Blockchain applications for human development

Anthony Galtier, Yann Jannin

***Abstract*— Although blockchain technology was originally developed as the underlying technology for cryptocurrencies like Bitcoin, it's properties of anonymity, trustlessness and immutability alongside it's distributed nature are of particular interest for many other applications. Blockchain has notably been put forward as one of the most promising technological solutions for human development issues around the world. In recent years, an increasing amount of projects and research have been undertaken with the aim of improving people's health, education, standard of living, political integration and overall quality of life. This paper studies a selection of these works using blockchain for human development. The chosen approach studies how the specific properties of blockchain technology may come as a solution for the considered problem and whether any alternative technology may be a better fit.**

I. INTRODUCTION

Blockchain, the underlying technology to the most popular cryptocurrencies such as Bitcoin, has attracted great attention and investment in recent years for a variety of applications that go well beyond what it was originally developed for. Recording information, transactions or any event is essential to most human activity. Furthermore, information is largely recorded in a digital form. In other words, much of our activity today requires some form of digital ledger.

Whereas until now, ledgers relied on a central validation system, blockchain, also known as distributed ledger technology (DLT), can operate without one in a distributed network of computers. There is thus no more need to trust a central authority to ensure the validity and recording of information. Cryptography furthermore insures that any information recorded in a blockchain cannot be corrupted and . These properties of decentralization, trustlessness, immutability and anonymity are what make blockchain technology stand out among other digital ledger technologies.

Amid many others, blockchain has inspired a great variety of applications aiming to tackle the most pressing human development challenges. This paper collects, organizes and studies some of these applications. The first section will provide some contextual information about human development and a more in detail presentation of blockchain technology. The second section studies a collection of blockchain applications organized according to the dimension of human development it tackles. The applications will be studied with a particular focus on the properties of decentralization, trustlessness and immutability and questioning if blockchain is actually the best solution. The last section is a discussion, comparing the studied applications and providing an outlook on the future of blockchain applications for human development.

II. CONCEPTS

A. Human development

The concept of human development originates from the economist Mahbub Ul Haq's work at the World Bank in the 1980s. The concept of human development is a concept of development that has to do with the creation and improvement of living conditions. Human development goes beyond just economic development to more accurately account for human well-being. The United Nations Development Program [10] describes human development giving people more freedom and opportunities to live lives they value. Human development takes into account health, education, standard of living, political and community life, sustainability, human security and rights and equality. The blockchain applications studied in this paper will be organized accordingly to the aforementioned dimensions of human development that they deal with.

B. Blockchain technology

Blockchain is a technology that emerged in 2008, when an individual using the pseudonym Satoshi Nakamoto released a paper describing a cryptocurrency using a blockchain, the Bitcoin. Since then blockchain is usually associated with Bitcoin or more generally cryptocurrencies, but there exist a lot of different applications of blockchain in various domains, as we will see in this paper. A blockchain is a distributed ledger that provides a way for information to be recorded and shared by a community. In this community, each member maintains his or her own copy of the information and all members must validate any updates collectively [9]. As its name indicates, in a blockchain data is stored in a special data structure: a chain of blocks. Each block stores a list of information that can represents practically anything else that can be described in digital form. In cryptocurrencies using blockchain, like Bitcoin, these blocks store transactions of the currency, but they can also store for example some code that executes some actions when some conditions are met, which are called smart contracts. Each block is linked to the previous block in the chain using cryptography, thanks to a hash function. A hash function produces a string of constant size from data whose size may vary. This hash code can be seen as a fingerprint of the data. A cryptographic hash function has some particular properties, indeed, a given input will always produce the same hash code and it is impossible to find two different inputs producing the same hash code. Also it is almost impossible to retrieve input data knowing only it's hash code, as the only way to do so is to try all possible inputs of the hash function until finding the

good hash. In addition to storing some data, a block stores the value of the hash code of this data, and the value of the hash code from the previous block in the chain. Thus, blockchain allows to get rid of of third-party intermediaries while maintaining trust in the ledger, thanks to cryptography. Yet we will see that some blockchains still need the authority of a central entity in some cases. One interesting property of a blockchain is that since every user on the network stores a copy of the blockchain, this redundancy of data allows it to be protected from disappearing. It is also impossible to modify or alter the content of a blockchain afterwards. As in any other database, there are two types of users of a blockchain : writers and readers. In a blockchain, writers are the users that can add new blocks to the chain, while readers can only access the information contained in the existing blocks of the chain without extending it. It is also important to note that writers cannot add whatever they want to the blockchain. Indeed a consensus between the writers must exist before a block is appended to the blockchain. That being said we can differentiate between permissionless blockchains and permissioned blockchains [18]. In a permissionless blockchain any user can join as a reader or as a writer at any time. Conversely, in a permissioned blockchain, there is a central authority that decides whether a user can be a writer, a reader or neither. We can again distinguish two sort of permissioned blockchains : public and privates ones. A public permissioned blockchain allows every user to access all the blockchain to to verify the correctness of the state of the blockchain, that is called public verifiability. Public verifiability relies on the transparency of the information contained on the blockchain. Conversely, a private permissioned blockchain does not allow public verifiability as the right to read the blockchain is limited. This kind of blockchain enables privacy of the data at the expense of transparency. In some cases where the information stored in the blockchain is sensitive, it is really important to ensure privacy of the users. As we can see it exists tensions between privacy and transparency. The choice of privileging transparency or privacy depends on the application case. However it is also possible to allow privacy in a transparent blockchain, but this is done using cryptographic techniques that are expensive in terms of computation.

III. Applications

In the following section a selection of blockchain applications for each dimension of human development will be studied with a a focus on the blockchain specific properties such as decentralization, trustlessness and immutability. The actual need for a blockchain for each case will be questioned based on Wüst and Gervais flowchart (figure 1). [18]

A. Health

Blockchain technology is standing out as a promising solution healtcare's lack of interoperablitity, allowing medical software apps and technology platforms to communicate securely and seamlessly, exchange data, and use the exchanged data across health organizations and app vendors. [19]. In

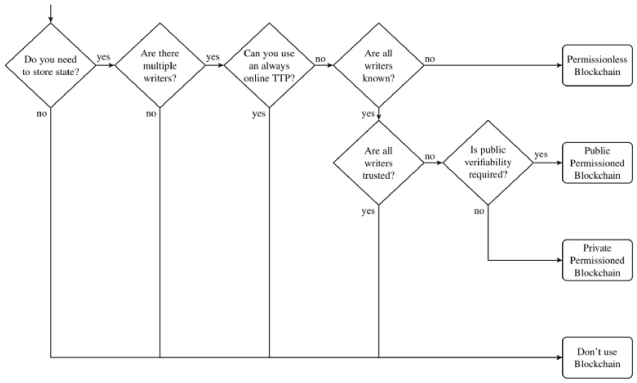

Fig. 1. Flowchart: Do you need a blockchain? Copied from: Karl Wust and Arthur Gervais. "Do you Need a Blockchain?" In:2018 Crypto Valley Conference on Blockchain Technology (CVCBT)(2018)

this paper, we will study two application most significantly contributing to human development. The first is a use of blockchain to prevent the spread of HIV [15], the second uses blockchain for food security purposes [3].

As no cure nor vaccine yet exists, the most effective way to contain and prevent the spread of the Human Immunodeficiency Virus (HIV) is to protect susceptible populations. This means to identify HIV-infected and high risk individuals and provide them with treatment and behavioural intervention. The blockchain application proposed by Liu et al. consists in a digital vaccine strategy that allows HIV high risk populations to check the infection status of each other conveniently and anonymously to prevent high-risk sexual activity and thus prevent the spread of the virus. [19] The technical implementation of the digital vaccine strategy is represented in the following figure.

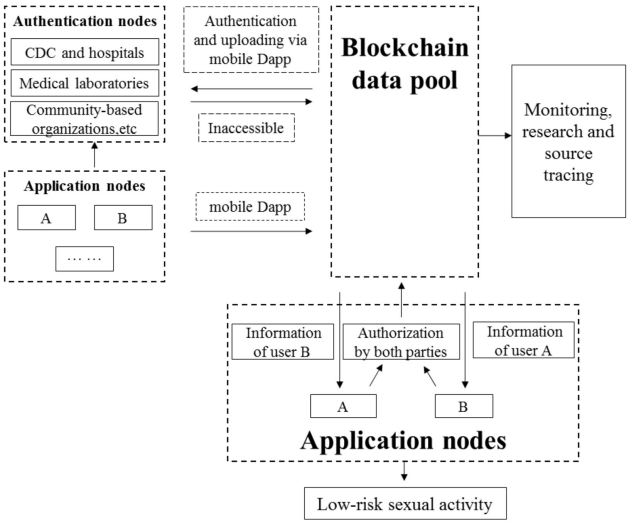

Fig. 2. Technical flowchart of the HIV digital vaccine strategy. A and B represent HIV-high-risk individuals. Copied from: Jia Liu. "HIV digital vaccine strategy: An application of blockchain technology in preventing the spread of HIV"

End users are individuals susceptible of being HIV-

infected, certified HIV testing agencies and third party users such as the government or research groups. The nodes of the blockchain network comprise of application nodes representing the HIV high-risk individuals, and authentication nodes, representing the certified HIV testing agencies. Authenticating nodes are write authenticated HIV test results of contributing individuals into the blockchain. Application nodes, corresponding to these individuals can then authorize other application nodes to access information regarding them. The proposed system relies on the issuance and circulation of tokens. Tokens can be issued to third party users like the government or medical research groups to access data about the population.

As described in the proposal paper, blockchain is a convenient solution for this digital vaccine strategy as it offers properties of anonymity for the users and credibility in the stored data as it is immutable. These two properties are a necessity for this application. The properties of trustlessness and decentralization on the other hand may not be necessary. Although the paper argues that a centralized system managed by a government would lead to low acceptability, there is no guarantee that a decentralized would work any better. In fact, confronting this application to the flowchart in figure 1, one can argue that a blockchain is not the best solution. This digital vaccine strategy does require to store HIV-test data and involves several writers. However, an always online trusted third party (TTP) can arguably used and even if a a TTP were not to be used, all writers are known and can be trusted. This application, according to the work of Wust and Gervais on the necessity of blockchain, a distributed database with shared write access would be a better solution.

Blockchain has been of particular interest for agriculture and food security. AgriLedger [3] uses blockchain technology and a mobile application to enable farmers in developing areas to perform various transactions such as hiring custom seeders and harvesters, cooperating with other farmers for bargaining power, taking their crop to market, monitoring it through the production process and more. AgriLedger has developed more than 12 blockchain projects for these purposes. [2]. These projects involve record-keeping and tracing in a network of farmers where no trusted third party exists and where trust cannot always be assumed between the different farmers. Thus, yes, data needs to be stored, data is written by multiple parties, an always online TTP cannot be used, all writers are known but cannot be trusted. Since public verifiability is required, according the Wust and Gervais's flowchart, the necessity of a blockchain is justified for this application and more specifically a public permissioned blockchain.

B. Education

Blockchain will play a big role in the digitization process of certificates issued by educational organizations. Nowadays, to issue their certificates, educational organizations relies on paper or digital certificates [9]. These digital certificates don't use any blockchain because they authenticate certificates using an intermediary authority that act as a trusted third-party (TTP). But this system has some drawbacks. Indeed, storing all the records of certificates in a single central organization creates a risk of having all the records destroyed in case of natural disaster or war. For instance in Syria the entire education system collapsed due to the civil war, thus it is hard to have a track of all certifications issued to students in the past. To get rid of a central authority to authenticate certificates, a blockchain solution has been developed. When a certification is issued, the organization issuing it combines the certificate with a unique identification number proper to the student (public key) and generates a digital fingerprint for the student's certificate with an hash function (cf. section I.B). This digital fingerprint is stored in a blockchain and digital certification is given to the student. When a third person, like a recruiter, needs to authenticate the certificate given by the student, they just need to log in a website that checks whether the digital certificate matches the digital fingerprint stored in the blockchain.

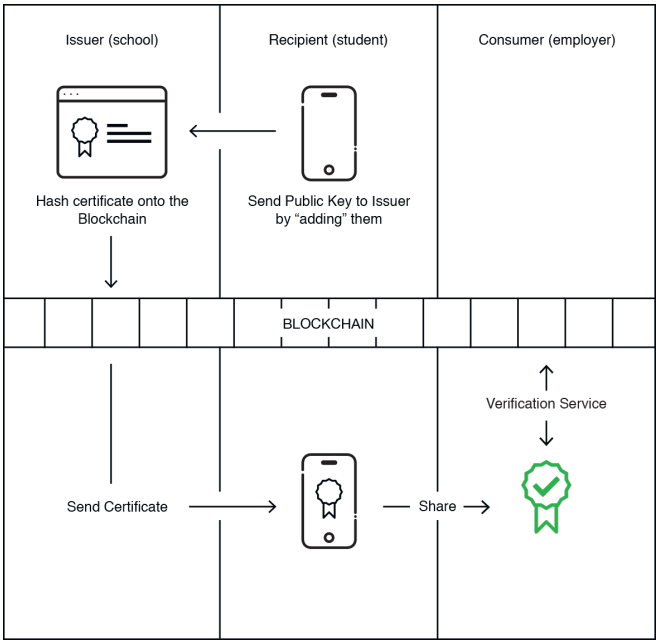

Fig. 3. Diagram representing the operation of the authentication of a certificate using a blockchain [9]

With the blockchain we can always have a record of the certificate, even if the organization that delivered it closes down or is destroyed. Following Wust and Gervais flowchart a blockchain is not the proper solution, as all writers here are educational organizations, thus we can consider that they are trust worthy. However, in this application a blockchain is still used, to benefit from the redundancy of information and the absence of a central intermediate allowed by a blockchain. Since 2018, the Massachusetts Institute of Technology (MIT), in Boston, is using this principle to issue diplomas to all of its students [14].

We will now see how blockchain can help students to pay for their higher education, which is an important issue

in some countries where tuition fees are very high. Some universities are now accepting to be paid by students with cryptocurrencies which can be very useful for some students who cannot pay with usual means of payment. Indeed, students do not always have access to bank accounts or credit cards, depending on the country they are from, their age or employment status. That can be an obstacle for some people to access higher education that is solved by using cryptocurrencies. For this application, the use of blockchain is relevant as blockchain is the underlying technology for cryptocurrencies like Bitcoin. The University of Nicosia (UNIC), in Cyprus, was in 2013 the first university to accept Bitcoin for tuition [17]. To address this problematic of school tuition, blockchain could also in the future allow to develop an effective voucher-based system [9]. Nowadays, some countries or private sponsors help students to afford tuition by providing them vouchers that they can spend at any educational organization or at a list of approved educational organizations. But managing such a system requires a large administration. Blockchain could help reduce all the bureaucracy required. Funding would be given to students as vouchers on a blockchain. We could also imagine that vouchers can be programmed to be unlocked gradually throughout the student's schooling, based on the performance and grades of the student. That can be implemented in a blockchain thanks to smart contracts, pieces of code written in the blockchain that execute transaction when some conditions are met. Writing promises of funding in a blockchain represents a security for the student, as they cannot be modified or cancelled after they have been added to the blockchain. Implementing such a system of smart contracts is possible with the Ethereum blockchain, that allows to define smart contracts. Thus a blockchain is needed for this application, because Ethereum relies on a permissionless blockchain.

C. Standard of living

A great barrier to the improvement of people's standard of living in developing countries especially but not only, is exclusion from financial services. On one hand, mainstream financial intuitions tend to settle in prosperous neighbourhood. In poorer neighbourhoods, they tend to be fewer and further apart. On the other hand, in developing countries especially, to avoid money laundering, financial institutions require a variety legal documents and minimum financial standards to actually be provided with a service such as a simple checking account. However, the great majority of the population in developing areas cannot meet these requirements and thus cannot benefit from financial services for their small businesses and other financial activities.

Here again, a variety of projects based on blockchain technology have stood out to provide exclude populations with access to financial services and thus allowing them to grow their businesses and improve the standard of living.

BitPesa [5] is a project born from the limits of M-Pesa, a mobile application that took of in Kenya to provide basic banking services to the excluded population. Although successful, it many people are still left out and Bitpesa expects it to be blockchain that will help to reach these people. Bitpesa uses the bitcoin blockchain to act like a bank open to everyone, including small and micro-enterprises. Bitpesa allows users to very cheaply perform payments and transfers internationally using Bitcoin as the intermediary currency. Bitpesa is only one of more than 30 similar projects based on blockchain based cryptocurrencies for money transfer services. Most of these project, like Rebit [16] in the Philippines focus on remittance services. Remittances consist in money transfers from foreign workers to their home country and represent, alongside international aid, one of the largest financial inflows to developing countries. Bitpesa, Rebit and other similar projects rely on blockchain in it's application for cryptocurrencies. Outstanding other important properties of cryptocurrencies, is the fact that they are permissionless and thus allow anyone to participate in the system, without excluding anyone like mainstream financial institutions. The need for a blockchain in this financial application as justified as the need of a blockchain as the underlying technology for a cryptocurrency.

D. Political and community life

One of the most prominent areas of blockchain applications in human development is identity services. A trusted identity is essential for one's participation in political, community and economic life. Refugees for example may have lost all their paperwork and blockchain project like Building Blocks in Jordan [12], are providing refugees with a digital identity based on a eye scan. Once registered in the refugee camp digital identity system, they can purchase goods and participate in community life. Many other similar identity services based on blockchain have taken off, even IBM, Microsoft and other big companies are teaming up on these projects to provide a legal identity to the estimated 1.1 billion people deprived of one. [11] Decentralization of identity services provided by these blockchain application removes the dependence of one's identity on any government or authority and related trust issues. With such systems, individuals own their identity and be sure, since it is immutable that it won't be lost. Although ideally, an always online TTP, represented bu governments or international authorities could be used, as we see with the present refugee crises around the world, it is not always the case. Thus, as reflected by the flowchart, a public permissioned blockchain is a good alternative solution.

Beyond identity services and still within the field of political and community life improvement, some projects are trying to use blockchain to defend people's freedom of speech. Publicism is consists in a decentralized news medium. On one hand, the property of anonymity of blockchain users allows journalist facing censorship to publish information and on the other, the property of immutability prevents this information from being censored. The use of a permissionless blockchain is justified for this application as it requires information to be stored and no TTP can exist in order to prevent any chance

of censorship. Information is furthermore written by several journalists that may not all be known.

E. Security and rights

In terms of security and rights, there are a few interesting projects, among these, there is BitLand [1] that attempt to tackle land property right problems in developing areas. Developing areas are characterized by weaker institutions and that often cannot provide a reliable a land registry causing land ownership disputes, fraud, and difficulty to obtain loans. Bitland started off in Ghana and aims at creating a reliable digital land registry based on blockchain technology. Similar projects accross the world exist like Fatcom in Honduras or the Swedish land ministry [4]. All these projects are at an experimental stage and despite positive media support and investment, they remain at an early development stage. Considering the problem of land registries, anonymity is not a necessary property one is looking for. Since there is no trustworthy central institution that can do provide a reliable registry, decentralization is key. Likewise, trustlessness and immutability are necessary to make the registry reliable and functional. Confronting the problem to Wüst and Gervais flowchart, we can justify the use of blockchain technology as solution. Land property transactions and information need to be stored. Multiple owners and buyer are involved, there are thus multiple writers. In developing areas, public institutions are too weak to act as an always online TTP. All owners and buyers should be identified, all writers are thus known but some may be tempted to fraud, they are thus not all trusted. Ownership of land should be publicly verifiable at least for taxation purposes. From this, we can conclude that a publicly permissioned blockchain application can be a solution for land property registries.

F. Sustainability

Development and integration of blockchain technologies in the Supply Chain Management can help people improve their way of consuming, by making it more sustainable, both environmentally and socially [6]. Supply Chain Management (SCM) can be defined as the management of all the resources, means, methods, tools and techniques intended to drive as effectively as possible the global chain of supply and delivery of a product or service to the final consumer [8]. Nowadays a lot of companies have developed blockchain-linked solution to improve the efficiency of the SCM, but blockchain can also help consumers trace the provenance of goods and services along the supply chain, to identify a product's input materials, including the material's quantity, quality and origin. For social sustainability we can quote the announce made in march 2018 by the Coca-Cola Company, saying that they are working on a project using blockchain to fight forced labour [7]. The purpose is to create a secure registry for workers and their contracts using blockchain in order to $\ll$ increase transparency and efficiency of the verification process related to labor policies within our supply chain $\gg$ said a Coca-Cola official. U.S. State Department, one NGO and a tech company will help Coca-Cola to develop this solution. Another example is the London-based startup firm Everledger that certifies and tracks trade in diamonds using blockchain, to reduce sales of stolen gems or conflict stones from warlorsd [18]. Traceability can also help consumers to know more about the ecological impact of products. By linking blockchain and the Internet of Things, with sensors recording and writing on the blockchain the environmental impacts of manufacturing processes, it becomes possible to know the ecological footprint of a product. For instance, Walmart is tracking its pork supply chain in China by recording information such as farm origin and storage temperature in the blockchain [13]. Companies can also track the consumption of energy or materials during the manufacturing process of a given product. Knowing the ecological footprint of a company or a consumer thanks to the blockchain can be useful for authorities to reward sustainable behaviors with incentives such as tax rebates. For these applications of traceability, using a blockchain is relevant according to Wust and Gervais flowchart. Indeed we need to store data and multiple writers are involved along the supply chain. Also there isn't a TTP available all along the supply chain, especially in third world countries where corruption is important, and writers can not be trusted, as companies could for exemple try to alter some data about the products they sell in order to reduce their ecological or social impact. Thus a permissioned blockchain is needed. Public verifiability is an important part of traceability so a public permissioned blockchain appears to be the most adequate. Yet, some privacy might be requested for companies at some point of the supply chain, to respect trade secret. That can be achieved in a public permissioned blockchain but with computationally expensive cryptography to ensure some privacy.

IV. Discussion

Blockchain can be a good solution to several human development applications. Blockchain technology is particularly well suited solution for identity services and banking services. It can enable banking services for the previously unbankable people allowing them to achieve transactions and grow their businesses despite all. We have firthermore seen that in refugee camps in Jordan, blockchain allows people without any official documents to purchase goods by identifying themselves with their eyes offering them an official form recognition and better integration in their community. Lastly, the usefulness of blockchain for human development purposes is not limited to developing areas as we've seen with the university of Nicosi's acceptance of cryptocurrency payments of tuition fees.

That said, in some cases blockchain is not the only solution. As we saw for digital certifications from educational organizations, a solution already exists that works very well without using blockchain, but a blockchain solution still has been developed to get rid of a TTP. In some other cases, you are even better off without a blockchain like for instance when developing an application to keep track of HIV spread thanks to digital vaccine.

Blockchain may be a good solution now for problems faced by developing countries, where institutions are weaker and cannot be relied upon. However, looking into the future, as a country develops, one should expect this to change and as institutions grow stronger they will probably be able to act more reliably as an always online TTP. The need for a blockchain in several applications will thus disappear as they would be less performant than alternative solutions using a TTP. On the other hand, governments and well established institutions could and in some cases already are adopting blockchain technology themselves in many fields, among which we can quote the implementation of smart contracts. Thus blockchain will not disappear even with the emergence of strong and trust worthy institutions all around the world.

V. CONCLUSIONS

As the emergence of Internet changed many things in our lives in the past decades, Blockchain could induce a lot of technological improvement to today's world. In this paper we studied how it is helping human development. After briefly explaining what human development is, and of course what blockchain and its main properties are, we listed some applications of blockchain in the different areas of human development. We can therefore affirm that blockchain applications are much more extensive than their contribution to cryptocurrencies to which this technology is very often associated to. Moreover, in many problems related to human development, especially in developing countries, blockchain is a key technology to implement solutions that couldn't exist without it. However, even if blockchain is a cutting edge technology, one should keep in mind that it is not the solution to every problem, as sometimes a more usual data structure like a database with shared write is the more appropriate and least constraining solution.

REFERENCES

[1] URL: http://www.bitland.world/about/.

[2] 10104997427432193. *How Blockchain Helps Smallholder Farmers in Developing Countries*. 2018. URL: https://futureofag.com/how-blockchain-helps-smallholder-farmers-in-developing-countries-64bf6f13c049.

[3] *Agriledger*. URL: http://www.agriledger.io/.

[4] Shefali Anand. *A Pioneer in Real Estate Blockchain Emerges in Europe*. 2018. URL: https://www.wsj.com/articles/a-pioneer-in-real-estate-blockchain-emerges-in-europe-1520337601?mod=searchresults&page=1&pos=3.

[5] *BitPesa*. URL: https://www.bitpesa.co/.

[6] Guillaume Chapron. "The environment needs cryptogovernance". en. In: *Nature News* 545.7655 (May 2017), p. 403. DOI: 10.1038/545403a. URL: http://www.nature.com/news/the-environment-needs-cryptogovernance-1.22023.

[7] "Coca-Cola, U.S. State Dept to use blockchain to combat forced labor". en. In: *Reuters* (Mar. 2018). URL: https://www.reuters.com/article/us-blockchain-coca-cola-labor-idUSKCN1GS2PY.

[8] *definition de supply chain management*. URL: https://www.glossaire-international.com/pages/tous-les-termes/supply-chain-management.html.

[9] Alexander Grech and Anthony F. Camilleri. *Blockchain in Education*. Englisch. Luxembourg: pedocs, 2017. ISBN: 9789279734977. URL: http://nbn-resolving.de/urn:nbn:de:0111-pedocs-150132.

[10] *Human Development Reports*. URL: http://hdr.undp.org/en/content/what-human-development.

[11] *Identification for Development (ID4D) Global Dataset*. 2018. URL: https://datacatalog.worldbank.org/dataset/identification-development-global-dataset.

[12] Russ Juskalian. *Inside the Jordan refugee camp that runs on blockchain*. 2018. URL: https://www.technologyreview.com/s/610806/inside-the-jordan-refugee-camp-that-runs-on-blockchain/.

[13] Reshma Kamath. "Food Traceability on Blockchain: Walmartâs Pork and Mango Pilots with IBM". en. In: *The JBBA* 1.1 (June 2018), p. 3712. ISSN: 2516-3957. DOI: 10.31585/jbba-1-1-(10)2018. URL: jbba.scholasticahq.com.

[14] *Le MIT utilise la blockchain pour certifier les diplÃŽmes obtenus par les Ã©tudiants*. fr-FR. Mar. 2018. URL: https://www.blogdumoderateur.com/blockchain-certification-diplomes/.

[15] Jia Liu. "HIV digital vaccine strategy: An application of blockchain technology in preventing the spread of HIV (Preprint)". In: (2018). DOI: 10.2196/preprints.12308.

[16] *Rebit*. URL: https://rebit.ph/.

[17] *University of Nicosia in Cyprus is the First to Accept Bitcoin and Offer a Master's in Digital Currencies*. en-US. Nov. 2013. URL: https://www.ccn.com/university-nicosia-cyprus-first-accept-bitcoin-offer-masters-digital-currencies/.

[18] Karl Wust and Arthur Gervais. "Do you Need a Blockchain?" In: *2018 Crypto Valley Conference on*

Blockchain Technology (CVCBT) (2018). DOI: 10.1109/cvcbt.2018.00011.

[19] Peng Zhang et al. "Blockchain Technology Use Cases in Healthcare". In: *Advances in Computers Blockchain Technology: Platforms, Tools and Use Cases* (2018), 1–41. DOI: 10.1016/bs.adcom.2018.03.006.