across industries have often seemed unsure about what to do with it. This report starts from a shared recognition that blockchain can serve as a pragmatic solution to problems across industries and that the technology is in a state of constant evolution from a capable yet underdeveloped technology to a more refined and mature solution poised to deliver on its initial promise to disrupt (Deloitte, 2019).



An introduction to blockchain

Blockchain is most commonly identified as the underlying technology that makes cryptocurrencies possible (Wu and Tran, 2018). It is a digital, secure, public (in most cases) record book of transactions, frequently described as a distributed ledger. 'Block' describes the way this ledger organizes transactions into blocks of data, which are then arranged in a 'chain' that links to other blocks of data in the order of creation. Parties with no particular trust in each other can conduct transactions based on digital data over a peer-to-peer network with fewer, or no, third parties or intermediaries becoming involved. The transactions could correspond to almost any digital assets, from money, insurance policies, contracts, land titles, medical and educational records, birth and marriage certificates, or buying and selling goods and services to digital identities.

Blockchain proponents have claimed that it has the potential to engender wide-ranging changes in the economy, industry and society and disrupt organizations, particularly those that rely on identity and trust for their day-to-day operations. Such claims are made on the basis of the early promise of the decentralized technology to transform systems and infrastructure with increased efficiency, reduced costs and greater transparency and trust as well as the increasing number of investments (both public and private) that have been directed towards making that promise a reality. As a technology, it is arguably the most significant innovation in digital identity since the advent of Internet protocols such as DNS and HTTP. Boucher et al. (2017) believe that blockchain will eventually shift some control over daily interactions with technology away from central authorities and redistribute it among users. Systems will consequently become more transparent and, to an extent, more democratic. The implications for sectors that are dedicated to creating a social impact, such as education, are significant.

Who invented blockchain?

In 1979, Ralph Merkle (1979) introduced the concept of a Merkle tree. In 1992, it was used by Bayer et al. (1993) to propose a computational methodology to time-stamp documents cryptographically in a way that made them tamper-proof. They also introduced the concept of cryptographic hash functions and mentioned the chaining together of hash functions in a linear list. In 1997, British cryptographer Adam Back came up with Hashcash,[1] which he described as a 'mechanism to throttle systematic abuse of un-metered internet resources such as email and anonymous remailers'. Hashcash was the first attempt at utilizing a **proof of work** function. In 1998, the first ever 'cryptocurrency', called B-money,[2] was proposed. Both Hashcash and B-money employed some of the same protocols that were used in 2008 by Satoshi Nakamoto (possibly a pseudonym) when he published a paper titled 'Bitcoin: a peer-to-peer electronic cash system' that introduced the concept of Bitcoin (2008). This immensely popular paper did not mention the word 'blockchain', but it introduced the elaborate concept to explain Bitcoin, a cryptocurrency invented by Nakamoto. In his paper, Nakamoto referred to Merkle trees and cryptographic hash functions as the foundation of his invention. In 2009, Nakamoto made the Bitcoin network available as the first open-source program founded on the principles of a complete peer-to-peer electronic cash system that would eliminate the use of an intermediary and instead use cryptographic proofs to generate trust.[3]

Bitcoin alone was an innovative concept in its own right, but the underlying blockchain technology that made it function was the real breakthrough given its possible applications across multiple scenarios and domains. The inventor(s) of blockchain eventually chose to remain anonymous, collaborating only with a small group of interested parties to release the first working version of the Bitcoin network. Nakamoto last communicated with the early Bitcoin group in 2010 and has not been heard from since. While there has been much speculation about and occasional claims to Nakamoto's real identity, it has never been conclusively resolved.[4]

What is a blockchain?

A blockchain is a shared, decentralized and distributed ledger that can be used to record any kind of transaction across several computers (also called a peer-to-peer network). The information

1 See http://www.hashcash.org
2 See http://www.weidai.com/bmoney.txt
3 See *History of bitcoin 2007-2014* for key dates and milestones: https://bitcointalk.org/index.php?topic=5138618.msg50867799#msg50867799
4 See https://blockonomi.com/who-is-satoshi-nakamoto

related to transactions on a blockchain is stored in blocks in the form of a unique hash where each proceeding block contains a reference to the hash of the previous block, thus connecting them in a chain (Gupta, 2017; Iansiti and Lakhani, 2017; Kastelein, 2017). Blockchain technology uses cryptographic and algorithmic functions to record and synchronize data across a network in an immutable manner (Boucher et al., 2017).

Blockchain can be called a subset of distributed ledger technology (DLT) (Houben and Snyers, 2018). At face value, it is simply a shared database, which is why it is also known as a distributed ledger, although distributed ledgers can be built with other technologies as well. What differentiates blockchain from traditional database technology is that, instead of having a single database stored by a database owner who maintains and shares the data, in a blockchain network, all participants have their own copy of the database (Hileman and Rauchs, 2017). A blockchain network ensures that everyone on the network is in agreement when it comes to the correctness and authenticity of the data, everyone has the same copy of this agreed-upon data and no one person can alter the data once it is on the network. This makes it possible for large numbers of individuals or entities, whether collaborators or competitors, to come to a consensus on information and immutably store this agreed-upon record of 'the truth'. Blockchain has therefore been described as a 'trust machine' as well as a 'trustless technology' (Economist, 2015; Scott, 2015; Zwitter and Boisse-Despiaux, 2018).

As a technology that allows large groups of people and organizations to reach an agreement and permanently record information without a central authority being involved, blockchain has significant potential as a tool for building a fair, inclusive, secure and democratic digital economy. This has direct implications for how we perceive many of our economic, social and political institutions.

Why call it a blockchain?

In its simplest form, a blockchain is a type of distributed ledger technology (DLT) where transactions are recorded with an immutable cryptographic signature called a 'hash', and then 'grouped in blocks'. A blockchain is a secure, digital, decentralized ledger of transactions, often described as a **distributed ledger.**

'Block' describes the way this ledger organizes transactions into blocks of data, which are then organized in a 'chain' that links to other blocks of data. Every new block includes a hash of the previous one, chaining them together – hence a 'blockchain' (Grech et al., 2021). A block is made up of a header and a body, where the header contains the hash of the previous block and a time stamp, and the body contains the transaction data. In this way, each block is chained to the previous one and confirms the integrity of the previous block. The consensus protocol is an integral component of blockchain, ensuring that only valid transactions are added to the chain. Multiple sources validate an entry before it is added to the chain. Once it is added, it cannot be changed and the record is distributed. The record lives in multiple places at once, and the links make it easy to see if anyone has changed any part of the chain, which protects the system from any unauthorized changes being made (See Figure 1).

The blockchain is therefore a ledger linking sequential 'blocks' of transactions whereby:

- Every person who wishes to trade any asset across a private or public network requires access to the network and must install the blockchain software on their device. The software is used to write to the ledger, store a copy of the entire ledger and keep all the copies of the ledger perfectly synchronized. In a permissionless blockchain network, every node on the network can install the software and have access to a copy of the entire ledger. This makes it possible for anyone to transact directly on the blockchain within the network without any third-party-imposed conditions hindering that access.
- The transaction records, or blocks, in the blockchain are linked together cryptographically, rendering them tamper-proof. Unlike records in digital databases, which can be altered, once a transaction is recorded and time-stamped on the blockchain it is impossible to alter or delete it.

- The network of computers uses known algorithms to validate the transaction. Completed blocks are linked to each other in the order they are completed, forming a blockchain. When someone requests a transaction, the transaction is broadcast to a peer-to-peer network of computers. Once verified, the transaction is bundled with other transactions, creating a new block of data.
- The blockchain records the facts of the transaction – that is:

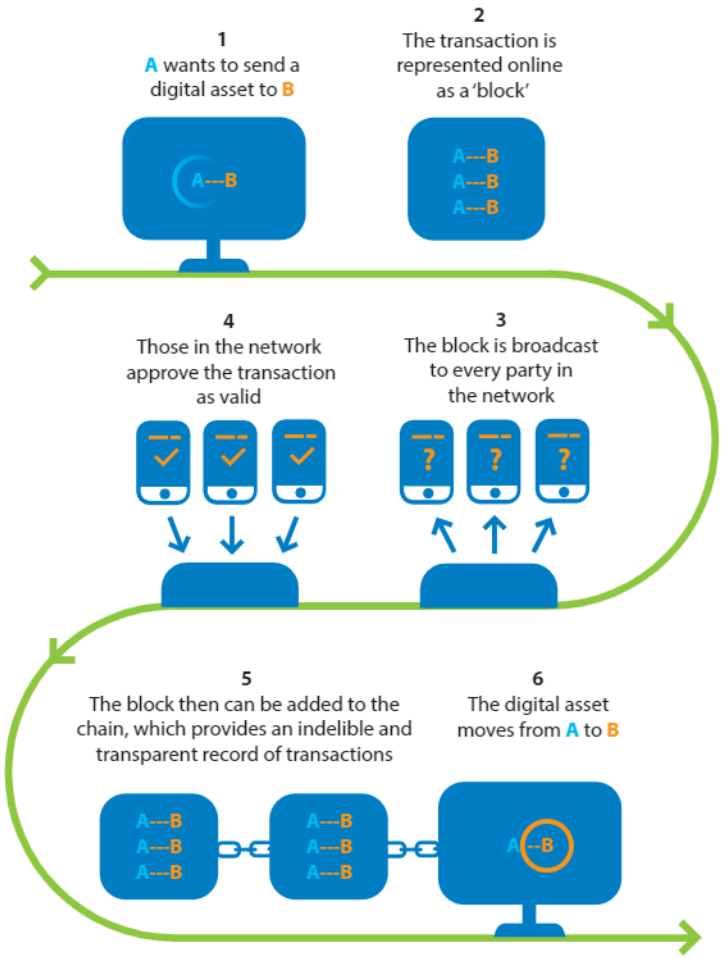
  a) what asset has been transferred,

  b) the parties involved in the transaction, and

  c) the structured information or metadata related to the transaction.

- The blockchain assigns every piece of information a unique signature: if someone alters that information, its unique code will no longer work.
- All parties involved in a transaction – and **only those parties** – must provide their consensus before a new transaction record is added to the network. All other nodes in the network will **only** verify that the two parties have the appropriate capacity to enter into the transaction. Thus, as soon as one party agrees to send the asset and the other agrees to receive it, and the nodes verify that each party has the capacity to conduct the transaction, the transaction is completed. All computers in the network continually and mathematically verify that their copy of the ledger is identical to all the other copies on the network. The version running on the majority of computers is assumed to be the 'real' version, so the only way to hack the records would be to take control of over half of the computers on the network. For a blockchain running on thousands, or even millions, of computers, this would be a near-impossible task. Destroying the ledger entirely would require deleting every copy of it in the world.

Figure 1. How a blockchain works



Source: Adapted from Grech and Camilleri (2017, p. 40)

What is a ledger?

Ledgers have been a part of civilization for about 7,000 years. They were first used to record business dealings and transactions in ancient Mesopotamia (modern-day Iraq) (Friedlob and Plewa, 1996). The ledger itself evolved from a simple recording system to double-entry bookkeeping, a system developed and pioneered by Romans and Jewish traders soon after in the Middle East.

Ledgers serve as an accounting tool to record all financial transactions, both debited and credited, and are used to determine the owner of an asset at any point in time. They perform this function by serving as a central and final authoritative list of transfers of the asset in question. Initially, ledgers were maintained manually on paper, but with the advent of computers, records were digitized to mimic the paper-based accounting system.

In a system or society that has agreed to use a ledger to determine ownership of a particular asset, all that is required to transfer ownership between two parties is an entry in the ledger indicating that this transfer has happened.

From a technical perspective, a ledger is simply a list of **sequential, time-stamped transactions.** Figure 2 shows how a typical ledger entry is structured.

Figure 2. Typical ledger entry

Transaction no.	Date & time	Sender	Asset	Receiver
#	dd-mm-yy hh:mm	Person 1	Description of asset transferred, e.g. a unit of currency, a deed to a property or a certificate	Person 2
#	dd-mm-yy hh:mm	Person 1	Description of asset transferred, e.g. a unit of currency, a deed to a property or a certificate	Person 2

Source: Adapted from Grech and Camilleri (2017, p. 17)

'This simple concept of keeping an authoritative list of transfers of an asset enables the systematic transfer and accumulation of capital, and as such the ledger has been referred to as the technology that makes capitalism possible (Winjum, 1971; Yamey, 1949)' (Grech and Camilleri, 2017, p. 17). Banks, insurers and stock exchanges offer examples of how ledgers are used by large groups of people to record, maintain and verify information about assets.

What is a distributed ledger?

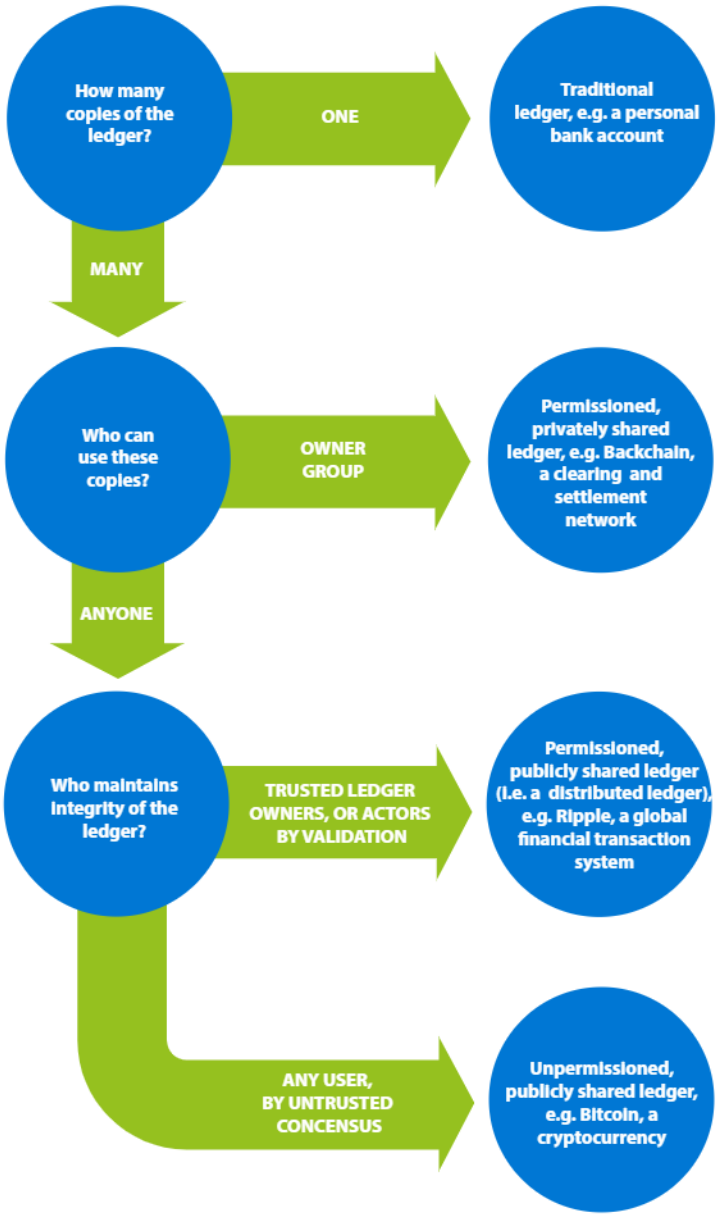
The simplest description of a distributed ledger is that it is similar to a spreadsheet but is shared across a network instead of being vested with (or belonging to) a single provider (Krause et al., 2017). Every change is replicated, recorded and agreed on by everyone. Physically, the ledger is duplicated across many computers, so it is more difficult to subvert or destroy. Distributed ledgers use cryptography to make them resilient to attack or unauthorized change. Usually the ledger's cryptography is developed over a period of time, so it becomes increasingly difficult

to break. This makes it immutable, since it is extremely improbable that anyone would go back and subvert the ledger's history. From the perspective of a database, the claim is that a distributed ledger can be a more open, transparent and verifiable shared database than a centralized database in that it is held and updated independently by each participant (or node) in a large network.

The distribution of the ledger is unique: records are not communicated to various nodes by a central authority but are instead independently constructed and held by every node. That is, every single node on the network processes every transaction, comes to its own conclusions and then votes on those conclusions to verify that the majority of nodes in the network agree with the conclusions.

Once there is consensus, the distributed ledger is updated, and all the nodes maintain their own identical copy of it. This architecture allows for a new dexterity via a system of record that goes beyond being a simple database, as it is possible to verify any given content in a distributed way in any node. Figure 3 illustrates the taxonomy of a distributed ledger.

Figure 3. Distributed ledger taxonomy



Source: Adapted from Grech and Camilleri (2017, p. 37)

What can be stored on a blockchain?

A blockchain is typically used to store three kinds of records:

1. Asset transactions
2. Smart contracts
3. Digital signatures and certificates

Asset transactions

Records of asset transactions typically take two forms:

- Money expressed in units of a currency: Each single unit of the same currency has an identical value to that of every other single unit at any one time. Currencies are also intra-convertible (with fiat currencies) at an exchange rate. The most common form of currency based on blockchain is Bitcoin.
- Documentary evidence of ownership rights, legally known as title deeds: These are commonly used to represent immovable property such as land, or intangible property such as intellectual property rights or academic records.

Smart contracts

Smart contracts are effectively small computer programs stored on a blockchain that can perform a transaction with pre-specified instructions built into it. Therefore, a smart contract is typically a declaration such as 'transfer X to Y if Z occurs'. Unlike a regular contract whereby parties must execute the contract for it to take place after they have reached an agreement, a smart contract is self-executing – that is, once the instructions are written to the blockchain, the transaction will take place automatically when the appropriate conditions are fulfilled, with no further actions required by either the primary parties or third parties. An added value is that because the code resides in the blockchain, it is immutable – so all parties can trust it – and auditable.

A decentralized autonomous organization (DAO) is one of the most composite forms of a smart contract wherein a group of people with shared interests operate together (Shermin, 2017). Ethereum is by far the most extensively used public smart contract development platform, and Hyperledger Fabric is the most used consortium infrastructure platform. The rules of governance are pre-defined in the code and executed automatically (Buterin, 2014). The promise represented by smart contracts is that after an industry's important digital records are verifiable, a whole new ecosystem of technical automation could start to evolve. This could consequently establish new social structures and norms based on increased visibility and trust across a network of participants, greatly reducing the administrative and infrastructure costs (Ojetunde et al., 2017). In short, smart contracts have the potential to enable civic efficiencies, economic alignment through shared purpose, self-sovereignty and institutional transformation (Rauchhaus, 2009; Szabo, 1996). Within this context, smart contracts represent an automated view of the future.

Certificates and digital signatures

In its most essential form, certification is the issue of a statement from one party to another that a certain set of facts are true. Signatures are proof that the statement was issued from and to those parties. A blockchain can be used to either store the certificates themselves, or to store only the proof that such certificates have been signed. It can therefore take on the function of a public certificate registry (Baldi and Chiaraluce, 2017).

What is the difference between a traditional database, distributed ledger technology and a blockchain?

A traditional database running on the World Wide Web tends to use a client-server network architecture (Raj et al., 2020). Control of the database remains with administrators, allowing for access and permissions to be maintained by a central authority. A user (client) with permissions associated with their account can change entries that are stored on a centralized server. Whenever users access a database via their computer, they will get the updated version of the database entry. The traditional database model works when the designated authority in charge of the data can be trusted to act in the public interest.

Control of the database remains with administrators, allowing for access and permissions to be maintained by a central authority.

Distributed ledger technology (DLT) can be considered as a set of protocols and supporting infrastructure that facilitate the creation and maintenance of a record of immutable transactions shared by all participants in a network. DLT shifts the responsibility of validating transactions from a central authority to the entire network of users.

Not all DLTs are a blockchain. A blockchain is a **specific type of DLT** in which transactions are stored in blocks that are linked with each other in a unique time-stamped sequence. The blocks are cryptographically linked together across a peer-to-peer network, forming a chain. Any new additions to the database can be initiated by creating a new block, information about that block is transmitted across the network and, once validated via consensus mechanisms, it is officially added to the chain.

Blockchain is associated with decentralized control as it solves two main problems associated with centralized control: the principal–agent dilemma and the high costs of coordination (Shermin, 2017).

The principal–agent dilemma is an economic theory that describes when one person or entity (**the agent**) is in a position to make decisions and take actions on behalf of another person or entity (**the principal**) (Eisenhardt, 1989). A dilemma arises when the priorities of the agent and the principal are misaligned, and the agent is motivated to act in their or its own interests and contrary to the principal's interests.

Centralized databases make users dependent on administrators: anybody with sufficient access to that type of system can destroy, corrupt or withhold access to the data stored in it. This also creates a situation whereby a single point of failure can expose the information to large-scale risks from malicious elements. Actors that have control responsibilities – such as banks, elected officials and brokers – invest significantly to keep centrally held databases from being altered by hackers or anyone else who might wish to profit from another's loss. The result is often high transaction costs, delays and overall inefficiencies in reaching or enforcing transaction agreements. If central administrators fail to ensure the secure custody of information, the impact and consequences can be very serious.

Decentralized control alters the entire governance structure, mitigating the risks associated with centralized power, removing intermediaries and enforcing security (Tapscott and Tapscott, 2016). In a blockchain network, transactions are processed by a network of users acting as a consensus mechanism so that everyone is creating the same shared system of record simultaneously. Blockchains allow parties that do not trust each other to share information without involving a central administrator.

Why use a blockchain?

Blockchains allow users to prove their identities, protect ownership of digital assets and verify transactions without an intermediary.

Box1. Five reasons to use a blockchain

1 Transparency: Anyone with access to the network can view a history of transactions in real time.

Potential impact: A money trail can be tracked and monitored more accurately in areas like aid distribution.

2 Immutability: Blockchains protect data from being tampered with; no single entity is able to change past data without alerting the network.

Potential impact: Immutability protects areas like voter authentication and land title registrations.

3 Reduced counterparty risk (and subsequently lower-cost payments): Blockchains allow anyone to send money to anyone without an expensive or corrupt intermediary being involved.

Potential impact: Money sent across borders or into natural disaster zones will move quickly. In addition, many critical elements of our economy allow people to trade with each other without fear that the other party will back out. Banks perform this function, but they often add high administration costs and slow processing times to the system. Blockchain's smart contracts guarantee that a contract will be fulfilled when a specific action is completed.

4 Efficient provisioning of identities: Blockchains can create and manage identities for people at a lower cost and in a more secure manner through digital signature technology, which gives people a public key (similar to an account number) and a private key (similar to a password).

Potential impact: Marginalized and underserved populations, like the underbanked and unbanked, may secure unprecedented access to services.

5 History of itself: Most centralized databases keep information that is up to date at a particular moment. They are effectively a snapshot of a moment in time. Blockchain databases can keep not only information that is relevant now, but also all the information that came before.

Potential impact: Blockchain technology can create databases that have histories of themselves. They grow like ever-expanding archives of their own history while also providing a real-time self-portrait. The expense required to compromise or change these databases has led people to call a blockchain database immutable.

Sources: Allessie et al., 2019; Atzori, 2017; Back et al., 2014; Galen et al., 2018; Warburg, 2016

What is the relationship between self-sovereignty, identity and blockchain?

The early literature on blockchain makes frequent references to 'self-sovereignty' and individuals' ability to own and control their own identity online (Ferdous et al., 2019; Lemoie and Soares,

Photo: Unsplash

2020; Lilic, 2015; Seifert, 2020; Smolenski, 2020). According to Lewis (2017), public blockchains facilitate self-sovereignty in the sense that individuals become the final arbiters of who can access and use their data and personal information. Within an education context, the term is becoming synonymous with the empowerment of individual learners to own, manage and share details about their credentials without needing to call upon the education institution as a trusted intermediary.

Self-sovereign identity can also be understood as citizens acquiring significant self-authority over the way their personal data and identity are shared online, and being able to control how and to whom this information is released or shared with in return for access to services they may require – again, without the need of constant recourse to a third-party intermediary to validate such data or identity.

> Identity is … the starting point of trust and confidence in interactions between the public and government; it is a critical enabler of service delivery, security, privacy, and public safety activities; and it is at the heart of the public administration and most government business processes. How identity information is collected, used, managed, and secured is of critical interest to leaders in the public sector. (Government of Canada, 2011)

Identity is complicated territory for citizens, particularly those who need to verify it, since the process requires the assessment of personal attributes, personal history, relationships or transactional histories, or a combination thereof. Digital identity is tantamount to a human right, yet there is still no fail-safe method to deal with one of the major flaws of the Internet: identifying people or machines online. Whenever citizens have been obliged to, or have willingly/unwillingly agreed to, divulge their online identity, more complex issues have emerged, such as the use of private algorithms by Silicon Valley giants to maximize the commercial use of users' personal data harnessed from social media websites.

Technology is fundamentally changing our ability to represent ourselves.

Technology is fundamentally changing our ability to represent ourselves. At the same time, the nature of our connected world is changing our perception of identity and trust. The cryptography at the core of blockchain technology promises to address identity lacunae and wrestle ownership and control of personal data back to the individual user. People, businesses and institutions should be able to store their own identity data on their own devices and provide it efficiently to those who need to validate it without relying on a central repository of identity data.

Blockchain does not just provide a new way of digitizing pieces of paper that have an intrinsic value, such as our credentials; it also provides us with the means to take control of our identity online and manage it appropriately. According to Hanson and Staples,

> the assessment of identity is used to minimise any perceived gap in trust. This gap is proportional to the measure of risk, which reflects the perception of the identity and any potential losses. The trade-off is often a loss of privacy in exchange for access to high value transactions. The downside has historically been the loss of privacy where the transaction is asymmetrically of moderate to minimal value to the individual being vetted compared to the risk presented to the other party. [...] In order to verify certain attributes of their identity to complete the transaction they also expose other attributes of their identity they may not wish to disclose. This disclosure places all of their attributes, on that document, at risk of further unwanted disclosure or illegal use. (Hanson et al., 2017, p. 13)

Different blockchain implementations address these principles in different ways and to different degrees, but in principle, blockchain applications will enable digital claims to be verified instantly and for free, dramatically cutting the time for anti-money laundering (AML) measures and know your customer (KYC) credential verification. Although issues remain in terms of the technology's speed, blockchain remains significantly faster and cheaper than current document verification processes and systems. Companies and governments, for example, can de-risk both their staff hiring and data management practices by deploying blockchain solutions to seamlessly verify that applicants for jobs actually have the qualifications they claim, while storing less data and only the most relevant data for their services. From a business process perspective, end users secure direct control of their own data without the need to involve intermediaries and the risk of identity fraud is reduced significantly in the process.

Not all blockchains or applications of different types of blockchains will embrace the principles underpinning the social value proposition of blockchain technology in their entirety. Of all the blockchain networks currently in use, Bitcoin, a public blockchain, is a good example of an application of the technology that embodies the entire set of social value principles.

How does blockchain increase trust?

A United Kingdom Government study (UK Government Chief Scientific Adviser, 2016) suggests that trust is a calculated risk between two or more people, organizations or nations. In an online environment, the way to establish trust can essentially be distilled down to on two fundamental points:

1. Authentication: Prove that you are who you say you are.
2. Authorization: Prove that you are allowed to do what you say you will do.

If the authenticating or authorizing party is not satisfied with the response, they can still choose to allow the requestor to proceed, but they would be incurring risk. However, there is no viable relationship unless the parties trust one another. In this sense, being trustworthy in a society is analogous to being creditworthy.

Galen et al. (2018) note that "that "there are three key elements needed to establish trust: 1) identity, or who's who; 2) ownership, or who owns what; and 3) verification, or what's true" (p. 7).

Who is who: Blockchains solve the identity problem through the use of digital signatures. Each user is issued with a set of two digital codes (a public key, similar to an account number, and a private key, similar to a password, both of which are autogenerated) that allows them to easily prove an identity and issue authorized transactions.

Who owns what: Blockchains solve the ownership problem through a technology called cryptographic hashing. A cryptographic hash is simply a piece of data that has been run through a maths function and transformed into a shorter piece of data. Putting the hash of the signature of a file's hash in a blockchain makes the owner of the private key associated with the signature the owner of the file in that blockchain.[5] In a blockchain, each block contains a hashed representation of the data in the previous block. If you change any previous pieces of data, that change will be reflected throughout the chain, making it easy for the system to see and reject fraudulent attempts to manipulate the data. This allows blockchains to create immutable data, otherwise known as tamper-proof records.

What is true: Blockchains solve the verification problem by making it feasible for a group of people to publicly verify that a transaction is true, without the need for a trusted intermediary to become involved. In blockchain terminology, this is called distributed consensus. Blockchains' ability to verify transactions with fewer intermediaries becoming involved is a key benefit that can lead to lower costs for many applications in this report.

This basic concept of trust remains unchanged in the digitized world where we have to rely upon many actors, most of whom we will never meet, to act in good faith and on our behalf: trust is often granted only for a very specific application, within a specific context and for a specific period. In a global, digital economy, the challenges of maintaining trust – with the resultant checks and balances – are becoming increasingly expensive, time-consuming and inefficient.

Blockchain might provide a viable alternative to the current procedural, organizational and technological infrastructure required to create institutionalized trust.

Blockchain might provide a viable alternative to the current procedural, organizational and technological infrastructure required to create institutionalized trust. The improved trust between stakeholders is associated with the use of decentralized public ledgers as well as cryptographic algorithms that can guarantee that approved transactions cannot be altered after being validated. The distributed ledgers contribute to trust by establishing a fact at a given point in time, which can then be trusted. They achieve this by automating the three roles of the trusted third party: validating transactions, safeguarding transactions and preserving transactions.

The hope is that just as the Internet reinvented communication and impacted social behaviour, blockchain may help address the current lacunae in transactions, contracts and trust – the underpinnings of business, government and society.

What is immutable about a blockchain?

An immutable record is an unchangeable record whose state cannot be modified after it has been created. Immutability is associated with security and its core properties of confidentiality, integrity, availability, resilience and irreversibility. Blockchain data cannot be easily changed for two reasons: First, they are stored in a chain of blocks where each block is identified by a unique and time-stamped hash function that also contains a reference to the hash of the previous block, thus linking the blocks together in a perfect sequence, preventing any insertion of a new block between them. Second, they are continually replicated across many different locations, and to tamper with the data, at least 51 per cent of the nodes on the network need to be changed.

5 See https://en.bitcoin.it/wiki/Proof_of_Ownership

With private and public key cryptography part of blockchain's underlying protocol, transactional security and confidentiality become virtually unassailable. Trust zones – including open public ledgers and permission-based shared or private blockchains in which participation is limited to select entities – can also be established.

Blockchain's resilience therefore stems from its very structure: it is designed as a distributed network of nodes in which each one of these nodes stores a copy of the entire chain (Chopra et al., 2020). Once a transaction is verified and approved by the participating nodes, it is virtually impossible for someone to alter the transactional data. Attempts to change data in one location will be interpreted as fraudulent and an attack on the overall integrity of the chain by other participants, and the attempt will therefore be rejected. If a transaction is made in error, a new transaction must be used to rectify the error, and both transactions are then visible in the ledger.

What does blockchain technology have to do with disintermediation?

By replacing intermediaries with mathematics, blockchain offers a unique way of establishing and maintaining trust. Participants on a blockchain are linked together in a marketplace where they can conduct transactions and transfer ownership of valued assets to each other in a transparent manner and without the assistance or intervention of third-party mediators or intermediaries. It acts as a value network operates – that is, without a defined central authority.

By replacing intermediaries with mathematics, blockchain offers a unique way of establishing and maintaining trust.

With blockchain, peer-to-peer consensus algorithms transparently record and verify transactions without the oversight or intervention of a third party – potentially reducing or even eliminating costs, delays and general complexity. For instance, blockchain can reduce overhead costs when parties trade assets directly with each other, or quickly prove ownership or authorship of information. Outside the blockchain world, the latter task is currently next to impossible without involving either a central authority or an impartial mediator. Moreover, blockchain's ability to guarantee authenticity across institutional boundaries is likely to help parties focus on new ways of authenticating records, content and transactions. Greater decentralization of the Internet would place more control in the hands of the user – or more specifically, the user's devices – instead of relying on clouds operated by tech giants such as Google or Amazon. Tim Berners-Lee's latest Web decentralization initiative Solid, being developed by Massachusetts Institute of Technology (MIT) in conjunction with Mastercard, Qatar Computing Research Institute and Oxford University, signals a move towards the decentralized approach in practice. With Solid and Inrupt, a commercial venture that has developed from Solid, the aim is to give users control of their data through 'personal online data stores' (PODs).[6]

What is the difference between public and permissioned (or private) blockchains?

Generally speaking, the various methods of classifying blockchains are often differentiated based on how users are granted access to view, read and write data to the chain. At time of writing, a blockchain can be classified on the basis of:

- the nature of the data accessibility (Lin and Liao, 2017), and
- the need for authorization to participate (Rennock et al., 2018).

6 See https://solid.mit.edu

Tables 1–3 show the discrete features of different types of blockchain.

Based on the nature of the data accessibility

Table 1. Types of blockchain based on the nature of data accessibility

Public	**Anyone can read and create transactions.**
Private	Only one organization, or all subsidiary organizations within the same group, is allowed to read and submit transactions.
Consortium	Multiple organizations form a consortium and are allowed to submit transactions and read transactional data.
Hybrid	Any of the three blockchains – public, private or consortium – can be combined to facilitate transactions.

Source: Adapted from Lin and Liao (2017)

Based on the need for authorization to participate

Table 2. Types of blockchain based on the need for authorization to participate

Permissioned	Permission is required to join this type of blockchain. Only authorized parties are allowed to run nodes to verify transactions in the blockchain network.
Permissionless	No permission is needed to participate in this type of blockchain. Everyone is allowed to participate in the verification process and can join the blockchain network with their own computational power.

Source: Adapted from Rennock et al. (2018)

Apart from the very distinct classifications, features from each can be combined to create new permutations as shown in **Table 3** (below).

Table 3. Types of blockchains and their features

Type of Blockchain		Characteristics	Security/Anonymity	Scalability
Closed	Private Permissioned	Only authorized nodes can join and read	High level of security and low level of anonymity	Very high
Closed	Private Permissionless	Only authorized nodes can join, read and write	High level of security and low level of anonymity	High
Open	Public Permissioned	Anyone can join and read	Moderate level of security and high level of anonymity	Medium
Open	Public Permissionless	Anyone can join, read, write and commit	Low level of security and high level of anonymity	Low

Source: Alex Grech, 2021 [created for the purposes of the current publication]

Bitcoin is the most extensively documented use case available when it comes to public permissionless blockchains. Bitcoin is a write-uncontrolled, read-uncontrolled database. That means anyone can write a new block into the chain, and anyone can read a block in the chain. Anyone can use its cryptographic keys, anyone can be a node and join the network, and anyone can become a miner to service the network and seek a reward. Miners can abandon a node, return if and when they feel like it, and get a full account of all network activity since they left. Basically, anyone can read the chain, anyone can make legitimate changes and anyone

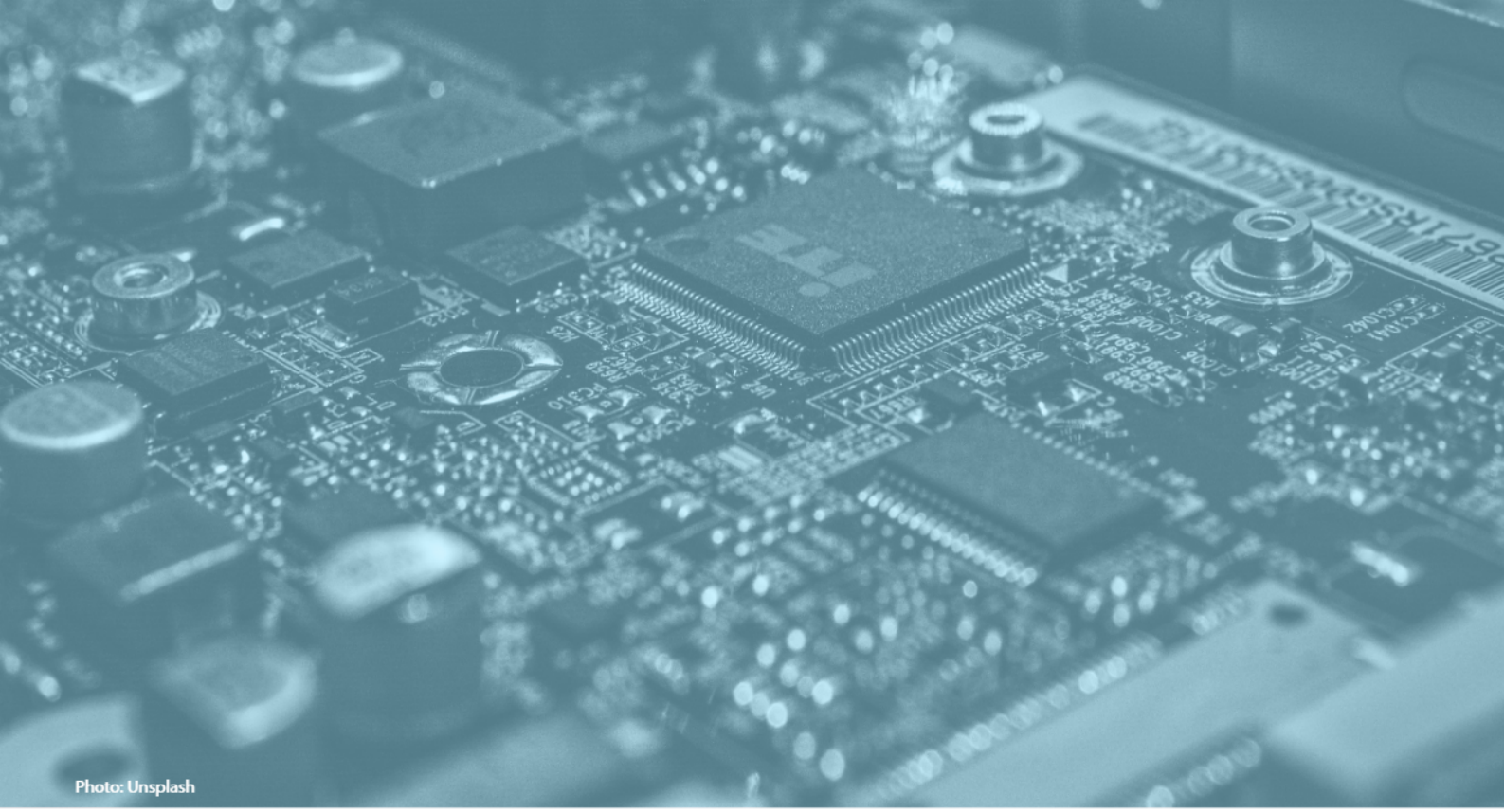


Photo: Unsplash

can write a new block into the chain (as long as they follow the rules). Bitcoin allows for total decentralization and is therefore also described as a censor-proof blockchain (GIZ, 2019).

Blockchain networks can also be built so that participants require permission to read or edit the information on the blockchain. This limits the parties that can transact on the blockchain and establishes who can serve the network by writing new blocks into the chain.

Blockchain networks can also be built so that participants require permission to read or edit the information on the blockchain.

For example, Ripple[7] runs a permissioned blockchain. The start-up determines who may act as a transaction validator on its network – it has included Consultants to Government & Industries (CGI), MIT and Microsoft as transaction validators – while also building its own nodes in different locations around the world.

A blockchain developer may choose to make the system of record available for everyone to read but may not wish to allow just anyone to be a node, thus ensuring the network's security along with a certain control over transaction verification or mining. This mix-and-match situation is reflected in the various ways entrepreneurs are experimenting with the technology. Such blockchains have commonly been referred to as hybrid blockchains.[8]

Permissioned blockchains may or may not involve proof of work (Porat et al., 2017) or some other system requirement from the nodes. This feature leads to a politically complex situation, as there are experts who consider private blockchains that use no proof of work (i.e. blockchains with no mining) to not be blockchains at all but simply shared ledgers.

Blockchain performance has much to do with decisions about whether to deploy a solution that uses a public blockchain or a permissioned one.

While blockchains can be used as systems of record and are therefore ideal as transaction platforms, their performance is considered slow in comparison to current digital transaction technology such as Visa and PayPal. While this aspect of its performance will certainly improve,

7 See https://ripple.com
8 See https://101blockchains.com/hybrid-blockchain

the nature of blockchain technology requires that some speed be sacrificed. The way distributed networks are employed in blockchain technology means they do not share and compound processing power: they each independently service the network, then compare the results of their work with the rest of the network until there is consensus that something happened.

A permissioned blockchain, like a centralized database, can be write-controlled and read-controlled. That means the network, or the protocol, can be set up so only permissioned participants can write in or read the database. But if confidentiality is the only goal and trust is not an issue, blockchain databases offer no advantage over a centralized database.

Hiding information on a blockchain requires lots of cryptography and a related computational burden for the nodes in the network.

Hiding information on a blockchain requires lots of cryptography and a related computational burden for the nodes in the network. There is no more effective way to do this than simply hiding the data completely in a private database that does not require network connectivity.

When is the use of a blockchain appropriate?

The United States Department of Homeland Security (DHS) Science and Technology Directorate is among many organizations that have developed a decision flow chart to rationalize the use of blockchain technology for an organization use case (Yaga et al., 2018). It hypothesized that the use of blockchain is suitable in circumstances where certain features apply.

Box 2. Circumstances where the use of blockchain is suitable:

- → Distributed participants
- → Want or need for lack of trusted third party
- → Workflow is transactional in nature (e.g., transfer of digital assets/information between parties)
- → A need for a globally scarce digital identifier (i.e., digital art, digital land, digital property)
- → A need for a decentralized naming service or ordered registry
- → A need for a cryptographically secure system of ownership
- → A need to reduce or eliminate manual reconciliation and dispute resolutions
- → A need to enable real time monitoring of activity between regulators and regulated entities
- → A need for full provenance of digital assets and a full transactional history to be shared among participants

Source: Yaga et al., 2018, p. 41

Wüst and Gervais (2018), IBM[9] and CoinDesk (Hochstein, 2018) have all attempted to answer this question as well. The Institute of Electrical and Electronics Engineers (IEEE) has also come up with its version of a decision tree to decide if a blockchain solution is indeed what an organization needs.[10]

9 See https://www.ibm.com/topics/benefits-of-blockchain
10 See https://spectrum.ieee.org/computing/networks/do-you-need-a-blockchain

What is a decentralized app?

A decentralized application (dApp) is a Web application with a set of key components distributed to a decentralized network (such as a blockchain). It supports services similar to those offered by typical consumer applications but grants users greater control over their data, which eliminates the need for centralized intermediaries to manage the data and so makes the service 'decentralized' (Cai et al., 2018). In practice, this means there is a significant reduction in the risk of a single point of failure, since dApps run on a decentralized network such as Ethereum (as opposed to a backend application code executed on centralized servers). Standard blockchain advantages, such as transparency, immutability and high security, are also evident. Smart contracts can be considered as dApp backends that are executed in an Ethereum Virtual Machine environment. No central point of control exists, so no single entity is in a position to control and manipulate data. A dApp will perform the same function irrespective of the execution environment in which it is being run.

Box 3. Standard features of a dApp

1. The application's source code must be open and accessible to all network members.
2. It must be capable of operating autonomously through a decentralized consensus mechanism, without any one entity being in control of the majority of its tokens. It may be possible to adapt its protocol in response to proposed improvements and market feedback, but all changes must be decided through user consensus.
3. The application's data and records of operation must be cryptographically stored in a public, decentralized blockchain.
4. The application must use a cryptographic token (Bitcoin or a token native to its system) to enable access. Any contribution of value from miners or farmers should be rewarded in the application's tokens.
5. The application must generate tokens according to a standard cryptographic algorithm acting as a proof of the value that nodes contribute to the application (proof of work or proof of stake). Bitcoin, for example, uses the proof of work algorithm.
6. The application must use some form of internal currency to support the development process, motivate the underlying network and its consensus mechanism and provide users with the means to exchange value. It creates a healthy economic system around the app and sustains its development.

Source: Adapted from Johnstone et al. (2014) and Chrono.tech (2019).

Peer-to-peer (P2P) networks

In its simplest iteration, a P2P network is a network that is established when two or more devices are connected with the objective of sharing resources. What differentiates a P2P network from conventional network systems is that it forms an ecosystem where the computers are connected through a single server computer. It can also be seen as a network where multiple computer systems are connected through a single server that enables the transfer of files from one end to the other. Moreover, a peer-to-peer network also serves the role of a permanent infrastructure that can connect more than a dozen computers in a small region amidst the conventional offline environment.

Photo: Unsplash

Decentralized networks started with P2P content delivery and media-sharing protocols such as Gnutella, eDonkey and BitTorrent. These protocols enabled users to share files and download content faster because they could connect to multiple peers and through many channels instead of one centralized storage server. Media-sharing networks also allowed users to gain access to free licensed media content; this may well have contributed to the successful adoption and popularity of the technology.

P2P networks are highly scalable because of the ease and speed with which new peers can be added without the need to perform any central configuration on the server. They are also extremely difficult to bring down. Even if one of the sections is about to shut down, other peers continue to operate and communicate, even if a single unit is not able to perform its functions. File processing speed is quick, ensuring it is extremely easy to have the same file stored on multiple peers, and downloadable simultaneously, from multiple locations.

Blockchain for decentralized applications

Decentralized apps are a new type of software program designed to exist on the Internet in a way that is not controlled by any single entity. Where Bitcoin is a decentralized value exchange, a decentralized application aims to achieve functionality beyond transactions that exchange value. Many types of decentralized apps are starting to emerge as blockchain technology continues to progress. In a completely decentralized world, most operations are facilitated by peer-to-peer networks and the idea of centralized entities ceases to exist.

Decentralized apps are a new type of software program designed to exist on the Internet in a way that is not controlled by any single entity.

Decentralized apps can use blockchain for addressing various purposes or even operate as blockchains in their own right. The application itself does not run application-specific functionality on a server: its functionality runs on end-points. However, the application may use non-app-specific servers with the caveat that they must not be part of the trusted computing base. This is the case with storage systems such as Amazon S3 and Dropbox where data are signed and verified end-to-end, meaning that the storage systems do not need to be trusted in order to offer data.

What is an ICO?

ICO stands for initial coin offering. It refers to the creation and sale of digital tokens. In an ICO, a project creates a certain amount of a digital token and sells it to the public, usually in exchange for other cryptocurrencies such as Bitcoin or Ether (Adhami et al., 2018). The public could be interested in the tokens on offer for either or both of the following reasons:

1. The token has an inherent benefit: It grants the holder access to a service, a say in an outcome or a share in the project's earnings.
2. The benefit will be in increasing demand: This will push up the token's market price.

Tokens, especially those from successful sales, are usually listed on exchanges, where initial buyers can sell their holdings and new buyers can come in at any time. As a type of digital crowdfunding, token sales enable start-ups not only to raise funds without giving up equity, but also to bootstrap their project's adoption by encouraging its use by token holders.

Buyers can benefit from both the access to the service that the token confers and its success through appreciation of the token's price. These gains can be realized at any time, usually by selling the tokens on an exchange. Buyers can also demonstrate their increasing enthusiasm for the idea by purchasing more tokens in the market.

What is a DAO?

A decentralized autonomous organization (DAO) is an organization that can fully function without a people-based management structure (Hassan and De Filippi, 2020). A DAO can also be defined as an organizational system that maintains and sustains itself based on smart contracts in which users determine its future direction by voting.

A decentralized autonomous organization (DAO) is an organization that can fully function without a people-based management structure.

Imagine a washing machine that operates and maintains itself. All anybody has to do is put in the dirty clothes and take out the clean clothes. The system operates, gets the water and detergent, etc., and carries out routine maintenance itself. Every activity in its working cycle is already programmed. Users can then determine how they want the washing machine to improve with time by voting on proposals by other users on how to improve the washing machine's code. This hypothetical washing machine is an illustration of how a DAO works.

A DAO has three core characteristics. First, it is a programmed set of rules. This set of rules is programmed onto a smart contract platform that exists on the Internet as an open source code. Second, it functions autonomously. This means that its day-to-day activities are based purely on the written code. Third, it is coordinated through a distributed consensus protocol. This means that decisions regarding the future of the platform are taken by the community of users according to the agreed initial plan.

An important part of a DAO is its funding. DAOs are often funded by a crowd sale or (more popularly) an ICO. The tokens issued by a DAO should have a use of some sort in order to make

them worthy of constant transactions. Beyond this, the ability to influence the future of a DAO through voting is often determined through token ownership. Token ownership of a DAO is tantamount to shareholder status. In many cases, the number of tokens owned by individuals determines their voting power.

Once a DAO is deployed, it becomes completely independent.

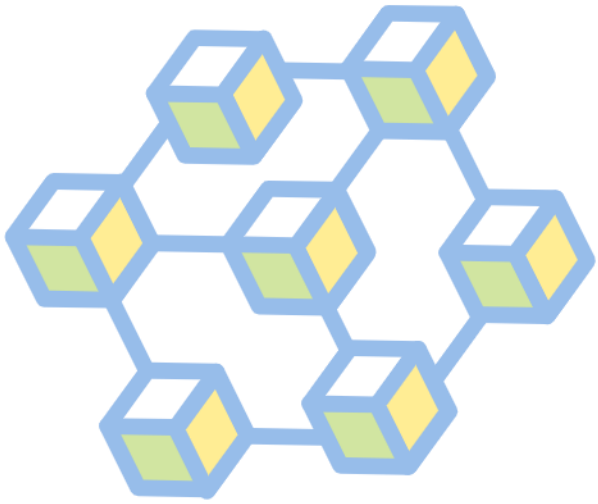
Once a DAO is deployed, it becomes completely independent. Even the founders and developers can no longer claim ownership of it. Furthermore, the system becomes fully autonomous and open source, with all financial transactions and program rules recorded on the blockchain. Decisions about how a DAO spends its money are reached via consensus. Anyone with the required stake can make proposals regarding the future of a DAO. However, to avoid spam, a monetary deposit may be required to make a proposal. It is important to note that a DAO cannot build products, write code or develop hardware. Contractors are appointed through a consensus mechanism to undertake these functions.

What is an NFT?

A non-fungible token (NFT) is a special type of digital asset or token that often represents a real-world object. Every NFT has a unique digital signature, so they can prove their uniqueness and cannot be exchanged with another digital asset token. This characteristic is the reason they are called non-fungible tokens, or NFTs.

NFTs are based on blockchain technology, usually, but not always, the Ethereum ERC-721 blockchain. NFTs share some fundamental characteristics in addition to their discrete variations: immutability (inherited directly from the ledger), transparency, the ability to demonstrate property (ownership), uniqueness (singularity) and programmability. It is important to note that NFTs are themselves digital assets and not simply representations of digital assets.

NFTs can be applied in several asset domains – for example, tickets (e.g. as souvenirs of an event), digital art (e.g. allowing artists to show their work directly to the public without intermediaries and with lower associated costs) or 'content' sales (raising funds by selling audio or video content, usually related to art or music).



Part 2

Blockchain and its application in education

Part 2: Blockchain and its application in education

The majority of blockchain initiatives in the education sector are either in development or in the piloting phase. The fundamental processes, inputs and outputs within the education system represent opportunities to put the technology to meaningful use – for example, digital credentials and transcripts, student identity and record management, blockchain-based payments, intellectual data management and smart contracts.[11] It is worth mentioning that there are several successful nation state initiatives (e.g. DigiLocker[12] in India) underway that are also legitimate pathways to issuing, storing and verifying digital certificates without intermediaries that do not use blockchain technology. The focus of the text that follows is, however, exclusively on the affordances provided by the use of blockchain technology.

11 See Grech and Camilleri (2017) for an extensive review of these areas.

12 DigiLocker is an online digitization service provided by the Government of India to its Aadhar-card-holding citizens since 2015 to promote paperless governance. Read more at: https://negd.gov.in/digilocker#:~:text=DigiLocker%20is%20a%20flagship%20initiative,through%20a%20Digital%20Document%20Wallet

Uses of certificates issued to learners

Certification describes any process by which a certificate is issued as verification of a claim. Certificates are used widely throughout the lifelong learning journey of learners. They are typically issued to recognize:

- the completion of a specific learning experience, such as a school-leaving certificate in formal education, or a certificate attesting a mobility experience (Erasmus exchange, international exchange programmes, etc.);
- the totality of learning achieved in a specific area, such as a certificate attesting the award of a degree;
- discrete units of learning through the achievement of specific learning objectives, such as an award certificate for microlearning, the completion of modules or the achievement of credits;
- specific experiences that contribute to learning, such as certificates attesting the completion of an apprenticeship or other kind of work experience;
- the acquisition of specific skills, such as through certificates awarded in procedures;
- the recognition of prior learning;
- the achievement of certain excellence criteria, such as winning certain prizes for achievement, or graduating with honours; or
- the specific level of competence achieved in specific areas, through the issue of examination certificates or grade cards.

While most educational certificates in higher education are issued on paper, some institutions are now issuing digital credentials based on public key infrastructures (PKIs). For example, the University of Gottingen digitally signs its bachelor's and master's qualifications.

Uses of certificates for accreditation

Accreditation is a procedure by which an authoritative body formally recognizes that a body or person is competent to carry out specific tasks (ISO, 2017). It is usually attested by means of a certificate. Multiple forms of accreditation are used in education:

- Educational organizations are accredited to be licensed to operate. For example, accreditations issued by governments to universities or schools, and accreditations issued by software companies to training centres to teach specific software packages.
- Specific educational programmes are accredited to be taught by accredited educational organizations.
- Teachers are often accredited for a specific skill set to be allowed to claim that they are teachers and teach in specific schools.
- Agencies that accredit schools and teachers are themselves accredited by high-level supervisory agencies that ensure they issue their accreditation according to set rules. An example of such an accreditation is that awarded by the European Quality Assurance Register (EQAR)(For more information on EQAR, see its website at https://www.eqar.eu.)

Many of these certificates and accreditations are typically linked into accreditation chains. For example, a student may be awarded a certificate attesting a degree only if it has been issued for an accredited programme, which was issued by an accredited university, which in turn was accredited by an accredited quality assurance agency.

Uses of certificates for tracking intellectual property

Registering and tracking intellectual property (IP) is a key part of all academic systems. Intellectual property creates value, and its use may result in costs being incurred. To this end, a host of central authorities are used to manage intellectual property of various kinds. In particular:

- Research journals certify that a piece of research is new and has been conducted in line with rigorous scientific standards. This information is used to determine **scientific truth**.
- Data companies certify the number of times a piece of research or an open educational resource (OER) has been used. This information is used to determine the **significance of the research or the OER** and often to compensate the author accordingly.
- Patent offices certify the first inventor of an invention and award them a monopoly to market and profit from that invention for a number of years.

Uses of certificates for financial matters

Certificates are also used extensively for financial reasons, including to track:

- payment receipts,
- student grant awards,
- student loan awards, and
- waivers of and modifications to student loans.

Limitations of certification

The digitization of educational certificates is still far from being mainstreamed. This is because of a number of limitations that can be broadly grouped as technical, organizational and arising from lack of trust.

Technical limitations

All certificates in education are subject to a similar set of problems:

1. Certificates are time-intensive and expensive to issue, maintain and verify.
2. Public key infrastructures require using a certification authority as an intermediary to issue and verify the certificates, creating a dependency that is open to abuse. In particular, certification authorities have traditionally leveraged their position to charge extremely high fees for access to their services.
3. Both original and verification records face a risk of being destroyed in the event of mismanagement, natural or human-triggered disasters or wars.
4. There is a lack of interoperability between systems issuing different types of certificates.
5. From a data protection perspective, verification of the records requires:

→ the issuing organization to retain copies of the certificates, to be able to verify the authenticity of certificates issued by it,

→ reliance on a central party for the root certificates, or

→ paper certificates with sufficiently sophisticated in-built security and anti-tampering features to be able to be assessed as authentic without reference to an external database.

Organizational limitations

There are a number of organizational limitations to the digitalization of certificates. For example:

- a lack of agreement on technical standards for the issuing of certificates,
- inconsistent implementation of rules – for example, for recognition of mobility experiences,
- lack of trust in any one organization to act as the key arbiter of the rules, and
- the use of manual procedures for their recognition and verification.

Open Badges is the world's leading format for digital badges. Rather than representing a specific product or platform, Open Badges are a type of digital badge that is verifiable, portable, packed with information about skills and achievements, and issued, earned and managed by using a certified Open Badges Platform. The Open Badges Initiative (OBI) promulgated by Mozilla has attempted with some success to provide a standard for certifying non-formal learning (Clements et al., 2020). In early 2016, IMS Global announced its commitment to Open Badges as an interoperable standard for digital credentials, and later that year, Mozilla announced that stewardship of the Open Badges standard would transition officially to IMS Global. In late 2018, Mozilla announced that it would retire the Mozilla Backpack and migrate all users to Badgr.

Rather than representing a specific product or platform, open badges are a type of digital badge that is verifiable, portable, packed with information about skills and achievements, and issued, earned and managed by using a certified Open Badges Platform.

The Groningen Declaration Network is also trying to address these limitations by applying a stakeholder network approach to discussing issues relating to Digital Student Data Portability (DSDP) (Giralt and Leeuw, 2013). The Common Microcredential Framework launched by the European MOOC Consortium in 2019 – consisting of FutureLearn, France Université Numérique (FUN), OpenupED, Miríadax and EduOpen – is another attempt to create standardization for formal or non-formal microcredentials (Resei et al., 2019).

Limitations of trust

In most countries, the educational sector is regulated to ensure that only quality providers offer educational services, and thus safeguard the quality of educational credentials. Diploma mills are organizations that operate outside this regulatory system and offer lower-quality educational credentials. Currently, no system of certificates allows for automatically checking whether the certificate issuer is also an accredited provider.

Blockchain methods for credentialing

There are three distinct methods through which blockchain might be used for credentialing – that is, for the issue and recognition of certificates. They are presented in Table 4.

Table 4. Comparison of different data storage models for blockchain-based credentials

Method	What is stored on a blockchain	Implications
Method 1: Blockchain-based PKI infrastructure	PKI certificates used by institutions to sign digital documents are stored on the chain. The actual certificate is held entirely off-chain.	It is only possible to automatically verify the identity of the issuer. A separate (but possibly integrated) system would be required to verify the identity of the receiver.
Method 2: Blockchain-secured digital credentials	A hash of the digital certificate together with the public key of the institution issuing and the individual receiving the certificate is stored on the blockchain. The actual certificate is stored off-chain.	Records are immutable. It is possible to automatically verify the identity of the receiver.
Method 3: Credentials issued on a blockchain	The actual content of the credential is stored on-chain, together with the public key of the institution issuing and the individual receiving the certificate.	Records are immutable. It is possible to automatically verify the identity of the receiver. It is possible to automatically recognize and transfer credits between institutions and to create automatically stackable credentials.

Source: Alex Grech, 2021 [created for the purposes of the current publication]

How blockchain may help improve current certification practices

Using the first two methods, the proofs necessary to authenticate the certificates will be stored completely, securely and permanently on a blockchain. Thus, even if the institutions that issued the certificates were to cease operations or disappear, or if a natural disaster eliminated the records, the certificates held by users would still be verifiable against the records stored on a blockchain.

Furthermore, once institutions issue a certificate, they do not need to dedicate further resources to continue to store the certificate, or to confirm the validity of that certificate to third parties, since third parties will be able to verify the certificates directly themselves against the record stored on a blockchain.

The primary advantage of the third method is that not only would the proofs of the validity of a certificate be stored on a blockchain, but also the certificate itself would be stored on a blockchain. Thus, not only the authentication proofs but also the certificate itself would become permanent and immutable.

Automatic recognition and transfer of credit

If certificates were stored directly on a blockchain, smart contracts could be used to code various portability, transfer and stackability arrangements directly onto the chain. Therefore, the transfer of credits between institutions, the awarding of degrees and other transactions that involve the transfer and accumulation of credits could be verified and executed automatically. Contrast this with the present system whereby each transaction is manually checked and then approved by a university or higher education institution official.

Immutability of automatically authenticated certificates

Under all the methods, certificates in wallets, once shared, would serve as stand-alone proof of the certificates they represent. Therefore:

- users would secure granular control over their certificates and be in a position to choose with whom and under which conditions to share them, and
- any institution (e.g. employers or higher education institutions) that is verifying certificates would save significant resources in doing so, since verification would happen automatically.

Blockchain and credentialing of learning

This section identifies opportunities for using blockchain for the credentialing of lifelong learning and gives examples of its application in the credentialing space.

Issuing of notarized certificates

Educational institutions can already issue digital certificates that are notarized on a blockchain, enabling stakeholders (students, the labour market and public and private institutions) to recognize the learning achieved.

Authentication of certificates

In a world where notarization of certificates on a blockchain becomes the norm, institutions would be able to create software that automatically authenticates certificates in any internal process that requires the submission of certificates – including admission, recruitment, promotion, etc. Using such systems, only once certificates were automatically flagged as valid would they then be forwarded to the relevant department for processing.

Creation of verified institutional identities

Accreditation of higher education institutions and education programmes is a complex area whereby each entity has its own accreditation procedures, which may involve multi-step workflows. Furthermore, when online and international qualifications are factored in, there are literally hundreds of different accreditation workflows across the globe. It may be difficult for a non-expert such as a student to determine whether an institution is indeed a bona fide, quality accredited institution, particularly in an online or transnational context. Some diploma/degree mills have been known to set up fake accreditation organizations and fake university networks to make themselves look legitimate (CHEA and UNESCO, 2009).

The only way to determine beyond reasonable doubt that an institution's credentials are legitimate is to have a system in place to verify each step of an accreditation procedure against a database of approved workflows for accredited institutions.

Blockchain certificates can be issued to legal persons and institutions as well as to natural persons.

Blockchain certificates can be issued to legal persons and institutions as well as to natural persons. Thus, accreditation bodies could also link their accreditation certificates to a blockchain. This would allow for verification that not only did student X receive a certificate from institution Y, but also that institution Y was certified by accreditation organization Z.

Assuming that the institutions involved would share their certificates in a public registry, such a system could be used to ensure that the educational organization issuing the certification was licensed by government, or to verify that the educational organization had specific quality certifications – for example, that an MBA provider was actually certified with the European Quality Improvement System (EQUIS) accreditation.

This could allow for the creation of multi-step verifications, whereby with a single click an individual could check:

- with the institution to verify if it had really issued the certificate,
- on the quality of the accreditations that the institution claims to have,
- with the accrediting bodies to verify if they had really issued the certificate to the institution,
- by which authority the accrediting bodies issue the accreditation, and
- with the authority to verify if they had really authorized the accrediting bodies to operate.

By providing easy and automatic access to assess the authenticity of qualifications, such a solution would significantly limit the ability of diploma mills to appear authentic to third parties.

Automatic transfer and accumulation of credit on a blockchain

The automatic transfer and accumulation of credit on a blockchain implies that a network of organizations that issue, transfer and accumulate credits would act in concert as a DAO. In a DAO, the rules of the organization are encoded as smart contracts on a blockchain, and any changes to those rules occur through votes that take place on-chain to update those same smart contracts.

The automatic transfer and accumulation of credit on a blockchain implies that a network of organizations that issue, transfer and accumulate credits would act in concert as a DAO.

A DAO on a blockchain will often replicate (automate) an existing organizational structure where a multitude of parties with limited trust in each other need to negotiate complex transactions within a set of commonly agreed rules. Such an environment exists among universities that recognize and transfer credits between themselves.

Thus, using a blockchain, credit transfer agreements, once agreed by consensus among the organizations running a chain, could be written as smart contracts whereby, upon fulfilment of the conditions of the contract, the credits would automatically be transferred.

The same process applies to accumulation. A smart contract could be programmed to automatically issue a degree upon the achievement of certain credit targets, according to the policy of the institution, ensuring that the transfer and accumulation rules are applied predictably and reproducibly across all cases.

Sharing and verification of experiential certificates on a blockchain

Experiential certificates essentially cover all credentials evidencing learning or skills that are not pegged to the national qualifications framework. These might be set to comprise, for example:

- credentials from formal education, issued by foreign jurisdictions, as typically verified by the ENIC-NARIC centres in Europe, or
- all forms of certificates awarded via non-formal and informal learning.

In this case, rather than an institution uploading data to a chain, learners would store their own evidence of learning received from any source – whether formal, non-formal or informal – and when shared, a blockchain would be used for instant verification of the authenticity of these documents. Each uploaded claim would be checked and validated by other nodes on the blockchain. Once a certain number of users confirm the claim to be true (and depending on the reputation of the users verifying the claim), the claim would receive a trust score, which is a score of its verifiability.

Maturity

The technology for digital notarization of credentials is already sufficiently advanced for multiple organizations, including the Government of Malta and the University of Nicosia, to deploy it in live – albeit controlled and small-scale – settings. Several other governments as well as the European Commission are analysing the feasibility of deploying blockchain-based notarization systems in multiple settings. In Germany, the Fraunhofer Institute for Applied Information Technology has developed a hybrid PKI/blockchain solution for certificates. In order to support the European Union (EU) Digital Single Market, the Connecting Europe Facility (CEF) programme[13] created a set of generic and reusable digital service infrastructures (DSIs), also known as building blocks. The purpose of a CEF building block is to provide shared and reusable software, specifications and services to support adoption by EU institutions and European public administrations. In 2018, EU member states got together to create the European Blockchain Partnership (EBP) to collaborate on building the European Blockchain Services Infrastructure (EBSI).[14] The EBP has thirty signatory countries, all the EU states as well as non-EU members, the United Kingdom, Norway and Liechtenstein. In 2019, EBSI[15] became a CEF Building Block. EBSI is being built to promote the use of cross-border government services and infrastructure by leveraging a network of blockchain nodes that are being set up across Europe. The project includes an ongoing pilot for the accreditation of European diplomas. As of March 2022, there were thirty-six live nodes across Europe.

Several companies already offer organizations the option of issuing their own blockchain-certified credentials.

Several companies already offer organizations the option of issuing their own blockchain-certified credentials. For instance, Accredible[16] and Gradbase[17] allow for anyone to issue and verify blockchain-secured certificates, while Learning Machine currently offers the service as a one-stop-shop service using the open Blockcerts standard. Salesforce Blockchain[18] is being positioned as an ideal platform for the verification of learning credentials.

13 See https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/The+Vision
14 The European Blockchain Services Infrastructure (EBSI) is a joint initiative of the European Commission and the European Blockchain Partnership (EBP) to deliver EU-wide cross-border public services using blockchain technology. The EBSI will be a network of distributed nodes across Europe (the blockchain), leveraging an increasing number of applications focused on specific use cases.
15 See https://youtu.be/m2uj7fgb2JI
16 See https://www.accredible.com
17 See https://www.gradba.se/en
18 See https://www.salesforce.com/news/press-releases/2019/05/29/salesforce-introduces-the-first-low-code-blockchain-platform-for-crm

Box 4. Case study: Malta blockchain credentials for TVET

In September 2017, the Ministry for Education and Employment signed a one-year contract with Learning Machine to deploy a nation state pilot and issue digital credentials notarized via the Blockcerts open standard.[19] Blockcerts focuses on every aspect of the credentials value chain: creation, issuing, viewing and verification of the certificates using blockchain technology as the infrastructure. The pilot was initiated to create a verifiable proof of credentials – including technical and vocational education and training (TVET) credentials for citizens – with participating institutions including the Malta College for Arts, Sciences & Technologies (MCAST), the Institute for Tourism Studies and the National Commission for Further and Higher Education (NCFHE). The pilot provided three main functionalities:

1. Issuance and registration of academic certificates (using the Learning Machine certificate issuance environment).
2. Storage and presentation (Blockcerts application).
3. Verification (third-party verification web page).

Credential recipients could receive, verify, store and share their academic and TVET credentials on a blockchain via a digital wallet, which also installs the Blockcerts application. By adding their academic institution as an issuer, the citizen could receive from their institutions digital records that are verified by that institution. Recipients could share these credentials with others and these third parties could in turn use Blockcerts to verify the credentials.

What the recipient sees is the record itself, the content of the record and the signed hash of the content, which is stored on the blockchain. The content of the record includes the public key of the recipient of the record, presenting the ownership of that record.

For issuing institutions, Learning Machine created functionalities that allow institutions to:

- import/manage recipient lists,
- easily collect recipient public keys,
- design templates for digital records (content, layout, metadata),
- issue records to entire cohorts,
- track aggregate analytics of how records are being used online, and
- view profiles that show all records issued to an individual.

Over 2,000 certificates were issued during the pilot stage. In February 2019, the Maltese Government announced that it had extended its contract with Learning Machine for a further two years to enable the pilot to extend to all academic and TVET institutions in Malta and to explore how the technology could be deployed for public records.

For more information on the project, see https://www.cryptoninjas.net/2019/02/25/malta-rolls-out-blockcerts-blockchain-credentials-foreducation-and-employment

Business-to-business and business-to-consumer model

Early-stage pilots are already underway for the issuing of formal certificates directly on blockchains. The University of Maribor is running a blockchain-based platform called EduCTX, levering on the concept of the European Credit Transfer System (ECTS) (Turkanović et al., 2018), while the MicroHE Project[20] is investigating their use for the recognition of microcredentials. In 2020, the European Consortium of Innovative Universities (ECIU) launched the vision for ECIU

19 Blockcerts is an open standard for the issuance and verification of records or credentials using blockchain technology. The standard is defined so that anyone can use the base code to develop their own software to issue and verify these records or credentials. The Blockcerts standard has been created to not be dependent on a specific blockchain. However, the Blockcerts pilot in Malta is based on the Bitcoin blockchain.

20 See https://microcredentials.eu

University 2030,[21] which is to collaborate and create a virtual European university where learners, teachers and researchers may cooperate with cities and regions, businesses and citizens to solve real-life challenges in a unique and flexible way; verifiable, digital credentials would underpin the accreditation process. Widespread adoption in these cases will depend on the uptake of these technical standards by large numbers of stakeholders and are likely to require regulatory incentives.

Cost-savings and speed

Blockchain facilitates scenarios that may contribute to significant cost-savings for all parties involved in issuing and verifying the certificates – and in particular for institutions, students and employers – because verification would become instant and automatic, without requiring any of the manual procedures currently in use.

Blockchain facilitates scenarios that may contribute to significant cost-savings for all parties involved in issuing and verifying the certificates.

Should these solutions be deployed at scale, they could result in significant cost-savings and time-savings for institutions in that they would be able to automatically verify not just the **authenticity** of certificates, but also the **content** of those certificates. Since automation requires standardized processes and procedures, we believe standardization is the only way to achieve these savings. In addition, start-up costs and time for this scenario are likely to be high because of the complexity of the arrangements in place and the need to codify them to a blockchain-based system.

Prerequisites

Any institution can theoretically launch its own notarization service, without the need for standards, as long as it provides a link to the verifier on the certificate. However, in a scenario where hundreds or even thousands of different verification modalities exist, it would become burdensome to create automatic verifiers for them all. Thus, there is a case for having commonly agreed technical standards for notarization. Learning Machine and a number of associated organizations have created Blockcerts, a set of open source libraries, tools and mobile apps enabling a decentralized, standards-based, recipient-centric ecosystem, to allow trustless verification through blockchain technologies. The W3C Verifiable Claims Working Group is working towards a global standard for these claims.[22]

Prospect

Stakeholders in the education sector are interested in moving towards secured digital certificates for reasons already cited in this report. In such a scenario, PKI-based certificates or blockchain-secured certificates are the only realistic options for the digitalization of credentials. Blockchain-secured certificates have evolved significantly from PKI in terms of the immutability of the certificates and the absence of a need to rely on a central issuer. We therefore believe that

21 See https://assets-global.website-files.com/562fb917aa38ca2e349b422e/5fa153b1c8e6ad03c125f699_20201195%20ECIU%20-%20Opmaak%20visie%202030%204.pdf

22 The W3C, or World Wide Web Consortium, was formed during the early days of the Internet by Tim Berners-Lee and the European Commission to codify open standards that would be used by everyone to transact information across the new, global digital infrastructure of the Web. It is now doing the same for blockchain applications that make use of the Web, such as verifiable credentials. The W3C is the leading independent Internet standards body in the world, and its credentialing standards are already seeing uptake by governments, including the Canadian Government, the US Government and the European Commission.

such certificates stand a high chance of stakeholder acceptance and adoption in the absence of artificial barriers (such as proprietary, lock-in solutions) being set up.

Should accreditation agencies in federal states choose to adopt blockchain, the creation of verified institutional identities can also be considered a feasible prospect in the near future.

The automatic accumulation and transfer of credits could be one of the most desirable use cases for blockchain technology.

The automatic accumulation and transfer of credits could be one of the most desirable use cases for blockchain technology. Nevertheless, this is likely to be a long-term prospect since it would require the development of significant new technology in the form of smart contracts, the creation of governance structures between the participating organizations and definitive codification of the rules for transfer and accumulation under every scenario.

The sharing of experiential certificates has higher prospects of adoption in the near future than formal higher education certificates. Nevertheless, successful uptake will depend on the quality of the validators in the validation network. If agencies validating non-formal and informal learning in line with legislation were to adopt the technology, there would be excellent chances for the technology to have a high impact on trusted norms. In the short term, such services might be used by employers to organize their own validation networks for skills and credentials with the help of specialized private validation organizations.

Management of intellectual property using blockchain

The World Intellectual Property Organization defines intellectual property (IP) as 'creations of the mind, such as inventions; literary and artistic works and designs'.[23] As such, all knowledge generated by universities and all creations of staff and students within universities can be classified as intellectual property.

The generation and management of IP is key to the business model of many educational organizations, particularly universities. First, much of the IP that universities generate supports teaching and research activities. Second, universities have developed capabilities in supporting the process of translating knowledge with immediate application into the wider society and economy. Third, the research base – and indeed innovation in education – creates new knowledge and provides a broad foundation for innovation throughout academia and business, often communicated through scholarly conferences, publications or collaborative research and teaching, but also through technology transfer. These activities also feed into future commercial and public applications. Therefore, the main method of measuring the performance of academics in universities is tracking the new IP they generate and the value of that IP, usually measured using indicators such as academic citations.

Universities often employ a mixture of licensing strategies, depending on their missions. Broadly speaking these tend to fall into two categories:

- Open licensing: Involves waiving many of the rights an institution has to its IP so that the general public may use it in the public interest.
- Closed licensing: Involves protecting the IP, usually in the form of copyrights, trademarks, patents or a combination of two or more of these so that it may be commercialized.

23 See https://www.wipo.int/about-ip/en

In the context of IP management, ledgers are used for:

- registering when a work was first created and by whom, which is necessary to determine ownership,
- tracking changes in ownership or licensing of IP, and
- tracking instances of third-party use of IP, often for the purpose of allocating credit or royalties.

Current state

Currently, tracking intellectual property is a costly endeavour undertaken by specialized organizations, usually when there is a significant business case to do so. Thus, collecting agencies track IP usage of music and videos to collect royalties, while journal companies track citations of articles, since these data are valuable as a metric for measuring the quality of academic research and determining professional progression in academia. Specialized law firms track usage of patents to collect the associated royalties.

Limitations

Due to the complexity of tracking IP, it is difficult for people who are self-publishing to track and commoditize the reuse of their intellectual property, even with the rise of alt-metrics. For instance, the reuse of open educational resources (OER) is generally either not tracked or tracked with extremely simple metrics with limited use.

Most companies that manage IP on behalf of organizations have gained a near-monopolistic hold over their industries due to the inherent network effects in IP management. This has led to significant criticism within academia that they hold too much power over the production and use of IP and that they abuse this power, mainly via exorbitant licensing and charging policies. The most visible example of such criticism might be the Cost of Knowledge campaign against Elsevier (Heyman et al., 2016). Thus, the open education and open science (and related open source) movements have arisen largely as a countermovement to the policies of such companies.

Description

Under this scenario, educators or institutions creating intellectual property would use a blockchain to notarize the date of publication and the material published, thus creating an intellectual property claim. Additionally, a blockchain could be used to track use, using a variety of usage-metrics depending on the use case, of this IP once it has been published.

Evolution from the current state

From a structural standpoint, this scenario is very similar to the processes based on the existing databases for the management of IP. However, IP management has until now required intermediaries, namely publishers, whose business model involves exploiting the rights of others just as they equally seek to defend and protect their own rights acquired from others (Seeber and Balkwill, 2007). As such, they will usually put limits on how authors may use their IP in return for those services, often in the form of high costs for access and restrictions on the sharing and use of the intellectual property within them. This has limited the uptake of open licensing models over closed licensing models.

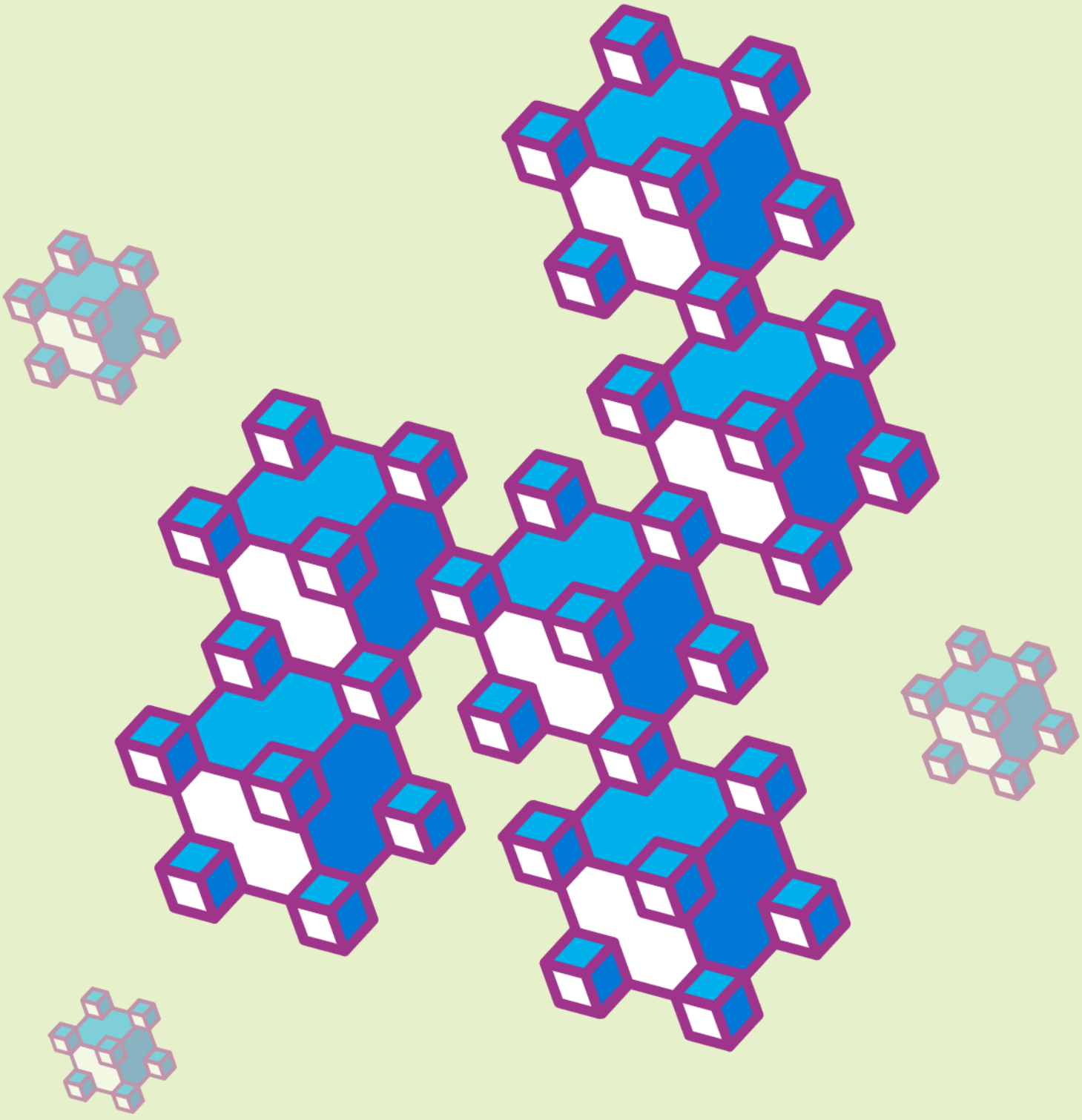
Using a blockchain eliminates the need for an intermediary to manage IP ledgers. Coupled with the possibilities the Internet offers for anyone to publish and distribute material openly, it may lead to a significant disruption in the models and stakeholders involved in IP management.

Part 3

Usage areas

Part 3: Usage areas

This section looks beyond the affordances of blockchain to the credentialing of learning to identify a set of additional user areas that may resonate with the education sector.



Notarization of intellectual property rights on blockchains

Description

People who create intellectual property (IP) would simply publish the time and date of publication and a reference to the publication on a blockchain. Thus, anyone could create a verifiable property right without the need for an intermediary and with little to no administration.

Usually, this would be done by storing the hash of the published item on a blockchain, which also offers the possibility of registering an IP right without needing to publicly share the underlying source material. This changes a key premise of today's copyright and patent laws.

The chain would typically be managed directly by the rights holders or their representatives without the need to involve any intermediary.

Here, rather than just track the publication of IP, a blockchain could also be used to track its use. The chain would typically be managed directly by the rights holders or their representatives without the need to involve any intermediary. Potential use cases could include:

- tracking the use and reuse of academic publishing and open educational resources (OER), and awarding academic credits in proportion to use-levels, and
- collecting royalties directly from users in relation to the degree of use and redistributing those royalties to rights holders.

Critically, all these uses could be managed by the rights holders themselves, thus obviating any need to hand over any part of those rights to a management organization.

Implications

The notarization of IP on blockchains would lead to the same savings as described in the section on the notarization of credentials on blockchains. Automatic publication, tracking and rewarding of IP based on blockchains would lead to massive cost-savings for people using that IP. However, this would destroy a major source of revenue for the publishers and companies that deal with tracking IP usage. Since the costs of open publishing can by definition not be recouped for royalties, such a significant decrease in costs is likely to encourage open publication.

Usage scenario

Under this scenario, a special-purpose blockchain would be created to allow educators to announce the publication of their resources and link to both those resources and any other resources they used in creating their material. Coins would be awarded to educators in line with the level of reuse of their respective resources.

In an open scenario, coins could not be spent and would instead be used to determine the prominence of an author. In a closed scenario, coins would have monetary value and would result in monetary compensation. A more advanced implementation might automatically scan resources to identify what percentage of other resources were reused and automatically award the author accordingly.

Photo: Pixabay

Evolution from the current state

There is likely to be a short-term prospect for the notarization of IP on blockchains since it offers a clear evolution from the current systems and requires no changes to legislation or policies to become operational.

Data management companies may also consider moving their internal usage and reusage records to blockchains for reasons of efficiency, security and immutability.

Data-management companies may also consider moving their internal usage and reusage records to blockchains for reasons of efficiency, security and immutability.

However, the decentralization of databases to stakeholders is only likely in the mid- to long term and is highly dependent on political considerations. Current systems for citation tracking and concepts of academic performance built on these are entrenched in education systems. An emerging alt-metrics movement is challenging some of these preconceptions but is still very much in its infancy. Thus, while blockchain could facilitate the rise of alt-metrics and the democratization of systems based on them, it is not the key factor in enabling their adoption.

Maturity

Technologically, blockchain-based IP management has already arrived. Munich-based Bernstein Technologies offers blockchain-based notarization services for inventors to establish the ownership of original work. Binded (previously known as Blockai) enables artists to claim copyright on their art/photographs on a blockchain and is already working in conjunction with the US Copyright Office, Instagram and Twitter. Blocknotary does essentially the same thing, but for iOS users. Singapore-based Concensum connects the copyright of digital content with its authors to protect their assets worldwide. *Ledger Journal* is an academic journal notarized on a blockchain, while Everipedia is a Wikipedia fork that rewards editors for publication activity via cryptocurrency.

Educational funding, performance-based pay and microcredit for education via blockchain

Description

Payments are the transfer of money from one party to another. As explained earlier, in the pre-blockchain era, secure digital payments required the services of a trusted intermediary to keep the definitive ledger showing the true state of accounts. This increases the complexity of the transaction and covering the costs and/or fees of the intermediary increases the costs. Complex financial transactions involving multiple parties may require the services of multiple intermediaries, leading to significant administrative, time and cost overheads on any kind of financial transaction. Two of the reasons digital payments have failed to replace cash payments in many countries to date are a reluctance to trust the intermediary with the information and a desire to not incur these costs. In specific cases, the cost of payments may be so high as to prevent certain types of payments taking place. Thus, centralized payment ledgers may not be suitable for the use of micropayments.

Educational organizations apply a host of different funding models, including performance agreements, global budgets, formula-based budgets and tuition fees (Strehl et al., 2007). Additionally, students paying tuition fees may themselves be subject to performance agreements or formula-based budgets enforced by the organizations that are funding them. The theory of property rights and the theory of transaction costs stipulate that the structure of property rights and the structure and amount of transaction costs influence the benefits and damages for the actors and therefore also determine their decision-making. Under given institutional conditions, actors will choose the forms of resource usage and property rights alternatives that maximize their benefits. This theory also explains why innovation in funding in education can have limited uptake: a variety of institutional and individual funding models are available for education globally. Across the entire education system, millions of financial transactions are made every day, mediated by banks and financial institutions and supported by public institutions. The costs per transaction can range between a few cents and several thousand euros, depending on complexity and size. However, when it comes to student payments and funding arrangements, the following limitations remain commonplace:

- It can be costly to make payments. Credit card fees and bank transfer fees, in particular for students from developing countries, can be prohibitive. Access to the banking system can also be an issue for students with migrant backgrounds or specific religious beliefs.
- Performance-based funding arrangements, whether for institutions or for students, require costly administration processes to track the performance and then authorize payments accordingly, as well as to track cases of potential fraud and abuse.
- Funding agreements for tuition involve multi-year commitments to services, which require considerable work to codify in terms of legal agreements. Despite this, funding conditions are sometimes changed after the initial agreement, to the detriment of students, the organizations or both.
- In most countries the calculation of needs-based financial aid for lower-income students is not enough to establish parity with better-off students.

Microloans and microcredits are becoming more popular in education. These options help establish a direct connection between lender and borrower, and sometimes contribute to zero-interest loans. Nevertheless, problems with third-party intermediaries persist.

Usage scenario

Under this scenario, payments in education would be made via blockchains, using either fiat currencies or cryptocurrencies. Such payments could include state funding, payment of scholarships, payment to content providers, microcredit, etc. Funding formulas and agreements would be coded directly onto the chain to release funding based on pre-set conditions, which would be monitored and triggered automatically. The use of smart contracts could also create a viable method of payment to and from students once those conditions are met.

Blockchain-based payments could also be applied to payments to staff or institutions via smart contracts on a blockchain. For example:

- Staff could be automatically incentivized when reaching certain performance targets in terms of publications, student grades or intellectual property transfer.
- Institutions could be automatically incentivized when reaching certain performance targets in terms of student numbers, mean grades or publication output.

Evolution from the current state

Blockchain-based payments may facilitate reduced payment costs for all students, but for the underbanked and unbanked, they will reduce the scope of what is currently a significant barrier to education, particularly in the developing world. For funding organizations such as governments, a reduction in the costs of administering formula-based funding models and performance-based funding models would increase the attractiveness of these models in education. Private funding organizations – including companies and NGOs – would also be more willing to participate in funding education if a blockchain allowed for better and more cost-effective targeting of their investments. Finally, codification of agreements in immutable smart contracts would provide guarantees of funding for the duration of an individual's studies by locking funds up in escrow and releasing or returning them based on pre-set criteria, with funding rules only being changed subject to the agreement of all parties.

Maturity

Low-level management of educational funding using blockchains may lead to rapid entry into the marketplace. Some governments are experimenting with blockchains for government payments, while some universities – for example, the University of Nicosia (UNIC) – now accept payments in cryptocurrencies. Additionally, several start-ups are building platforms to connect private companies, individuals and content creators and manage payments between them on blockchains.

Low-level management of educational funding using blockchains may lead to rapid entry into the marketplace.

US-based non-profit Kiva implemented the Kiva Protocol in collaboration with the Government of Sierra Leone and other UN agencies for the facilitation of microloans in 2018, although the scope of its application is much wider than just education. In 2019, Kiva collaborated with its partners at the Bank of Sierra Leone, the National Civil Registration Authority and UN Capital Development Fund to engage with financial service providers across Sierra Leone to help integrate electronic know your customer (eKYC) capability into existing bank onboarding and compliance systems. Brazil-based Moeda launched a blockchain-based digital marketplace that

allows peer-to-peer payments and microfinancing of digital loans through fiat-pegged digital tokens. London-based start-up Pigzbe launched a blockchain-based 'piggy wallet', with the intention of educating children about twenty-first-century finance and facilitating international micropayments. The World Food Programme (WFP) launched a project called Building Blocks, a blockchain-based cash transfer programme for refugees that successfully transferred about US$1 million to 10,000 Syrian refugees. In 2019, UNICEF launched its own Cryptocurrency Fund to receive donations aimed at funding open source technology benefiting children and young people around the world. In 2020, this fund issued US$100,000 to eight start-ups to continue the development of their open source technology centred on social good. rTree is an organization that leverages cryptocurrency donations to support reforestation in collaboration with Trees for the Future,[24] which has planted 200 million trees since 1989. In 2019, the US State Department awarded its first ever blockchain grant to New America, ConsenSys and Harvard to build a blockchain-based system to track the health and well-being of factory workers in Mexico. It was deployed in 2019 as a pilot, followed by another successful deployment in 2020.

Payment of tuition fees via blockchains

Description

Under this scenario, students would pay their tuition fees via blockchain-based cryptocurrencies. Another possible application scenario includes government, or sponsor, funding for tuition which would be given to students as 'vouchers' on a blockchain. The vouchers could be programmed to release tranches of funding to either the student or the educational organization, based on performance criteria such as grades.

Implications

Cost-savings will mainly be linked to a reduction in bank charges for payments, which can be significant in the case of cross-country monetary transfers. Additionally, the adoption of blockchain-based smart contracts could automate large amounts of administration in formula-based funding, significantly lowering the cost of managing such systems. In both cases, blockchain promises instant payments without the frequent delays that are normally blamed on the complexity of such transactions.

Evolution from the current state

From a blockchain perspective, the Ethereum blockchain, among others, already supports such a capability. To use this system, one would require software to build the smart contracts easily and upload them to a blockchain, and the data sources – such as a database of student grades – for the smart contracts to know whether the conditions of the contract have been fulfilled. Many implementations of smart contracts try to put all the required data sources on blockchains in order to have the same level of trust in all the data. Within the public sector, adoption of any cryptocurrency-based funding algorithms is likely to be dependent upon central government uptake of blockchain for internal transactions, since all rules regarding financial transfers within government are regulated at Ministry of Finance/Central Bank levels.

Should government adopt blockchain for internal financial transactions, it is likely that the sophistication of these systems will increase incrementally over the coming years, with more sophisticated performance-funding algorithms being developed to match policy priorities. Within the private sector, we believe that companies that are in the business of acting as clearinghouses for educational content (i.e. connecting creators, learners and funders) will increasingly adopt blockchain for payments in the near future, since it would significantly reduce the fees they would need to pay banks and other financial institutions.

24 See https://trees.org

Maturity

The payment of tuition fees using blockchain is already happening. However, rather than institutions directly accepting cryptocurrency, it is more likely that they will accept money transfers that have been enabled via blockchains – for example, the Ripple or Stellar networks – and that have fixed value in terms of fiat currencies. A small number of universities across the world have taken the lead in making way for blockchain-based payments, including the University of Nicosia, King's College in New York, the University of Cumbria in the United Kingdom, the European School of Management and Technology in Berlin and Lucerne University of Applied Sciences and Arts in Switzerland. Efforts are underway to create a new blockchain-based payment system for universities called Unit-e, spearheaded by MIT, Stanford University, Carnegie Mellon University and the University of California, Berkley.

Minimization of confidential student information

Description

Within educational ecosystems, students need to regularly identify themselves in different parts of the ecosystem, including the university itself and its various parts as well as the library and various other student services such as dorms, canteens, etc. In such cases, either:

- each part of the ecosystem will collect the student data automatically, meaning that administrative overheads are incurred in re-verifying student identities multiple times and students waste time submitting this information, or
- parties will use single sign-on, whereby one shared copy of the student data is kept in a centralized database and used by all parties within the organization.

Under both of these models, an unknown number of people might have access to a student's personal information, which might include detailed records of financial and social status, education and even health status or religious beliefs. Keeping these data safe requires managing access rights for all those people and ensuring that their devices are also secure and hack-proof – a mammoth undertaking. Recent years have seen a spate of abuses of data held by institutions, including data leaks, lost data, misused data and hacked data. Education is one of the most targeted sectors for data breaches.[25] Educational organizations also require large amounts of student data to determine eligibility for admissions, generating large quantities of new personal data in the form of student performance data. This results in:

- high costs to store and manage access to student data,
- high costs associated with legislative compliance, in particular in light of the General Data Protection Regulation (GDPR), and
- high risks from costs associated with potential breaches of data or privacy.

Furthermore, educational organizations do not necessarily share student information with different parts of the ecosystem, resulting in students having to go through unnecessary bureaucracy, as well as creating multiple points of access to student data and increasing overall risk. A typical example is where a student needs to prove their eligibility for enrolment to the admissions office at a university by providing an authenticated copy of their high school certificate and is then requested to provide another copy to the examinations office to qualify for sitting examinations.

25 See https://thepienews.com/news/education-among-most-targeted-data-breach-sectors

Data minimization is a principle that states that data collected and processed should not be held or further used unless they are essential for reasons that were clearly stated in advance to support data privacy. Under Europe's GDPR, this is defined as data that are adequate, relevant and limited to what is necessary for the purposes for which they are processed. Organizations can be fined up to 4 per cent of global turnover or €20 million (whichever is greater) for breaches of the regulation. While there are certain exceptions to these laws for public institutions, there is a higher public expectation of proper data handling in the public sector. Data minimization assumes that all data storage systems will be compromised or attacked at some stage, and that the best defence is to not store unnecessary data in the first place, thus minimizing risk exposure. As such, it is also a tool to simplify and reduce the costs of data storage arrangements.

Data minimization assumes that all data storage systems will be compromised or attacked at some stage, and that the best defence is to not store unnecessary data in the first place, thus minimizing risk exposure.

Usage scenario

Under this scenario, organizations that require student data to verify eligibility for access to certain services would check the data and then use a blockchain to:

- store a hash of a certificate attesting the student's identity and eligibility to access services, and
- store the hash of the evidence provided.

The organizations would then be able to delete all the data they held, thus creating no data exposure. Students would be able to verify their identity by presenting the certificate, which could be validated against the blockchain entry without exposing the underlying data.

Evolution from the current state

By using verified self-sovereign identities, only the persons responsible for verifying the student's identity in the first instance require access to the data. Since the rest of the organization may only need to know that the student is eligible for access to services, the blockchain is used to create a verifiable, trusted student ID. This allows the rest of the organization to identify students without having access to the underlying data, which students can keep in their possession. This means that the organization no longer needs to manage the complex systems for access rights and only needs to secure the device or network where the initial verification is taking place. This would save significantly on the costs of securing the network against data breaches, staff training on data protection and managing access rights. Additionally, personnel interacting with the student within the organization do not need to take on the responsibility of keeping sensitive data private, since they will not need to have that data in the first place.

Maturity

Initiatives in this sector to date are mostly coming from the private sector. Edgecoin offers BaaS (blockchain-as-a-service) based on the Ethereum platform within the education sector to issue

decentralized and smart credentials that remain securely encrypted on the blockchain. Oasis Labs is a start-up from the University of California, Berkeley, which to date has focused its efforts on securing healthcare records and e-commerce platforms offering user privacy-as-a-service; the technical solution can possibly be migrated to the education sector in its entirety.

Management of student identity within educational ecosystems

Description

Student identity within education systems is normally managed by centralized databases, with student records retained by the institution in perpetuity.

Usage scenario

Under this model, a specified entity within an educational institution would be responsible for determining a student's identity and then issuing them an attestation, such as in the form of a student ID. The underlying data that were used to verify the student's identity would then be deleted, with the student ID serving as proof in and of itself of eligibility for access to services across the institution.

Implications

Adoption of blockchain-based identity solutions would significantly lower compliance costs with data protection legislation in any institution that adopted them.

Adoption of blockchain-based identity solutions would significantly lower compliance costs with data protection legislation in any institution that adopted them.

However, since institutions would, by default, hold very little information about users, they would need to re-request information in specific scenarios, possibly leading to slower processes in certain cases. For instance, if information on a medical condition was not stored in a database, the student might need to re-share the information with each lecturer or administration official who had a need to know about it.

Evolution from the current state

Considering that there is a significant compliance aspect to this proposal, with respect to the GDPR, a certification system for software solutions would significantly assist in the adoption of these sorts of solutions. Additionally, most implementations of such systems assume universal adoption of smartphones or smartwatches as the data management device on the part of all users. Therefore, institutions would need to require such devices, or supply them to students as necessary.

It is unlikely that institutions would self-develop such software. Student data management is generally done using software supplied by student information system vendors. Should vendors adopt a blockchain-based solution as a feature in their architectures, the chances of adoption would be high; however, the technical challenges involved indicate that this is a mid- to long-term prospect.

Maturity

Several companies – for example, uPort, Civic and Persona – are launching sovereign self-identity solutions that could be applied to this use case. Currently, these would require institutions to undertake significant technical work to tie these systems into their current student information systems. Computer giant IBM has been actively investing in this area and collaborating with companies like Credly, CULedger, SecureKey and MyCelia. ID2020 is a multi-stakeholder collaboration consisting of private companies and foundations leveraging the use of blockchain technology to ensure identity as a universal human right. Their goal is to provide funding and other forms of support to high social impact digital identity projects across the globe. In 2021, in response to the COVID-19 pandemic, the ID2020 alliance launched the Good Health Pass Collaborative[26] with the intention to create interoperable digital health pass systems.

Creating a decentralized educational Web via a blockchain

Description

Web 2.0 is often described as the social Web. It is built on top of Web applications that allow for collaboration between people – whether that collaboration happens via a social network, business productivity tools or knowledge platforms such as Wikipedia.

Each of these applications is run by a single company or foundation that both controls access to the data and hosts the physical servers that store the data. Using social media and online social networking platforms involves trusting the central party to not abuse that data. Specifically, users must trust the central parties to:

- provide witness – that is, to certify identity and ensure that the persons using the platform are who they say they are and that any content they post is real and legitimate;
- be honest and transparent in all transactions – that is, to operate the platforms in exactly the way they have promised to operate them in their user policies;
- be secure – that is, ensure that unauthorized third parties cannot read or write the data, or in other words, prevent hacking;
- not abuse their monopoly by imposing unfair/exceptional costs on their services; and
- allow people to communicate – that is, give everyone an equal voice on the platform, in line with its mission and rules.

The corollary is that these institutions may individually or collectively cause significant harm or even social chaos by abusing the trust placed in them to accurately maintain their services and policies. The inference is that these institutions have the power to use or abuse their control over their applications and exert significant control over individuals and societies within their immediate remit. The most public example of this to date is that breaches of data policies at Meta resulted in congressional hearings in the United States of America and a special hearing of the European Parliament in Europe. Within education, centralized networked apps are used extensively for a variety of purposes. The types of apps used include:

- student information systems,
- learning management systems,

26 See https://www.goodhealthpass.org/wp-content/uploads/2021/02/Good-Health-Pass-Collaborative-Principles-Paper.pdf

- real-time communication tools such as videoconferencing and chat apps,
- collaborative office productivity tools including word processors, spreadsheets, presentation software, etc.,
- open archives and library tools,
- crowd-sourced reference databases, and
- social networks, including education-focused professional networks.

While some of these apps are run by the institutions themselves on their own servers, the large majority are run and controlled by companies that license the software to institutions. Thus, those companies must be trusted to properly handle the data. This architecture usually means that:

- users have to give up various degrees of control over their own data to the hosting organizations to enable the applications to work and often in return for the use of ostensibly free services,
- users have no control over where and how their data is stored or backed up,
- it is difficult to enforce and monitor local data protection standards if companies are operating globally,
- users cannot easily transfer their data from service to service, and
- hosts can charge for software-as-a-service, which locks users into long-term high-cost contracts, which are not easy to change once started.

Usage scenario

With decentralized apps, users can pick and choose mainstream storage providers like Dropbox or BitTorrent to host their data, and applications will be able to read the data with the user's consent. The app ensures that all data are signed, verified and encrypted end-to-end, so users can treat storage providers like dumb hard drives, easily changing storage providers or storing the data on their proprietary devices.

At the same time, developers are no longer exposed to risks for hosting user data. Since users bring their own storage and use public key cryptography for authentication, applications do not have to store anything and so there is nothing to steal if they are hacked. Moreover, many Web applications today can be re-factored so that everything happens client-side, obviating the need to run dedicated application servers.

Evolution from the current state

Institutions can use decentralized apps to provide educational technology to students without needing to configure hosting or lock into contracts with proprietary service providers. This marks a drastic change from the existing scenario where they have to go through multiple layers of administrators to get to the desired state.

Maturity

Tim Berners-Lee, the inventor of the World Wide Web, and several MIT researchers presented Solid, their version of the decentralized Web, in 2018. Solid is an open source project that is being developed over the existing Web and has been explained by Berners-Lee as follows: 'Solid changes the current model where users have to hand over personal data to digital giants

in exchange for perceived value. As we've all discovered, this hasn't been in our best interests. Solid is how we evolve the web in order to restore balance – by giving every one of us complete control over data, personal or not, in a revolutionary way.'[27] Universities such as the Open University in the United Kingdom are closely monitoring Solid to determine if it can support the management of personal data in the field of education.

Decentralized social apps for education

Description

With the mainstreaming of social media, the way students consume information and knowledge has changed. Social media has become ingrained in our daily lives to such an extent that it is essential to evaluate its effects on students and the education sector as a whole. Using social media–based apps as pedagogical tools, while constructive, presents many unwarranted risks such as data mining from user-produced content and other privacy issues together with exposure to unsuitable content. Decentralized social media apps offer a solution to this conundrum.

With the mainstreaming of social media, the way students consume information and knowledge has changed.

Usage scenario

Every application used in education, including learning management systems, collaboration software, office software, etc., could be migrated to decentralized apps. Some of the features that such apps can offer include public/private browsing, data encryption and control over who can and cannot access one's social network. True decentralized apps will require active developer communities to program them. Furthermore, they will require users to have access to high-bandwidth and high-performance devices.

Implications

The total real cost of a decentralized app infrastructure is likely to be higher than that of a centralized app infrastructure. Furthermore, decentralized apps will be slower than centralized ones. However, in a time of multi-core processors in phones, and near-universal broadband Internet, these performance costs are likely to be insignificant.

Additionally, the adoption of decentralized apps means that the real cost of running the apps – such as electricity, bandwidth and storage – will be transferred to users. However, these will be the only costs; with no need to pay service fees or margins to third parties, the cost benefit is transferred to the end users.

Maturity

Blockstack has already launched an infrastructure for decentralized apps, and entry-level office-collaboration apps have already been created. Diaspora and Mind are other apps that have already reached about a million users each. Indorse is a LinkedIn-like decentralized platform based on Ethereum to validate skills using decentralized consensus from the user community. Decentralized apps are likely to be an area of high innovation in coming years, but they require all apps to essentially be rewritten from the ground up.

27 See https://inrupt.com/one-small-step-for-the-web

The demand for decentralized apps is likely to be significant, as truly private, free educational software is a major plus for all stakeholders within higher education and the technical and vocational education and training (TVET) sector. Just as open source software has been adopted in bulk in other areas once it reached a certain usability threshold, the adoption of blockchain-enabled decentralized apps is likely to be significant should good enough software be developed. The rate of adoption will depend firmly on the availability of financial incentives for such development to take place.

Just as open source software has been adopted in bulk in other areas once it reached a certain usability threshold, the adoption of blockchain-enabled decentralized apps is likely to be significant should good enough software be developed.

Other scenarios

The scenarios presented above have been assessed as having clear potential benefits for students, higher education institutions and the public sector. A number of other scenarios were considered but were assessed as low impact, either because they only had a tangential impact on teaching and learning or because blockchain has yet to provide an adequately obvious added value.

Voting

Election-style voting occurs in multiple contexts in higher education, such as in the case of student self-government or to determine the holders of specific posts within universities.

Many companies are developing blockchain-based solutions for voting, since blockchain can allow a complete audit trail of votes to be kept and allow voters to check that votes were counted. However, these solutions are being developed in the context of high-security, high-stakes polls and remain expensive and complex to use.

While it is likely that at some point such voting systems might reach economies of scale to make voting-as-a-service applications available to any organization at low cost, it is unlikely that the education context provides a compelling use case for such applications.

Decentralized autonomous organizations

This scenario involves using blockchain for everything or creating blockchain universities where all financial, administrative and governance systems of a university are linked to a blockchain and, wherever possible, automated via smart contracts.

Such a scenario imagines that once governance decisions are taken and voted on via a blockchain, the entirety of the administration will essentially run itself automatically with minimal human intervention.

BitDegree launched an ICO to develop these institutions. However, initial applications involve the inclusion of only a handful of the hundreds of processes in a typical higher education institution. It remains to be seen if blockchain technology can handle such a level of complexity with more efficiency than existing legacy systems.

Research lifecycle management

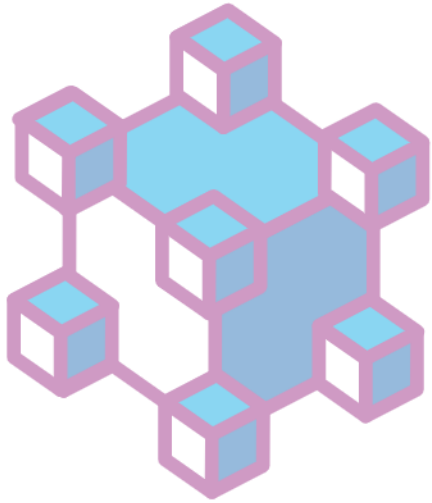
The practice of preregistration – the process to submit the research rationale, hypotheses, design and analytic strategy of an intended research project to a journal before publication – is gaining increasing traction in the scientific community as a means of avoiding problematic research methods such as p-hacking or withholding publication of data.

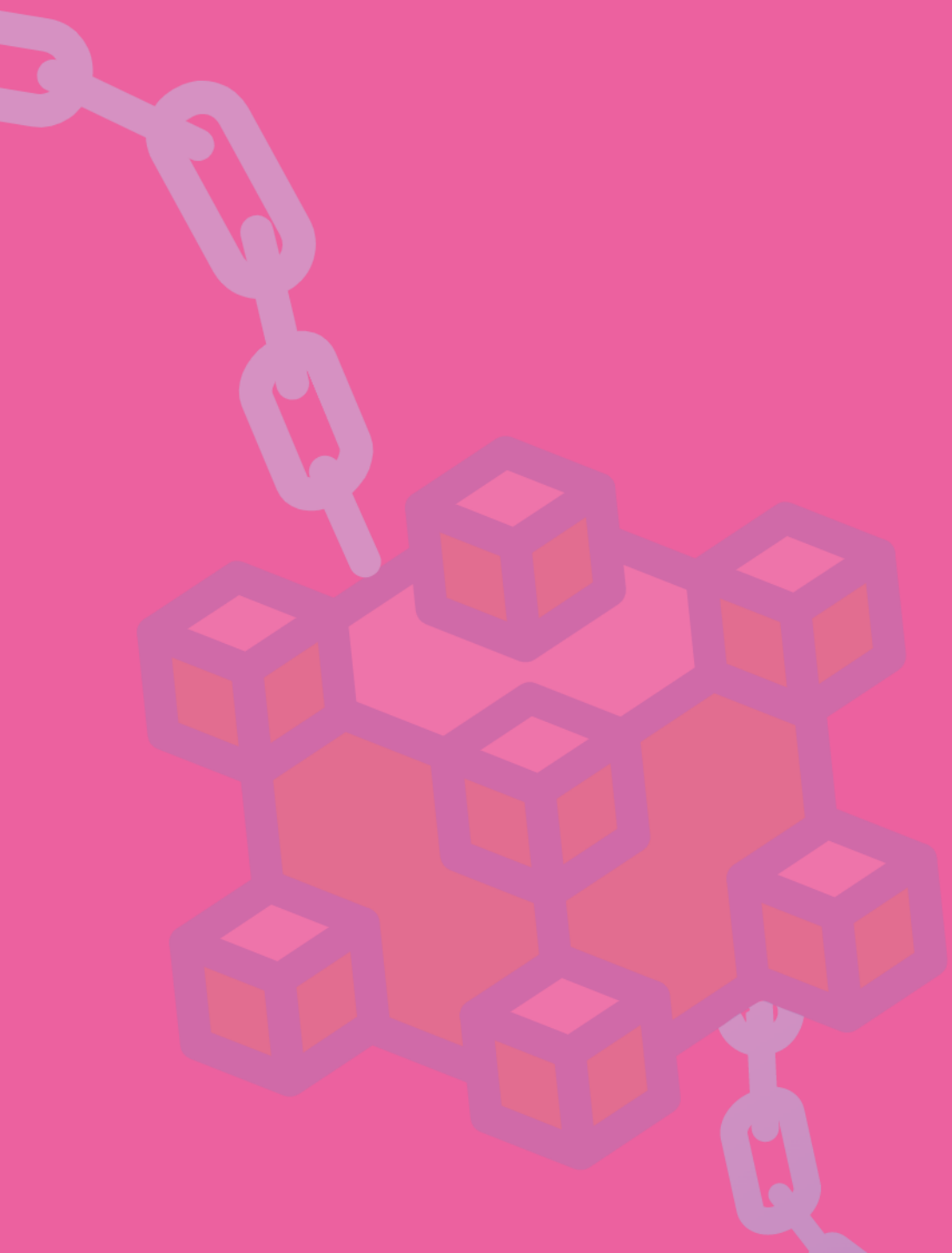
Blockchains provide an easy way to preregister studies without the need for intermediaries, while ensuring full public access to preregistration data. The fact that blockchains are immutable is particularly relevant in this context, since any change to study parameters must be logged as a new entry, guaranteeing that the full lifecycle of the research can be tracked.

Blockchains provide an easy way to preregister studies without the need for intermediaries, while ensuring full public access to preregistration data.

Examinations

Blockchain has applications for managing the logistics of widely deployed examinations. Certain examinations need to be distributed to potentially hundreds of examination centres around the world, unlocked at precisely the same time and then closed again at the end of the appointed time. Smart contracts could be used to produce a self-executing contract to release and close examinations at the appropriate times. They could also be coupled with identity systems to link only authorized students to examination papers.



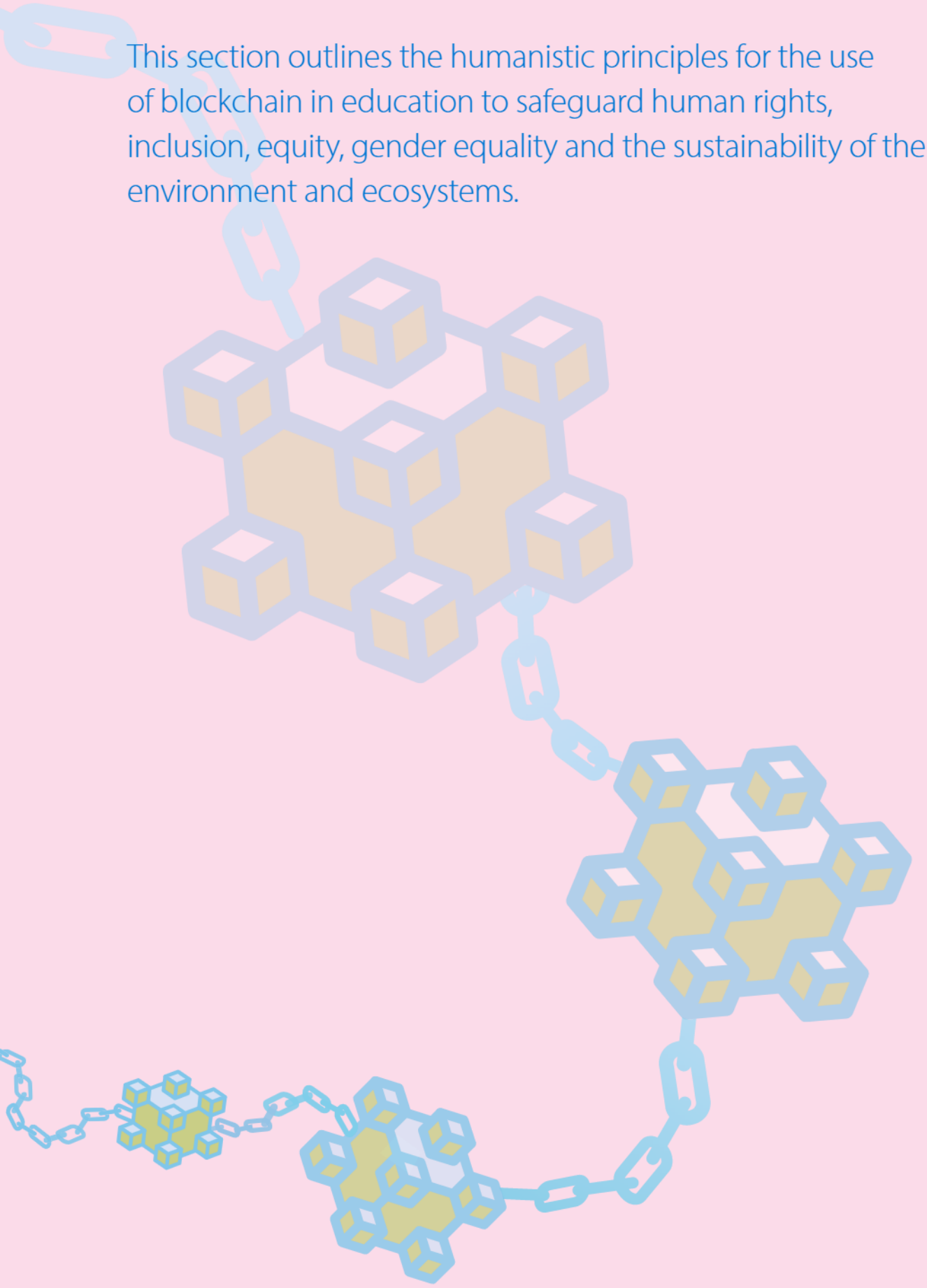


Part 4

Humanistic principles

Part 4: Humanistic principles

This section outlines the humanistic principles for the use of blockchain in education to safeguard human rights, inclusion, equity, gender equality and the sustainability of the environment and ecosystems.



Humanistic vision for the use of blockchain in education

UNESCO's humanistic vision for the use of digital technology in education is featured in the *Beijing Consensus on Artificial Intelligence in Education* (UNESCO, 2019*a*), *Recommendation on the Ethics of Artificial Intelligence* (UNESCO, 2022*b*), *AI and Education: Guidance for Policy-makers* (UNESCO, 2021) and *Guidelines for ICT in Education Policies and Masterplans* (UNESCO, 2022*a*). It should be treated as a guiding principle for the use of blockchain in education.

Humanistic vision

Any form of technology that is used in education must respect human rights and human dignity. Technological innovation should be accessible to all and used to promote inclusion, equity, gender equality, and cultural and linguistic diversity, and to support the sustainable development of the environment and ecosystems. The design, implementation and use of blockchain should respect and protect data privacy, human autonomy and human agency throughout the life cycle of the blockchain system.

Policy-makers and decision-makers must avoid technology-first approaches, known as **techno-solutionism**. Instead, they should ensure that human capacities are genuinely enhanced and human agency defended before deciding whether any technology – including blockchain – should be adopted. Furthermore, they should also consider how technology can make a positive contribution to the context in which it is potentially being introduced.

The principle of proportionality

The choice of whether to adopt blockchain systems – and if so, which type to use – should be guided by the principle of proportionality. Those who are in a position to make decisions about the introduction of blockchain systems should do their due diligence – that is, examine the benefits and drawbacks of blockchain-based solutions, especially potential trade-offs between the application of blockchain and other priorities – before embarking on this path. The decision-making process should be guided by UNESCO's humanistic vision so that the technology does not contribute to the marginalization of vulnerable groups, women and girls, people with disabilities, or cultural, linguistic and economic minority groups. In contexts where blockchain solutions may have an irreversible impact, the final decision about its form and adoption should be made by a human. Blockchain tools should only be used when their benefits clearly outweigh any associated risks and when robust scientific analysis determines that they are context-appropriate. For example, given that a permissioned blockchain network enables users to set rules about access, the validation mechanism and participation, it is more commonly chosen than other blockchain network options to support the issuing and verification of certificates, including the setting-up of identities, authentication of the issuers, verification and sharing of academic records and storage of certificate credentials in a distributed manner.

Blockchain tools should only be used when their benefits clearly outweigh any associated risks and when robust scientific analysis determines that they are context-appropriate.

Data privacy protection

When organizations are adopting blockchain in education, users' data should be collected, used, shared, archived and deleted in compliance with international or national general data protection regulations such as the General Data Protection Regulation of the European Union, General Data Protection Regulation (European Union, 2016) or Recommendation on the Ethics of Artificial Intelligence (UNESCO, 2022*b*). Data protection frameworks should be developed during the design phase of the blockchain solution to provide a valid legal basis, including societal and ethical considerations, for the collection, use and processing of personal data. The informed consent of the data owners or the guardians should be applied as the pre-condition for the collection and use of students' data. When adopting existing or developing new data protection frameworks, the framework must also cover adequate impact assessments throughout the application process to reveal its hidden impact on data privacy. Taking a privacy by design approach would help in this respect. Responsibility for the protection of data privacy and security in a blockchain system should always ultimately lie with human actors, including the designers, providers and institutional managers. To this end, the technological and institutional designs should ensure auditability and traceability of the systems.

Responsibility for the protection of data privacy and security in a blockchain system should always ultimately lie with human actors, including the designers, providers and institutional managers.

Gender equality

In 2015, the United Nations adopted gender equality as one of the core objectives of its 2030 Agenda for Sustainable Development. At UNESCO, gender equality became a priority in 2007, at the thirty-fourth session of UNESCO's General Conference. Since then, a series of action plans and guidelines were launched to foster women's empowerment around the world. To further guide UNESCO's work towards achieving gender equality in and through education, the Organization has developed the UNESCO strategy for gender equality in and through education 2019–2025 (UNESCO, 2019b). Its objectives are to strengthen education systems to be gender-transformative and promote gender equality, as well as to empower girls and women through education for a better life and future. The strategy has three thematic priorities: better data to inform action; better legal, policy and planning frameworks to advance rights; and better teaching and learning practices to empower. It also aims at closing the gender digital divide: eliminate gender inequality in access to digital devices, empower women and girls by teaching them digital skills, and increase women's and girls' self-efficacy in the study of technology and participation in related industries.

Blockchain technology may well have the potential to create value by breaking gender norms and putting power in the hands of those most in need. It promotes financial and economic inclusion and, in the process, facilitates the participation of female blockchain experts and enthusiasts. Statistically, a disproportionately large number of women and sexual minorities are unbanked (Robino et al., 2020). Some of the key systemic issues causing this inequity are lack of a government-issued ID (due to either non-existence or destruction); mobility, economic and social constraints; and financial illiteracy. Someone who has no access to government-issued ID may also have no access to healthcare services such as birth control and emergency services; be unable to obtain a driving licence, buy, sell or inherit property, or obtain a passport and voter ID; and be at risk of being trafficked. Blockchain-powered identity management systems could

provide a way to mitigate this situation. By essentially operating as a one-stop shop that can enable verifiable and indestructible digital records, it could truly make a difference. However, access to digital records is rendered moot if women and girls do not have access to digital devices or digital education to begin with. Blockchain technology can be used to democratize financial resources and facilitate the implementation of transparent loan and payment systems. Efforts are already being made in this direction. In 2015, the BitGive Foundation launched a real-time blockchain-powered tool called GiveTrack[28] to both track and donate funding for social sector project deployments. The self-sovereign identity projects by ID2020 alliance, uPort, Civic and the Sovrin Foundation[29] also focus on or fund digital identity projects. The development of both immutable and mobile certification systems in non-formal and formal learning will also contribute to women's and girls' empowerment in many regions across the world.

As an emerging technological domain, blockchain could promote gender equality by reducing the digital gender divide.

The gender gap in digital competencies is becoming wider. Women and girls are 25 per cent less likely than men and boys to know how to leverage digital technology for basic purposes, four times less likely to know how to program computers and thirteen times less likely to file for a technology patent (EQUALS and UNESCO, 2019). As an emerging technological domain, blockchain could promote gender equality by reducing the digital gender divide. A cursory review of the overall blockchain ecosystem shows a clear gender divide when it comes to employing women. The most recent survey conducted by Longhash, in December 2018, presents a picture of significant under-representation of women (Custer, 2018). Only 14.5 per cent of blockchain start-up team members were women, only 7 per cent of blockchain start-up executives were women and only 8 per cent of advisers were women. If anything, these figures indicate an existing trend of a lack of gender-based diversity in the tech sector as a whole. There is therefore room for much improvement in deciding who is involved as an active player in shaping the future of blockchain (Frizzo-Barker, 2020). Blockchain systems could advance the achievement of gender equality. It is crucial that they do not exacerbate the current gender gaps in several fields in the real world.

Gender stereotyping and biases – and the harassment and bullying that often accompanies them, including in online environments – should not be embedded in or amplified by blockchain systems. Positive role models are key for gender equality, so it is important to increase access to female mentors and role models to help learners disrupt stereotypes about the role of women in technology. Training programmes should also centre on female educators, entrepreneurs and business owners.

More effort is required to ensure that the potential for digital technologies and blockchain to contribute to achieving gender equality is fully maximized and that women's and girls' human rights and safety are protected at every stage of the blockchain system life cycle. When allied with trends and movements like Crypto Chicks, She256, Black Women Blockchain Council, Coding Matters and Global Women in Blockchain, along with renewed intent to drastically decentralize the Internet,[30] partnerships can expand opportunities for innovation that benefit women and girls by empowering them with digital skills. Governmental agencies should have dedicated funds for financing gender-responsive schemes to increase self-efficacy in the study of technology and participation in digital technology industries – including in the field of blockchain.

28 See https://www.givetrack.org/
29 See https://sovrin.org/
30 See https://www.freecodecamp.org/news/what-is-web3/

Mitigating negative impacts on the environment and ecosystems

Digital innovations, primarily driven by commercial purposes, often harm the environment and ecosystems, even if they have sustainability objectives. Blockchain can contribute to increased carbon emissions because of the energy intensity of the processes related to it – for example, mining for cryptocurrencies, also called proof of work (page 20), and the use of fossil fuels to generate the electricity that mining computers use. Even the process of issuing and registering a token on the blockchain is energy-intensive. In fact, every transaction contributes to carbon emission. One study of the carbon emission flow of the Bitcoin blockchain showed that, by 2024, Bitcoin and Ethereum, the two most popular cryptocurrencies, will use 707 and 63 units of electricity respectively per transaction, which corresponds to 530 kilograms and 46 kilograms of carbon dioxide emission per transaction (Forex Suggest, n.d.).

Urgent measures are needed to reduce or neutralize the environmental impact of blockchain systems. Some effort has already been made to achieve this. The Crypto Climate Accord (CCA), inspired by the Paris Climate Agreement, is a private sector-led initiative that commits signatories to net zero emissions by 2030 (Crypto Climate Accord, n.d.), and the Ethereum community has announced a plan to transition to a new model called Proof of Stake to eliminate the current dependency on mining, thus reducing the carbon emission flow per transaction (Ethereum, 2022).

Blockchain technologies should therefore be continuously assessed to monitor their direct and indirect environmental impact – including their carbon footprint, their energy consumption and the environmental impact of the data and computing infrastructures – throughout the system's life cycle. When choosing digital solutions, given the resource-intensive character of blockchain and in line with the principle of proportionality, actors in blockchain systems should favour energy and resource-efficient methods for their implementation, use, etc. And appropriate evidence should be defined and collected to show that a blockchain system will indeed operate in a sustainable manner within an acceptable range of energy consumption. If the environment is likely to suffer in a particular context, blockchain should not be used.

The potential of blockchain technologies and other relevant digital innovations should be leveraged to support the research, development and mass adoption of a sustainable energy and sustainable digital infrastructure.

The potential of blockchain technologies and other relevant digital innovations should be leveraged to support the research, development and mass adoption of a sustainable energy and sustainable digital infrastructure.

The technological advantages of using blockchain in the financial sector should be harnessed to encourage and promote sustainable financing for sustainable development. Furthermore, blockchain could be used in the context of finding ways to protect and regenerate the environment and ecosystems. For example, blockchain systems could be used to support the protection, monitoring and management of natural resources and mitigation of climate-related problems; and to detect pollutants and thus help implement targeted interventions to prevent and reduce pollution.

Promoting the equitable use of blockchain

An equitable and inclusive approach to the use of blockchain should be promoted to ensure that the benefits of blockchain technologies are accessible to all and respond to the specific needs of different age groups, different language groups, people with disabilities, women and girls, and disadvantaged, marginalized and vulnerable people or people in vulnerable situations. All actors should make reasonable efforts to minimize and avoid reinforcing or perpetuating discriminatory or biased applications throughout the life cycle of the system.

Digital divides should be considered and addressed to promote inclusive access to and participation in the development of the technology.

Digital divides should be considered and addressed to promote inclusive access to and participation in the development of the technology. Within countries, equity should be promoted between rural and urban areas, and among different groups of people. At the international level, open standards, open data and data-sharing should be promoted to guide the technologically advanced countries towards sharing their technology resources with the least advanced countries to ensure that the benefits are experienced by all. In this way, developed countries could help least developed countries (LDCs), landlocked developing countries (LLDCs), small and island developing states (SIDS) and conflict-affected communities overcome a lack of necessary technological infrastructure, education and skills instead of taking advantage of it.

Furthermore, digital and knowledge divides within and between countries – including in terms of access and quality of access to technology and data – should be addressed throughout a system's life cycle. While reliable connectivity to the Internet is relatively limited in several countries, there has been a growth in trading in cryptocurrencies – a key component of the blockchain – in some countries (Yiga, 2021). Over the last six years, a small number of pilot implementations of blockchain technology that do not involve cryptocurrencies have been documented in Kenya (for student identification) (Kenya Ministry of Information, Communications and Technology, 2019). There are a few examples of universities in developing countries taking steps to develop courses in blockchain technology, such as the University of Namibia (Zaaruka et al., 2021). International organizations should take on the responsibility of providing platforms for international cooperation to support open source technology development and sharing of domain knowledge.

International organizations should take on the responsibility of providing platforms for international cooperation to support open source technology development and sharing of domain knowledge.

As later adopters of digital technologies, developing countries, and especially LDCs, stand to benefit from a comprehensive effort to create and implement a common approach to the adoption of blockchain in education, such as block-powered decentralized credentialing and

certification that covers both non-formal and formal learning. In 2021, the Ministry of Education in Ethiopia, for example, announced a project to use blockchain to create educational records for 5 million students (Unlock Media, 2021). Ministers and senior officials in developing countries have emphasized the priority they would accord to developing a certification system that would allow skills training levels and academic progress to be recognized in equally effective ways, both within and outside a specific country. Digitally enabled credentials that are notarized and verified on the blockchain in a context that places equal emphasis on increasing access to tertiary education and advanced skills training may be particularly helpful for solving issues relating to the portability of credentials and interoperability of accreditation systems. The forced move to online learning because of the COVID-19 pandemic has highlighted the need to build an ICT infrastructure for education in all countries including in the least developed countries. Blockchain can provide a supportive infrastructure to meet key requirements such as decentralized Web and social apps, a rigorous identity verification system, improved mobility of students across boundaries and transparency in educational finance.

Technologies including blockchain systems can enrich cultural and creative industries, but can also lead to the dominance of a few prevalent languages and concentrate the supply of cultural content and pedagogy in the hands of only a few actors. The adoption of blockchain has potential negative implications for the diversity of languages, cultural expressions and pedagogical methodologies. When introducing blockchain technologies in LDCs, cultural and linguistic diversity and inclusiveness should be protected. This may be done by promoting local groups' active participation in the design, deployment, and monitoring and evaluation of blockchain systems, regardless of race, age, language, religion, ethnic origin, social origin, economic or social background, or disability. In line with the principle of proportionality, the choices of technological solutions should be protected, and the use of local languages and expressions or local cultural experiences should not be restricted by the use of blockchain.

Looking forward

Blockchain is a reliable technology for identity verification and management, which is a key consideration in the administration of education, learning and training at all levels. It can be deployed in support of a decentralized educational web, where dependence on proprietary services providers is minimized in compliance with data privacy protection regulations. The emerging usages are particularly important in the present context as governments have been forced to move education and training online, and they will also facilitate the verification of credentials of both learners and issuing institutions for cross-border studies and mobility. The potential of blockchain to make payments for educational services and fees more transparent has been validated by several institutions and organizations to date. Some countries have implemented blockchain projects in education despite limited connectivity, which promotes the equitable use of blockchain and digital equality in general. There is scope for increasing the participation of female professionals in implementing blockchain technology in education, especially when gender bias in identity verification and management is a concern. Future implementations of blockchain technology will need to be premised on minimizing or neutralizing its contribution to global carbon emissions and should be sensitive to the sustainability of the environment and ecosystems.

References

Adhami, S., Giudici, G. and Martinazzi, S. 2018. Why do businesses go crypto?: an empirical analysis of initial coin offerings. *Journal of Economics and Business,* Vol. 100, pp. 64–75. Available at: https://doi.org/10.1016/j.jeconbus.2018.04.001 (Accessed 4 August 2022.)

Allessie, D., Sobolewski, M. and Vaccari, L. 2019. *Blockchain for Digital Government: An Assessment of Pioneering Implementations in Public Services*. F. Pignatelli (ed.). Brussels, European Union. Available at: https://doi.org/10.2760/942739 (Accessed 4 August 2022.)

Atzori, M. 2017. Blockchain technology and decentralized governance: is the state still necessary? *Journal of Governance and Regulation*, Vol. 6, No. 1, pp. 45–62. Available at: https://doi.org/10.22495/jgr_v6_i1_p5 (Accessed 4 August 2022.)

Back, A., Corallo, M., Dashjr, L., Friedenbach, M., Maxwell, G., Miller, A., Poelstra, A., Timón, J. and Wuille, P. 2014. *Enabling Blockchain Innovations with Pegged Sidechains*. Victoria, Blockstream Corporation. Available at: https://www.blockstream.com/sidechains.pdf (Accessed 4 August 2022.)

Baldi, M. and Chiaraluce, F. 2017. A trusted cryptocurrency scheme for secure and verifiable digital transactions. *First Monday*, Vol. 22, No. 11. Available at: https://doi.org/10.5210/fm.v22i11.6981 (Accessed 4 August 2022.)

Bayer, D., Haber, S. and Stornetta, W. S. 1993. Improving the efficiency and reliability of digital time-stamping. R. Capocelli, A. De Santis and U. Vaccaro (eds), *Sequences II*. New York, Springer, pp. 329-334. Available at: https://doi.org/10.1007/978-1-4613-9323-8_24 (Accessed 4 August 2022.)

Boucher, P., Nascimento, S. and Kritikos, M. 2017. *How Blockchain Technology Could Change Our Lives*. Brussels, European Union. Available at: https://doi.org/10.2861/926645 (Accessed 4 August 2022.)

Buterin, V. 2014. Ether sale: a statistical overview. *Ethereum Blog* [Online]. Available at: https://blog.ethereum.org/2014/08/08/ether-sale-a-statistical-overview (Accessed 4 August 2022.)

Cai, W., Wang, Z., Ernst, J. B., Hong, Z., Feng, C. and Leung, V. C. 2018. Decentralized applications: the blockchain-empowered software system. *IEEE Access*, Vol. 6, pp. 53019–53033. Available at: https://doi.org/10.1109/ACCESS.2018.2870644 (Accessed 4 August 2022.)

Chopra U. K., Rathore A. K. and Pandey R. 2020. Rendering blockchain immutability in Chatserver: a node.js approach. P. Kapur, G. Singh, Y. Klochkov and U. Kumar (eds), *Decision Analytics Applications in Industry: Asset Analytics (Performance and Safety Management)*. Singapore, Springer, pp. 147-155. Available at: https://doi.org/10.1007/978-981-15-3643-4_10 (Accessed 4 August 2022.)

Clements, K., West, R. E. and Hunsaker, E. 2020. Getting started with open badges and open microcredentials. *The International Review of Research in Open and Distributed Learning*, Vol. 21, No. 1. Athabasca, Athabasca University Press, pp. 154–172. Available at: https://doi.org/10.19173/irrodl.v21i1.4529 (Accessed 4 August 2022.)

CHEA and UNESCO. 2009. *Toward Effective Practice: Discouraging Degree Mills in Higher Education*. Washington, DC/Paris, Council for Higher Education Accreditation (CHEA)/UNESCO. Available at: https://unesdoc.unesco.org/ark:/48223/pf0000183247 (Accessed 4 August 2022.)

Chrono.tech. (2019, January 17). What is a decentralised application and how it works. Chrono.tech Blog [Online]. Available at: https://blog.chronobank.io/what-is-a-decentralised-application-and-how-it-works-625514e207eb (Accessed 23 November 2022.)

Crypto Climate Accord. n.d. *Crypto Climate Accord* [Online]. Available at: https://cryptoclimate.org/accord/ (Accessed 4 August 2022.)

Custer, C. 2018. Blockchain's gender divide: a data story [Online]. Longhash. Available at: https://www.longhash.com/en/news/2337/Blockchain's-Gender-Divide:-A-Data-Story (Accessed 4 August 2022.)

Deloitte. 2019. *Deloitte's 2019 Blockchain Global Survey: Blockchain Gets Down to Business*. Hermitage, Deloitte Development LLC. Available at: https://www2.deloitte.com/content/dam/Deloitte/se/Documents/risk/DI_2019-global-blockchain-survey.pdf (Accessed 4 August 2022.)

Economist. 2015. The trust machine. *The Economist*, Vol. 417, No. 8962. Available at: https://www.economist.com/leaders/2015/10/31/the-trust-machine (Accessed 4 August 2022.)

Eisenhardt, K. M. 1989. Agency theory: an assessment and review. *Academy of Management Review*, Vol. 14, No. 1, pp. 57–74. Available at: https://doi.org/10.5465/amr.1989.4279003 (Accessed 4 August 2022.)

EQUALS and UNESCO. 2019. *I'd Blush If I Could: Closing Gender Divides in Digital Skills Through Education*. Geneva/Paris, EQUALS/UNESCO. Available at: https://unesdoc.unesco.org/ark:/48223/pf0000367416 (Accessed 4 August 2022.)

Ethereum. 2022. *The beacon chain* [Online]. Available at: https://ethereum.org/en/upgrades/beacon-chain (Accessed 4 August 2022.)

European Union. 2016. *General Data Protection Regulation*. Brussels, European Union. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679 (Accessed 4 August 2022.)

Ferdous, M. S., Chowdhury, F. and Alassafi, M. O. 2019. In search of self-sovereign identity leveraging blockchain technology. *IEEE Access*, Vol. 7, pp. 103059–103079. Available at: https://doi.org/10.1109/ACCESS.2019.2931173 (Accessed 4 August 2022.)

Forex Suggest. n.d. *Global impact of crypto trading* [Online]. Available at: https://forexsuggest.com/global-impact-of-crypto-trading (Accessed 4 August 2022.)

Friedlob, G. T. and Plewa, F. J. 1996. *Understanding Balance Sheets*. Hoboken, Wiley.

Frizzo-Barker, J. A. 2020. Women in blockchain: discourse & practice in the co-construction of gender and emerging technologies. *AoIR Selected Papers of Internet Research*. Chicago, Association of Internet Researchers. Available at: https://doi.org/10.5210/spir.v2020i0.11215 (Accessed 4 August 2022.)

Galen, D., Brand, N., Boucherie, L., Davis, R., Do, N., El-Baz, B., Kimura, I., Wharton, K. and Lee, J. 2018. *Blockchain for Social Impact: Moving Beyond the Hype*. Stanford, Stanford Graduate School of Business. Available at: https://www.gsb.stanford.edu/sites/gsb/files/publication-pdf/study-blockchain-impact-moving-beyond-hype.pdf (Accessed 4 August 2022.)

Giralt, V. and De Leeuw, H. 2013. The future of digital student data portability: The Groningen Declaration. *EUNIS 2013 Congress Proceedings*, Vol. 1, No. 1. Riga, Riga Technical University. Available at: https://doi.org/10.7250/eunis.2013.052 (Accessed 4 August 2022.)

GIZ. 2019. *Blockchain Potentials and Limitations for Selected Climate Policy Instruments*. Bonn, Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH. Available at: https://www.climateledger.org/resources/Blockchain-Potentials-Climate-Policy_2019.pdf (Accessed 4 August 2022.)

Government of Canada. 2011. *Federating identity management in the Government of Canada: a backgrounder* [Online]. Available at: https://www.canada.ca/en/government/system/digital-government/online-security-privacy/security-identity-management/federating-identity-management-government-canada-backgrounder.html (Accessed 4 August 2022.)

Grech, A. and Camilleri, A. F. 2017. *Blockchain in Education*. Brussels, European Commission. Available at: https://doi.org/10.2760/60649 (Accessed 4 August 2022.)

Grech, A., Sood, I., and Ariño L. 2021. Blockchain, self-sovereign identity and digital credentials: promise versus praxis in education. *Frontiers in Blockchain, Vol. 4.* Available at: https://doi.org/10.3389/fbloc.2021.616779 (Accessed 4 August 2022.)

Gupta, V. 2017. A brief history of Blockchain. *HBR's 10 Must Reads on AI, Analytics, and the New Machine Age*. Cambridge, Harvard Business Review. Available at: https://hbr.org/2017/02/a-brief-history-of-blockchain (Accessed 4 August 2022.)

Hanson, R., Reeson, A. and Staples, M. 2017. *Distributed Ledgers: Scenarios for the Australian Economy Over the Coming Decades*. Canberra, Commonwealth Scientific and Industrial Research Organisation. Available at: https://doi.org/10.4225/08/597b89ba1a94e (Accessed 4 August 2022.)

Hassan, S. and De Filippi, P. 2020. Decentralised autonomous organisation: glossary of distributed technologies. *Internet Policy Review*, Vol. 10, No. 2. Available at: https://doi.org/10.14763/2021.2.1556 (Accessed 4 August 2022.)

Hasselgren, A., Kralevska, K., Gligoroski, D., Pedersen, S. A. and Faxvaag, A. 2020. Blockchain in healthcare and health sciences: a scoping review. *International Journal of Medical Informatics*, Vol. 134, No. 104040. Available at: https://doi.org/10.1016/j.ijmedinf.2019.104040 (Accessed 4 August 2022.)

Heyman, T., Moors, P. and Storms, G. 2016. On the cost of knowledge: evaluating the boycott against Elsevier. *Frontiers in Research Metrics and Analytics*, Vol. 1, No. 7. Available at: http://dx.doi.org/10.3389/frma.2016.00007 (Accessed 4 August 2022.)

Hileman, G. and Rauchs, M. 2017. *Global Cryptocurrency Benchmarking Study*. Cambridge, University of Cambridge. Available at: https://www.jbs.cam.ac.uk/faculty-research/centres/alternative-finance/publications/global-cryptocurrency (Accessed 4 August 2022.)

Hochstein, M. 2018. *Don't use a blockchain unless you really need one* [Online]. New York, Coindesk. Available at: https://www.coindesk.com/dont-use-blockchain-unless-really-need-one (Accessed 4 August 2022.)

Houben, R. and Snyers, A. 2018. *Cryptocurrencies and Blockchain: Legal Context and Implications for Financial Crime, Money Laundering and Tax Evasion*. Brussels, European Union. Available at: https://doi.org/10.2861/263175 (Accessed 4 August 2022.)

Iansiti, M. and Lakhani, K. 2017. The truth about blockchain. *Blockchain: The Insights You Need from Harvard Business Review*. Cambridge, Harvard Business Review. Available at: https://hbr.org/2017/01/the-truth-about-blockchain (Accessed 4 August 2022.)

ISO. 2017. *Conformity assessment – Requirements for Accreditation Bodies Accrediting Conformity Assessment Bodies*. Geneva, International Organization for Standardization (ISO). Available at: https://www.iso.org/standard/67198.html (Accessed 4 August 2022.)

Johnstone, D. A., Yilmaz, S. O., Kandah, J., Bentenitis, N., Hashemi, F., Gross, R., Wilkinson, S. and Mason, S. (2014, June 14). The general theory of decentralized applications, dapps: the emerging wave of decentralized applications [Online]. Medium. Available at: https://djohnstonec.medium.com/the-general-theory-of-decentralized-applications-dapps-4901877d368 (Accessed 23 November 2022.)

Kastelein, R. 2017. *What Initial Coin Offerings Are, and Why VC Firms Care*. Cambridge, Harvard Business Review. Available at: https://hbr.org/2017/03/what-initial-coin-offerings-are-and-why-vc-firms-care (Accessed 4 August 2022.)

Kenya Ministry of Information, Communications and Technology. 2019. *Emerging Digital Technologies for Kenya Exploration & Analysis*. Nairobi, Kenya Ministry of Information, Communications and Technology (ICT). Available at: https://www.ict.go.ke/blockchain.pdf (Accessed 4 August 2022.)

Krause, S., Natarajan, H. and Gradstein, H. 2017. *Distributed Ledger Technology (DLT) and Blockchain*. Washington, DC, International Bank for Reconstruction and Development / World Bank. Available at: http://documents.worldbank.org/curated/en/177911513714062215/Distributed-Ledger-Technology-DLT-and-blockchain (Accessed 4 August 2022.)

Lemoie, K. and Soares, L. 2020. *Connected Impact: Unlocking Education and Workforce Opportunity Through Blockchain*. Washington, DC, American Council on Education (ACE). Available at: https://www.acenet.edu/Documents/ACE-Education-Blockchain-Initiative-Connected-Impact-June2020.pdf (Accessed 4 August 2022.)

Lewis, A. 2017. *A gentle introduction to self-sovereign identity* [Online]. Singapore, Bits on Blocks. Available at: https://bitsonblocks.net/2017/05/17/gentle-introduction-self-sovereign-identity (Accessed 4 August 2022.)

Lilic, J. 2015. *uPort; A Glimpse into a Next Generation Self Sovereign Identity System* [Online]. Sunnyvale, LinkedIn. Available at: https://www.linkedin.com/pulse/uport-glimpse-next-generation-self-sovereign-identity-john-lilic (Accessed 4 August 2022.)

Lin, I.-C. and Liao, T.-C. 2017. A survey of blockchain security issues and challenges. *International Journal of Network Security*, Vol. 19, pp. 653–659. Available at: https://doi.org/10.6633/IJNS.201709.19(5).01 (Accessed 4 August 2022.)

Merkle. R. 1979. *Secrecy, Authentication, and Public Key Systems*. Palo Alto, Stanford University. Available at: https://nakamotoinstitute.org/static/docs/secrecy-authentication-and-public-key-systems.pdf (Accessed 4 August 2022.)

Nakamoto, S. 2008. *Bitcoin: a peer-to-peer electronic cash system* [Online]. Available at: https://bitcoin.org/bitcoin.pdf (Accessed 4 August 2022.)

Nascimento, S. (ed.), Pólvora, A. (ed.), Anderberg, A., Andonova, E., Bellia, M., Calès, L., Inamorato dos Santos, A., Kounelis, I., Nai Fovino, I., Petracco Giudici, M., Papanagiotou, E., Sobolewski, M., Rossetti, F. and Spirito, L. 2019. *Blockchain Now and Tomorrow: Assessing Multidimensional Impacts of Distributed Ledger Technologies*. Luxembourg, Publications Office of the European Union. Available at: https://doi.org/10.2760/901029 (Accessed 4 August 2022.)

Ojetunde, B., Shibata, N. and Gao, J. 2017. Securing link state routing for wireless networks against byzantine attacks: A monitoring approach. *IEEE 41st Annual Computer Software and Applications Conference (COMPSAC) proceedings*, Vol. 1. New York, Institute of Electrical and Electronics Engineers (IEEE), pp. 596–601. Available at: https://doi.org/10.1109/COMPSAC.2017.208 (Accessed 4 August 2022.)

Porat, A., Pratap, A., Shah, P. and Adkar, V. 2017. *Blockchain Consensus: An Analysis of Proof-of-Work and Its Applications*. Stanford, Stanford University. Available at: https://www.scs.stanford.edu/17au-cs244b/labs/projects/porat_pratap_shah_adkar.pdf (Accessed 4 August 2022.)

Raj, S., Upadhya, P. T. and Pathak, S. 2020. A study of distributed file systems. *International Research Journal of Engineering and Technology (IRJET)*, Vol. 7, No. 5, pp. 5280-5285. Available at: https://www.irjet.net/archives/V7/i5/IRJET-V7I51013.pdf (Accessed 4 August 2022.)

Rauchhaus, R. W. 2009. Principal-agent problems in humanitarian intervention: Moral hazards, adverse selection, and the commitment dilemma. *International Studies Quarterly,* Vol. 53, No. 4, pp. 871–884. Available at: https://doi.org/10.1111/j.1468-2478.2009.00560.x (Accessed 4 August 2022.)

Rennock, M. J., Cohn, A. and Butcher, J. R. 2018. Blockchain technology and regulatory investigations. *Practical Law Litigation*. London, Thomson Reuters. Available at: https://www.steptoe.com/images/content/1/7/v3/171269/LIT-FebMar18-FeatureBlockchain.pdf (Accessed 4 August 2022.)

Resei, C., Friedl, C., Staubitz, T. and Rohloff, T. 2019. *Micro-credentials in EU and Global*. Graz, CORSHIP.eu. Available at: https://www.corship.eu/wp-content/uploads/2019/07/Corship-R1.1c_micro-credentials.pdf (Accessed 4 August 2022.)

Robino, C., Trivelli, C., Villanueva, C., Sachetti, F. C., Walbey, H., Martinez, L., and Marincioni, M. 2020. *Financial Inclusion for Women: A Way Forward*. G20 Insights. Available at: https://www.g20-insights.org/policy_briefs/financial-inclusion-for-women-a-way-forward/ (Accessed 4 August 2022.)

Scott, B. 2015. *Visions of a Techno-Leviathan: The Politics of the Bitcoin Blockchain*. Berlin, Rosa-Luxembourg-Stiftung. Available at: http://www.rosalux.de/publication/41131/visions-of-a-technoleviathan.html (Accessed 4 August 2022.)

Seeber, M. and Balkwill, R. 2007. *Managing Intellectual Property in the Book Publishing Industry: A Business-oriented Information Booklet*. Geneva, World Intellectual Property Organization (WIPO). Available at: https://www.wipo.int/edocs/pubdocs/en/copyright/868/wipo_pub_868.pdf (Accessed 4 August 2022.)

Seifert, R. 2020. Digital identities–self-sovereignty and blockchain are the keys to success. *Network Security*, Vol. 2020, No. 11. London, Mark Allen Group, pp. 17–19. Available at: https://doi.org/10.1016/S1353-4858(20)30131-8 (Accessed 4 August 2022.)

Shermin, V. 2017. Disrupting governance with blockchains and smart contracts. *Strategic Change*, Vol. 26, No. 5, pp. 499–509. Available at: https://doi.org/10.1002/jsc.2150 (Accessed 4 August 2022.)

Smolenski, N. 2020. *Digital credentials and the pursuit of self-sovereignty* [Video]. San Bruno, YouTube. Available at: https://youtu.be/Os859aPLWNQ (Accessed 4 August 2022.)

Strehl, F., Reisinger, S. and Kalatschan, M. 2007. Funding systems and their effects on higher education systems. *OECD Education Working Papers*, No. 6. Paris, OECD Publishing. Available at: https://www.oecd-ilibrary.org/education/funding-systems-and-their-effects-on-higher-education-systems_220244801417 (Accessed 4 August 2022.)

Szabo, N. 1996. Smart contracts: building blocks for digital markets. *EXTROPY: The Journal of Transhumanist Thought*, No. 16. Available at: https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html (Accessed 4 August 2022.)

Tapscott, D. and Tapscott, A. 2016. *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World*. London, Penguin Books.

Turkanović, M., Hölbl, M., Košič, K., Heričko, M. and Kamišalić, A. 2018. EduCTX: A blockchain-based higher education credit platform. *IEEE Access*, Vol. 6. New York, Institute of Electrical and Electronics Engineers (IEEE), pp. 5112–5127. Available at: https://doi.org/10.1109/ACCESS.2018.2789929 (Accessed 4 August 2022.)

UK Government Chief Scientific Adviser. 2016. *Distributed Ledger Technology: Beyond Blockchain*. London, Government Office for Science. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf (Accessed 4 August 2022.)

UNESCO. 2019*a*. *Beijing Consensus on Artificial Intelligence and Education*. Paris, UNESCO. Available at: https://unesdoc.unesco.org/ark:/48223/pf0000368303 (Accessed 4 August 2022.)

———. 2019*b*. *From Access to Empowerment: UNESCO Strategy for Gender Equality in and Through Education 2019-2025*. Paris, UNESCO. Available at: https://unesdoc.unesco.org/ark:/48223/pf0000369000 (Accessed 4 August 2022.)

———. 2019*c*. *UNESCO Priority Gender Equality Action Plan: 2014-2021, 2019 revision*. Paris, UNESCO. Available at: https://unesdoc.unesco.org/ark:/48223/pf0000370905 (Accessed 4 August 2022.)

———. 2021. *AI and Education: Guidance for Policy-makers*. Paris, UNESCO. Available at https://unesdoc.unesco.org/ark:/48223/pf0000376709 (Accessed 4 August 2022.)

———. 2022a. *Guidelines for ICT in Education Policies and Masterplans*. Paris, UNESCO. Available at: https://unesdoc.unesco.org/ark:/48223/pf0000380926 (Accessed 4 August 2022.)

———. 2022*b*. *Recommendation on the Ethics of Artificial Intelligence*. Paris, UNESCO. Available at: https://unesdoc.unesco.org/ark:/48223/pf0000381137 (Accessed 4 August 2022.)

Unlock Media. 2021. *Ethiopian Education Ministry signs agreement with Blockchain IOHK for blockchain based national student ID* [Online]. Unlock Media. Available at: https://www.unlock-bc.com/news/2021-05-01/ethiopian-education-ministry-signs-agreement-with-blockchain-iohk-for-blockchain-based-national-student-id (Accessed 4 August 2022.)

Warburg, B. 2016. *How the blockchain will radically transform the economy* [Video]. New York, TED. Available at: https://www.ted.com/talks/bettina_warburg_how_the_blockchain_will_radically_transform_the_economy/transcript (Accessed 4 August 2022.)

Winjum, J. O. 1971. Accounting and the rise of capitalism: an accountant's view. *Journal of Accounting Research*, Vol. 9, No. 2, pp. 333–350. Available at: https://doi.org/10.2307/2489937 (Accessed 4 August 2022.)

Wu, J. and Tran, N. K. 2018. Application of blockchain technology in sustainable energy systems: an overview. *Sustainability*, Vol. 10, No. 9, p. 3067. Available at: https://doi.org/10.3390/su10093067 (Accessed 4 August 2022.)

Wüst, K. and Gervais, A. 2018. Do you need a blockchain? *2018 Crypto Valley Conference on Blockchain Technology (CVCBT)*. New York, Institute of Electrical and Electronics Engineers (IEEE), pp. 45–54. Available at: https://doi.org/10.1109/CVCBT.2018.00011 (Accessed 4 August 2022.)

Yaga, D., Mell, P., Roby, N. and Scarfone, K. 2018. *Blockchain Technology Overview*. Washington, DC, U.S. Department of Commerce. Available at: https://doi.org/10.6028/NIST.IR.8202 (Accessed 4 August 2022.)

Yamey, B. S. 1949. Scientific bookkeeping and the rise of capitalism. *The Economic History Review*, Vol. 1, Nos. 2–3, pp. 99–113. Available at: https://doi.org/10.2307/2589824 (Accessed 4 August 2022.)

Yiga, E. 2021. *Crypto-currency adoption in Africa: The ups and downs* [Online]. African Renewal. Available at: https://www.un.org/africarenewal/magazine/june-2021/crypto-currency-adoption-africa-ups-and-downs (Accessed 4 August 2022.)

Zaaruka, B., Tjeriko, C., and Shilongo, H. 2021. *Paper #1: Overview of Digital Transformation in Namibia.* Windhoek, Bank of Namibia. Available at: https://www.bon.com.na/CMSTemplates/Bon/Files/bon.com.na/c7/c7dc8056-584a-4558-a5a3-2d20c7f73279.pdf (Accessed 4 August 2022.)

Zwitter, A. and Boisse-Despiaux, M. 2018. Blockchain for humanitarian action and development aid. *Journal of International Humanitarian Action*, Vol. 3, No. 1, pp. 1–7. Available at: https://doi.org/10.1186/s41018-018-0044-5 (Accessed 4 August 2022.)

Glossary

Architecture

In computer networks, architecture refers to how tasks are shared among the computers on the network. There are two commonly used models: client-server and peer-to-peer. While the client-server architecture is centred on a central server that accepts or rejects the requests from the other computers on the network, in a peer-to-peer architecture this task is allocated equally among all the computers on the network. Blockchain uses the peer-to-peer network architecture, also known as distributed architecture.

Blockchain protocol

Blockchain protocols are also known as consensus protocols or mechanisms and can be defined as a set of rules that ensure the synchronization of all the nodes within a network by providing a commonly agreed-upon method to bring all the nodes into agreement about the correct version of information on the chain. A number of different consensus protocols can be used on a blockchain based on the type of blockchain used and the participants involved.

Centralized control

Centralized control is a situation in which one component is designated as a central power that controls and manages all the other components. Centrally managed systems such as centralized databases are often located in a central location, which can be a server or a mainframe computer. Some of the most common examples of centralized control are conventional databases where all the information is kept and controlled by a centralized system that is usually owned by powerful conglomerates (e.g. Facebook, Google, NASDAQ, universities).

Client-server-network architecture

The client-server network architecture is a centralized computing model in which a central server controls the resources and data flow across the devices on the network. Every computer serves as either a client or a server. Servers are powerful computers dedicated to managing memory space and resources, whereas clients are the participating computers that rely on the servers for their resources.

Credential

Electronic or paper-based representation of the different types of learning acquired by an individual. A paper-based representation is most commonly referred to as a transcript.

Cryptography

Cryptography can be defined as the mathematical process used to secure information by encrypting it in the form of code to protect it from third-party unauthorized access. In blockchain, cryptography is used in two ways: first, by using a combination of public and private keys to secure individual ownership, and second, by using hashing mechanisms to make the information on the blockchain secure and immutable.

dApp

dApp is an abbreviation for decentralized application. In essence, dApps function in the same way as traditional smartphone applications; however, instead of running on a centralized network, they run on a peer-to-peer network of computers (or blockchain). dApps connect users and providers directly without the need for intermediaries.

Database

A database is an electronic collection of information organized in a single location to be shared with or accessed by recognized users. The electronic system also allows a set of users to update or modify the information stored in the database.

Decentralization

Decentralization is the transfer of power from a central authority to individual users. Blockchain enables the creation of a decentralized arrangement whereby data and information are held not by a single entity or a third party but in a public ledger that is managed by a consensus mechanism and distributed techniques in a peer-to-peer network containing multiple nodes.

Digital certificate

Digital certificates are issued by a third-party certification authority (CA), which can be government agencies or industry-based councils such as CASC (Certificate Authority Security Council). They function in the same way as identification documents such as a driving licence. A digital certificate binds a digital signature to a particular person or people.

Digital signature

A digital signature is a binary digital code attached to an electronic document to identify, verify and authenticate its signatory. It is similar to an 'electronic fingerprint' and ensures non-repudiation – that is, the sender cannot deny sending the message. Digital signatures use a standard cryptographic technique called public key infrastructure (PKI) to provide the highest-possible levels of security and universal acceptance. A private key, held by the owner and used for decryption, and a public key, for public sharing and used for encryption, form the basic tenets of this infrastructure.

Diploma/degree mills

Diploma mills are institutions that indulge in unethical practices of producing and issuing a vast amount of degrees or diplomas for a high fee and use inadequate assessment mechanisms, which are often unregulated. They contribute directly to low-quality education, no academic recognition and large-scale fraud.

Distributed ledger

A distributed ledger can be defined as a digital record of ownership that is replicated, synchronized and shared across multiple users, thus eliminating the need for an intermediary or administrator.

ENIC-NARIC

ENIC stands for European Network of Information Centres in the European Region. NARIC stands for National Academic Recognition Information Centres in the European Union. The Council of Europe and UNESCO founded the network in 1994 with the aim of developing joint policy and practice in all European countries for the recognition of qualifications throughout Europe. It also provided information on the recognition of non-European degrees and diplomas as well as opportunities for studying abroad. The NARIC network is similar to the ENIC network except that it is supported by the European Commission. The two networks collaborate very closely in conducting research and providing relevant information to concerned stakeholders.

Immutability

Immutability means the property of remaining unchanged over time. In a blockchain network, once information is stored in the blockchain, it cannot be modified. This is due to the distributed nature of blockchain, whereby the data are replicated over a number of nodes, thus creating multiple copies of the data blocks. Hashing, which is the process of assigning a sequential and unique hash to every block of data in a blockchain, also ensures immutability in a blockchain network.

Intra-convertible currency

A currency that can be freely exchanged (bought or sold) for another currency without any governmental restrictions.

Network

In computing, a network can be defined as a group of two or more devices that are linked to share resources, exchange files or allow electronic communications, including the sharing of data or other resources.

Nodes

A node is any computer or device that forms a part of a computer network. In a blockchain network, every node contributes to the basic infrastructure of the network by acting as both resource and validator. Every node is considered equal, but it is possible for different nodes to have different roles at different times. Every node holds a replicated copy of the ledger with varying roles such as issuing, verifying, receiving, informing, etc. Nodes are also responsible for implementing the consensus mechanisms that govern a particular blockchain.

Off-chain

Off-chain refers to activities that do not take place on the blockchain. Off-chain mechanisms can be employed along with on-chain mechanisms to complement each other.

Open public ledgers

Blockchain is usually referred to as an open public ledger, which simply means that all the information on it is open to the network participants. Bitcoin is an open public ledger. Permissions can be used to make blockchains private.

Peer-to-peer network

A peer-to-peer (P2P) network can be defined as a network with a distributed architecture whereby the participant computers, also known as peers or nodes, have equal access, authority and privileges and can communicate directly with each other. A P2P network is a decentralized operation in which peers serve as both suppliers and consumers of the available resources. In a blockchain network, the nodes may have different roles, but the ledger is equally replicated on every single node.

Permissions

Permissions in a blockchain have two roles: they define the kind of blockchain used and define roles for the nodes within a blockchain. On a micro level, blockchains are defined as permissioned or permissionless. There are three major types of permissions: read (who can see the transactions), write (who can generate transactions) and commit (who can update the ledger). On a macro level, they are defined as open or closed.

PKI

The purpose of PKI, or public key infrastructure, is to facilitate the secure transfer of information over electronic media for a wide range of activities. PKI uses public key cryptography wherein a mathematically linked pair of keys known as a public key (for public use) and private key (only for the owner's use) perform the function of encryption and decryption respectively.

PKI certificate

A PKI certificate is a digitally signed certificate that employs PKI for verification and authentication. The certificate is a trusted digital identity, used to identify and authenticate users, servers or things when communicating over untrusted networks. Public keys are stored on digital certificates to share them securely while using a private key to access the certificate. A PKI certificate is also called a digital certificate.

Records

A record is a piece of evidence that provides objective permanent proof of events, activities or results. In the context of blockchain, the most common records stored are transactions related to assets, smart contracts or digital signatures/certificates.

Shared or private blockchain

A shared blockchain (also called a permissionless blockchain) is a public network that is open to any participant and has set rules in place. These rules are used in the verification process for every transaction. Participants in a shared blockchain can remain anonymous and still look at the transactions.

A private blockchain (also called a permissioned blockchain) is a private network in which users set rules about access, the consensus mechanism, governance, participation, etc. In this type of network, a ledger administrator gives participants certain permissions. For example, participants do not have viewing access to all the transactions. Instead, they can only see transactions that they have been given permission to view.

Smart contracts

A smart contract is an auto-executing virtual agreement that is written in programming code with conditions predefined into it on a blockchain. Such agreements can be between two people (P2P), person-to-organization (P2O) or person-to-machine (P2M).

Time-stamped

Every block of data on a blockchain network is assigned the date and time of its issue. Time stamps are proof of 'what' has happened 'when' in a blockchain, thus ensuring that the blocks of data are connected in a sequential manner.

Trust

Trust is one of the key principles of blockchain technology. In conventional centralized environments, we establish blind trust without any pre-conditions, such as assuming that our financial information is safe with the banks. In a decentralized system, trust is established using mathematical and cryptographical techniques that are further reimposed via consensus between all the nodes involved.

Wallet

A digital wallet can serve as a data and information repository in which its owner can securely store, manage and use the contents. The content of a wallet can vary from education credentials to personal banking information. In the blockchain context, wallets were initially used to store the digital credentials for Bitcoin holdings and to enable owners of Bitcoins to access (and spend) them. In PKI, a wallet is simply a combination of the cryptographically linked public and private keys.

unesco
United Nations
Educational, Scientific
and Cultural Organization

Commonwealth of Learning

Education and blockchain

Blockchain is a verification infrastructure that offers a solution to the problem of how to verify digital identity.

This publication is aimed at policy-makers in education who have an interest in understanding the affordances of blockchain technology to the education sector.

Exploratory exercises with blockchain demonstrate that it is already possible to deploy the technology to cover credentialing and certification in both formal and non-formal learning. This publication presents the essential concepts and uses in a style accessible to policy-makers and experts who are not necessarily specialists in the area but need a quick introduction into the subject.

9 789231 005657

4 QUALITY EDUCATION

Sustainable Development Goals