11 Blockchain for Education: A New Credentialing Ecosystem

Natalie Smolenski
Hyland Credentials, United States

Blockchain technology is revolutionising the world of financial services by providing distributed networks for transacting digital currencies. This same digital infrastructure can be used to verify important claims and credentials, including educational and academic records. Within education, significant momentum exists worldwide to use blockchain technology for issuing, sharing, and verifying educational experiences and qualifications. This chapter provides an overview of blockchain technology and spotlights its use in education to create portable, interoperable, user-controlled digital credentials. These verifiable claims constitute a form of social currency that empowers students and workers with the ability to transfer their competencies and skills anywhere in the world they choose to live, study, and work.

Introduction

This chapter demonstrates the value of blockchain technology – a new digital verification infrastructure – for education. In short, blockchain technology enables anyone to validate claims about an individual or institution, including their characteristics and qualifications, and to do this instantly and with a very high level of certainty. This helps eliminate records fraud; facilitates the movement of learners and workers between institutions and geographies; and empowers individuals by giving them increased control over their own data.

The chapter is divided into several sections: 1) a general introduction to blockchain technology; 2) an explanation of how it benefits education; 3) a global survey of blockchain implementations for education led by both public and private sector entities; 4) and finally, a series of recommendations for policymakers and educational institutions regarding how to best approach the new technology.

The purpose of the first section of this chapter, "Understanding Blockchain Technology", is to help readers unfamiliar with blockchain to understand how it works before applying it to use cases in education. It provides an overview of the history and main concepts of blockchain as well as its main functions and use cases. In short, the main value of blockchain is to provide a mechanism to achieve consensus between multiple untrustworthy parties. The focus of this section is on digital currencies as the first concrete application of blockchain technology, but it also highlights other possible use cases.

Readers who understand blockchain technology well may therefore skip this first section and move directly to section 2, "Benefits of Blockchain for Education", which demonstrates how blockchain can be used to reliably verify and transfer degrees, academic records, and other types of credentials. While blockchain shows potential promise for other educational use cases, such as streamlining administrative processes, credentialing is by far the most mature application of blockchain technology in education today and therefore the focus of this report.

The third section, "Real-World implementations," provides the reader with a survey of the global market for verifiable digital credentialing solutions employing blockchain technology. As this market is rapidly evolving, this section can be considered current as of the second quarter of 2021 but will likely change significantly in the following months and years. One of the most exciting testimonies to the promise of blockchain technology has been its immediate global uptake; this is true for education as well as for other industries.

As a truly global network technology, therefore, blockchain mirrors the World Wide Web. The fourth section, "Driving Change", therefore recommends that governments, solution providers, and educational institutions privilege international portability and platform interoperability for blockchain credentialing solutions they adopt or build. The COVID-19 crisis has only underscored the need for secure, instant, verifiable digital data transfer between institutions as well as between individuals and institutions. As with any digitisation project, moving to a verifiable digital credentialing model requires both budgetary investment and change management. However, by choosing solutions and providers building on open standards, organisations can future-proof their projects and ensure their long-term viability.

Ultimately, a shift to blockchain-enabled, verifiable credentials creates a global ecosystem of interoperable records, a new scaffolding of trust to underpin the global mobility of labour and services. It also supports a "lifelong learning" model of education, in which traditional educational institutions are stops along a pathway of ongoing personal development that occurs both within and beyond educational institutions. The 21st century economy, and the digital natives who have been born and come of age in this economy, have internalised this model of personal development and expect their credentials to reflect the same convenience, security, and portability as other digital data formats. Educational institutions are therefore in the exciting and perhaps unprecedented position of serving as a global vanguard for new technology adoption: academic records, secured by transnational digital ledgers that become the first non-currency use cases for a next-generation social currency of trust.

Understanding blockchain technology

A breakthrough in computer science

Until 2009, digital money never saw wide adoption. Why? Because it was too easy to "double spend" it: too easy for someone to pretend they have digital money they do not have and spend it over and over. The ability for anyone to create money at will would render any form of such money worthless.

Computer scientists spent decades attempting to solve this problem, which finally saw an elegant resolution with the Bitcoin protocol for peer-to-peer electronic cash transactions (Nakamoto, 2008[1]). Bitcoin was the first "blockchain": the first chain of uneditable transactions validated by adversarial nodes in a network. But we will return to what blockchain and Bitcoin are in a moment. Before we can truly understand the significance of the blockchain breakthrough, we first need to understand how it solves an even more foundational computer science problem: the Byzantine Generals Problem (BGP).

The BGP involves coordinating action among multiple parties, some of whom are untrustworthy and unreliable. In the canonical BGP example, multiple Byzantine Generals are planning to attack a city, but the attack will only be successful if they *all* attack at the same time. If *all* of these parties cannot coordinate on a single action, everyone loses, but if they all coordinate on the same action, everyone wins (Moskov, 2018[2]). It is a binary situation: complete failure or total victory. A total victory requires something very hard to come by in any social group: consensus.

Computer systems that reliably produce consensus among multiple untrustworthy or adversarial parties are known as "byzantine fault-tolerant" (BFT). Examples of systems that require byzantine fault tolerance are aircraft flight control systems, spacecraft flight control systems, nuclear power systems, and digital currency systems (Wikipedia, n.d.[3]; Binance Academy, n.d[4]). These systems utilise different solutions to the Byzantine Generals Problem, or different *consensus mechanisms.* A consensus mechanism is a way of arriving at consensus among parties who do not trust one another. Different consensus mechanisms emerged to address the different needs and purposes of various byzantine fault-tolerant systems.

For example, if you are trying to track a stock-keeping unit (SKU) throughout multiple stops in a supply chain, and you do not trust all the links in that supply chain to always tell you the truth, you may want a BFT system with certain characteristics. On the other hand, if you are trying to track the spending of digital currency, and everyone in the network is incentivised to pretend they have more currency than they actually do, an even more robust consensus mechanism is necessary. Not all BFT systems are blockchains. But Bitcoin, the first implementation of blockchain technology, is a BFT system that emerged to track the ownership and spending of digital currency. In addition to solving the BGP, it also solved the double-spend problem through a consensus mechanism known as "proof of work" (Wikipedia, n.d.[5]).

Think of proof of work as CAPTCHA, but for computers. With CAPTCHA, a website requires you to prove that you are a human by solving a puzzle that is easy for a human to solve, but hard for a computer to solve. If you can solve this puzzle, the receiving computer will allow you to send data or subscribe to a service. Similarly, computers that are asked by other computers to do something for them – like send money from one party to another – may also require that requesting computers demonstrate that they have solved a complex puzzle before their request is granted. Verifying that this puzzle has been solved by requesting computers is "proof of work."

Proof of work is intended to make communication between computers more costly in order to eliminate frivolous and fraudulent use of the network. For example, proof of work prevents Distributed Denial of Service (DDoS) attacks and SPAM – where adversarial users throw sand in the gears of a network by flooding it with malicious or nonsensical data. As computers get faster and smarter, proof of work becomes harder and harder – more expensive in terms of processing power. This is necessary in order to keep BFT networks secure, stable, and usable. But the tendency towards more processing power also means increased energy usage, which is why proof-of-work systems like Bitcoin have been criticised for their environmental impacts (Temple, 2019[6]). In response, clusters of computers running the Bitcoin protocol now frequently use renewable energy sources and are located in cold climates in order to save on energy required to cool them (Baydakova, 2019[7]; Morris, 2018[8]). Despite Bitcoin's relatively high energy usage, however, several influential studies that quantified that energy usage in the past have been demonstrated to be profoundly inaccurate (DiChristopher, 2017[9]). Claims that the Bitcoin network would use as much electricity as the rest of the world by 2020 have manifestly not come to pass (Cuthbertson, 2017[10]). And as computer processing power becomes more energy efficient, the Bitcoin network does too – without sacrificing the security and usability needed to serve as a long-term store of value for digital currency (American Chemical Society, 2019[11]). In fact, a recent white paper by investment management firm Ark Invest suggests that Bitcoin mining could play a key role in incentivising the shift towards renewable energy by helping to manage supply and demand in energy markets (Ark Invest, 2021[12]).

So, Bitcoin is a byzantine fault-tolerant network designed to securely maintain and even grow the value of its digital currency by preventing the double-spend problem through proof of work. But why is it called a blockchain?

Blockchains and distributed ledgers

As mentioned above, not all byzantine fault-tolerant systems are blockchains. While there is debate about what exactly makes a blockchain different from other BFT systems, there is broad agreement that the word "blockchain" refers to a type of distributed ledger that records an append-only, immutable database of transactions. The word "blockchain" was first used in connection with Bitcoin to refer to a ledger of digital currency transactions. Bitcoin's inventor, Satoshi Nakamoto, initially called it a "proof-of-work chain" or a "timechain" because transactions are appended to the ledger in a sequential, timestamped manner that preserves the record permanently in the order it was created (Messari, 2019[13]). In addition, these transactions are grouped together in "blocks", which are deposited to the chain after a set period of time. (In the case of Bitcoin, new blocks of transactions are added to the chain every 10 minutes.) This block-based architecture easily lent itself to the term "blockchain," which was "coined" by the early Bitcoin community.

What about BFT systems that do not rely on blocks of transactions appended to an immutable database? Those are sometimes called "distributed ledgers" (DLTs). Distributed ledgers may or may not track the allocation of currency in a network and usually use consensus mechanisms different from proof of work. They may even be editable by parties with the right permissions. Some people separate DLTs from blockchains and treat them as different things, while others consider blockchains to be a specific type of DLT.

Box11.1 Public/Private, open/permissioned - What's the difference?

Blockchains have rules about who can write transactions to their network and who can run nodes of the chain and validate those transactions. The following guidelines provide a general rubric for understanding the differences between different types of blockchains.

Writing to chain:

Public: Anyone can write transactions to the chain and view those transactions once they have been written.

Private: Only permissioned parties may write transactions to the chain and view transactions once they have been written.

Running nodes and validating transactions:

Open: Anyone can run nodes and validate transactions on the chain. ("Open" in this context does not mean "open source". Many private blockchains are based on an open source codebase but are private because use of the network is gated.)

Permissioned: Only permissioned parties may run nodes and validate transactions on the chain.

Blockchains can be any of the following combinations: Public/Open, Public/Permissioned, or Private/Permissioned. (Although Private/Open blockchains are possible in theory, in practice all private chains are also permissioned.)

Note that just because a transaction has occurred on a public blockchain and anyone can view it does not necessarily mean anyone can understand what it means. This is because public blockchains usually record transactions pseudonymously or anonymously and hash the transaction content so that it is not readable by people. This is a necessary step to preserve privacy on a public platform. (This is also why the criticism of public blockchains as not privacy preserving is often misleading.)

In order to verify transactions on public blockchains, a human user relies on technical standards that provide a series of technical steps for verifying those transactions. This verification is generally facilitated by an application, like a web browser or mobile wallet. Applications that verify past transactions may do so in an open and free manner or gate verification behind a paywall or some other access barrier.

For example, some credentialing companies that use public blockchains to anchor transactions charge for credential verification as part of their business model. With permissioned or private blockchains, credential verification may also be gated either behind a paywall or behind some type of authentication service.

We do not have to choose a side in this debate to understand that the distinction between blockchains and DLTs arose because different BFT networks are created for different purposes. The major differentiating factor between different BFT networks is their relative level of centralisation or decentralisation. In other words, to what extent is a network's infrastructure supported by, and consensus determined by, an authority or authorities? For some use cases, a more centralised blockchain architecture makes sense; for others, it does not. Below we examine different implementations of more or less decentralised blockchains in light of the stakeholders making use of them for particular purposes.

Decentralisation vs. centralisation

It is useful to see Bitcoin as an archetypal example of a decentralised blockchain. It is decentralised because of the main problem it arose to solve: the problem of an infinitely growing money supply that eventually devalues the money itself. Governments throughout history have been incentivised to create more and more money in order to fund wars, prop up markets, pay back debts, and for many other reasons (Bhatia, 2021[14]). The problem with this is that over time, it results in devaluation of the currency, which destroys the savings and wealth of ordinary people (Alden, 2021[15]). To prevent currency devaluation, Bitcoin was created to be digitally scarce, with a fixed supply of

21 million coins. No individual or government can change this due to the rigidity of the underlying bitcoin protocol. This means that the bitcoin currency was designed to be scarce and therefore to increase in value over time. (The Bitcoin protocol is usually referred to in uppercase, while the bitcoin cryptocurrency is not capitalised. The bitcoin cryptocurrency is sometimes abbreviated as BTC.)

Some in the Bitcoin community expect a dramatic and permanent spike in the value of bitcoin due to a process known as "hyperbitcoinisation" – in effect, the opposite of hyperinflation (Krawisz, 2014[16]; Kenobit, 2018[17]). Although Nakamoto never said so explicitly, the way he architected Bitcoin's monetary policy suggests that he expected the value of one bitcoin to rise so high that most people would never own a full coin. For this reason, Nakamoto subdivided each bitcoin into 100 million satoshi. Thanks to satoshi, people do not need to own even one bitcoin in order to transact with the currency and use it as a long-term store of value.

Nakamoto's intent to protect the value of bitcoin from the interventions of activist monetary policy makes it clear that bitcoin is designed to be a stateless currency. That means it is architected to avoid the possibility of being captured by any centralised authority. Because the Bitcoin blockchain is open and public, anyone is able to run full or partial nodes of the protocol and commit transactions to the network using proof of work. Transactions on the network are pseudonymous and moving towards anonymity (Nuzzi, 2019[18]). All of the network code is open source, meaning anyone can contribute to it, and it is maintained on a volunteer basis by a group of core developers and cryptographers. People who are unhappy with how Bitcoin is governed can also fork the code to create competing blockchains, and the open marketplace lets users decide which chain they want to use to store their value and transact their money. So far, bitcoin has by far the largest market capitalisation of any blockchain-based cryptocurrency. As of April 2021, the cryptocurrency is worth over USD 1 trillion, the fastest asset to reach this milestone in recent history (Ali, 2021[19]). The next most valuable cryptocurrency, ether (ETH), is currently worth about one-third of the Bitcoin network, at over USD 300 billion (CoinMarketCap, n.d.[20]). We will return to Ethereum, the blockchain network underpinning ether, below.

Understandably, this level of decentralisation has not endeared Bitcoin to some governments (McWhinney, 2019[21]). Banks – particularly central banks – have been especially reticent about the stateless cryptocurrency (Steenis, 2017[22]), partly because it offers an alternative store of value and medium of exchange that remains unaffected by their monetary policy interventions. In addition, many companies and industry consortia are reluctant to use open, public blockchains, preferring private or permissioned-public models that allow them to exert more control over who gets to use the network and in what capacity. In addition, decentralisation does come with technical trade-offs: greater near-term efficiencies in network speed and transaction processing are often easier to achieve in more centrally-controlled networks. This is because networks that gate access only to trusted parties eliminate some of the need for byzantine fault tolerance: the more you trust the participants in a network to behave honestly, the less need you have for robust BFT, which tends to slow down a network's decision-making.

In part due to dissatisfaction and discomfort with Bitcoin – but also because Bitcoin inspired a generation of developers with the potential to generate enormous personal wealth on the basis of token seigniorage by minting their own cryptocurrencies – other cryptocurrencies and DLT architectures quickly arose which may preserve some aspects of the decentralisation of the Bitcoin network, but with more centralised characteristics that presume a higher concentration of trusted actors. Some are quite open about being fully centralised systems. As noted above, many of these centralised blockchains have no associated cryptocurrency and instead act as infrastructure for the delivery of services, for which their architects may charge. Accordingly, we can think of decentralisation as a spectrum; it can manifest to a greater or lesser degree in different parts of a blockchain's architecture.

Here it is also important to note that there is considerable controversy over what constitutes decentralisation. Some architectural decisions that read as decentralised to some may appear highly centralised to others. Part of the difficulty is that the blockchain space is laden with value judgments and strong ideological commitments. This means that for some, decentralisation is simply and straightforwardly good, while centralisation is bad. The opposite also holds true; some have castigated decentralised architectures as immoral, criminal, or worse. This is an area of ongoing and often heated debate. In this paper, I do not adopt "good" or "bad" value judgments with regards to decentralisation or centralisation. Rather, I stress that these characteristics of a system will necessarily be adapted to what that system is made for.

Ethereum, the second most valuable blockchain today in terms of market capitalisation (CoinMarketCap, n.d.[20]) is an example of a blockchain modelled on the highly decentralised architecture of Bitcoin. Like Bitcoin, Ethereum is an open, public blockchain; anyone can transact on the network, run nodes, and contribute to the network's open source code. In 2018, the US Securities and Exchange Commission determined that both bitcoin and ether cannot be considered securities because no third party carries out "entrepreneurial and managerial functions" with regards to their issuance and value (Sharma, 2018[23]; Pisani, 2018[24]).

However, there are two major differences between Bitcoin and Ethereum which have contributed to their very different developmental trajectories. One is that, whereas Bitcoin was built to be the most secure form of digital money available, Ethereum was built to be a distributed "virtual machine"—an infrastructure for running decentralised applications. Ethereum's associated cryptocurrency, ether, is called "gas" because its primary (though not only) function is to power applications on the network rather than to serve as a long-term store of value or universal medium of exchange. As a virtual computing platform, Ethereum allows the inclusion of executable code known as "smart contracts" within its blockchain transactions. Smart contracts allow organisations to automate and coordinate action at scale. Using *if* -> then logic, smart contracts execute certain functions (generally the payment of money) when contractually-defined conditions are met (CoinTelegraph, n.d.[25]). This feature of Ethereum has given rise to a class of applications called "decentralised applications," or DApps, whose bylaws and procedures are embedded in smart contracts (Wikipedia, n.d.[26]) Although smart contracts can also be executed on Bitcoin, Ethereum's more extensive and developer-friendly smart contracts functionality has made it the most popular blockchain choice for DApps and the most actively used blockchain today (Leising and Kharif, 2020[27])

Another major difference between Bitcoin and Ethereum is that Bitcoin's founder chose to remain anonymous and withdrew from visible participation in the network's management two years after the network was launched (Bernard, 2018[28]). Although many individuals have claimed to be Satoshi Nakamoto in the ensuing years, none have been able to prove this conclusively, and none have been able to exercise significant influence over the network's technical roadmap. By contrast, Ethereum's main inventor, Vitalik Buterin, is well-known and maintains an active role in the governance of the Ethereum network. For example, Buterin has been one of the primary drivers behind the decision to transition Ethereum from a proof-of-work (PoW) to a proof-of-stake (PoS) consensus mechanism, a change referred to as Ethereum 2.0 (Foxley, 2020[29]).

Buterin's prominent role in Ethereum network governance was perhaps most visible after a famous 2016 incident known as the "DAO hack". An attacker exploited a bug in an Ethereum smart contract run by a Decentralised Autonomous Organisation (DAO) to appropriate at least USD 89 million worth of ether (Kar, 2016[34]). Buterin led a group that hacked the hacker and re-appropriated the funds, but an anonymous letter purportedly from the attacker claimed that they had taken them legally, as they were only performing actions allowed by the smart contract (and "code is law") (Siegel, 2016[35]). Buterin, however, feared that acquiescing to the hacker's logic would destroy investor trust in Ethereum and any future DApps and DAOs built on it. So he proposed a "hard fork" of the network, which would roll it back to a time before the attack and return the stolen money to DAO investors.

The decentralised nature of the Ethereum network did mean that the majority of miners running the Ethereum protocol still had to choose to adopt Buterin's proposal, but his stature in the community, and the support he enjoyed from other Ethereum founders, made it likely that they would. Indeed, most Ethereum developers did choose to run the forked code, making the new, rolled-back Ethereum (ETH) the most widely-accepted version of the blockchain. Some, however, refused; they continued running the un-forked blockchain, which is now known as Ethereum Classic (ETC). By contrast, none of the people claiming to be Satoshi Nakamoto were able to influence the technical roadmap of Bitcoin during the "Bitcoin Civil War" of 2017 (Dinkins, 2017[36]). Instead, the Civil War resulted in a number of minor Bitcoin forks – Bitcoin Cash (BCH), Bitcoin Gold (BTG), Bitcoin Satoshi's Vision (BSV) – which to this day remain much smaller chains from a value and adoption standpoint compared to the original Bitcoin (BTC) (CoinMarketCap, n.d.[20]).

The ongoing involvement of Buterin and the other Ethereum founders in the network's governance has enabled different possibilities for the network – in particular its adaptation for use by enterprises and governments looking to streamline core business applications and services. Ethereum's smart contracts functionality enables organisations to execute tasks that require a considerable amount of coordination between parties who may not trust or even know one another: settle payments, provide escrow services, pay out investor dividends, enable secure electronic voting, track SKUs through a supply chain, and many other functions. The company ConsenSys, founded by Ethereum co-founder Joseph Lubin, focuses entirely on delivering enterprise-ready DApps using Ethereum (ConsenSys, n.d.[37]).

Box 11.2 Proof of stake

Proponents of proof of stake (PoS) argue that the ever-increasing energy cost of proof-of-work (PoW) mining has made running blockchain nodes prohibitive for ordinary people because it has resulted in a centralisation of mining power among powerful groups called "mining pools" (Muzzy, 2020[30]). To remedy this, PoS requires the miner (or "forger," as they are sometimes called to differentiate them from users of PoW) to put their own cryptocurrency at risk to validate a transaction rather than expending energy to solve complex mathematical problems. The penalty for dishonest dealing in a PoS system is having one's cryptocurrency confiscated to various degrees. In the case of Ethereum, moving to a PoS system has also been explained as the necessary precondition for securely scaling the network's transactional capacity.

However, PoS has its critics as well. Research firm Messari has pointed out that PoS has the potential to create a system of class-based blockchain governance, where the wealthiest participants in a blockchain network have the most say over what is true, or validated on the network (Watkins, 2020[31]). This risk is particularly acute for those blockchains that implement "on-chain governance" – a way of placing control over a network's technical roadmap in the hands of token holders rather than core developers, who are sometimes perceived to be unaccountable to network users (Messari.io., 2019[32]). Simply put, there is a risk that wealthy token holders could skew decisions about the governance of PoS systems to maximise profit for themselves.

Wealthy token holders may be the initial investors in a network who receive large cryptocurrency allocations in return for early support. They may also be later investors who purchase large amounts of the network's cryptocurrency and use it to frequently validate transactions, thus accruing more and more rewards for validation – a "rich get richer" dynamic that eventually squeezes out smaller crypto holders from the network (Watkins, 2020[31]). Other critics of PoS argue that scaling the transactional capacity of a blockchain network doesn't necessarily need to occur on-chain. For example, the need to scale "slow" PoW systems like Bitcoin has given rise to a thriving industry of "Layer 2" applications that allow users to conduct most transactions off-chain while using the blockchain only as a final settlement layer (Coin Telegraph, n.d.[33]).

It is important to note here that no blockchain network – Bitcoin, Ethereum, or otherwise – has arisen to solve the problem of wealth inequality or redistribution. Today, owners of every cryptocurrency are a very small number of people compared to the world's population, which necessarily skews the distribution of cryptocurrency wealth. While blockchain networks are critical interventions for helping us reimagine governance in the 21st century, their social effects are highly targeted and should not be mistaken as replacements for all other policy and social platforms.

But many established institutional actors are not interested in using a public, open digital infrastructure to implement smart contract-based applications. The Enterprise Ethereum Alliance (n.d.[38]) was formed in order to build versions of Ethereum that are public/permissioned or private and which have purpose-built functionality for the specific use cases targeted by client enterprises (Sharma, 2019[39]). The EEA has grown to over 200 companies implementing centralised versions of Ethereum that are funded and managed by specific companies or governments. One prominent example of an enterprise Ethereum implementation is the European Blockchain Services Infrastructure (EBSI), a public-permissioned blockchain created by the European Commission to deliver cross-border public services (CEF Digital, n.d.[40]). In the private sector, EEA member J.P. Morgan spearheaded the development of Quorum, a permissioned implementation of Ethereum built specifically for the financial industry (Quorum, n.d.[41]).

In 2015, the Linux Foundation announced the Hyperledger Project, an initiative by a consortium of technology, finance, and supply chain companies to build private blockchains that allegedly improve upon the scalability and reliability of existing public chains (Wikipedia, n.d.[42]). The Hyperledger Project now includes multiple blockchain "toolkits" that enable organisations or consortia to create private blockchains that meet their specific business requirements. None of these toolkits create blockchains with cryptocurrencies, leading many to refer to them as distributed ledgers instead. Popular toolkits today include Hyperledger Fabric and Hyperledger Sawtooth. Hyperledger Besu is an Enterprise Ethereum codebase that was contributed in 2019 (Castillo, 2019[43]). In the credentialing world, Hyperledger toolkits have been used by companies including Salesforce, Workday, and Greenlight to build blockchain networks that they manage (Lemoie and Souares, 2020[44]). Companies including Amazon, IBM, Oracle and SAP also use Hyperledger toolkits to provide "Blockchain-as-a-Service" (BaaS) offerings for clients using their cloud infrastructures (Amazon, n.d.[45]; IBM, n.d.[46]; Oracle, n.d.[47]; SAP, n.d.[48]). Some non-profit associations also use Hyperledger toolkits (among others) to build blockchain infrastructures for the delivery of public and commercial services. A few well-known examples include the Alastria consortium in Spain (Alastria, n.d.[49]) and the LACChain initiative from the IDB Lab (ConsenSys, 2020[50]).

The blockchain platform R3 Corda is another example of a private, enterprise-ready blockchain implementation. Founded in 2014, R3 is a private corporation that built a blockchain to manage and synchronise financial agreements (Wikipedia, n.d.[51]). The Corda platform, open sourced in 2016, was built to conform to the technical requirements and standards of the financial industry. Since that time, Corda has evolved to accommodate the needs of multiple industries (its main competitor is arguably Hyperledger Fabric, which was developed a few years later) (Shin, 2020[52]). Corda's conservative approach to programming languages and cryptographic standards appeared to be rewarded recently by an IEEE study which identified it as the only blockchain platform compatible with NIST standards and therefore qualified for use by the US Federal Government (Jessel, 2020[53]). In an interesting twist, however, the first US Federal Government implementation of blockchain is actually a procurement platform for the Department of Health and Human Services built on Hyperledger Fabric (Malone, 2020[54]).

Finally, a growing crop of cryptocurrencies pegged to the value of national fiat currencies – so-called "stablecoins" – have arisen to facilitate exchange of fiat currency into cryptocurrencies and vice versa. These stablecoins are typically "run and entirely controlled by the private companies that issue them and receive traditional bank deposits in return for issuing their respective currencies to their customers" (Dagger, 2020[55]). However, decentralised stablecoins are emerging as well, largely to circumvent a number of cumbersome and contradictory legal injunctions against the use of centralised stablecoins (Fitzpatrick, 2020[56]). As state central banks begin issuing digital fiat currencies, however, the transition to government-run centralised stablecoins will likely accelerate.

Costs and limitations

Blockchains are no small undertaking. They emerged to solve the Byzantine Generals Problem: how do you create consensus among a large number of adversarial actors who cannot be trusted? The answer – a decentralised network of nodes validating transactions according to a shared consensus mechanism – only works if it is deployed at scale. If a blockchain has too few validators, it is easy for malicious actors to attack it by gaining enough network power to override the consensus in their favour or to someone else's detriment. This is known as a 51% attack. Conversely, if a small network consists only of trusted actors, then it doesn't really need byzantine fault tolerance, making it generally much less expensive and more efficient to use traditional databases and applications.

Creating, deploying, and operating a blockchain network is a massive undertaking. Public blockchains finance their operations through stakeholder incentives tied to their native cryptocurrencies: the reward for mining bitcoin and ether by validating transactions on these networks (and thereby keeping them running and secure) is the bitcoin or ether cryptocurrency itself. In addition, transaction fees are assessed and paid to block validators in the network's cryptocurrency.

Satoshi Nakamoto designed Bitcoin with a limited supply of bitcoin (21 million) and the assumption of hyperbitcoinisation: that, if the network became successful, the value of bitcoin would skyrocket and much of the global economy would eventually run on the basis of bitcoin transactions. This means that as revenue from mining decreases and use of the network increases, the cost of running and maintaining Bitcoin could be subsidised by transaction fees alone. (Think of VISA or MasterCard as contemporary analogues.)

Ethereum founders, by contrast, did not cap the absolute amount of ether. Ether are awarded for every block mined, with an amount that has decreased over time (EthHub, n.d.[57]; ConsenSys, 2019[58]) and an annual cap of 18 million new ether (Sharma, 2019[59]). Vitalik Buterin made a bet that ether would not reach 100 million in circulation for at least a century (Buterin, 2016[60]), but due to the network's popularity, this milestone was instead achieved in 2018 (Varshney, 2018[61]). As a result, Buterin has proposed capping the total amount of ether at

120 million to avoid inflation (or 144 million if that cap is missed), but this proposal has not yet been accepted (Varshney, 2018[61]). Like Bitcoin, users of Ethereum also pay transaction fees, but more importantly, smart contracts require ether (gas) to run. In other words, Ethereum staked its future dominance not on becoming the world's reserve currency, like Bitcoin, but on becoming the world's computer. This combination of transaction fees and gas could finance the Ethereum network in the event that mining rewards disappear.

Permissioned and private blockchains, by contrast, usually do not have corresponding cryptocurrencies. This means they must be funded at a large cost that easily adds up to hundreds of thousands to millions of dollars each year. In some cases, like managing a supply chain for an entire industry, such a cost may be justified and can be distributed among member organisations to generate return on investment. But in cases where only one organisation is seeking to streamline internal processes, the cost usually far outweighs the value. Using blockchains where a private database will do then becomes an expensive, over-engineered experiment likely to end in failure.

The sheer scale needed to make operating blockchains cost-effective is beginning to swing the pendulum of the market back towards public blockchains. After all, blockchains only provide value through network effects, but each private blockchain is, by design, its own gated network. If each company develops its own private blockchain, the world may end up with a sea of private networks built on different standards that are not interoperable. The problem of data silos repeats itself all over again – this time, after considerable R&D expenditure.

Ernst & Young has been the most vocal industry player, arguing that the era of private blockchains is effectively over. Paul Brody, EY's Global Blockchain Leader, writes:

> *"what has typically happened thus far is that for every organization willing to join a consortium or someone else's network, two companies started their own. Not much hope for a network effect here. Blockchains, like most network technologies, are natural monopolies. The more users they have, the more useful they become, and once they achieve a position of dominance, [private blockchains] tend to start aggressively extracting "rents" from their members. Having seen this pattern in several consumer applications, at EY we believe most enterprises will prefer to stick to their legacy tools rather than let themselves experience a similar fate facing an all-powerful private blockchain monopolist in the B2B space. Public blockchains like Ethereum offer a better choice for enterprise users. Even if they do achieve monopoly-like dominance, there is no controlling entity to extract excess profits — there is only an ecosystem of competing service providers." (Brody, 2019[62])*

Brody compares public blockchains to the internet, which is a shared infrastructure that is not controlled by a single enterprise but underpins value for all enterprises. This is an apt analogy. During the early days of the internet, many companies and governments insisted on having their own "intranets" – private networks that could only be accessed internally. Over time, however, only the most mission-critical intranets remained, while most digital business processes transitioned to the World Wide Web. A similar trend is playing out now in the blockchain world, with many enterprises insisting on private blockchains in the belief that they are more secure and efficient, only to realise after considerable investment that they have undercut the network's value by limiting access to it.

Brody's contention that public blockchains have matured considerably with regards to privacy may benefit from some context. From the beginning, public blockchains have restricted the kind of data that can be placed on-chain to public keys, hashes and, in some cases, smart contracts. However, it is possible for hackers to "game" public smart contracts – as happened with the 2016 DAO hack – by exploiting vulnerabilities. Similarly, public keys tied to known identifiers can be used to perform "network analysis," tracking a user's transactions on a blockchain (Chainalysis, n.d.[63]). This capability is used by law enforcement to track criminal financial activity on blockchains (Weinstein, 2015[64]). Although hashes are virtually impossible to reconstruct to reveal transaction data, there is ongoing debate about whether or not they could constitute personally identifiable information if used incorrectly (Mearian, 2018[65]; Longstaff, 2018[66]).

Zero-knowledge proofs (ZKPs) address these concerns by concealing all transaction data on public blockchains. While this is attractive to many users of blockchains, some governments and law enforcement agencies are concerned about the use of ZKPs due to the limits it would place on their ability to investigate financial crimes. Until recently, Zcash and Sovrin (a codebase also donated to the Linux Foundation under the name Hyperledger Indy) have been the main public blockchains employing zero-knowledge proofs (Sharma, 2019[67]; The Sovrin Foundation, 2018[68]). Enabling this functionality for Bitcoin and Ethereum could be particularly valuable due to the large network effects of those networks. Today, however, there are a variety of approaches to data minimisation (restricting the type and amount of data that can be verified) using blockchain networks in addition to ZKPs.

Is there a role for some private blockchain implementations going forward? Undoubtedly, as there is a role for some intranets. But the purpose of blockchain technology – to facilitate transactions, agreements, and exchange of data among untrusted actors at a very large scale – can only be realised in the long term through interoperability. This does not necessarily mean that there will be one blockchain to rule them all, but rather that blockchain architectures that facilitate exchange and data validation at the largest scale will likely gain the greatest adoption.

Open standards

Blockchains alone do not guarantee data portability or system interoperability. As indicated in Box 11.1, data anchored to a blockchain is only useful if it can be reliably understood and verified. Since public blockchains do not encode plaintext data on-chain, and permissioned and private blockchains have widely varying standards as to what is and is not stored on-chain, validating identity, financial transactions, agreements, and many other things requires a standardised way of sharing, verifying, and reading blockchain-anchored data.

This is where open standards come into play. Open standards are not applications; they are standardised ways of formatting, writing, sharing, retrieving, and verifying data. The advent of blockchain technology has spurred considerable innovation in open standards as companies, governments, and individual contributors realise the need for a shared method for verifying what is true. Shared methods reduce vendor-dependency, helping organisations and individuals avoid the kind of lock-in that comes from platform-dependent ways of managing data.

Perhaps the most prominent organisation developing open standards for blockchain-anchored data today is the World Wide Web Consortium (W3C). The W3C was formed during the early days of the internet (1994) by Tim Berners-Lee, MIT, CERN, DARPA, and the European Commission to codify open standards that are used to transact information across the global digital infrastructure of the web (W3C, n.d.[69]). The W3C is the leading independent internet standards body in the world, sourcing volunteer contributions from many individuals and organisations.

Among the first standards the W3C is developing for blockchain-anchored data are credentialing standards: how to verify whether claims being made about one party by another are valid. The most notable of these standards are Verifiable Credentials (VCs) (W3C, n.d.[70]) and Decentralised Identifiers (DIDs) (W3C, n.d.[71]). The verifiable credentials open standard was made a full W3C recommendation in 2019. It is designed to work in tandem with a new standard for blockchain-anchored digital identifiers, known as Decentralised Identifiers (DIDs), which was submitted for recommendation status in April 2021.

The intent of the W3C DID standard is to add privacy and flexibility functionality to the public key cryptography which is currently used to identify individuals and organisations making use of blockchain technology. Taken together, verifiable credentials and DIDs enable the evolution of a blockchain-agnostic, privacy-protecting, feature-rich ecosystem for secure, tamper-evident digital credentials. For these reasons, the US Department of Homeland Security has been issuing grants to companies working in this space to speed along the development of these new standards (US Department of Homeland Security, 2019[72]; US Department of Homeland Security, 2017[73]; US Department of Homeland Security, 2019[74]). VCs and DIDs are also seeing uptake by governments including Canada (VON, n.d.[75]; Benay, 2019[76]), Singapore (OpenCerts, n.d.[77]), South Korea (Insights, 2020[78]), and the European Commission (Du Seuil and Pastor, 2019[79]; EU Blockchain Observatory and Forum, 2019[80]).

It is important to note that the VC and DID standards are agnostic with regards to a digital record's form factor or content. They function similarly whether records are educational, financial, professional, or vital. To address the need for standardisation on record content and form factors within industries, additional standards bodies have been formed. As this paper focuses on the applications of blockchain to the education industry, our focus here will be on those implementations. At the W3C, this includes the Verifiable Credentials for Education Task Force (W3C, n.d.[81]) and the Educational and Occupational Credentials in Schema.org Community Group (W3C, n.d.[82]). Other standards for educational credential descriptions include the Common Microcredential Framework (CMF) launched by the European MOOC Consortium (Konings, 2019[83]), the Credential Transparency Description Language developed by the Credential Engine (Credential Engine, n.d.[84]) and the Badge Alliance (Alliance, n.d.[85]), as well as the Comprehensive Learner Record (CLR) standards under the custodianship of IMS Global (IMS Global, n.d.[86]). The W3C works closely with some of these institutions – like the Credential Engine and IMS Global – to complement their efforts and create globally interoperable records definitions.

The W3C is not, however, the only organisation working on interoperability for decentralised credentialing standards. Credentialing is only one application of verifiable claims under the broader umbrella of digital identity. Other groups working on the next generation of web-based identity infrastructure include Rebooting Web of Trust (RWoT) (Web of Trust, n.d.[87]), the Internet Identity Workshop (IIW) (Internet Identity Workshop, n.d.[88]), the T3 Innovation Network at the US Chamber of Commerce Foundation (US Chamber of Commerce Foundation, n.d.[89]), the Digital Credentials Consortium (MIT Open Learning, 2020[90]), the Trust Over IP Foundation (hosted at the Linux Foundation) (Trust Over IP Foundation, n.d.[91]) (The Linux Foundation, 2020[92]), and the Decentralised Identity Foundation (DIF) (Decentralized Identity Foundation, n.d.[93]). Most recently, the Learning Technology Standards Committee (LTSC) at the IEEE (IEEE, n.d.[94]) and the Learning Economy Foundation (Learning Economy Foundation, n.d.[95]) have proposed an “Internet of Education (IoE)” (Internet of Education, n.d.[96]) to unify these and other consortia working on technical standards for education and credentialing (Education, n.d.[97]).

There is considerable overlap among participants in these groups, although they have different target memberships. The Trust Over IP Foundation and DIF are primarily corporate membership organisations; the T3 Innovation Network is a public-private membership organisation; the Learning Economy Foundation attracts members with a background in education technology and policy; the Digital Credentials Consortium is an academic membership organisation; and RWoT and the IIW attract technologist volunteers passionate about internet privacy and autonomy regardless of affiliation. The W3C functions as a kind of node for technical consensus formation between these groups as well as others.

Self-sovereign identity

Efforts to build a standards-based architecture for decentralised identity over the web have strong overlaps with the Self-Sovereign Identity (SSI) movement. There is wide disagreement about what exactly “self-sovereignty” is or whether it is desirable, but those who identify themselves as part of this movement typically are motivated by giving individual users of digital technologies greater control over their personal data (Smolenski, 2016[98]). This means, among other things, removing their dependence on platforms and governments to manage this data. Indeed, data portability and platform independence may be the two most defining characteristics of self-sovereign digital identity, with some arguing that these descriptions are more useful in practice than the term “self-sovereign” (Renieris, 2020[99]).

Arguably the most well-known articulation of the principles of self-sovereign identity was made by computer scientist Christopher Allen in a widely-circulated 2016 blog post (Allen, 2016[100]). Since that time, there has been considerable debate about what each of these principles mean and what technological implementations best address them. Adherents of various SSI or SSI-adjacent philosophies actively participate in developing standards for digital identity through the aforementioned standards bodies, and their points of view often differ widely. In addition, SSI standards development must contend with existing legal regulations around the use of cryptography and data protection. This sometimes results in the proliferation of technical implementations within standards definitions rather than their consolidation. Nevertheless, progress continues to be made towards interoperable, user-centric standards for verifiable credentials and digital identity (T3 Innovation Network, 2020[101]).

Benefits of blockchain for educational credentialing

Blockchains arose as infrastructures to verify transactions across an adversarial network – that is, a network with untrusted parties. Although blockchain functionality can be extended to execute automated business processes via smart contracts, its primary value remains in serving as a shared, single source of truth. Blockchain’s conjoined verification and smart contract functionality has the potential to automate educational business processes like credential transfers, academic record transfers, credential equivalency establishment, and even the administrative apparatus of the university.

Blockchains are not a prerequisite for automating business processes, however. Many existing software applications do this, and those employing workflows, intelligent process automation (IPA), and robotic process automation (RPA) have significantly advanced much of this functionality. So when is using blockchains mission-critical for achieving automation objectives? It may be the case if said automation must occur across a network of adversarial, uncoordinated actors. If it does, a follow-up question is whether sufficient network effects can be achieved to produce a return on the high ongoing cost of building and maintaining a blockchain network.

To make this more concrete, let's take an example that is often used to illustrate the benefits of blockchain in education: automating the establishment of credit equivalencies as students transfer from one school to another. While some argue that blockchains will solve this problem (and some vendors have built blockchain networks specifically to do so), credit equivalencies could also be automatically determined by existing applicant tracking systems and databases using widely agreed-upon definitions of what credits mean and widely-accepted standards for educational data transfer. In other words, the primary obstacle to automated credit transfers to date has not been technological, but social: every jurisdiction (down to even the university or school) often has its own credit definitions and may be reluctant to make those transferable by using definitions established elsewhere. This example illustrates that, at times, "blockchain" may be presented as a solution to problems that actually require off-chain forms of social consensus building. In some regions, this may be easier at the higher education level, as common definitions and standards for credits have been established and endorsed. This is, for example, the case in the European Union, with its European Credit Transfer System.

Perhaps blockchain could be the missing piece that enables an application to coordinate action across many different parties who would otherwise require a trusted third party to act as a mediator. But the most prominent example of an education provider who took such an approach supports the case made above: that blockchain may not yet provide a level of automation value that warrants its use. Woolf University, initially hailed as a "Blockchain University" in global media reports (Young, 2018[102]; Vander Ark, 2018[103]), was originally built on a distributed ledger platform (Parisi, 2018[104]). As Woolf Founder Joshua Broggi explained, "We use a blockchain to create efficiencies by managing custodianship of student tuition, enforcing regulatory compliance for accreditation, and automating a number of processes." (Vander Ark, 2018[103]). Woolf experimented with different blockchain models in its early years of operation, but later moved away from blockchain technology. Instead, Woolf now highlights its offering as a cloud-based SaaS platform for organisations and students, delivering the social mission of access to quality education from anywhere in the world. Woolf now refers to itself as "The Borderless University," and is indeed used by faculty and students from all over the world (Woolf University, n.d.[105]). Web-based applications enabled streamlining the administrative apparatus of the university without blockchain.

By contrast, other companies creating blockchain-based education platforms prominently feature their use of blockchain. These include ODEM (Maaghul, 2019[106]) and BitDegree (BitDegree, 2017[107]), both of which use the public Ethereum blockchain and have their own ERC20 tokens. In the United States, the Learning Economy Foundation (Learning Economy Foundation, n.d.[95]) has proposed a vision for a blockchain-based "ecosystem" that unites credentialing authorities, students, employers, education technology firms, and others in a shared marketplace where educational outcomes are incentivised through monetisation ("rewards"). Learning Economy Foundation co-founders, Chris Purifoy and Jacksón Smith, describe their vision as follows in a cover story for *G20 Summit Magazine*: "By quantifying the true value of education, a whole economy can be built around it to pay students to learn, educators to create substantive courses, and stewards to help the Learning Economy grow. Blockchain provides a decentralised way for everyone adding value to global education to coordinate around the commonwealth without the friction of individual partnerships." (Purifoy and Smith, 2018[108])

Learning Economy founders anticipate that building their blockchain platform will create a "Learning Gold Rush" (the title of their Implementation Roadmap) (Learning Economy Foundation, n.d.[109]) where everyone is incentivised to teach, learn, and employ through financial rewards administered by the network.

The Learning Economy model has stretched the promise of blockchain the furthest, conjecturing that blockchain networks will be able to not only coordinate social action, but do so in a way that creates sufficiently motivating financial rewards that are automatically administered to all stakeholders in a marketplace, realising the hazily-defined goal of "improving learning outcomes" from the bottom up. While the nobility of this vision is laudable, it borders on a utopianism that is out of step with the actual capabilities of any blockchain network. In the long term, it is the standards-based credentialing projects in which Learning Economy is engaged that will likely see the most success (see "Real-World Implementations", below).

In the near term, therefore, the primary value of blockchain for education is likely more basic: it makes credential verification an order of magnitude faster, cheaper, and more secure. When used in combination with open standards, blockchains remove ongoing dependencies on issuing institutions, software providers, and third parties to verify official records. Moreover, blockchains enable direct ownership of digital credentials by both issuers and recipients.

It cannot be emphasised enough that use of *open technology standards* for digital credential issuance, storage, sharing, and verification is the precondition for realising these benefits of blockchain technology (Jagers, 2018[110]). Just like any other type of software, a blockchain can become a walled garden if there is no way to make the data it references communicable to others. Accordingly, the development of shared open standards for verifiable credentials is one of the most rapidly evolving areas of the blockchain technology stack.

The W3C Verifiable Credentials and Decentralised Identifier standards described in the previous section are seeing some of their first real-world applications in the education industry. This is largely due to the digital credentialing work educational institutions, non-profits, and education technology companies have engaged in for years and which has laid the groundwork for the formulation of the W3C standards. An early version of verifiable credentials, Blockcerts (Blockcerts, n.d.[111]), was developed by MIT and the company Learning Machine specifically for educational certificates like diplomas and transcripts. Blockcerts, in turn, grew out of the Open Badges standard for portable digital credentials, which was spearheaded by the Mozilla Foundation in 2011 and came into the custodianship of IMS Global in 2017 (Wikipedia, n.d.[112]).

Blockcerts made notable security and portability improvements to Open Badges that enabled its use for a wider range of high-stakes credentialing use cases, like diplomas and transcripts (Federation of State Medical Boards, 2019[113]). The Blockcerts reference libraries were published in 2016 under an MIT Free and Open Source Software (FOSS) license (Learning Machine Newsroom, 2016[114]). In 2017, Learning Machine was the first company to launch a commercial Blockcerts issuing platform, which it sold to educational institutions to issue digital diplomas and other educational certificates (Hyland Credentials, n.d.[115]). Other companies soon followed suit, and some schools developed their own Blockcerts issuing platforms as well (McMaster University Office of the Registrar, n.d.[116]; Unviersidad Carlos III de Madrid, 2018[117]). In a related project, the Government of Singapore forked the Blockcerts codebase to create their own open standard for digital credentials, OpenCerts (OpenCerts, n.d.[118]). In 2020, Learning Machine was acquired by enterprise content services firm Hyland and rebranded Hyland Credentials.

As the W3C Verifiable Credentials specification has matured, custodians of both Blockcerts and Open Badges (as well as OpenCerts) have committed to updating the standards to be compliant with the verifiable credentials specification. This is possible because the VC standard is flexible enough to accommodate many different credential types. As the education industry standardises around using VCs, credential exchange and interoperability across software platforms will be significantly enhanced (T3 Innovation Network, 2020[101]). In addition, the work being done to standardise the definitions of educational credentials will significantly facilitate the processing and exchange of educational records between schools and across borders.

Benefits of using blockchain technology in combination with these emerging open standards for educational credentials include the following: eliminate records fraud; streamline and reduce the cost of records sharing and verification, and; return control of personal data to individuals and reduce institutional risk.

Eliminate records fraud

Current state

Academic records fraud is pervasive and widespread. Studies estimate that over 100 000 degrees are simply purchased each year in the United States (Accredited Online Colleges, n.d.[119]); this would possibly include more than half of all PhDs (Ezell and Bear, 2012[120]). Moreover, validating the authenticity of a record is a separate process from validating the authenticity of a school: a "real" diploma may be purchased from a fake school, and fake diplomas that look like they are from real schools may also be purchased. In 2012, there were more than 3 300 unrecognised universities worldwide, many of them simply diploma mills (Ezell and Bear, 2012[120]); today the number is likely much higher. Moreover, real schools may have their academic records tampered by recipients looking to increase their chances of admission to particular jobs or programmes of study. The problem of records modification is so acute in some areas that, according to anecdotal reports, some secondary schools have simply stopped issuing academic transcripts (Smolenski, 2018[121]).

Professional licenses are forged with a frequency similar to academic records. In the United States alone, an Ohio State University Study estimated that up to 2 million medical practitioners may be practicing with fraudulent diplomas or licenses (Gibson, 2017[122]). Major news stories routinely surface in countries around the world about professionals practicing without licenses or with forged licenses (Gibson, 2017[122]) (CNN, 2020[123]). For the above reasons, an ecosystem of Credential Verification Organisations (CVO's) has arisen to validate the authenticity of schools and records; however, their efficacy has been limited.

The problem of fraud and of non-accredited higher education institutions delivering worthless degrees has been identified as a problem limiting the benefits of the internationalisation of higher education (OECD, 2004[124]). In 2005, UNESCO and the OECD issued "Guidelines for quality provision in cross-border higher education", which was followed by the establishment of a database of accredited institutions that is maintained by UNESCO (OECD, 2005[125]). This database is, however, difficult to make comprehensive and keep updated.

Blockchain with open standards

Blockchain provides a decentralised, transnational verification infrastructure to avoid fraud, facilitate international student mobility, and safeguard the public from professionals with illegitimate credentials anywhere in the world. Blockchain technologies, used in combination with leading open standards like Blockcerts and Verifiable Credentials, make use of advanced cryptography in combination with digital signatures to validate both the provenance of a credential (which institution issued it) and the authorised recipient (to whom it was issued). Digital signatures and hashed data, combined with an immutable blockchain ledger, ensure that a credential has not been tampered. Decentralised verification allows any third party (employer, government, school, or individual) to validate whether a credential was really issued by the claimed organisation to the claimed individual and whether any changes to the credential have been made since issuance. Credential revocation and expiration can also be instantly validated with the highest level of confidence. And just as these technical standards can be used to validate credentials issued to individuals, they can be used to validate institutional credentials as well, including elements like accreditation status.

Streamline and reduce the cost of records sharing and verification

Current state

Today, an individual applying for employment or further study must request their official academic records from their school, often for a fee, depending on the country or institution. They must also request that those records be sent by the school or by a software provider with whom the school contracts to the institution to which she is applying. The receiving institution then validates the credential by checking its integrity using the software vendor's solution, by contacting the school, or by checking with a third-party Credential Verification Organisation. The process is time consuming and often costly.

That is the best-case scenario, in which the issuing institution still exists and is able to locate, validate, or send the records to the receiving institution (relying party). In many cases, however, particularly in countries where political disturbances or natural disasters have struck, records have been destroyed, and issuing institutions may no longer be functional. In such cases, many record owners (the subjects of their own records) will have opportunities for employment, residency, citizenship, or further study closed to them because their qualifications or even identities cannot be validated.

When the records that must be verified were issued in a foreign country, an even more complex process called the Apostille is triggered. In 1961, a group of countries signed a treaty abolishing the requirement to legalise foreign public documents (Hague Convention, 1961[126]). Countries that are signatories to the Apostille Convention make use of an Apostille process to authenticate documents issued by designated authorities. Countries that are not signatories of the Convention require an Authentication Certificate from federal authorities of the issuing country to validate the authenticity of a foreign public document (US Department of State, Bureau of Consular Affairs, n.d.[127]). The authentication process involves conveying the original physical document, often with a supplementary request form and a fee, to a government institution authorised to issue the Apostille or Authentication Certificate. This institution will then issue a stamp on the document or a supplementary Certificate and mail the document(s) back to the recipient, who then must convey it to the authority of the foreign country in which they intend to live, work, or study. This process takes several months on average and causes the recipient to incur a financial cost. If documents cannot be authenticated, the recipient loses opportunities for travel, employment, and further study.

Blockchain with open standards

The combination of blockchain with open standards allows issuing institutions to issue records to recipients only once. After that, recipients can prove cryptographically that the record was issued to them and by which institution.

Recipients can share their records at their own discretion, and even choose which data within a record to disclose. Records may be verified by anyone to whom the recipient grants record access, instantly and for free. This facilitates not only the validation of academic credentials, like diplomas and transcripts, but also any document that must be Apostilled (as well as the Apostille Certificate itself). In 2020, companies Hyland and Hedera Hashgraph announced a proof of concept to anchor electronic Apostilles to a blockchain in partnership with the Texas Secretary of State (Texas Blockchain Council, 2021[128]). This proof of concept leveraged both verifiable credentials and PDF hashing, along with application-based workflow management to streamline and automate much of the process of issuing and verifying Apostilles.

With blockchain credentialing based on open standards, even if an issuing institution ceases to function, records are lost, or the software vendor whose product was used to issue such digital credentials no longer exists, the recipient still owns verifiable versions of their records and can share and verify them at will. As verifiable credentials are also fully machine-readable, schools verifying incoming records can pre-screen them for qualifications for particular programs of study. This dramatically cuts the receiving institution's overhead associated with validating records while removing friction for recipients as they seek opportunities for further learning.

When verifiable credentials standards are used, it also doesn't matter whether the organisation needing to verify a credential is located in the same country or in a different country from the one in which it was issued. Any authority in a foreign country can validate an individual's identity documents and qualifications by checking the document integrity, the cryptographic identifiers of issuer and recipient, and the status of the record. In short, use of the blockchain combined with open standards could, over time, significantly reduce or even eliminate the need for an international Apostille process or certificates of authentication.

As a result, open standards for blockchain-based credentialing stand to increase trust in the immigration process and international travel in general. This is why government departments like the US Department of Homeland Security have been investing in the development of Verifiable Credentials and Decentralised Identifiers: they see them as anti-counterfeiting technology standards for use by federal agencies like Customs and Border Protection (CBP) and the Transportation Security Administration (TSA).

Ultimately, the use of verifiable digital records, enabled by blockchain technology and open standards, will significantly reduce both the human and technological overhead currently associated with validating records issued both on paper and using legacy digital formats.

Return control of personal data to individuals and reduce institutional risk

Current state

Today, individuals may have in their possession copies or even originals of their official records, but they generally cannot have them validated by a third party without first requesting that the institutions that issued those records re-authenticate or re-send authenticated versions of those records. This often renders the official records actually in the possession of the individual functionally worthless. It disempowers the very person the records are about by removing their ability to share and verify them, re-inscribing their dependency on issuing institutions and third-party verification organisations. In effect, individuals cannot be said to own their records, even if those records are in their possession.

The current state also increases liability for institutions, who are tasked with being the lifelong curators and validators of official records on behalf of their constituents. Not only must institutions retain and safeguard growing troves of personal data, but since they are the ones sharing documents on behalf of individuals, they must comply with onerous regulations to protect the privacy of record subjects. Fines for mishandling data can be punitively high, particularly under new legislation such as the EU General Data Protection Regulation (GDPR).

Blockchain with open standards

Once a blockchain-anchored credential is issued to an individual using open standards, the individual is in possession of a digital file that attests to the provenance and integrity of the credential, as well as to their custodianship of it. Now individuals have a usable record that they can share instantly, without charge, with anyone they choose. Digital blockchain records can be re-used indefinitely without any need for re-issuance or additional validation by the issuing authority or any other party.

Since the locus of records ownership and sharing shifts to the individual, while verification is decentralised, issuing institutions no longer need to share records on behalf of their constituents and can dramatically reduce their internal records maintenance burden. This eliminates the need for storing large amounts of personal data for long periods of time and de-risks institutional data management by dramatically reducing the circumstances under which an institution must share a constituent's personal data.

Summary

The benefits of using blockchain technology in combination with open standards for educational credentialing – like W3C Verifiable Credentials and Decentralised Identifiers, among others – amount to an impressive list which can be grouped into three major categories:

1. *Security*. Open standards for blockchain credentialing prevent fraud, mitigate risk for institutions that both issue and validate official documents, and protect the brands and reputations of education providers as well as qualification holders. As verifiable credentials adoption increases, their use in credentialing, screening, and hiring will likely become an industry best practice or even a legal requirement.

2. *Public good*. Blockchain records that use open standards remove barriers to accessing opportunity and facilitate economic development by increasing trust in institutions and workforce qualifications while mitigating the devastating effects of political conflicts and natural disasters. When people control their own records, they are free to continue using them anywhere in the world, while relying parties enjoy a high level of confidence in credentials issued anywhere.

3. *Efficiency*. Blockchain records that use open standards dramatically increase the efficiency and convenience of records management: the need to re-issue or manually verify documents drops by an order of magnitude; the need to use other record formats is removed over time; and records sharing and verification is instant and free. Processes like credit transfers, which are notoriously complex and time consuming for educational institutions, can be automated with the advent of machine-readable, verified course content.

A consensus is growing behind these benefits. A recent report by the US Chamber of Commerce Foundation's T3 Innovation Network on the benefits of adopting self-sovereign approaches to learner records summarised them as follows:

- "Learners have control over who can access their record(s), including aspects of their records, and when they are allowed to access them.
- Authentication is cryptographically secured, most typically on distributed ledgers, making the credentials verifiable, and accessible regardless of the state of the issuing organisation at the time of verification.
- Online verification of learners and issuers can be secured and streamlined.
- Verifiable credentials can support verification of non-traditional achievements providing evidence of learning in various contexts." (T3 Innovation Network, 2020[101]).

The benefits of an approach to credentialing that leverages both blockchain technology and open standards make it a valuable component of digitisation projects for any institution that issues or validates official documents. Such an approach is the prerequisite for creating a truly interoperable global ecosystem for digital credentials: where anyone can exchange academic records with anyone else and instantly screen and verify them without fear of fraud. Due to their deep investment in credentialing economies, education providers have been among the first to implement blockchain credentialing programs. The following section reviews several examples of educational institutions that have embarked on this path.

Real-World implementations

Any situation in which fraud must be prevented is a potential blockchain use case. This is because, as the previous sections have described, the blockchain is primarily an infrastructure for verifying claims. For this reason, blockchain is set to revolutionise every «trust industry,» from banking to insurance to law enforcement, healthcare, and supply chain management (McCauley, 2019[129]). It is education, however, that has been at the forefront of blockchain technology adoption, as the verification of academic credentials continues to be an ongoing and pressing need (Grech and Camilleri, 2017[130]).

But verifying qualifications is a requirement far beyond the education industry; employers worldwide have a clear interest in receiving credentials they can rely upon with the highest degree of confidence. Multilateral institutions like the Inter-American Development Bank have noted that credentialing human capital in a verifiable way is one of the easiest ways to create trust in a global economy (Cabrol, 2018[131]). For this reason, the American Council on Education observes, "blockchain, in particular, holds promise to create more efficient, durable connections between education and work. It can provide the technological fabric to help displaced workers translate their skills for new education opportunities and employers, and may hold particular value for those currently underserved by the existing education-to-employment paradigm." (Lemoie and Souares, 2020[44]).In particular, the shift towards a lifelong learning model for education and the ever-increasing mobility of learners and workers make verifiable credentials a prerequisite for economic momentum in the twenty-first century. The term "ecosystem" is frequently used by blockchain technologists, employers, and educational institutions to describe the ideal state of credential exchange and verification.

This section features several examples of real-world implementations of blockchain-based credentialing in education from countries around the world. Note that not all of the projects that have been built to date have real users yet (or customers, if they are commercial). Some of these projects have been announced, but little public information is available to track their implementation or uptake. Accordingly, this list is to be taken as a snapshot of what the blockchain credentialing market looks like in the first few years of its development, with the understanding that this landscape will continue to rapidly evolve.

United States

It can be said that the birth of open technical standards for verifiable digital credentials occurred at MIT. In 2015, the Learning Initiative division of the MIT Media Lab began working on a project to anchor academic credentials to the blockchain (MIT Media Lab, n.d.[132]). Soon thereafter, the company Learning Machine (since 2020, Hyland Credentials) joined forces with this team to bring the project to fruition (MIT Media Lab, n.d.[133]). In 2016, Blockcerts, the open standard for digital credentials, was published under an MIT Free and Open Source Software (FOSS) license at blockcerts.org (Blockcerts, n.d.[111]). In 2017, the Blockcerts references libraries allowed anyone to create their own software applications for issuing, storing, sharing, and verifying secure digital credentials. The verifiable credentials technology was intentionally made open source in order to avoid vendor lock-in and create an open ecosystem for credentialing applications. Blockcerts is also blockchain-agnostic, meaning that it supports anchoring to most blockchain network types. Current implementations include Bitcoin, Ethereum (Learning Machine, 2018[134]), and Hyperledger Fabric (Castro-Iragorri, 2018[135]). In 2017, Learning Machine launched a commercial credential issuing system. In 2019, it announced that it would update Blockcerts to become a W3C Verifiable Credential (Jagers, n.d.[136]).

A number of US universities and K-12 institutions issued credentials using Blockcerts to their students and graduates (Hargrave and Karnoupakis, 2020[137]). These include MIT (Durant, 2017[138]), SNHU (Kelly, 2018[139]), Union Public Schools in Tulsa, Oklahoma (Friedman, 2019[140]), ECPI University (Southside Daily Staff, 2018[141]), Maryville University (Learning Machine Company Newsroom, 2019[142]), and Central New Mexico Community College (Salas, 2018[143]), among others. In 2020, the first statewide implementation of blockchain credentialing in the United States was launched by the New Mexico Higher Education Department (Hyland Newsroom, 2020[144]).

In February 2020, a consortium of research institutions around the world announced bloxberg, a fork of Blockcerts designed to anchor proof of scientific research to a private blockchain network (Bloxberg, 2020[145]).

A host of new projects are also emerging. In February 2020, the Digital Credentials Consortium (DCC) issued a white paper on the digital credentials infrastructure for the future, aligned with the W3C Verifiable Credential model and with the EU General Data Protection Regulation (Digital Credentials Consortium, 2020[146]). In 2018, MIT and eleven other international universities from Canada, Germany, Italy, Mexico the Netherlands, the United States founded the Digital Credentials Consortium to develop an infrastructure for issuing, sharing, and verifying digital credentials of academic achievement in higher education. A report released by the American Council on Education and the US Department of Education's Office of Educational Technology provides a useful survey of blockchain credentialing initiatives in the United States (Lemoie and Souares, 2020[44]):

- Workday Credentials is a platform for issuing blockchain-anchored records using the W3C Verifiable Credentials standard (Workday Credentials, n.d.[147]). It uses a private implementation of Hyperledger Fabric to anchor records (Ledger Insights, 2020[148]; Meetup, 2020[149]).

- Pistis.io provides web and mobile wallets for recipients to upload documents and hash them to a blockchain built on Hyperledger Fabric (Pistis.io, n.d.[150]).
- Greenlight provides a blockchain network currently used by five independent school districts in North Texas to exchange academic records and help lower-income students apply to multiple colleges at once. The network is a private implementation of Hyperledger Fabric (Lemoie and Souares, 2020[44]).
- Salesforce has launched the Trusted Learner Network, a private blockchain network powered by Hyperledger Sawtooth.
- Arizona State University is currently using Salesforce's Trusted Learning Network to send course completion records to the two-year schools from which their students have transferred (Lemoie and Souares, 2020[44]).
- ODEM and BitDegree also include credentialing as one of the functionalities of their Ethereum-based education marketplaces.
- The San Jose State University School of Information is applying for a grant to use an SSI universal resolver to "enable individuals with verifiable digital credentials to gain access to resources at all participating libraries." (Lemoie and Souares, 2020[44]).
- The Learning Economy Foundation is involved with the Arizona State University Trusted Learner Network implementation (Arizona State University, n.d.[151]). It is also leading blockchain credentialing projects in Colorado (the C-Lab) (Learning Economy Foundation, n.d.[152]), North Dakota (the ND ILR Co-Lab) ((n.a.), n.d.[153]), Florida (the Broward County OpenCLR Lab) (Learning Economy Foundation, n.d.[154]), and the Asia-Pacific Region (Asia-Pacific AP Lab) (Learning Economy Foundation, n.d.[155]).

Canada

The Government of Canada may have taken the lead internationally in terms of self-sovereign credentialing applications. In 2018, the Digital Identity Office at the Treasury Board of Canada Secretariat released "Canada's trusted digital identity vision," a short film demonstrating a future in which citizens can apply for and manage a variety of government services and benefits online using private, secure forms of authentication (Treasury Board of Canada Secretariat, 2018[156]). The Province of British Columbia was among the first to implement a live digital credentialing project using SSI: the OrgBook, which uses Hyperledger Indy to manage verifiable credentials for over 1 million active businesses in the province (Lemoie and Souares, 2020[44]).

In 2019, the Government of Canada Talent Cloud initiative started to certify "Free Agent" public sector workers using Blockcerts (Benay, 2019[76]; Talent Cloud | Nuage de talents, 2018[157]). The Talent Cloud is a public sector talent marketplace that reimagines a skill and credential recognition ecosystem for Canada's Public Service (Government of Canada Talent Cloud, n.d.[158]; Greenspoon, 2018[[159]; World Government Summit et al., 2018[160]). Public sector workers can maintain a profile on the Talent Cloud that includes validated qualifications and experience, which serve as evidence of skill when applying for any public sector job.

McMaster University in Hamilton, Ontario, also built its own Blockcerts issuing system, which is used to issue digital diplomas to graduating students today (McMaster University Office of the Registrar, n.d.[116]).

Most recently, the Association of Registrars of the Universities and Colleges of Canada (ARUCC) has announced a partnership with Digitary to build a national credentialing network for Canadian higher education institutions (Hamdani, 2020[161]). Digitary has, in turn, partnered with Evernym to implement a blockchain-based credentialing solution (Crace, 2019[162]). Evernym's solutions implement W3C Verifiable Credentials leveraging the Sovrin and Hyperledger Indy blockchain networks.

European Union and United Kingdom

Within the European Union, the country that has made the farthest advances in applying blockchain for educational credentialing is Malta. Since 2017, Malta has branded itself the "Blockchain Island" as a result of Prime Minister Joseph Muscat's decision to embark on the "calculated risk" of investing in blockchain technology to fight corruption, cut bureaucracy, and diversify the country's booming tech sector (Al Ali and van der Walt, 2018[163]).

In January 2017, Malta's Ministry for Education and Employment (MEDE) started to implement the world's first nationwide pilot project for issuing academic credentials to a blockchain (Sixtin, 2017[164]; Cocks, 2017[165]). Since that time, the project has expanded in scope to include all educational institutions in Malta (Sansone, 2019[166]).

In Spain, the Alastria blockchain network was designed and built by a consortium of over 500 businesses, government institutions, and universities with the aim of facilitating digital services, including academic credentialing (Alastria, n.d.[49]). SmartDegrees also emerged, using the Ethereum-based Quorum blockchain to anchor digital credentials (SmartDegrees, n.d.[167]). Vottun is another Spanish blockchain credentialing firm, this one using the public Ethereum blockchain (Vottun, n.d.[168]).

In Central Europe, SAP launched its TrueRec credentialing platform using Ethereum, which it piloted with KU Leuven University (Jonkers, 2018[169]). The Slovenian firm 0xcert created their own open standard for tokenising and transferring ownership of digital credentials as well as other digital assets (0xcert, n.d.[170]).

Within the United Kingdom, GradBase offers a blockchain credentialing system using the Bitcoin blockchain (GradBase, n.d.[171]). PwC UK has introduced "SmartCredentials," a credentialing platform built on a permissioned version of Ethereum (PwC UK, n.d.[172]). The Open University's Open Blockchain initiative (The Open University, n.d.[173]) explores a number of applications of blockchain credentialing, primarily using Ethereum: blockchain-anchored Open Badges and Blockcerts. These include QualiChain (The Open University, n.d.[174]), a platform for matching employers with job seekers, and PeerMiles (The Open University, n.d.[174]), an initiative to recognise the reviewing records of researchers. These are both research projects rather than commercial software applications.

All of these initiatives will need to reckon with the standardisation being introduced not only by the W3C, IEEE, and ISO, but also by the European Blockchain Services Infrastructure (EBSI), a collection of blockchain networks under development by the European Commission and European Blockchain Partnership, a coalition of EU member states dedicated to researching public sector applications of blockchain technology. The EBSI is funded by the Connecting Europe Facility, which is responsible for supporting the mandate for a Digital Single Market throughout the EU (CEF Digital, n.d.[40]). The purpose of the EBSI is to serve as an infrastructure for cross-border digital services. In this sense it is similar in scope to Spain's Alastria network, but with a pan-European mandate. A number of participants in the Alastria project are now coordinating build-out of the EBSI.

The EBSI currently makes use of Hyperledger Besu (a permissioned implementation of the Ethereum codebase) and Hyperledger Fabric, but its intention is to become blockchain-agnostic. Technical documentation of this open source project is available to the public (CEF Digital, n.d.[175]). The four initial use cases targeted by the EBSI are:

1. Notarisation of documents for auditing purposes;
2. Certification of diplomas;
3. The European Self-Sovereign Identity Framework (ESSIF); and
4. Trusted data-sharing (Allen, 2016[100]; CEF Digital, n.d.[176]).

Version 1.0 of the EBSI launched in February 2020, and future releases are anticipated on an annual basis (Smolenski, n.d.[177]). Open market consultations have begun to help shape future development grants for private firms intending to build services on the network.

The EBSI is separate from the Europass project, another EU-wide digital credentialing initiative. The Europass is overseen by the Commission's Directorate-General for Education and Culture and aims to make skills portable and recognisable across Europe. Since 2012, the Europass web portal has allowed individuals to create an electronic portfolio of their academic credentials and other qualifications, their "European Skills Passport". These five standard documents are not anchored to a blockchain, but are stored in XML format and may be digitally signed by the issuing institution using signing keys provided by authorities trusted under the eIDAS regulation for electronic identification and signatures. Through the European Skills/Competencies, Qualifications and Occupations (ESCO) initiative, Europass profile holders can also be matched with job opportunities via the ESCO semantic classification (European Commission, n.d.[178]).

In 2018, a set of requirements for digitally signed Europass documents were elaborated, drawing heavily on the established eIDAS trust framework. This set of requirements is referred to as the European Digital Credentials Infrastructure (EDCI) (everis, n.d.[179]). Distinct from the EBSI, the EDCI does not employ blockchains for verification, with the exception of the accredited status of issuing authorities. These are to be anchored to a blockchain—presumably, eventually this will be the EBSI. The EDCI is in effect an open standard for issuing, receiving, storing, sharing, and verifying digitally signed documents, much like Blockcerts and Verifiable Credentials. As the EDCI was not elaborated in partnership with the W3C, however, it diverges from the verifiable credentials specification in several respects, most notably by requiring the use of XML rather than JSON. These discrepancies are currently being reconciled within the W3C Credentials Community Group.

Middle East and North Africa

The Middle East and North Africa (MENA) region has been the site of considerable enthusiasm for blockchain technology, particularly since the announcement of the United Arab Emirates' "Blockchain Strategy 2021" in 2018 (The United Arab Emirates' Government portal, n.d.[180]). The initiative aims to place 50% of government transactions on a blockchain by 2021 and has been closely involved with the Smart Dubai 2021 (Smart Dubai 2021, n.d.[181]) initiative. As part of its strategic push towards blockchain, the UAE government has sponsored numerous start-up competitions to identify local vendors who may be able to supply public and private sector services.

One UAE-based provider in the academic credentialing space is Educhain. Having won the Techstars start-up competition, they went on to implement several blockchain credentialing pilots with UAE educational institutions in both higher education and K-12 segments. These include United Arab Emirates University (UAEU, 2019[182]), the University of Dubai (CNN, n.d.[183]), and AMSI (AMSI, n.d.[184]).

In 2020, the firm Shahada was launched (Smartworld, 2020[185]). It sells a SaaS platform, also called Shahada, to create and issue blockchain-anchored digital credentials. Its website states that "Shahada builds on the open standards developed by MIT" (Shahada, n.d[186]). Shahada is a joint venture between Smartworld, a leading UAE systems integrator, and Grape Technology, a UAE-based start-up specialising in blockchain technology (Shahada, n.d.[186]). The firm has successfully issued blockchain-anchored credentials for the University of Dubai (Zawya, 2020[187]). It has also integrated its platform with UAE Pass, which ensures recipient identity verification for government and commercial services throughout the country (Smartworld, 2020[185]).

In Egypt, Zewail City of Science and Technology signed an MOU with start-up Intelli Coders to build "BlockCred," (Abdou, 2019[188]) a blockchain credentialing system for educational and professional training programmes in the city (BlockCred, n.d.[189]). BlockCred is a DApp built on the Blockstack blockchain platform.

First in the MENA region to issue blockchain-anchored academic credentials was King Abdullah University of Science and Technology (KAUST) in Saudi Arabia (Company Newsroom of Learning Machine, 2018[190]). In 2018, it used Learning Machine (now Hyland Credentials) to issue its first Blockcerts-compliant digital diplomas. The University of Bahrain soon followed suit (Global Blockchain Business Council, n.d.[191]). As of November 2020, both universities continue with their digital credentialing initiatives.

Latin America and the Caribbean

Latin America has been the site of a growing number of blockchain credentialing initiatives in recent years. The projects that have announced implementation have generally employed the Blockcerts open standard for digital credentialing. These include the issuance of digital diplomas by Tecnológico de Monterrey, Mexico's premier technical research university (Longino Torres, 2019[192]). Universidad Autónoma de Nuevo León implemented a Blockcerts credentialing project in partnership with Learning Machine via a local implementation partner, SYSARTEC (SYSARTEC, 2020[193]). The Ministry of Labor in the Bahamas and the Caribbean Examinations Council also delivered Blockcerts pilots for workforce training, graduation certificates, and examination results (Munro, 2018[194]; Jamaica Observer, 2019[195]).

Another solution provider offering a Blockcerts credentialing system in the region is Xertify, a Colombia-based digital credentialing company (Xertify, n.d.[196]). The Dirección Estatal de Profesiones in the State of Querétaro in Mexico has been using Xertify to issue a digital Cédula Profesional (professional license) for many types of practitioners (La Fuente Querétaro, 2020[197]; @profesionesqro, 2020[198]). Xertify also works with universities in the region, including Universidad ECCI (@xertifyco, 18 June 2020[199]) and Universidad Quindío (@xertifyco, 12 June 2020[200]) in Colombia, to issue digital diplomas.

Prince Consulting, a software services firm based in Argentina, has also implemented Blockcerts credentialing projects for educational institutions through its subsidiary, OSCity (Prince Consulting, n.d.[201]).

A major regional project, sponsored by the Inter-American Development Bank, is modelled on Alastria: LACChain. Led by a coalition of public and private organisations, the project aims to build a blockchain for the delivery of commercial and public services in the region (ConsenSys, 2020[50]).

Asia Pacific

In Singapore, blockchain credentialing saw quick uptake. A couple of notable start-ups created platforms for issuing credentials anchored to the Ethereum network: Attores, a blockchain development firm offering "smart contracts as a service," and Indorse, a reputation platform designed to match candidates with job opportunities. In 2017, Attores piloted blockchain diplomas with Ngee Ann Technical University (McSpadden, 2017[202]). Since their initial launch, Attores and Indorse have merged, preserving the Indorse brand and pivoting to become a professional development tool for software engineers (Indorse, n.d.[203]). In the same timeframe, the Government of Singapore developed OpenCerts, an open standard for issuing blockchain-anchored digital credentials built by forking and modifying the Blockcerts codebase (OpenCerts, n.d.[118]). It has since strongly encouraged universities to use OpenCerts by partnering with local software development firms who can build issuing applications using the OpenCerts open source reference libraries (OpenCerts, n.d.[77]).

In 2018, the Ministry of Education in Malaysia announced a project to issue academic credentials to the NEM blockchain, built by the Council of ICT Deans at Malaysian Universities (Asia Blockchain Review, 2018[204]).

In 2019, Pallavan Learning Systems (PLS) became the first K-12 institution in India – and potentially the world – to issue Blockcerts to their students. The Pallavan School in Jhalawar, Rajhastan and Vasant Valley School in New Delhi issued multiple types of credentials: School Leaving Certificates, Language Certificates, Character Certificates, Letters of Recommendation, and Five Areas of Development Mark Sheets (Company Newsroom of Learning Machine, 2020[205]).

In 2019, the Hong Kong University of Science and Technology (HKUST) began issuing award certification letters as Blockcerts using a system it built in-house (HKUST Academic Registry, n.d.[206]). HKUST continues to evolve the system to issue degree diplomas and transcripts.

Driving change

The adoption of new technologies presents opportunities and challenges for institutions looking to adapt existing practices and workflows. These challenges broadly fall into two categories: ideas and logistics.

Ideas challenges include:

1. Needing to think in new ways.
2. Emotionally accepting new trade-off decisions: new ideas have different advantages and disadvantages than do old ones.
3. Difficulty imagining what change will look like.
4. Changes to roles and responsibilities that people may feel comfortable with.
5. Difficulty imagining what success will look like.
6. Separating means from ends: the same ends (i.e. security, empowerment, confidence, risk mitigation) may be better achieved using different means from what is employed today.

Logistical challenges include:

1. How do we implement a new technology and associated processes?
2. What happens to our legacy technology investments?
3. How expensive will it be?
4. Who will be there to guide and support us through the change?

5. How can we utilise our internal resources most effectively?
6. Can we go back to the old way of doing things if the new way does not work?
7. Are there hidden traps or tricks we are unaware of?

These challenges can be navigated by skilful leadership within organisations that helps teams implementing new technologies understand both the why (ideas) and the how (logistics) of change. This means helping people think about change in a way that is both enthusiastic about the real benefits it promises and realistic about the work required to successfully bring it about.

In the transition to verifiable credentialing for education, there are two broad stakeholder groups who have an outsized say in how that change comes about: policymakers and educational institutions. This section presents a few suggestions for how these groups may approach this aspect of technological transformation.

What can policymakers do?

Many look to policymakers to understand if what they are doing is in line with the values and laws of their community; policymakers are also often sought out for normative guidance: what should be done? As such, policymakers should consider what kinds of goals they have in mind for their communities and whether or not a new technology is instrumental in achieving those goals.

In the case of verifiable credentials, the advantages are quite clear: they increase trust across the board, speed up economic transactions, streamline the process of applying to schools and jobs, facilitate and add security to cross-border mobility, and empower holders with verifiable records of lifelong learning. Within education, it seems clear that implementing blockchain-based credentialing solutions benefits educational institutions, students, employers, and as a result, entire economies.

When examining existing laws and policies, it is good to ask if a regulation intended to achieve a particular objective (for example, validating that a credential was issued by the correct authority) is tied to a technical implementation that is too specific. Legislation that mandates particular technical implementations can end up stifling innovation, as technology evolves at a rapid clip that often can't be anticipated. As a general rule, effective policy provides frameworks for a solution to a problem rather than being overly prescriptive about the solution itself. This enables the ingenuity of a community to flourish while setting clear guidelines about the boundaries of what is legally acceptable.

As people in positions to set priorities for a community, policymakers can also determine how funds are allocated to new technology projects. This may include spending on R&D initiatives, a public investment fund providing capital to young start-ups, investing in education and training in underserved communities, and providing support for new technology pilots or more mature implementations.

Some governments may choose to fund the build-out of their own blockchain networks or technology standards. However, these projects should bear in mind that the value of verifiable digital credentials lies in two things: 1) international portability and 2) platform independence. Any technology infrastructure, whether built by the public or private sector, that creates lock-in or limits utility across borders will create challenges to adoption and scalability. It will also create additional bureaucratic hassles, which is at odds with the promise of verifiable credentials. Accordingly, government-led technology projects should keep closely in sync with the work of global standards bodies like the W3C, IEEE, ISO, and others, to ensure that what is developed for their populations has usability internationally and across software platforms.

Resources can also be allocated in the form of time and attention. Policymakers taking the time to understand the motivations and concerns of technologists working on new solutions to problems can go a long way towards speeding along the rate of innovation in a community. In taking this initiative, policymakers also open the door for technologists to understand their concerns and ideas as well. Where policymakers and technologists see one another as hostile, cooperation stalls and mistrust can polarise a society. But time spent building something together across differences of opinion and background is time well spent.

What can educational institutions do?

When approaching the idea of using blockchain-anchored verifiable credentials, one of the first things educational institutions can do is recognise that the technology landscape is changing. The 21st-century economy requires portable, verifiable digital credentials, and students will increasingly expect them from any institution they attend. The COVID-19 pandemic, in particular, has highlighted the need for schools to issue portable, secure documents that can be received, shared, and verified safely at a distance. While using blockchain technology may not be in an institution's immediate plan, nevertheless being informed about the landscape of offerings and thinking through implementation best practices can begin today.

As for the question of how to implement the technology, there are many ways for educational institutions to begin issuing and verifying blockchain credentials. Issuing institutions who opt for solutions based on open standards, like W3C Verifiable Credentials and Blockcerts, have two main paths forward: either by building their own applications for credential issuing using the open source reference libraries or by licensing a vendor-supported product or service to issue standards-compliant records. Those who choose solutions that are not based on open standards limit their options to either vendor-supported services or idiosyncratic solutions built and maintained in-house. These may run into data portability and interoperability issues over time.

Whatever path they choose, any institution contemplating the issuance of its official records using the blockchain may use the following brief recommendations as a guide.

1. *Identify use cases.* The blockchain is the most secure verification structure available for credentials, so it is best suited for records that must be verified with a high level of certainty. In education, these records include, but are not limited to, diplomas and degrees, transcripts, school leaving certificates, diploma supplements, comprehensive learner records, student IDs, and examination results. For education professionals, teaching licenses or warrants or certification of continuing professional education are promising places to start. Blockchain is less needed for more ephemeral credentials that only need temporary validation. However, the latter may "stack up" to higher-level credentials that are anchored to a blockchain.

2. *Future-proof your initiative by committing to open standards.* Many vendors in the blockchain credentialing space have created custom solutions in which credentials only display and verify within their vendor-controlled software system or blockchain network. This ties ongoing access, sharing, and verification of credentials to that particular vendor. Rather than making your organisation's use of official records dependent upon a software provider and risking having to "re-do" a digital credentialing implementation if you switch services, choose open architectures to make your credentialing solution a lasting one. Insist upon the use of open standards (Blockcerts, verifiable credentials) and blockchains that are either public (like Bitcoin or Ethereum) or permissioned and private blockchains maintained by institutions with a public mandate, like governments or consortia of well-established organisations (for example, the EBSI). This increases the likelihood that those organisations will have the resources and longevity to maintain an expensive permissioned or private blockchain network over time.

If, as an institution, you choose to contract with a vendor to provide a blockchain credentialing solution rather than building one in-house, below are a series of recommendations that will help you make the best vendor selection for your institution.

1. *Choose a software provider experienced in the delivery of credentialing solutions based on open standards.* The market for digital credentials is growing, and with it a growing number of vendors are offering solutions. A subset of those vendors are committed to using open standards, and a smaller subset of those vendors have experience successfully implementing digital credentialing projects. An experienced vendor should be able to point to case studies in which their software was used to successfully deliver and build on a high-stakes digital credentialing project, then describe how their process could be adapted to your institution's needs.

2. *Select a vendor who will help you create and execute on an implementation plan.* Blockchain credentialing is a relatively new field. As such, a change management component is a critical part of any successful implementation. Ask vendor candidates about their typical onboarding and implementation process and how

they will help you introduce this new credentialing initiative alongside your current credentialing practices. How will you define objectives? How will you measure success? A strong vendor partner is available to assist with these questions.

3. *Be prepared to budget for your blockchain credentialing initiative.* Blockchain credentialing is an exciting field that leverages cutting-edge new technology to deliver unparalleled convenience and certainty with regards to digital claims. This is an advanced technology, however; not a commodity. Your institution should be prepared to set aside an annual budget item to cover the costs of the initiative, much in the same way you budget for issuing paper or PDF digital records. Over time, you can sunset older ways of credentialing and potentially create savings by switching fully to a verifiable credentials model. Financial return on investment will vary based on your institution's current credentialing practices, blockchain credentialing vendor selection, and implementation model. You may want to request a return on investment (ROI) analysis from vendors prior to selecting your provider(s), but be aware that this will require you reveal the current costs (in time, personnel, and money) of your existing credentialing practices.

While there is always a switching cost associated with the adoption of new technologies, it is time for educational institutions to begin the transition to blockchain-anchored verifiable credentials. Not only must the proliferation of academic and professional fraud be firmly rooted out, but the continuing growth in the global mobility of learners and workers alongside mass displacement due to conflict, natural disasters (including climate change), and most recently the pandemic make verifiable credentials a critical precondition not only for streamlining the movement of learners between educational institutions and from education to employment, but of preserving public safety as people live and work across highly varied jurisdictions and geographies (Jagers, n.d.[207]). As educational institutions have been forced to move operations online and internationalise in unprecedented ways due to the COVID-19 pandemic, the shift to verifiable digital credentials forms an integral part of any institution's overall digitisation strategy.

Conclusion

The global education landscape is rapidly changing. By 2030, over 7 million students are expected to travel internationally for higher education (Holon IQ, 2018[208]). The rapid growth of developing economies in Asia and Africa is expected to fuel a massive expansion of the education sector, adding over 350 million post-secondary graduates and 800 million secondary graduates to the global marketplace (Holon IQ, 2018[209]). The world's teaching capacity is already strained, but over 100 million new teachers will be required to meet the projected need (Holon IQ, 2018[209]).

This represents a significant opportunity for new technologies, including artificial intelligence, process automation, digital education marketplaces, and blockchain to help scale global education infrastructure. The vital role of technology in meeting the needs of this generation of students is expected to propel the global education technology market to USD 10 trillion by 2030 (Holon IQ, 2018[209]). In all economies, the need for technology-driven upskilling and reskilling is keenly felt.

COVID-19 has slowed enrolment in higher education somewhat, but not uniformly, and not permanently (Hess, 2020[210]; Miller, 2020[211]). It is mostly a response to the still heavily brick-and-mortar status quo for the delivery of education. As valuable as such a model is, it is seeing difficulty both with responding to a communicable disease pandemic and scaling its operations to accommodate virtual education delivery. In addition, many brick-and-mortar higher education institutions are loss-making, relying on donations and grants to make ends meet. Many were already financially precarious before COVID-19 struck, and the pandemic has accelerated insolvency for some (Thys, 2020[212]).

As institutions adapt, however, we will likely see enrolments continue to grow as a result of projected population growth. Educational institutions will increasingly rely on time-saving and cost-saving technologies to streamline administrative operations, deliver educational content, conduct assessments, credential students, and connect them with employment opportunities.

What does this mean for credentialing? The most easily credentialed skills – and the most valuable credentials to have in the labour marketplace – will likely continue to be associated with hard skills, or skills that can be most easily quantified and tested (Trilling and Fadel, 2009[213]). Jobs and professions requiring credentials are most likely to remain in technical and analytical fields. This does not mean, of course, that soft skills are not critical for professional success (Beheshti, 2020[214]); only that they are less easily quantified, tested, and credentialed. Despite flourishing movements to credential a broader range of learning experiences (Parrish, Fryer and Parks, 2017[215]), competencies, and skills (Reed, 2016[216]), employers are likely to continue relying on personal recommendations, evidence of past achievements, and reputation to assess soft skills in prospective applicants.

Nevertheless, where credentials are required or desired, being able to share, receive, and verify them instantly in a portable, interoperable digital format will quickly become a table-stakes expectation. The blockchain is an ideal technology to enable this, since it acts as a distributed, digital verification infrastructure for records and claims. With growing momentum among technologists and policymakers to return control of personal data back to users, an international standards movement has arisen to ensure that blockchain-anchored credentials are issued, stored, shared, and verified in a manner that protects user privacy and is independent of any particular vendor infrastructure.

This paper has described how these international technology standards for verifiable credentials are being applied in the sphere of education. As this field is evolving rapidly, the market landscape described here will likely look very different in even a few months. However, the standards described here will likely remain critical connective tissue for a rapidly accelerating global ecosystem of credential exchange. Institutions looking to implement a verifiable credentialing program should look to these standards to ensure that their projects protect privacy, empower users, and ensure credential mobility for all.

The early adoption of verifiable credentials for academic records by some educational institutions has placed the education industry at the forefront of one of the most significant technological innovations since the advent of the internet: a new "trust layer" for digital claims that has broad applicability across industries and use cases. Much as blockchain technology represents a distributed, tamper-proof version of an accounting ledger, verifiable credentials standards are mechanisms to detect tampering and validate a credential's provenance and recipient in a decentralised manner. This technology will likely see parabolic adoption in coming years as institutions move to prevent fraud, streamline the processing and verification of claims, and return control of personal data to end users. The end result is an ecosystem that enables individuals to maintain a lifelong record of achievement and seamlessly transfer between institutions and geographies to live, work, and study.

As the world of learning and work continues to become more mobile and interconnected, people require higher levels of digital trust in order to live, learn, and do business together. Facilitating that trust is both the value and the promise of blockchain technology.

Annex 11.A
Appendix: Technical glossary

Blockchain: A type of distributed ledger that records an append-only, immutable database of transactions. Blockchains were originally used to maintain a record of who owns digital currency, thereby preventing the reproduction and tampering of digital assets. This same technology can be employed to verify the integrity of and track ownership of any digital asset, including academic credentials.

Cryptography: "Secret writing." A way of protecting information by using codes so that only intended recipients may read or use it.

Decentralised Identifier (DID): A globally unique identifier that does not require a centralised registration authority because it is registered with distributed ledger technology or other form of decentralised network.

Distributed Ledger Technology (DLT): A database that is consensually shared and synchronised across multiple sites. Each site of the DLT network runs a part of its infrastructure and can write or access the entries shared across that network based on permission controls. Any changes or additions made to the ledger are reproduced across all sites. A blockchain is a type of distributed ledger, usually with an attendant cryptocurrency.

Self-Sovereign Identity (SSI): "A set of technical standards and a set of community-promulgated principles seeking to enable a shift towards more individual control over digital identities and personal data."[1]

Verifiable Credential (VC): A digital credential that is tamper evident and whose provenance (authorship) can be cryptographically verified.

Note

1. T3 Innovation Network. "Applying Self-Sovereign Identity Principles to Interoperable Learning Records: Principles, Challenges, and Community Guidance." US Chamber of Commerce Foundation. June 2020. p. 2; https://www.uschamberfoundation.org/sites/default/files/media-uploads/Applying%20SSI%20Principles%20to%20ILRs%20Report.pdf

References

(n.a.) (n.d.), *ND Integrated Learner Record: Phase II Project Charter*, https://docs.google.com/document/d/1hiKCNepcPQkCDHy7yFT9x613RWjK7Mjk/edit (accessed on 5 February 2021). [153]

@profesionesqro (2020), *Twitter*, https://twitter.com/profesionesqro/status/1256225566631567360. [198]

@xertifyco (12 June 2020), *Twitter*, https://twitter.com/xertifyco/status/1271571738044792832. [200]

@xertifyco (18 June 2020), *Twitter*, https://twitter.com/xertifyco/status/1273813449311760390. [199]

0xcert (n.d.), *Blockchain API gateway*, https://0xcert.org/ (accessed on 16 November 2020). [170]

Abdou, M. (2019), *MOU between Zewail City and Intelli Coders, LLC to use blockcred.io for academic credentials issuing*, Medium, https://medium.com/blockcred/mou-between-zewail-city-and-intelli-coders-llc-to-use-blockcred-io-a3124bafe143 (accessed on 26 June 2020). [188]

Accredited Online Colleges (n.d.), *Fake Schools, Fake Degrees: Avoiding Diploma Mills*, https://www.accredited-online-college.org/avoiding-diploma-mills/ (accessed on 16 November 2020). [119]

Al Ali, N. and E. van der Walt (2018), *Blockchain Island Dream Is 'Calculated Risk' Says Malta Leader*, Bloomberg, https://www.bloomberg.com/news/articles/2018-09-10/blockchain-island-dream-is-calculated-risk-says-malta-leader (accessed on 16 November 2020). [163]

Alastria (n.d.), *Alastria*, https://alastria.io/en/la-red/ (accessed on 13 November 2020). [49]

Alden, L. (2021), *A Century of Fiscal and Monetary Policy: Inflation vs Deflation, LynAlden.com.*, https://www.lynalden.com/fiscal-and-monetary-policy/. [15]

Ali, A. (2021), *Bitcoin is the Fastest Asset to Reach a $1 Trillion Market Cap*, Visual Capitalist, https://www.visualcapitalist.com/bitcoin-is-the-fastest-asset-to-reach-a-1-trillion-market-cap/. [19]

Allen, C. (2016), *The Path to Self-Sovereign Identity, Life with Alacrity*, http://www.lifewithalacrity.com/2016/04/the-path-to-self-sovereign-identity.html (accessed on 17 November 2020). [100]

Alliance, B. (n.d.), *Badge Alliance*, https://www.badgealliance.org (accessed on 28 June 2020). [85]

Amazon (n.d.), *Blockchain on AWS*, https://aws.amazon.com/blockchain/ (accessed on 13 November 2020). [45]

American Chemical Society (2019), *Estimating the environmental impact of Bitcoin mining*, Science Daily, https://www.sciencedaily.com/releases/2019/11/191120080246.htm. [11]

AMSI (n.d.), *Our Schools | First in the World to Implement Blockchain-based Digital Academic Credentials for Students*, https://amsi.ae/amsi-news/183-our-schools-first-in-the-world-to-implement-blockchain-based-digital-academic-credentials-for-students (accessed on 17 November 2020). [184]

Arizona State University (n.d.), *Trusted Learner Network*, https://trust.asu.edu/ (accessed on 16 November 2020). [151]

Ark Invest (2021), *SolarBatteryBitcoin.*, Github, https://github.com/ARKInvest/SolarBatteryBitcoin (accessed on 4 May 2021). [12]

Asia Blockchain Review (2018), *Malaysian Ministry of Education Applies Blockchain Technology as a Certificate Verification against Degree Fraud*, https://www.asiablockchainreview.com/malaysian-ministry-of-education-apply-blockchain-technology-as-a-certificate-verification-against-degree-fraud/ (accessed on 17 November 2020). [204]

Baydakova, A. (2019), *Bitcoin Mining Farms Are Flourishing on the Ruins of Soviet Industry in Siberia*, CoinDesk, https://www.coindesk.com/bitcoin-mining-farms-are-flourishing-on-the-ruins-of-soviet-industry-in-siberia (accessed on 17 November 2020). [7]

Beheshti, N. (2020), *5 Of The Most In-Demand Soft Skills Companies Are Looking For This Year*, Forbes, https://www.forbes.com/sites/nazbeheshti/2020/01/28/5-of-the-most-in-demand-soft-skills-companies-are-looking-for-this-year/?sh=5393bb2e56c7 (accessed on 17 November 2020). [214]

Benay, A. (2019), *Securing the future of talent mobility in the Government of Canada*, https://tbs-blog.canada.ca/en/securing-future-talent-mobility-government-canada (accessed on 13 November 2020). [76]

Bernard, Z. (2018), *Everything you need to know about Bitcoin, its mysterious origins, and the many alleged identities of its creator*, Business Insider, https://www.businessinsider.com/bitcoin-history-cryptocurrency-satoshi-nakamoto-2017-12?IR=T (accessed on 17 November 2020). [28]

Bhatia, N. (2021), *Layered Money: From Gold and Dollars to Bitcoin and Central Bank Digital Currencies.*, Nikhil Bhatia. [14]

Binance Academy (n.d.), *Byzantine Fault Tolerance Explained*, Binance Academy, https://academy.binance.com/blockchain/byzantine-fault-tolerance-explained (accessed on 25 June 2020). [4]

BitDegree (2017), *Revolutionizing Global Education with Blockchain - White Paper*, https://www.bitdegree.org/bitdegree-vision.pdf (accessed on 17 November 2020). [107]

Blockcerts (n.d.), *Blockcerts*, https://www.blockcerts.org (accessed on 16 November 2020). [111]

BlockCred (n.d.), *BlockCred*, https://www.blockcred.io/ (accessed on 17 November 2020). [189]

Bloxberg (2020), *"bloxberg: The Trusted Research Infrastructure"*, https://bloxberg.org/wp-content/uploads/2020/02/bloxberg_whitepaper_1.1.pdf (accessed on 5 February 2021). [145]

Brody, P. (2019), *How public blockchains are making private blockchains obsolete*, Ernst & Young, https://www.ey.com/en_us/innovation/how-public-blockchains-are-making-private-blockchains-obsolete (accessed on 17 November 2020). [62]

Buterin, V. (2016), *Let's talk about the projected coin supply over the coming years*, Reddit, https://www.reddit.com/r/ethereum/comments/5izcf5/lets_talk_about_the_projected_coin_supply_over/dbc66rd/ (accessed on 17 November 2020). [60]

Cabrol, M. (2018), *Technology is Creating a Human-Centric Economy, and It's Based on Trust, Inter-American Development Bank*, https://blogs.iadb.org/caribbean-dev-trends/en/technology-is-creating-a-human-centric-economy-and-its-based-on-trust/ (accessed on 16 November 2020). [131]

Castillo, M. (2019), *Hyperledger Unanimously Approves First Ethereum Codebase For Enterprises*, Forbes, https://www.forbes.com/sites/michaeldelcastillo/2019/08/29/hyperledger-unanimously-approves-first-ethereum-codebase-for-enterprises/#838c037794cc (accessed on 17 November 2020). [43]

Castro-Iragorri, C. (2018), *Hyperledger Supporting Blockcerts Compliant Digital Diplomas across Colombian Universities*, Hyperledger Global Forum, https://hgf18.sched.com/event/G8rr/hyperledger-supporting-blockcerts-compliant-digital-diplomas-across-colombian-universities-carlos-castro-iragorri-universidad-del-rosario (accessed on 16 November 2020). [135]

CEF Digital (n.d.), *EBSI Documentation home*, https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITALEBSI/EBSI+Documentation+home (accessed on 17 November 2020). [175]

CEF Digital (n.d.), *European Blockchain Services Infrastructure*, European Commission, https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/EBSI (accessed on 13 November 2020). [40]

CEF Digital (n.d.), *Use Cases and Functional Documentation*, https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITALEBSI/Use+Cases+and+Functional+Documentation (accessed on 17 November 2020). [176]

Chainalysis (n.d.), *Chainalysis*, https://www.chainalysis.com/ (accessed on 13 November 2020). [63]

CNN (2020), *Almost 1 in 3 pilots in Pakistan have fake licenses, aviation minister says*, https://edition.cnn.com/2020/06/25/business/pakistan-fake-pilot-intl-hnk/index.html (accessed on 16 November 2020). [123]

CNN (n.d.), *University blockchain experiment aims for top marks*, https://edition.cnn.com/videos/tv/2018/06/28/blockhain-university-dubai-global-gateway.cnn (accessed on 17 November 2020). [183]

Cocks, P. (2017), *Malta first to launch education blockchain certification*, Malta Today, https://www.maltatoday.com.mt/news/national/80704/government_launches_first_blockhain_initiative_in_education (accessed on 16 November 2020). [165]

Coin Telegraph (n.d.), *What Is Lightning Network And How It Works*, Cointelegraph, https://cointelegraph.com/lightning-network-101/what-is-lightning-network-and-how-it-works (accessed on 27 June 2020). [33]

CoinMarketCap (n.d.), *CoinMarketCap*, https://coinmarketcap.com/ (accessed on 25 June 2020). [20]

CoinTelegraph (n.d.), *What Are Smart Contracts? Guide For Beginners*, https://cointelegraph.com/ethereum-for-beginners/what-are-smart-contracts-guide-for-beginners (accessed on 27 July 2020). [25]

Company Newsroom of Learning Machine (2020), *First Blockcerts Issued in India: Pallavan School and Vasant Valley School, Facilitated by Pallavan Learning Systems and Learning Machine, Issue Blockchain Credentials*, https://learningmachine.newswire.com/news/first-blockcerts-issued-in-india-pallavan-school-and-vasant-valley-21072917 (accessed on 17 November 2020). [205]

Company Newsroom of Learning Machine (2018), *Press Release: KAUST Set to Be First University in Middle East to Issue Blockchain Credentials Using Blockcerts Open Standard*, https://learningmachine.newswire.com/news/kaust-set-to-be-first-university-in-middle-east-to-issue-blockchain-20703496 (accessed on 17 November 2020). [190]

ConsenSys (2020), *Latin American and Carribean Citizens Are Coordinating COVID-19 Deconfinement With This New Ethereum Application*, ConsenSys, https://consensys.net/blog/news/latin-american-and-carribean-citizens-are-coordinating-covid-19-deconfinement-with-this-new-ethereum-application/ (accessed on 17 November 2020). [50]

ConsenSys (2019), *The Thirdening: What You Need To Know*, ConsenSys, https://media.consensys.net/the-thirdening-what-you-need-to-know-df96599ad857 (accessed on 17 November 2020). [58]

ConsenSys (n.d.), *About*, https://consensys.net/about/ (accessed on 26 June 2020). [37]

Crace, A. (2019), *Digitary & Evernym Collaborate*, The PIE News, https://thepienews.com/news/digitary-evernym-collaborate-boost-credentialing/ (accessed on 16 November 2020). [162]

Credential Engine (n.d.), *Credential Transparency Description Language (CTDL) Handbook*, https://credreg.net/ctdl/handbook (accessed on 13 November 2020). [84]

Cuthbertson, A. (2017), *Bitcoin Mining on Track to Consume All of the World's Energy by 2020, Newsweek*, https://www.newsweek.com/bitcoin-mining-track-consume-worlds-energy-2020-744036 (accessed on 17 November 2020). [10]

Dagger, M. (2020), *A Comprehensive Guide to Decentralized Stablecoins*, Hackernoon, https://hackernoon.com/a-comprehensive-guide-to-decentralized-stablecoins-22f66553c807 (accessed on 17 November 2020). [55]

Decentralized Identity Foundation (n.d.), *Decentralized Identity Foundation*, https://identity.foundation/ (accessed on 13 November 2020). [93]

DiChristopher, T. (2017), *No, bitcoin isn't likely to consume all the world's electricity in 2020.*, CNBC, https://www.cnbc.com/2017/12/21/no-bitcoin-is-likely-not-going-to-consume-all-the-worlds-energy-in-2020.html (accessed on 17 November 2020). [9]

Digital Credentials Consortium (2020), *Building the digital credential infrastructure for the future*, https://digitalcredentials.mit.edu/wp-content/uploads/2020/02/white-paper-building-digital-credential-infrastructure-future.pdf. [146]

Dinkins, D. (2017), *SegWit Locked-in, But Questions Remain About Bitcoin's Level of Decentralization*, CoinTelegraph, https://cointelegraph.com/news/Bitcoin-is-decentralized-but-not-distributed-and-that-fact-likely-contributed-to-Bitcoins-civil-war (accessed on 17 November 2020). [36]

Du Seuil, D. and C. Pastor (2019), *Understanding the European Self-Sovereign Identity Framework (ESSIF)*, https://ssimeetup.org/understanding-european-self-sovereign-identity-framework-essif-daniel-du-seuil-carlos-pastor-webinar-32/ (accessed on 13 November 2020). [79]

Durant, E. (2017), *Digital Diploma debuts at MIT*, MIT News, https://news.mit.edu/2017/mit-debuts-secure-digital-diploma-using-bitcoin-blockchain-technology-1017 (accessed on 16 November 2020). [138]

Education, T. (n.d.), *The Internet of Education*, https://docs.google.com/document/d/1tWiaiU95OvS_ktVDbSjQlwl6CZVUzgikWuTunTde8U0/edit (accessed on 13 November 2020). [97]

Enterprise Ethereum Alliance (n.d.), *Entethalliance*, https://entethalliance.org/ (accessed on 13 November 2020). [38]

EthHub (n.d.), *Monetary Policy*, https://docs.ethhub.io/ethereum-basics/monetary-policy/ (accessed on 13 November 2020). [57]

EU Blockchain Observatory and Forum (2019), *EU Blockchain Observatory and Forum: Workshop Report, e-Identity, Brussels, November 7 2019*, https://www.eublockchainforum.eu/sites/default/files/reports/workshop_5_report_-_e-identity.pdf. [80]

European Commission (n.d.), *ESCO and the new Europass: occupations and skills for lifelong career management*, https://ec.europa.eu/esco/portal/news/fd542061-178a-4a04-81ae-b3b0eccb3edd (accessed on 17 November 2020). [178]

Everis (European Commission) (n.d.), *Europass framework for digitally-signed credentials*, https://ec.europa.eu/futurium/en/system/files/ged/europass_background-info_framework-digitally-signed-credentials.pdf (accessed on 17 November 2020). [179]

Ezell, A. and J. Bear (2012), *Degree Mills: The Billion-dollar Industry That Has Sold Over A Million Fake Diplomas*, Prometheus Books. [120]

Federation of State Medical Boards (2019), *Healthcare and Digital Credentials: Technical, Legal, and Regulatory Considerations*, https://www.fsmb.org/digitalcredentials/ (accessed on 16 November 2020). [113]

Fitzpatrick, L. (2020), *Expect A Huge Backlash If Stablecoins Are Banned*, Forbes, https://www.forbes.com/sites/lukefitzpatrick/2020/04/27/expect-a-huge-backlash-if-stablecoins-are-banned/#634415c261d2. [56]

Foxley, W. (2020), *Vitalik Buterin Clarifies Remarks on Expected Launch Date of Eth 2.0.*, CoinDesk, https://www.coindesk.com/vitalik-buterin-clarifies-remarks-on-expected-launch-date-of-eth-2-0. [29]

Friedman, S. (2019), *Union Public Schools Launches Blockchain-Based Credentials*, https://thejournal.com/articles/2019/04/30/union-public-schools-launches-blockchain-based-credentials.aspx. [140]

Gibson, K. (2017), *Your MD may have a phony degree*, CBS News, https://www.cbsnews.com/news/your-md-may-have-a-phony-degree/ (accessed on 16 November 2020). [122]

Global Blockchain Business Council (n.d.), *Chain Reaction: Blockchain Enters the Mainstream - 2020 annual report*, https://www.lw.com/thoughtLeadership/gbbc-report-blockchain-enters-mainstream (accessed on 17 November 2020). [191]

Government of Canada Talent Cloud (n.d.), *Talent Cloud*, https://talent.canada.ca/en (accessed on 16 November 2020). [158]

GradBase (n.d.), *GradBase*, https://www.gradba.se/en/ (accessed on 16 November 2020). [171]

Grech, A. and A. Camilleri (2017), *Blockchain in Education*, European Commission Joint Research Centre | Edited by Andreia Inamorato dos Santos, https://publications.jrc.ec.europa.eu/repository/bitstream/JRC108255/jrc108255_blockchain_in_education(1).pdf. [130]

Greenspoon, A. (2018), *The value of 'free agents' inside the public service*, Policy Options, https://policyoptions.irpp.org/magazines/november-2018/the-value-of-free-agents-inside-the-public-service/ (accessed on 16 November 2020). [159]

Hague Convention (1961), *Convention Abolishing the Requirement of Legalisation for Foreign Public Documents*, https://www.hcch.net/en/instruments/conventions/full-text/?cid=41. [126]

Hamdani, Z. (2020), *ARUCC teams up with Digitary to build Made for Canada network*, Global Education Times, https://www.globaleducationtimes.org/news/north-america/arucc-teams-up-with-digitary-to-build-made-for-canada-network/1690/?fbclid=IwAR271A6g9UK3yjtND-Uclm3ymmD3h8hBToEsPa_MG4hUdjAjzvODMD81I0E (accessed on 16 November 2020). [161]

Hargrave, S. and E. Karnoupakis (2020), *Blockchain Success Stories: Case Studies from the Leading Edge of Business*, O'Reilly Media. [137]

Hess, A. (2020), *College enrollment is down because of the pandemic—and community colleges have been hit the hardest*, CNBC, https://www.cnbc.com/2020/10/01/how-the-coronavirus-pandemic-has-impacted-college-enrollment.html (accessed on 17 November 2020). [210]

HKUST Academic Registry (n.d.), *Electronic Documents Verification Program*, https://registry.ust.hk/verify/info (accessed on 17 November 2020). [206]

Holon IQ (2018), *Education in 2030: The $10 Trillion dollar question*, https://www.holoniq.com/2030/ (accessed on 17 November 2020). [209]

Holon IQ (2018), *Global Student Flows*, https://www.holoniq.com/global-student-flows (accessed on 17 November 2020). [208]

Hyland Credentials (n.d.), *Customer Stories*, https://www.hylandcredentials.com/customer-stories (accessed on 16 November 2020). [115]

Hyland Newsroom (2020), New Mexico Higher Education Department selects Hyland Credentials for Higher Education, https://news.hyland.com/new-mexico-higher-education-department-selects-hyland-credentials-for-higher-education/ (accessed on 16 November 2020). [144]

IBM (n.d.), *IBM Blockchain Services. Blockchain consulting that turns strategy into business outcomes.*, https://www.ibm.com/blockchain/services/ (accessed on 13 November 2020). [46]

IEEE (n.d.), *Learning Technology Standards Committee (LTSC)*, https://sagroups.ieee.org/ltsc/ (accessed on 13 November 2020). [94]

IMS Global (n.d.), *Comprehensive Learner Record*, https://www.imsglobal.org/activity/comprehensive-learner-record (accessed on 13 November 2020). [86]

Indorse (n.d.), *Indorse*, https://indorse.io/metamorph (accessed on 17 November 2020). [203]

Insights, L. (2020), *South Korea has global ambitions for decentralized identity systems*, https://www.ledgerinsights.com/south-korea-decentralized-identity-ambitions/ (accessed on 13 November 2020). [78]

Internet Identity Workshop (n.d.), *Internet Identity Workshop*, https://internetidentityworkshop.com/ (accessed on 28 June 2020). [88]

Internet of Education (n.d.), *Internet of Education*, https://www.internetofeducation.org/ (accessed on 13 November 2020). [96]

Jagers, C. (2018), *The Blockchain in Education*, Learning Machine Blog, https://medium.com/learning-machine-blog/the-blockchain-in-education-5a322fe9fe86. [110]

Jagers, C. (n.d.), *A Passport to Greater Opportunity*, Learning Machine Blog, https://www.learningmachine.com/passport-greater-opportunity/ (accessed on 17 November 2020). [207]

Jagers, C. (n.d.), *Future Proof*, Learning Machine Blog, https://www.learningmachine.com/future-proof (accessed on 16 November 2020). [136]

Jamaica Observer (2019), *CXC to provide students with e-certificates after successful trial*, http://www.jamaicaobserver.com/latestnews/CXC_to_provide_students_with_e-certificates_after_successful_trial?profile=1228 (accessed on 17 November 2020). [195]

Jessel, B. (2020), *Ethereum, Fabric, Corda, And Multichain. Only One Is Government Ready - New Report*, Forbes, https://www.forbes.com/sites/benjessel/2020/04/21/ethereum-fabric-corda-and-multichain-only-one-is-government-readynew-report/#4f0443ae263b. [53]

Jonkers, R. (2018), *SAP Blockchain for Higher Education*, https://www.slideshare.net/RobJonkers/sap-blockchain-for-higher-education (accessed on 16 November 2020). [169]

Kar, I. (2016), *The developers behind Ethereum are hacking the hacker that hacked it*, QZ, https://qz.com/713078/the-developers-behind-ethereum-are-hacking-the-hacker-that-hacked-it/ (accessed on 24 November 2020). [34]

Kelly, R. (2018), *Southern New Hampshire U Issues Blockchain Credentials to College for America Grads*, https://campustechnology.com/articles/2018/06/11/southern-new-hampshire-u-issues-blockchain-credentials-to-college-for-america-grads.aspx (accessed on 16 November 2020). [139]

Kenobit, O. (2018), *Hyperbitcoinization: Winner Takes All*, Medium, https://medium.com/coinmonks/hyperbitcoinization-winner-takes-all-69ab59f9695f (accessed on 24 November 2020). [17]

Konings, L. (2019), *Electronic Platform for Adult Learning in Europe (EPALE): EMC launches Common Microcredential Framework*, https://epale.ec.europa.eu/en/content/emc-launches-common-microcredential-framework (accessed on 24 November 2020). [83]

Krawisz, D. (2014), *Hyperbitcoinization, Satoshi Nakamoto Institute*, Satoshi Nakamoto Institute, https://nakamotoinstitute.org/mempool/hyperbitcoinization/ (accessed on 24 November 2020). [16]

La Fuente Querétaro (2020), *Profesionistas podrán tramitar cédula en línea*, https://periodicolafuente.com/profesionistas-tramitar-cedula-en-linea/ (accessed on 17 November 2020). [197]

Learning Economy Foundation (n.d.), *Broward OpenCLR Lab*, https://www.learningeconomy.io/browardlab (accessed on 16 November 2020). [154]

Learning Economy Foundation (n.d.), *C-Lab: A Learning Economy Co-Lab*, https://www.learningeconomy.io/clab (accessed on 16 November 2020). [152]

Learning Economy Foundation (n.d.), *Learning Economy Foundation*, https://www.learningeconomy.io/ (accessed on 13 November 2020). [95]

Learning Economy Foundation (n.d.), *Memo: AP-Lab Co-Lab Learning Ecosystems for the Asia-Pacific Region*, https://docs.google.com/document/d/1pzdcZdus734OF2olk1ZZjFY6vdjZY3G8-IVPZlqf4cA/edit#heading=h.9tijzbwkqbxf (accessed on 24 November 2020). [155]

Learning Economy Foundation (n.d.), *Roadmap*, https://www.learningeconomy.io/#Roadmap (accessed on 16 November 2020). [109]

Learning Machine (2018), *Blockcerts Enables Multi-Chain Issuing and Verification of Official Documents*, https://learningmachine.newswire.com/news/blockcerts-enables-multi-chain-issuing-and-verification-of-official-20680828 (accessed on 16 November 2020). [134]

Learning Machine Company Newsroom (2019), *Press Release: Maryville University Partners With Learning Machine to Issue Digital Diplomas Using Blockcerts*, https://learningmachine.newswire.com/news/maryville-university-partners-with-learning-machine-to-issue-digital-21036653 (accessed on 24 November 2020). [142]

Learning Machine Newsroom (2016), *Learning Machine and MIT Media Lab Release Blockchain Technology for Educational Credentials*, https://learningmachine.newswire.com/news/learning-machine-and-mit-media-lab-release-blockchain-technology-for-11633933 (accessed on 16 November 2020). [114]

Ledger Insights (2020), *Workday sees blockchain as key to employee credentialing*, https://www.ledgerinsights.com/workday-blockchain-employee-credentialing/ (accessed on 16 November 2020). [148]

Leising, M. and O. Kharif (2020), *Ethereum Races Clock to Collect Enough Coins for Big Upgrade*, Bloomberg, https://www.bloomberg.com/news/articles/2020-11-23/ethereum-races-clock-to-collect-enough-coins-for-huge-upgrade. [27]

Lemoie, K. and L. Souares (2020), *Connected Impact: Unlocking Education and Workforce Opportunity through Blockchain*, American Council on Education, https://www.acenet.edu/Documents/ACE-Education-Blockchain-Initiative-Connected-Impact-June2020.pdf (accessed on 24 November 2020). [44]

Longino Torres, J. (2019), *¡Hola, futuro! Inicia Tec era de títulos universitarios en blockchain*, Tecnologico de Monterrey, https://tec.mx/es/noticias/nacional/educacion/hola-futuro-inicia-tec-era-de-titulos-universitarios-en-blockchain?&utm_source=twitter&utm_medium=social-media&utm_campaign=addtoany (accessed on 17 November 2020). [192]

Longstaff, B. (2018), *Why hashed Personally identifiable information (PII) on the blockchain can be safe*, Medium, https://medium.com/meeco/why-hashed-personally-identifiable-information-pii-on-the-blockchain-can-be-safe-b842357b9663 (accessed on 24 November 2020). [66]

Maaghul, R. (2019), *Why ODEM is building on the Ethereum blockchain*, ODEM Blog, https://blogs.odem.io/why-odem-is-building-on-the-ethereum-blockchain (accessed on 24 November 2020). [106]

Malone, K. (2020), *Blockchain Saving HHS $30M on First Accelerate Contract*, MeriTalk, https://www.meritalk.com/articles/blockchain-saving-hhs-30m-on-first-accelerate-contract/ (accessed on 24 November 2020). [54]

McCauley, A. (2019), *Unblocked: How Blockchain will Change Your Business (and What to Do About It)*, O'Reilly. [129]

McMaster University Office of the Registrar (n.d.), *Digital diplomas*, https://registrar.mcmaster.ca/digitaldiplomas/#:~:text=McMaster%20University%20issues%20graduates%20a,protect%20and%20verify%20the%20diploma (accessed on 16 November 2020). [116]

McSpadden, K. (2017), *Ngee Ann Polytechnic to pilot blockchain diplomas*, partners Attores, e27, https://e27.co/ngee-ann-polytechnic-to-pilot-blockchain-diplomas-partners-attores-20170526/ (accessed on 17 November 2020). [202]

McWhinney, J. (2019), *Why Governments Are Afraid of Bitcoin.*, Investopedia, https://www.investopedia.com/articles/forex/042015/why-governments-are-afraid-bitcoin.asp (accessed on 24 November 2020). [21]

Mearian, L. (2018), *Will Blockchain Run Afoul of GDPR? (Yes and no)*, Computerworld, https://www.computerworld.com/article/3269750/will-blockchain-run-afoul-of-gdpr-yes-and-no.html (accessed on 24 November 2020). [65]

Meetup (2020), *[Hyperledger SF] Workday and AWS discuss Hyperledger Fabric [Mon, Feb 24]*, https://www.meetup.com/Hyperledger-SF/events/267518767/ (accessed on 16 November 2020). [149]

Messari (2019), *Timechains*, https://messari.io/article/timechains (accessed on 24 November 2020). [13]

Messari.io. (2019), *On-chain Governance*, https://messari.io/article/on-chain-governance (accessed on 24 November 2020). [32]

Miller, L. (2020), *Four Bright Spots in a Year That's Irreversibly Changed Higher Ed Admissions*, Liaison International for Inside Higher Ed, https://narratives.insidehighered.com/bright-spots-year-changed-admissions/index.html (accessed on 17 November 2020). [211]

MIT Media Lab (n.d.), *Digital Certificates Project*, https://certificates.media.mit.edu/ (accessed on 16 November 2020). [133]

MIT Media Lab (n.d.), *Project: Digital Academic Credentials*, https://www.media.mit.edu/projects/media-lab-digital-certificates/overview/ (accessed on 16 November 2020). [132]

MIT Open Learning (2020), *University-led Digital Credentials Consortium explores technology for digital academic credentials*, https://openlearning.mit.edu/news/university-led-digital-credentials-consortium-explores-technology-digital-academic-credentials (accessed on 24 November 2020). [90]

Morris, C. (2018), *Bitcoin Mining Uses More Energy Than Homes Do in Iceland*, Fortune, https://fortune.com/2018/02/13/iceland-bitcoin-mining-electricity/ (accessed on 24 November 2020). [8]

Moskov, A. (2018), *What is the Byzantine Generals Problem?*, CoinCentral, https://coincentral.com/byzantine-generals-problem/ (accessed on 9 November 2020). [2]

Munro, A. (2018), *Good clean use case: Bahamian students graduate on the blockchain*, finder, https://www.finder.com.au/good-clean-use-case-bahamian-students-graduate-on-the-blockchain (accessed on 17 November 2020). [194]

Muzzy, E. (2020), *What Is Proof of Stake?*, Consensys Blog, https://consensys.net/blog/blockchain-explained/what-is-proof-of-stake/ (accessed on 24 November 2020). [30]

Nakamoto, S. (2008), *Bitcoin: A Peer-to-Peer Electronic Cash System*, http://www.bitcoin.org (accessed on 24 November 2020). [1]

Nuzzi, L. (2019), *Schnorr Signatures & The Inevitability of Privacy in Bitcoin*, Medium, https://medium.com/digitalassetresearch/schnorr-signatures-the-inevitability-of-privacy-in-bitcoin-b2f45a1f7287 (accessed on 24 November 2020). [18]

OECD (2005), *Guidelines for quality provision in cross-border higher education*, http://www.oecd.org/education/innovation-education/35779480.pdf. [125]

OECD (2004), *Internationalisation and Trade in Higher Education*, OECD, http://dx.doi.org/10.1787/9789264015067-en. [124]

OpenCerts (n.d.), *Collaborate*, https://opencerts.io/collaborate (accessed on 13 November 2020). [77]

OpenCerts (n.d.), *OpenCerts*, https://opencerts.io/ (accessed on 16 November 2020). [118]

Oracle (n.d.), *Oracle Blockchain Enterprise Edition*, https://www.oracle.com/database/technologies/blockchain-platform-enterprise-edition.html (accessed on 13 November 2020). [47]

Parisi, B. (2018), *Woolf University: Will Blockchain Make College Affordable?*, In the Mesh, https://inthemesh.com/archive/woolf-university-will-the-blockchain-make-college-more-affordable/ (accessed on 24 November 2020). [104]

Parrish, J., J. Fryer and R. Parks (2017), *Expanding the Academic Record: Revolutionizing Credentials*, NACE, https://www.naceweb.org/job-market/trends-and-predictions/expanding-the-academic-record-revolutionizing-credentials/ (accessed on 17 November 2020). [215]

Pisani, B. (2018), *Bitcoin and ether are not securities, but some initial coin offerings may be*, SEC official says, CNBC, https://www.cnbc.com/2018/06/14/bitcoin-and-ethereum-are-not-securities-but-some-cryptocurrencies-may-be-sec-official-says.html#close (accessed on 24 November 2020). [24]

Pistis.io (n.d.), *Pistis.io*, https://pistis.io/welcome/ (accessed on 16 November 2020). [150]

Prince Consulting (n.d.), *Prince Consulting*, http://princeconsulting.biz/ (accessed on 17 November 2020). [201]

Purifoy, C. and J. Smith (2018), *G20: Of Currency, New Gold Standards & Rocket Fuel to Coordinate Global Impact*, G20 Leaders Summit Magazine, https://www.learningeconomy.io/post/g20-cover-story-of-currency-new-gold-standards-and-rocket-fuel-to-coordinate-global-impact (accessed on 24 November 2020). [108]

PwC UK (n.d.), *Smart Credentials*, https://www.pwc.co.uk/blockchain/smart-credentials.html (accessed on 16 November 2020). [172]

Quorum (n.d.), *Quorum*, https://www.goquorum.com/ (accessed on 13 November 2020). [41]

Reed, M. (2016), *Co-Curricular Transcripts? Questions about a potentially good idea*, Inside Higher Ed., https://www.insidehighered.com/blogs/confessions-community-college-dean/co-curricular-transcripts (accessed on 17 November 2020). [216]

Renieris, E. (2020), *SSI? What we really need is full data portability*, Women in Identity Blog, https://womeninidentity.org/2020/03/31/data-portability/ (accessed on 24 November 2020). [99]

Salas, R. (2018), *CNM named 'Innovator of the Year' for their use of blockchain tech*, KOB4, https://www.kob.com/albuquerque-news/cnm-named-innovator-of-the-year-for-their-use-of-blockchain-tech-/5189370/ (accessed on 16 November 2020). [143]

Sansone, K. (2019), *Malta is first country to put education certificates on blockchain*, Malta Today, https://www.maltatoday.com.mt/news/national/93148/malta_is_first_country_to_put_education_certificates_on_blockchain#.XG67xpNKg0o (accessed on 16 November 2020). [166]

SAP (n.d.), *Intelligent Technologies*, https://www.sap.com/products/intelligent-technologies/blockchain.html (accessed on 13 November 2020). [48]

Shahada (n.d.), *Shahada*, https://www.shahada.ae/ (accessed on 2 November 2020). [186]

Sharma, R. (2019), *What is the Enterprise Ethereum Alliance?*, Investopedia, https://www.investopedia.com/tech/what-enterprise-ethereum-alliance/ (accessed on 24 November 2020). [39]

Sharma, R. (2019), *Why Is Ethereum Co-founder Proposing a Hard Cap?*, Investopedia, https://www.investopedia.com/news/why-ethereum-cofounder-proposing-hard-cap/ (accessed on 24 November 2020). [59]

Sharma, R. (2019), *Zero Knowledge Proofs' Could Boost Blockchain Adoption on Wall Street*, Investopedia, https://www.investopedia.com/news/zero-knowledge-proofs-could-boost-blockchain-adoption-wall-street/ (accessed on 24 November 2020). [67]

Sharma, R. (2018), *SEC Official Declares Ether Is Not a Security*, Investopedia, https://www.investopedia.com/news/sec-officially-declares-ether-not-security/#:~:text=Ether%20is%20not%20a%20security%2C%20according%20to%20Bill%20Hinman%2C%20U.S.,Commission%20Director%20of%20Corporate%20Finance.&text=After%20Bitcoin%2C%20ether%20is%20th (accessed on 24 November 2020). [23]

Shin, A. (2020), *Hyperledger Fabric vs R3 Corda: A Business Perspective*, Medium, https://medium.com/@kaishinaw/hyperledger-fabric-vs-r3-corda-a-business-perspective-cf935824de9 (accessed on 24 November 2020). [52]

Siegel, D. (2016), *Understanding the DAO Attack*, CoinDesk, https://www.coindesk.com/understanding-dao-hack-journalists (accessed on 24 November 2020). [35]

Sixtin, E. (2017), *Malta Introduces First Blockcerts Pilot in Europe*, BTCManager, https://btcmanager.com/malta-introduces-first-blockcerts-pilot-in-europe/ (accessed on 16 November 2020). [164]

Smart Dubai 2021 (n.d.), *Smart Dubai 2021*, https://2021.smartdubai.ae/ (accessed on 24 November 2020). [181]

SmartDegrees (n.d.), *SmartDegrees*, https://www.smartdegrees.es/en/home-en/ (accessed on 16 November 2020). [167]

Smartworld (2020), *Press Release: Smartworld and Grape Technology announced the launch of Shahada, a digital certificate protocol built on blockchain technology*, https://www.smartworld.com/smartworld-and-grape-technology-announced-the-launch-of-shahada-a-digital-certificate-protocol-built-on-blockchain-technology/ (accessed on 17 November 2020). [185]

Smolenski, N. (ed.) (n.d.), *Interview with Lluís Alfons Ariño Martín, Convenor of the Digital Diplomas Use Case for the EBSI.* [177]

Smolenski, N. (ed.) (2018), *Conversation with a private tutor living and working in China.* [121]

Smolenski, N. (2016), *Identity and Digital Self-Sovereignty*, Medium, https://medium.com/learning-machine-blog/identity-and-digital-self-sovereignty-1f3faab7d9e3 (accessed on 24 November 2020). [98]

Southside Daily Staff (2018), *Here's a new way ECPI University is issuing its degrees*, Wydaily, https://wydaily.com/local-news/2018/11/05/heres-a-new-way-ecpi-university-is-issuing-its-degrees/ (accessed on 16 November 2020). [141]

Steenis, H. (2017), *Bitcoin's bite: why central banks should clamp down on cryptocurrencies*, Schroders, https://www.schroders.com/en/uk/private-investor/insights/markets/bitcoins-bite-why-central-banks-should-clamp-down-on-cryptocurrencies/ (accessed on 24 November 2020). [22]

SYSARTEC (2020), *LinkedIn*, https://www.linkedin.com/feed/update/urn:li:activity:6745799560867700736/ (accessed on 4 May 2021). [193]

T3 Innovation Network (2020), *Applying Self-Sovereign Identity Principles to Interoperable Learning Records: Principles, Challenges, and Community Guidance*, US Chamber of Commerce Foundation, https://www.uschamberfoundation.org/sites/default/files/media-uploads/Applying%20SSI%20Principles%20to%20ILRs%20Report.pdf (accessed on 24 November 2020). [101]

Talent Cloud | Nuage de talents (2018), *Twitter*, https://twitter.com/GC_Talent/status/1066820323490897921 (accessed on 24 November 2020). [157]

Temple, J. (2019), *Bitcoin mining may be pumping out as much CO2 per year as Kansas City.*, MIT Technology Review, https://www.technologyreview.com/2019/06/12/873/bitcoin-mining-may-be-pumping-out-as-much-cosub2-sub-per-year-as-kansas-city/ (accessed on 24 November 2020). [6]

Texas Blockchain Council (2021), *Hyland and Hedera Hashgraph Present Blockchain Proof of Concept for Records Verification to Texas Secretary of State*, https://www.prnewswire.com/news-releases/hyland-and-hedera-hashgraph-present-blockchain-proof-of-concept-for-records-verification-to-texas-secretary-of-state-301204696.html?tc=eml_cleartime. [128]

The Linux Foundation (2020), *Cross-Industry Coalition Advances Digital Trust Standards*, https://www.linuxfoundation.org/press-release/2020/05/cross-industry-coalition-advances-digital-trust-standards/ (accessed on 13 November 2020). [92]

The Open University (n.d.), *Open Blockchain*, https://blockchain.open.ac.uk/ (accessed on 16 November 2020). [173]

The Open University (n.d.), *QualiChain*, https://qualichain-project.eu/ (accessed on 16 November 2020). [174]

The Sovrin Foundation (2018), *The Sovrin Network and Zero Knowledge Proofs*, The Sovrin Foundation, https://sovrin.org/the-sovrin-network-and-zero-knowledge-proofs/ (accessed on 13 November 2020). [68]

The United Arab Emirates' Government portal (n.d.), *Emirates Blockchain Strategy 2021*, https://u.ae/en/about-the-uae/strategies-initiatives-and-awards/federal-governments-strategies-and-plans/emirates-blockchain-strategy-2021 (accessed on 17 November 2020). [180]

Thys, F. (2020), *One Third Of Private 4-Year Colleges Are At High Risk Financially, Model Predicts*, WBUR, https://www.wbur.org/edify/2020/05/08/higher-education-financial-crisis (accessed on 17 November 2020). [212]

Treasury Board of Canada Secretariat (2018), *Canada's trusted digital identity vision*, https://www.canada.ca/en/treasury-board-secretariat/corporate/news/canada-trusted-digital-identity-vision.html (accessed on 16 November 2020). [156]

Trilling, B. and C. Fadel (2009), *21st Century Skills: Learning for Life in Our Times*, John Wiley And Sons, Inc. [213]

Trust Over IP Foundation (n.d.), *Trust Over IP Foundation*, https://trustoverip.org/ (accessed on 13 November 2020). [91]

UAEU (2019), *United Arab Emirates University Launches UAEU Passport, University-Wide Blockchain Applications to Streamline Student Services*, https://www.uaeu.ac.ae/en/news/2019/feb/uaeu_passport.shtml (accessed on 17 November 2020). [182]

Unviersidad Carlos III de Madrid (2018), A*creditaciones de Competencias Utilizando la Tecnología Blockchain en Cursos Spocs*, https://www.uc3m.es/sdic/articulos/2018/acreditaciones-utilizando-blockchain (accessed on 16 November 2020). [117]

US Chamber of Commerce Foundation (n.d.), *The T3 Innovation Network*, https://www.uschamberfoundation.org/t3-innovation (accessed on 13 November 2020). [89]

US Department of Homeland Security (2019), *News Release: DHS Awards $199K for Blockchain Credential Lifecycle Management*, https://www.dhs.gov/science-and-technology/news/2019/11/14/news-release-dhs-awards-199k-blockchain-tech (accessed on 13 November 2020). [74]

US Department of Homeland Security (2019), *News Release: DHS Awards 159K for Infrastructure to Prevent Credential Fraud*, https://www.dhs.gov/science-and-technology/news/2019/11/12/news-release-dhs-awards-159k-prevent-credential-fraud (accessed on 13 November 2020). [72]

US Department of Homeland Security (2017), *News Release: DHS S&T Awards $750K to Virginia Tech Company for Blockchain Identity Management Research and Development*, https://www.dhs.gov/science-and-technology/news/2017/09/25/news-release-dhs-st-awards-750k-virginia-tech-company (accessed on 13 November 2020). [73]

US Department of State, Bureau of Consular Affairs (n.d.), *Apostille Requirements*, https://travel.state.gov/content/travel/en/records-and-authentications/authenticate-your-document/apostille-requirements.html (accessed on 16 November 2020). [127]

Vander Ark, T. (2018), *Imagining a Blockchain University*, Forbes, https://www.forbes.com/sites/tomvanderark/2018/06/13/woolf-building-the-first-blockchain-university/?sh=41e45cff5ae5. [103]

Varshney, N. (2018), *Ethereum's supply has crossed 100M, here's what that means*, TheNextWeb, https://thenextweb.com/hardfork/2018/06/11/ethereums-total-supply/ (accessed on 24 November 2020). [61]

VON (n.d.), *Verifiable Organizations Network: Global Digital Trust for Organizations*, https://vonx.io/ (accessed on 13 November 2020). [75]

Vottun (n.d.), *Vottun*, http://vottun.com (accessed on 16 November 2020). [168]

W3C (n.d.), *Decentralized Identifiers (DIDs) v1.0*, https://w3c.github.io/did-core/ (accessed on 28 June 28). [71]

W3C (n.d.), *Educational and Occupational Credentials in Schema.org Community Group*, https://www.w3.org/community/eocred-schema/ (accessed on 28 June 2020). [82]

W3C (n.d.), *Facts about W3C*, https://www.w3.org/Consortium/facts.html (accessed on 13 November 2020). [69]

W3C (n.d.), *Verifiable Credentials Data Model 1.0*, https://www.w3.org/TR/vc-data-model/ (accessed on 24 November 2020). [70]

W3C (n.d.), *Verifiable Credentials for Education Task Force*, https://w3c-ccg.github.io/vc-ed/ (accessed on 13 November 2020). [81]

Watkins, R. (2020), *Power and Seigniorage in Proof of Stake*, Messari.io, https://messari.io/article/power-and-seigniorage-in-proof-of-stake (accessed on 24 November 2020). [31]

Web of Trust (n.d.), *Rebooting Web of Trust*, https://www.weboftrust.info/ (accessed on 13 November 2020). [87]

Weinstein, J. (2015), *How can law enforcement leverage the blockchain in investigations?*, Coin Center, https://coincenter.org/entry/how-can-law-enforcement-leverage-the-blockchain-in-investigations (accessed on 24 November 2020). [64]

Wikipedia (n.d.), *Byzantine fault*, https://en.wikipedia.org/wiki/Byzantine_fault (accessed on 25 June 2020). [3]

Wikipedia (n.d.), *Decentralized applications*, https://en.wikipedia.org/wiki/Decentralized_application#:~:text=A%20decentralized%20application%20(DApp%2C%20dApp,referred%20to%20as%20smart%20contracts (accessed on 27 July 2020). [26]

Wikipedia (n.d.), *Hyperledger*, https://en.wikipedia.org/wiki/Hyperledger (accessed on 28 June 2020). [42]

Wikipedia (n.d.), *Mozilla Open Badges*, https://en.wikipedia.org/wiki/Mozilla_Open_Badges (accessed on 26 June 2020). [112]

Wikipedia (n.d.), *Proof of work*, https://en.wikipedia.org/wiki/Proof_of_work (accessed on 25 June 2020). [5]

Wikipedia (n.d.), *R3 (company)*, https://en.wikipedia.org/wiki/R3_(company) (accessed on 28 June 2020). [51]

Woolf University (n.d.), *Woolf University*, https://woolf.university/ (accessed on 26 June 2020). [105]

Workday Credentials (n.d.), *Workday Credentials & WayTo™ By Workday*, https://credentials.workday.com/docs/overview/ (accessed on 16 November 2020). [147]

World Government Summit et al. (2018), *Case Study: Free Agents and GC Talent Cloud – Canada, Embracing Innovation in Government*, https://www.oecd.org/gov/innovative-government/Canada-case-study-UAE-report-2018.pdf (accessed on 24 November 2020). [160]

Xertify (n.d.), *Xertify*, https://xertify.co/ (accessed on 17 November 2020). [196]

Young, J. (2018), *Academics Propose a 'Blockchain University,' Where Faculty (and Algorithms) Rule*, EdSurge, https://www.edsurge.com/news/2018-10-25-academics-propose-a-blockchain-university-where-faculty-and-algorithms-rule. [102]

Zawya (2020), *Press Release: University of Dubai successfully publish e-Credentials of graduates on blockchain platform*, https://www.zawya.com/mena/en/press-releases/story/University_of_Dubai_successfully_publish_eCredentials_of_graduates_on_blockchain_platform-ZAWYA20200901071849/ (accessed on 17 November 2020). [187]

From:

OECD Digital Education Outlook 2021

Pushing the Frontiers with Artificial Intelligence, Blockchain and Robots

Access the complete publication at:

https://doi.org/10.1787/589b283f-en

Please cite this chapter as:

Smolenski, Natalie (2021), “Blockchain for Education: A New Credentialing Ecosystem”, in OECD, *OECD Digital Education Outlook 2021: Pushing the Frontiers with Artificial Intelligence, Blockchain and Robots*, OECD Publishing, Paris.

DOI: https://doi.org/10.1787/6893d95a-en