UCLouvain

LOUVAIN
School of Management

Louvain School of Management

What are the potential benefits of blockchain applications for the Université Catholique de Louvain ?

Author : Louis-Cédric Petre
Supervisor(s) : Bernard Paque & Christophe Lejeune
Academic year 2018-2019

First and foremost, I would like to thank both of my supervisors; Professors Bernard Paque and Professor Christophe Lejeune. Thanks to their various experiences and expertise, they were able to provide invaluable inputs and guidance throughout the writing of this thesis.

In a second place, I would like to thank all the people that have proofread this paper; Elisabeth Heroes, Leslie Marianne and Mathieu Baudelet. Their pertinent and critical reviews were of great help in improving this paper.

In addition to that, I would like to thank my parents as well as my friends who were always by my side to support me.

Last but not least, I would like to express my gratitude towards all the professors at the Louvain School of Management and Bocconi for always encouraging personal interests towards innovation and new trends. I have developed an avid willingness to discover disrupting technologies and game-changers in any industry and I owe that to them.

Table of content

1. Introduction 1
2. Problematic and research question 2
3. Methodology 2
4. Blockchain technology 4
   4.1. Origin 4
   4.2. Improvements 6
      4.2.1. Merkle tree 6
   4.3. How does it work 9
      4.3.1. Block 10
      4.3.2. Proof-of-work 11
      4.3.3. Genesis block 11
      4.3.4. Peer-to-peer network 12
      4.3.5. Tampering content 14
   4.4. Blockchain fork 14
   4.5. Types of blockchain 15
      4.5.1. Authorisation 16
      4.5.2. Access 17
5. Blockchain apparition in public knowledge 18
   5.1. Blockchain coverage boom 18
   5.2. Hype evolution 20
      5.2.1. Blockchain technology evolution 20
      5.2.2. Blockchain for data security apparition 22
      5.2.3. Evolution compared to other technologies 22
   5.3. Falling for the hype 23
6. Uses of blockchain 24
   6.1. Blockchain generations 24
      6.1.1. Blockchain 1.0 24
      6.1.2. Blockchain 2.0 25
      6.1.3. Blockchain 3.0 26
      6.1.4. Blockchain 4.0 27
7. Knowledge management 35
   7.1. Knowledge 35
   7.2. Processes and objectives 36
   7.3. Type of knowledge transferred in universities 37

7.4. Knowledge management cycles & application to university knowledge transfer 38
7.4.1. The Meyer & Zack Knowledge Management Cycle 38
7.4.2. Application of Meyer & Zack cycle in the UCL case 39
7.4.3. The Bukowitz & Williams knowledge management cycle 40
7.4.4. Application of the Bukowitz & Williams cycle in the UCL case 42
7.4.5. McElroy knowledge management cycle 42
7.4.6. Application of the McElroy cycle in the UCL case 44
7.4.7. Wiig knowledge management cycle 44
7.4.8. Application of the Wiig cycle in the UCL case 46
7.4.9. Comparison of knowledge management cycles 46
7.4.10. Application of Dalkir integrated cycle in the UCL case 47
7.4.11. Blockchain applications in UCL's Dalkir integrated cycle 47
7.5. Knowledge management models & application to university knowledge transfer 48
7.5.1. The von Krogh and Roos model of organisational epistemology 49
7.5.2. Application of the von Krogh and Roos model in the UCL case 49
7.5.3. The Nonaka and Takeuchi knowledge spiral model 49
7.5.4. Application of the Nonaka and Takeuchi model in the UCL case 51
7.5.5. The Choo Sense-making knowledge management model 51
7.5.6. Application of Choo's model in the UCL case 53
7.5.7. The Wiig knowledge management model 53
7.5.8. Application of the Wiig model in the UCL case 55
8. Blockchain use: Case of UCL 56
8.1. Proposing new initiatives & offering feedback 56
8.1.1. Blockchain implementation 56
8.1.2. Feasibility 58
8.1.3. Cost-benefit analysis 59
8.1.4. Conclusion 60
8.2. Securing degrees & verifying their authenticities 60
8.2.1. Current situation 60
8.2.2. Blockchain implementation: Blockcerts 61
8.2.3. Feasibility 64
8.2.4. Cost-benefit analysis 64
8.4.3. Benchmark with other solutions 68
8.4.4. Real-life example 70
8.4.5. Action plan 72
8.4.6. Risks 73

8.4.7. Improvements 74
8.5. Verification of an accreditation chain 74
8.5.1. Current situation 74
8.5.2. Blockchain implementation 75
8.5.3. Feasibility 75
8.5.4. Cost-benefit analysis 76
8.6. Other uses in education 76
8.6.1. Managing intellectual property 76
8.6.2. Capacity-currency transformation bank 77
8.6.3. Future possibilities 78
9. Conclusion 80
10. References 81
11. Appendices 85
Appendix 1: Wiig knowledge management model: degrees of internalization (Wiig, 1993) 85

1. Introduction

Nowadays, global university competition is at an all-time high. Universities come up with new innovative solutions to gain media attention, increase in the rankings and improve global recognition. Two of the key drivers of this competition are innovation and technology. This paper explores the potential applications of innovative trendy technology – blockchain – at the Université Catholique de Louvain. Innovative applications of blockchain in education would bring UCL at the front of the international stage. It would offer global press coverage and increase the university's reputation.

This paper focuses on the blockchain technology as it is an upcoming technology with an infinite number of applications that have yet to be explored. The scope of this thesis is though limited to the field of education and more specifically to UCL in order to provide tailor-made blockchain applications.

This thesis starts with an explanation of the problematic and the methodology to fully understand the structure of this paper. The next section explains how the blockchain technology works as it is key in the global comprehension of this paper. It continues with a short explanation of the important blockchain press coverage and why it is key to analyse blockchain potential applications. In addition to that, knowledge management processes in theory and applied to UCL are developed. They serve as a basis to discover, understand and analyse potential blockchain application leads. After that, a practical part is dedicated to the analysis of different potential applications for UCL. The most promising and interesting ones in the short to medium term are explored further. Finally, the thesis ends with an exploration of potential future uses that are not yet viable. A conclusion wraps up the paper with the most promising leads and ideas.

These most promising ideas include a blockchain-based application for UCL degree delivery that would allow students to own the verification of the authenticity of their degrees thanks to the blockchain technology. It also includes how to use the technology further and apply a worldwide-first use of the technology at UCL!

2. Problematic and research question

Universities are at the forefront of research and should be the first to try and use new discoveries. Thanks to their teams of researchers and the constant refreshing of knowledge done by their professors, universities should be able to implement first new technologies. While doing so, universities would remain in advance and ensure they develop the technology uses of tomorrow.

Unfortunately, for now, universities mostly focus on the theoretical part of projects. They produce new ideas and develop innovative solutions but they rarely implement them in the education field. Therefore, universities are both front runner in terms of theoretical research and late in innovation implementation. It is especially the case with technologies. Some research team works on the technologies of tomorrow, improving greatly the future. But at the same time, these technologies are not used in university. Indeed, the university almost never leverages new technologies for itself and its related stakeholders like students, professors, staff, etc.

Therefore, this paper explores the different possibilities for blockchain implementation in the education field and more precisely for universities. Ultimately, the objective is to analyse, weight and decide which blockchain implementations can be the most interesting and rewarding for the Université Catholique de Louvain. This would allow the UCL to remain a Belgian front runner in both technology research and technology implementation in the education sector.

The research question investigated is the following one: "*What are the potential benefits of the blockchain technology applications for the Université Catholique de Louvain ?"*.

3. Methodology

As of mid-2019, applications of blockchain in the education field are very limited both in terms of possibilities and in terms of actors. Therefore, this paper mostly focuses on what can be done and achieved in the future, based on the very little current applications and technology as such.

Therefore, to answer the research question, a few elements are required. First, it is primordial to fully understand the blockchain technology, its potential applications and how to leverage the technology for new innovative uses. Second, it is key to understand the knowledge

management transfer process in universities and more specifically at the Université Catholique de Louvain. Third, it is key to being able to converge both information in order to provide potential leads for educational uses of blockchain at UCL.

The main source of information used in this paper is qualitative. Indeed, most of the knowledge leveraged in this paper comes from research articles, white papers and start-ups. More importantly, the information used in this paper comes from people trying to improve current processes, disrupt the current way of doing business, change the way education work…; people trying to reshape the future and more specifically the future of education.

Most of the information was found in scientific papers available in online libraries. Nevertheless, part of the information was also retrieved from non-scientific sources to bring innovative ideas to the table. These non-scientific sources were used for their ideas and not for their theoretical background. The objective was to combine scientific stiffness and completeness of information with non-scientific latest innovative ideas available online. The main criteria of information selection used for this paper was to analyse if the source could either bring a new theoretical understanding of the blockchain technology or knowledge management process (that could help build up new solutions) or new innovative blockchain uses.

One of the main difficulties encountered while writing this paper was the constant evolution of technology. Indeed, from the beginning of the writing to the end, the blockchain technology had received so much attention and investment that the technology has evolved, and new uses were possible. To face this problem, applications were improved and reviewed once in a while with a final review beginning of July 2019.

Another important difficulty was the absence of used cases. Indeed, as applications of blockchain in education are very rare and at an early stage, it is impossible to base analyses and plans on something already achieved. To compensate for this issue, multiple sources were used: scientific and non-scientific ones. The objective was to combine both sources' advantages and to understand what all sources were thinking about potential applications.

4. Blockchain technology

This section aims to offer a global comprehension of blockchain technology. It starts with the origin of the technology and the different improvements that were added to the initial technology. Then, it continues with a subsection explaining how it concretely works. After that, another subsection covers the interesting blockchain fork phenomena. Finally, it ends with an explanation of the different kinds of blockchain.

4.1. Origin

The blockchain technology was created in 1991 by a group of researchers who were looking for a new way of timestamping digital documents. Haber and Stornetta started by tackling an important issue at that time: it was impossible to timestamp digital content. Protecting the information container was an option but the data could be changed. Therefore, they worked on a way to protect digital data from falsification. (Haber & Stornetta, 1991)

They were looking for a solution that should have the following two characteristics (Haber & Stornetta, 1991):

1. The data should be timestamped so that it is impossible to tamper even a bit without the change being apparent.
2. Every change that is made leads to a change in time and date.

To come up with a solution to meeting these requirements, they created a first "Naïve solution", then observed the issues and improved the solution. They continued this iterative process until they reached a satisfying solution. The naïve solution was a "digital safety-deposit box". Each user could give a document to a central institution called time-stamping service (TSS) which would keep a copy of the data as well as the time and date. Therefore, if the user believes the document has been tampered with, he can compare it with the version of the TSS. This solution includes several issues (Haber & Stornetta, 1991):

1. Privacy
2. Time and expense required
3. TSS's incompetence
4. Trust in TSS

Afterwards, they considered the fourth issue as solved to focus on the 3 first ones. They came up with two major improvements (Haber & Stornetta, 1991):

First, they improved their solution by implementing "*collision-free hash functions*".

> Note: *"A hash is a function that converts an input of letters and numbers into an encrypted output of a fixed length. A hash is created using an algorithm, and is essential to blockchain management in cryptocurrency."* (Investopedia, 2017)

These functions reduce bit-strings of variable lengths to bit-strings of fixed lengths. The functions *h* (= hash) have few properties. Firstly, it is easy to pick one member of the function randomly without affecting the others. Secondly, it is also easy to compute the functions (it does not require a long and complicated process). Lastly, it is impossible to have x; x' (x' being any other element of the function than x) satisfying h(x) = h(x') (that would be a collision). Therefore, the user does not need to send the document to the TSS but to compute hash value function h(x)=y. Thanks to this improvement, the privacy issue disappears, the time and expenses required drop considerably and the risk of a lack of TSS' competences is decreased as well (Haber & Stornetta, 1991).

Second, they implemented digital signatures. As showed by Rompel, one-way functions can be used to reach a very strong level of security.

> Note: "*A one-way function is a mathematical function that is significantly easier to compute in one direction (the forward direction) than in the opposite direction (the inverse direction). It might be possible, for example, to compute the function in the forward direction in seconds but to compute its inverse could take months or years, if at all possible."* (Suthar & Patel)

The document is received by the TSS which can check the signature and date and time of reception and can sign it as well before sending it to the client. These eliminate the issue of potential present or future competence issue of TSS as TSS can sign easily and unilaterally the document (Rompel, 1990)

Even if these improvements considerably enhance the solution of digital time-stamping, the fourth issue related to TSS trust is not fixed. Indeed, the best solution should consider that TSS is willing to cheat and alter the documents. If it is the case, the aforementioned is useless. There were two ways to solve this issue (Rompel, 1990):

First, the system could force TSS to produce very authenticable and unique time-stamps so it is hard to copy them. This technique is called linking. It creates time-stamps that are linked with each other and therefore form together a data structure. Modification of the data is impossible because it would invalidate the whole structure. Modification of date and time is

also impossible because the structure is following a temporal order: each document timestamp depends on the previous ones. It is, therefore, impossible to backdate the document, even for the original user who created it (Rompel, 1990).

Second, the trust in the TSS could be split among users in a way that changing the data, or the date or time of a document could be noticed by the others. This technique is called distributed trust. The user who wants to timestamp a document will request signatures from other users to uniquely identify at a certain date and time his document. The list of signatures from users known by a sequence randomly generated can't be modified without noticing the signers. Therefore, a question is rising: what if a challenger who wants to change the document corrupt a certain proportion of the users? Haber and Stornetta did different computations with various percentages of users corrupted and even with 90% of corrupted users, it would be impossible for the challenger to alter the document without noticing the owner (Haber & Stornetta, 1991).

The choice between these two options come with different trade-offs, balancing the advantages and disadvantages of each solution.

The linking method comes with several disadvantages which are (Haber & Stornetta, 1991) (Rompel, 1990):

1. Clients must wait for the second part of the certificate which depends on other users
2. The whole system depends on other users and how often they use the system
3. It does not ensure a service that gives the precise time but a timeframe in which the document was certified. This timeframe is bounded by two limits; the previous and next requests. Therefore, the timeframe can be large if the timing between the two requests is long. Hence, this method is at best use when a lot of requests are made.

On the other hand, the distributed trust technique launches all processing at the time of the request but requires a higher level of technology (Haber & Stornetta, 1991) (Rompel, 1990).

4.2. Improvements

4.2.1. Merkle tree

In 1992, Bayer, Haber and Stornetta wrote a paper to improve the 1991's solution for document's timestamping. They realised one of the issues of the previous model was that in both solutions (linking or distributed trust), the requirements for each timestamping was directly proportional to the number of observers. Therefore, they asked themselves a question:

"*What if an immense flood of banal transactions want their time-stamps to become part of the historical record, but history just isn't interested?*". It highlights the potential issue of having too many banal requests compared to the number of willing observers. Indeed, if there are too many banal requests and only a small number of active observers, it will cause an issue (Bayer, Stuart, & Stornetta, 1993).

They came up with a solution: implementing trees. With the previous linking system, if we consider N the number of documents required to get a trustworthy certificate, the verification process has a length of exactly N steps. Thanks to the implementation of trees, this number can be reduced from N to log (N) (Bayer, Stuart, & Stornetta, 1993).

Before going any further, it is important to note that the tree system was inspired by Merkle's work who patented the kind of tree that will be discussed in the following paragraphs.

For the purpose of the example, assume there are two users who would like to timestamp their documents. Instead of creating a hash value for each of them, a single hash value will be created and publicised.

> Note: *"A hash value is a numeric value of a fixed length that uniquely identifies data. Hash values represent large amounts of data as much smaller numeric values, so they are used with digital signatures. You can sign a hash value more efficiently than signing the larger value."* (Microsoft, 2017)

As it is validated by an observer, the combined hash value is trustworthy. Thus, the user can prove that the document existed before the common hash value was published. Indeed, as the document was part of the inputs to create the combined hash value, it was necessary existing before the combined hash value publication (Merkle, 1987).

If this technique is generalised and considers that N documents have a combined hash value established through a binary tree, then the user can easily prove the priority of his document. Indeed, he only needs the document and the $\log_2$ (N) hash values (from root to top) which were combined to form the common hash value. In addition, the user should note if the computed value was put before or after the combined hash value. Therefore, verification can easily be done by recompiling the path from root to top with this data (Merkle, 1987).

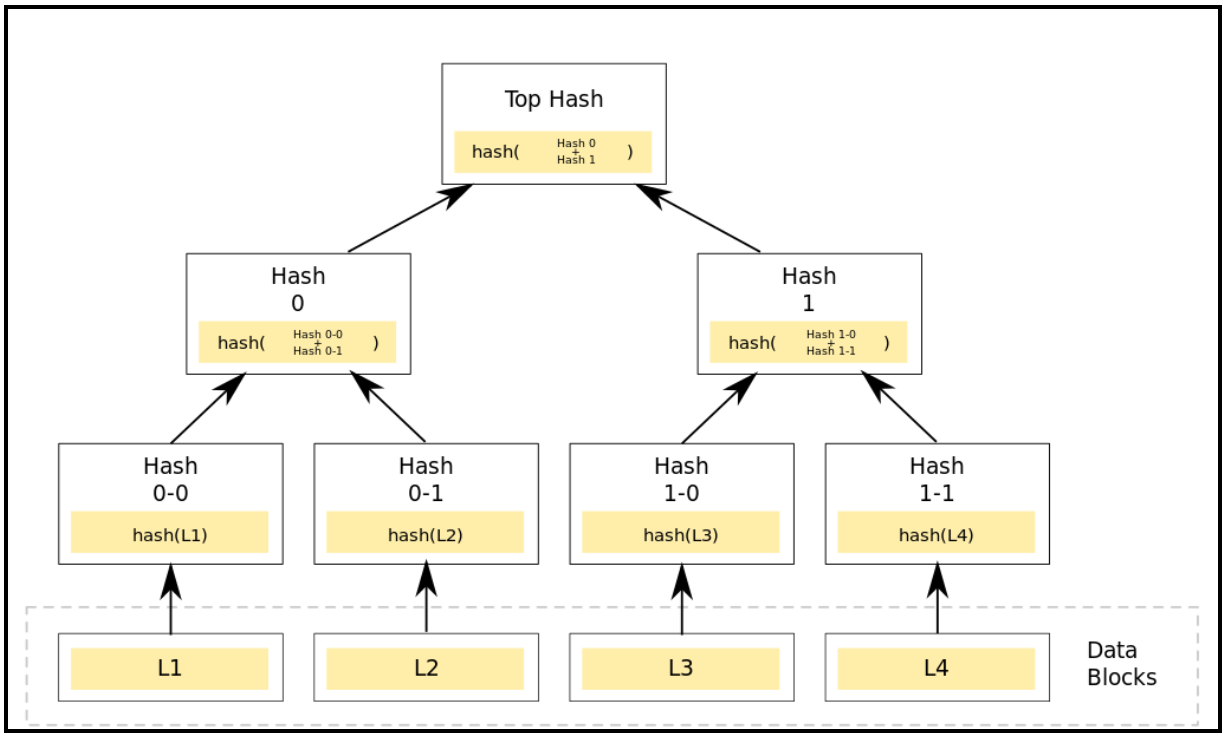


Figure 1: Example of Merkle's tree (Merkle, 1987)

As it can be seen in the figure above, the top hash is a combination of hash 0 and hash 1 which are themselves a combination of two other subsequent hashes. Therefore, in this example, four documents are timestamped thanks to one combined hash value which is the top hash (Merkle, 1987).

In the paper written by Bayer, Haber and Stornetta, they take the example of a world tournament to illustrate their thoughts. Indeed, once the hashing functions have been chosen, the local subtrees could be managed by heterogeneous local networks which would have a "*winner*" amongst the participants and these local winners will then compete to determine regional winners that could finally be combined into global winners. These ones would, therefore, be considered as the winner of all participants. To create such a system, there are two requirements (Bayer, Stuart, & Stornetta, 1993).

First, a global communication system should exist to ensure the global winner is above all participants (Bayer, Stuart, & Stornetta, 1993).

Second, a broadcast protocol should be agreed amongst participants. It will allow the system not to use any centralised institution and will ensure that the global winners are publicly observable (Bayer, Stuart, & Stornetta, 1993).

Thanks to this improvement, there are in 1992 three digital timestamping solutions which are the linear linking technique, the distributed trust option and the linking into trees solution. Bayer, Haber and Stornetta start to ask themselves if there are links between them and if one is superior to the others and should, therefore, be favored. At first, it seems that the linking into trees techniques is better than the two other options because it reduces the storage requirements while increasing the number of witnesses, but other trade-offs should be considered (Bayer, Stuart, & Stornetta, 1993):

1. In some cases, the point of timestamping is not only to have a trustworthy date for the document but also to have the sequential order in which the entries were made. Therefore, in these cases, the linear linking is preferred (versus the tree linking method) because it establishes the date by considering the previous and the next timestamped document in the system.
2. Even if the tree linking method increases the number of witnesses compared to the documents to be timestamped, this system does not guarantee a minimum amount of witnesses. On the contrary, the random witness solution offers this feature.
3. The linking into trees option does not ensure that witnesses will keep the records but it is the case while using the random witness solution.

Considering the second and third trade-offs, the random witness method creates a certificate that is published and therefore the timestamping can be witnessed by a large audience. It means that the final validity does not depend entirely on the witnesses keeping the records (Bayer, Stuart, & Stornetta, 1993).

In conclusion, the three different options should be chosen by considering the specific need of the user. A company could use each solution in a different situation or for a different purpose (Bayer, Stuart, & Stornetta, 1993).

4.3. How does it work

Blockchain was built upon the previously explained technology.

Blockchain, as it can be told by the name, is a chain of blocks that contains specific information. A blockchain is open to anyone so that the world is a witness of what happens in the chain. The main point is to eliminate the possibility of changing the information without being noticed by the other users. Indeed, this technology was originally created as timestamping to avoid people from tampering with the date or the content of a digital document.

The security of the blockchain is ensured thanks to the features of each block, the proof-of-work and the peer-to-peer network.

The objective of this section is to provide an understanding of how blockchain works. It covers different the explanation of different concepts necessary to the understanding of the blockchain technology: block, proof-of-work, peer-to-peer network, genesis block and tampering content.

4.3.1. Block

This section has been written based on three different articles (Nakamoto, 2008) (Iansity & Lakhani, 2017) (Morabito, 2017). To understand the blockchain technology, it is important to analyse how each block is built. Each block is composed of three parts:

1. The data

The data that is contained inside the block depends on the type of blockchain as it will be discussed in the section dedicated to the types od blockchains.

2. The hash

The hash is a sequence that uniquely identifies a block in the blockchain. It is built thanks to an improved model described in the previous section dealing with the origin of blockchain. As the hash value is linked to the content of the block, if the data inside the block changes, the hash value will change as well. Therefore, the change can be detected easily.

3. The hash of the previous block.

This feature makes a blockchain secure. Indeed, if the hash value of the previous block (n-1) changes, it will make the block (n) invalid as a component of this block (n) is the hash value of the previous block (n-1). The previous block is also sometimes called the Parent block. Here is an example of a blockchain composed of 3 different blocks:

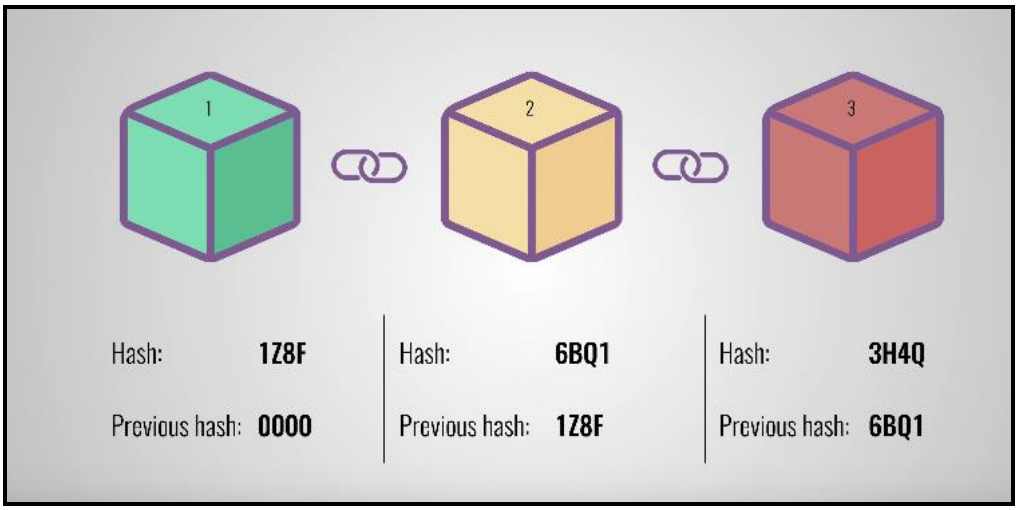


Figure 2: Example of blockchain (Simply Explained, 2017)

As it can be seen in the figure above, each block has a hash and the hash value of the previous block. Therefore, block 2 has a unique hash 6BQ1 and the hash value of the previous block so the hash value of block 1: 1Z8F. If someone tampers the data of block 1, it will immediately change the value of the hash to another sequence, for example, 5BS9. Therefore, the block 2 will not be valid anymore because one of its components is the value of the previous block which is supposed to be 1Z8F but as the previous block has been tampered with, it is now 5BS9. The invalidity of block 2 will lead to the invalidity of block 3 as they are linked and so on.

Thanks to the previous hash value aspect, the data is secured. Indeed, it is impossible to tamper a block without being noticed by the rest of the chain unless recalculating all hashes of next blocks. Since computers can calculate an incredible amount of hashes in a few seconds, the security is not entirely ensured with only the three features of a block. To face this issue, the blockchain has a special feature called proof-of-work.

4.3.2. Proof-of-work

Proof-of-work is a characteristic of the blockchain that slows down the creation of a new block. Therefore, if a challenger wants to tamper the data of a block and recalculate the hash values of all next blocks, he can't recreate all blocks quickly. For instance, with the Bitcoin blockchain, creating a new block takes 10 minutes.

4.3.3. Genesis block

Nevertheless, there is still an issue with the first block of the chain because it does not have any previous block as it is the first and as blockchain is not circular. This block is called the genesis block. It is used as a secure root for the blockchain. Every node knows the hash value and the block structure of this genesis block.

4.3.4. Peer-to-peer network

There is a third part of the blockchain technology that ensures the security of its content: the peer-to-peer network. Indeed, as mentioned before, a blockchain is open to anyone but when a new user enters the system, he gets a full copy of the current blockchain.

Therefore, if a user creates a new block, this block is sent to all users of the blockchain (also called nodes of the blockchain) so they can verify that the block is valid. If the block is considered valid, it is added to the record of the blockchain the user has. If most users validate the block, a consensus is reached, and the block is officially validated (Hammerschmidt, 2017).

The peer-to-peer network is a distributed network. Nowadays, there are three kinds of network:

1. Centralised network

Figure 3: Example of centralised network (Quantalysus, 2018)

A centralised network has a special characteristic of having a central institution that manages all the resources of the network. Therefore, if a user wants to access information, he must connect with this central power. It is mostly criticised for not being transparent, stringent and un-inclusive. Another big issue with a centralised network is security. Indeed, a challenger has only to hack one node, the central one, to get access to all information of the network.

2. Decentralised network

Figure 4: Example of decentralised network (Quantalysus, 2018)

This kind of network gives resources to individual nodes. It is not required to access a central node to get information as it is spread among the individual nodes. Therefore, when a node needs particular information, it makes the query and finds the information it is looking for in another node of the network. This kind of network is harder to hack because the information is spread in the network. Nevertheless, the virus that infected one node could reach other nodes due to the information sharing process.

3. Distributed network

Figure 5: Example of distributed network (Quantalysus, 2018)

The main difference between a decentralised network and a distributed network is the task distribution. Indeed, in a distributed network, the tasks are spread among the nodes of the network and each node is up-to-date with the state of the other nodes.

In a distributed network, each node works independently on its information, only the tasks are known by the other nodes.

According to (Morabito, 2017), "*Distributed systems are characterised by geography, parallelism, reliability, availability, and mistrust*".

Finally, it is important to notice that a decentralised network can be considered as a subset of a distributed network. Therefore, it is normal they share common characteristics.

4.3.5. Tampering content

In conclusion, to tamper with a block, the challenger should:

1. Tamper with all blocks of the chain
2. Redo the proof of work for each block
3. Take control of more than 50% of the peer-to-peer network

It is almost impossible, especially if the chain is long and well distributed. Furthermore, the users are anonymous on the blockchain as they are identified by a sequential number. Therefore, getting control of more than 50% of the network is particularly difficult. In addition to that, if one of the witnesses is not part of the controlled users, the tampering fails. Thus, way more than 50% of control is required. In fact, it is proven that even with 90% of control, tampering is still considered impossible (Haber & Stornetta, 1991).

4.4. Blockchain fork

A blockchain fork, as confirmed by its name, is when a blockchain separates into two or more different parallel chains (therefore forming a fork). Thus, there is a single genesis block for different chains. If the other chain(s) is/are abandoned, a new blockchain is created with a new genesis block (Baliga, 2017).

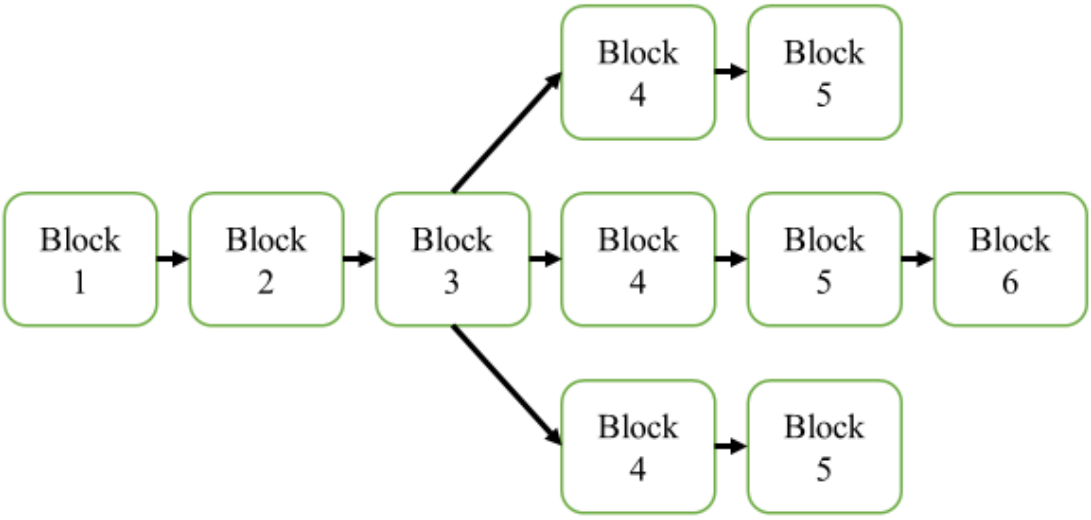


Figure 6: Blockchain fork

As it can be seen in the figure above, a blockchain fork occurs at block 3. It leads to three parallel chains. As two of them are abandoned at block 5, a new blockchain is created with block 6 as the genesis block.

A blockchain fork can occur for various reasons and can be accidental or forced.

An accidental blockchain fork (soft fork) is the result of an issue in a merger or incompatible software versions. Indeed, participants in the same network can use various versions of the same software. Quite often, a new version of the software is developed to fix a few bugs. Therefore, having users with different versions of the software represent different levels of risk towards the users. This differentiation can lead to a blockchain fork (Baliga, 2017).

A voluntary blockchain fork (hard fork) occurs when the developers want to change something in the underlying technology of the blockchain. When the change has been made, the users should agree to these consistent changes and correct usage of the technology in the future (Baliga, 2017).

In the special case of cryptocurrencies, only one blockchain can be correct at the end. During the process of forking, transactions should not be made because there is a risk of losing it. Therefore, companies do not like having forks because it creates a moment in time where they can't do any transactions without taking a risk. In addition, it is a lot of work as all kind of stakeholders (users, miners…) must be updated to the latest version (Baliga, 2017).

There are many examples of blockchain forks, especially in the cryptocurrency world:

- Ethereum hard fork into two blockchains: the "Ethereum" and the "Ethereum Classic" to fix an issue in the code that potentially allowed people to steal Ethereum (Coppola, 2016).
- Bitcoin hard fork into two blockchains: the "Bitcoin" and the "Bitcoin Gold" at block 478 558. The idea was to offer the opportunity to more people with a less powerful machine to mine Bitcoin too (Bitcoin gold).
- Bitcoin hard fork into two blockchains because of rising tensions between developers: the "Bitcoin" and the "Bitcoin Cash" at block 491 407 (Bitcoin Cash).
- Bitcoin hard fork into two blockchains: the "Bitcoin" and the "Bitcoin Private" at block 511 346 to allow a "founder-fee" (20% of mining going to the initial blockchain development and maintenance team) (Bitcoin Private).

4.5. Types of blockchain

The types of blockchains can be classified according to many criteria, this section will deal with the two most used ones: authorisation and access (Peters & Panayi, 2016).

In most cases, the permissionless blockchains are public and the permissioned blockchains are private (Peters & Panayi, 2016).

4.5.1. Authorisation

The authorisation criteria splits blockchains into two groups: permissionless and permissioned blockchains (Peters & Panayi, 2016).

4.5.1.1. Permissionless blockchains

Permissionless blockchains are blockchains where any users can take part in the verification process. It means that anybody can become a user and therefore a verifier without having to receive specific permission. The main motive of the permissionless characteristic is that verifiers are needed for the blockchain to work. Indeed, the network needs verifiers who check the validity of blocks of transactions (Peters & Panayi, 2016) (Boaventura, 2018).

But that is not it, they are required to ensure the proof-of-work consensus. Indeed, if a lot of verifiers check the validity of a block of transactions, the total amount of processing power that is given to the network will be high and it will be done at a very high pace. Therefore, if a challenger wants to tamper with this block of transactions, as explained in the proof-of-work concept, he should bring into the network more processing power than the total amount of processing power of all verifiers. It is very difficult to achieve and gets harder with the increasing number of verifiers. Even if this technique is costly in terms of computations (and energy), it offers the security characteristic to the blockchain (Peters & Panayi, 2016) (Boaventura, 2018).

According to Swanson, the advantage of a permissionless blockchain is that it allows accommodating both anonymous and "*pseudonymous*" actors (Swanson, 2015). In addition to that, a permissionless blockchain protects from Sybil attacks (Douceur, 2002).

> *Note:* A Sybil attack is a cyber-attack focusing on peer-to-peer networks that creates a lot of fake individual user accounts to get more influence (Douceur, 2002).

On the other hand, the disadvantage of a permissionless blockchain is that it requires to provide an incentive for the verifiers. Indeed, as their jobs are key to the well-functioning of the system, they should have an incentive to take part in the verification process. For example, in the cryptocurrency case, verifiers are paid for the blocks of transactions they check (Swanson, 2015).

Few well-known examples of permissionless blockchain are the Bitcoin and the Ethereum (Swanson, 2015).

4.5.1.2. Permissioned blockchains

Permissioned blockchains are blockchains that require an appointed trusted party to give permissions. In addition to them, other verifiers can be added if they are validated by the initial trusted parties or even a central authority. A permissioned blockchain system is close to the systems that are used in the financial sectors with users that can do certain verifications (Swanson, 2015) (Boaventura, 2018).

This kind of blockchain is purpose-built, it means they can be created for a specific purpose such as maintaining certain compatibility between other systems (Swanson, 2015).

Permissioned blockchains are mostly private so that permissions can only be given by members of an organisation or consortium. It ensures that a consensus should be reached amongst a group of pre-selected users. The responsibility is then borne by the users that can verify as they are named and known (Swanson, 2015).

Some examples of permissioned blockchains are the Ripple or Hyperledger (Swanson, 2015).

4.5.1.3. Comparison

One of the advantages of a permissioned blockchain is the scalability. Indeed, only a few numbers of users are selected to operate verification and can, therefore, handle a high number of transactions because they have received the computing power to do so as they were selected. On the contrary, in a permissionless blockchain system, the verifiers are not selected. Therefore, if the number of transaction increases, the computing power necessary to handle the verification will increase as well and then fewer users will have the capability to verify. This will lead to a certain centralisation (Swanson, 2015).

However, permissioned blockchain comes with a disadvantage as well: as the verifiers form a small group, it is easier for them to alter the rules or reject the transactions. There is no protection from censorship. On the contrary, the nature of permissionless system offers protection against censorship (Swanson, 2015).

4.5.2. Access

This classification criterion separates blockchains into two categories: public and private (Swanson, 2015).

With public blockchains, any user can read the transactions of the blockchain and submit one (Swanson, 2015).

Private blockchains are not accessible to everyone. The right to read and submit transactions is reserved for a specific group of users (Swanson, 2015).

5. Blockchain apparition in public knowledge

This first section serves as a preliminary analysis of where the blockchain stands in the technological life-cycle. It starts with an analysis of the blockchain coverage boom (in 2017). It continues with an analysis of the hype evolution a year after (in 2018), the evolution of the blockchain uses and a comparison with other technologies. Finally, a subsection is dedicated to a warning not to fall for the hype.

The objective is to understand broadly the stage of the technology, before going deeper into technical explanations.

5.1. Blockchain coverage boom

Nowadays, blockchain is a very trendy topic. The boom of the Bitcoin value (a cryptocurrency, one blockchain application) and its strong fluctuations caught the attention of the business world but what is the expert opinion about this trend?

According to Gartner, blockchain technology is indeed an emerging technology. In 2017, it was right in-between the "*Peak of Inflated Expectations*" and "*Trough of Disillusionment*". Therefore, it can be expected to be in the second category in 2018 (see Hype evolution for an update). This figure highlights the fact that blockchain will reach the "*Plateau of Profitability*" in 5 to 10 years so between 2022 and 2027. (Panetta, 2017)

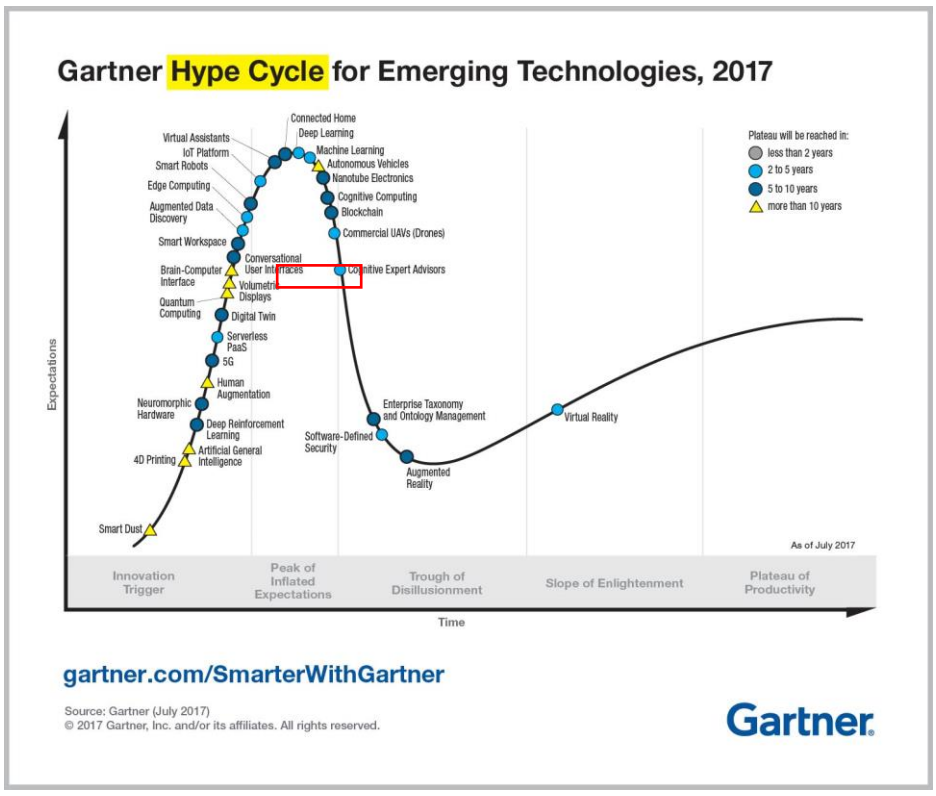


Figure 7: Gartner hype cycle for emerging technologies, 2017 (Panetta, 2017)

According to another article from Gartner, Blockchain is currently in a phase of experimentations. Every industry in the world is trying to implement blockchain in their process but mostly as experimentation. This phase of "*irrational exuberance*" has had two impacts: evolution and hucksterism (Pettey, 2018).

Evolution in the sense that, in the beginning, blockchain was very successful as a cryptocurrency but now, some are trying to make it evolve for other business purposes (it is going to be developed further in this paper) (Pettey, 2018).

On the other hand, it has also led to hucksterism. Indeed, some companies try to appear linked to the blockchain to benefit from the boom of the technology. For example, some companies changed their names to add the word blockchain to increase their stock prices. The SEC (Securities and Exchange Commission) said it would "*crack down on such companies*" (Price, 2018).

Today, companies should try different projects that involve the blockchain technology to be able to say if there is an added-value of using this technology in their case. This added-value can come from different part of the business, it can create more revenue, save costs or improve customer experience. However, Gartner's article is warning companies that obtaining the added-value may have to wait. Indeed, benefits should appear when the technology has evolved enough and becomes more reliable (Pettey, 2018).

Gartner experts believe that among them, companies should focus on the public permissioned kind of blockchain. This type of blockchain allows limited control over the rules and community inclusion. On the other hand, Gartner's articles advice businesses to think about public permissionless blockchains to let unknown users access the network (Pettey, 2018).

In the long-term, Gartner's articles all agree that blockchain will activate a huge transformation of industries (Pettey, 2018).

5.2. Hype evolution

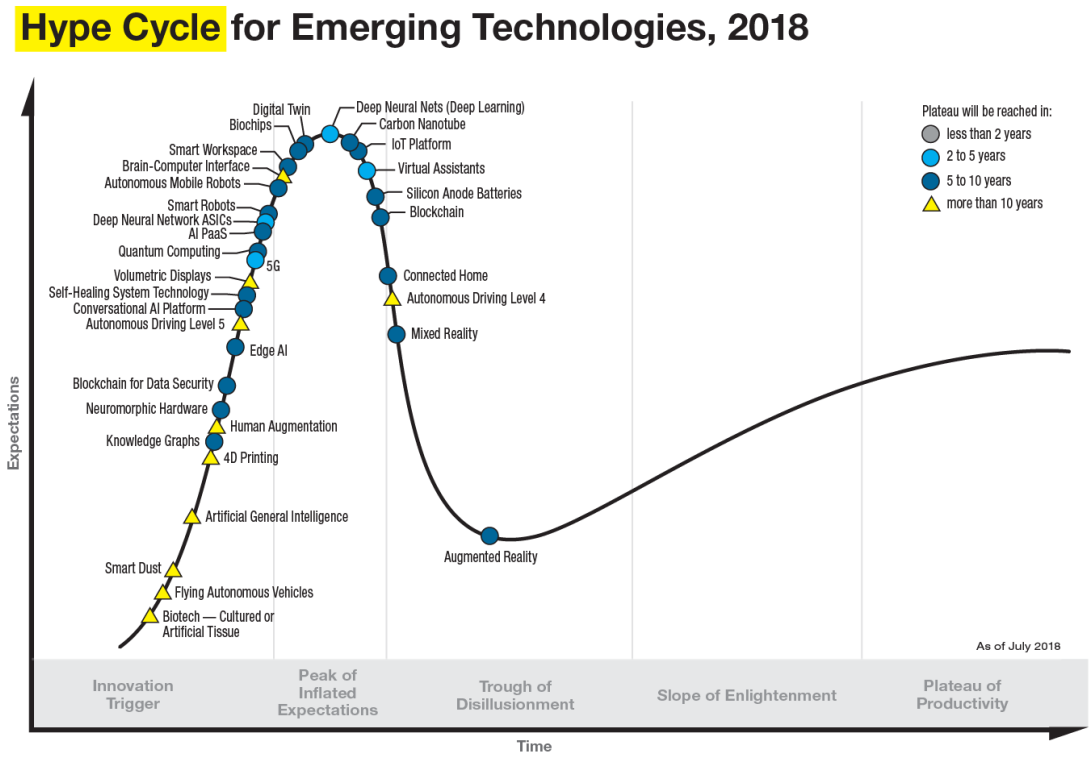


Figure 8: Gartner hype cycle for emerging technologies 2018 (Panetta, 2018)

The evolution of emerging technologies can be observed by analysing the differences between the Gartner hype cycles of 2017 and 2018. Indeed, both graphs are based on data that is computed by the same company, using the same assessment process. It makes the comparative analysis pertinent. There are a few elements that should be highlighted while comparing these charts (Panetta, 2018).

5.2.1. Blockchain technology evolution

First, as it can be seen from the two hype cycles figures, blockchain technology has not evolved along the Gartner hype cycle curve from July 2017 to July 2018. This interesting absence of evolution can be explained by the technology stage in the business life cycle. Indeed, as explained by Matt Higginson, Marie-Claude Nadeau, and Kausik Rajgopal (three McKinsey&Company partners) in January 2019, many prototypes of blockchain applications have been built and billions have been invested. Nevertheless, it did not lead to any major business revolution that could bring a real added-value and therefore that could be marketable and generate revenues. Once prototypes will truly perform, the blockchain technology will surf on increasing demand, characteristic of the growth phase (second stage of the technology life-cycle) (Higginson, Nadeau, & Rajgopal, 2019).

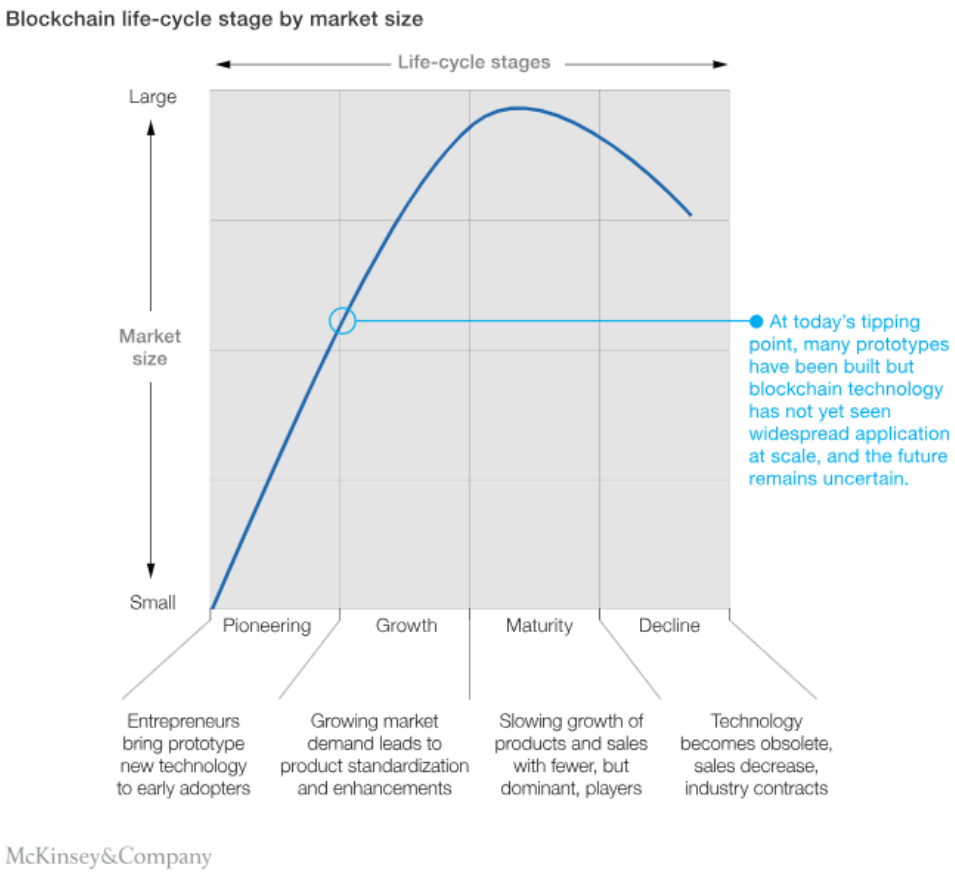


Figure 9: Blockchain life-cycle stage by market size (Higginson, Nadeau, & Rajgopal, 2019)

According to McKinsey&Company, one of the main reasons why the blockchain technology does not make it through the Pioneering-Growth border is the important presence of competition. Indeed, one of the first fields in which blockchain could reach the growth stage is the payment industry as it does not require a central entity managing the transactions. Nevertheless, at the same time, important amounts have been invested in disrupting fintech companies ($12 billion in US fintechs in 2018), creating an important competition for blockchain application developers (Higginson, Nadeau, & Rajgopal, 2019).

In addition to that, as it is the case with many disruptive innovations, companies must decide if they want to invest in the technology even if it means cannibalising their current sales and damaging their current business model. At this stage, as the blockchain technology has not yet delivered any concrete results for businesses, very few companies take the step towards this uncertain potential innovative business application (Higginson, Nadeau, & Rajgopal, 2019).

Finally, Occam's razor problem-solving theory states that the simplest theory tends to be the best. Therefore, the blockchain and its complexities might never be the final solution to many business problems as other simpler solutions exist (Higginson, Nadeau, & Rajgopal, 2019).

5.2.2. Blockchain for data security apparition

Another major difference between the Gartner hype cycle of 2017 and 2018 is the apparition of the "*Blockchain for data security*" technology in the innovation trigger part of the chart. It is expected to reach the final plateau in 5 to 10 years (starting from 2018).

During the 12-months period between the two Gartner reports, the European Union has officially launched the General Data Protection Regulation (GDPR) and allowed companies a short time to comply with the new data protection rules. As it affects every company doing business with European Union countries or dealing with EU citizens data, it created a huge demand for data protection solutions and blockchain appeared as an innovative solution for data protection.

Nevertheless, it is very important to make blockchain pass the GDPR requirements. Indeed, one of the main rules of the GDPR regulations is the right for each person to erase its personal data owned by a company when it is no longer pertinent. This "*right to be forgotten*" is a challenge as one of the key features of the blockchain technology is the immutability of the data contained in blocks. Fortunately, the GDPR regulations allow a "*pseudonymisation*". Therefore, the blockchain technology can be GDPR compliant if the chain does not contain personal information but a pseudonymised reference to the data. As a result, the personal information of each individual would be stored under a sequence of numbers, letters and symbols that could not be linked to the individual in question. This transformation of name into sequences would have to be done by an algorithm. As a consequence, a new challenge would appear; the protection of the pseudonymisation algorithm. Nevertheless, the protection of a single algorithm is way easier than protecting a huge volume of data about an important population (Panetta, Assess Blockchain for GDPR Compliance, 2018).

5.2.3. Evolution compared to other technologies

While looking at each emerging technology present in both graphs, some conclusions on their evolutions can be drawn. First, technologies that will reach the plateau of productivity in many years (more than 10 years represented by the yellow triangle being the highest timeframe) tend to have the lowest evolution and are nearly stagnant. For example, smart dust, artificial general intelligence and human augmentation did not evolve along the curve or moved a little bit forward. Second, more publicly-known emerging technologies tend to progress faster than less-known technologies. Indeed, the biggest advancements in the hype cycle were made by the 5G and the Internet of Things technologies which are both commonly known and even publicly awaited. Regarding the blockchain case, the technology benefited

from skyrocketing media coverage with the Bitcoin tremendous variation during the years 2017-2018. It led to a lot of public interest 3.7 million Google search result in two years (Carson, Romanelli, Walsh, & Ahumaev, 2018) but also private investments (according to McKinsey&Company, the financial sector invested no less than $1.7 billion annually (Higginson, Nadeau, & Rajgopal, 2019)). That is another reason why the technology has not yet come through the separation between the "*Peak of inflated expectations*" and the "*Trough of disillusionment*". Nevertheless, the massive media coverage has stopped and the Bitcoin value has dropped dramatically. Unless a major discovery is made, blockchain technology should reach the third phase of the Gartner hype cycle in 2019.

5.3. Falling for the hype

According to De Rossi (coordinator of the blockchain observatory of DEVO, the research lab of SDA Bocconi School of Management), the hype around the blockchain has been so intense that managers find nonexisting problems to justify the use of a blockchain project. Companies invest in blockchain projects that do not make economic sense. They create blockchains, but they often fail to have a critical mass of users and a strong community. These features are key to create the competitive advantage of the blockchain. Indeed, a blockchain's safety is directly proportional to the number of active users (as it decreases the potential chance of having a user that has control over more than 50% of blockchain users, the biggest vulnerability of the blockchain technology). Therefore, the more the information is widespread among many active users, the more the information is secured and the more valuable is the blockchain. In addition to that, most current companies developing blockchain projects (mostly in bank and insurance industry) are using permissioned blockchain (see Permissioned blockchains) which is a centralised and closed network. It only creates a redundancy issue as the information goes through many useless nodes (through central institution). It suffers from the disadvantages of the blockchain without getting the benefits of it. Therefore, at most 3 projects out of 2000 will see a successful profitable outcome (de Rossi, 2018).

Some listed companies are trying to surf on the blockchain wave in a different manner: they change their names and add the blockchain word in it. They do so to attract investors that are interested in investing in the trendy technology but that do not know actual companies developing blockchain applications. The SEC has warned the world that they will investigate these changes and that they expect more than an investor bait. The SEC chairman also warned investors against ICO ("Initial Coin Offering") as many of them do not follow US laws (Bain, 2018).

6. Uses of blockchain

This section has for objective to explain the potential uses of blockchain from a theoretical point of view. It will cover the different blockchain generations and what can be done with each of them. Finally, there is an emphasis on the technology front runner, a 4th generation blockchain: *Seele*.

6.1. Blockchain generations

Before going deeper into the different possible uses of blockchain technology, it is important to distinguish the different blockchain generations and what are their implications.

The blockchain technology has evolved tremendously from its origin in 1991 to these days. This development happened along with an evolution in the use of the blockchain, creating different generations. Each generation represents a specific new use of the blockchain. As of mid-2019, there are four blockchain generations, but more are to come as the research continues.

The first generation of blockchain focuses on cryptocurrencies, the initial objective of the technology. The second generation, built upon the first one, provides smart contracts. Then, the third one makes use of the previous generations to create applications for non-economic actors. Generation 4 refers to improvements compared to the third generation but no real definition of the fourth blockchain generation has been established yet (Singh, 2017).

Here is a good illustration of the different blockchain generations, representing well that each new generation is built upon the previous one:

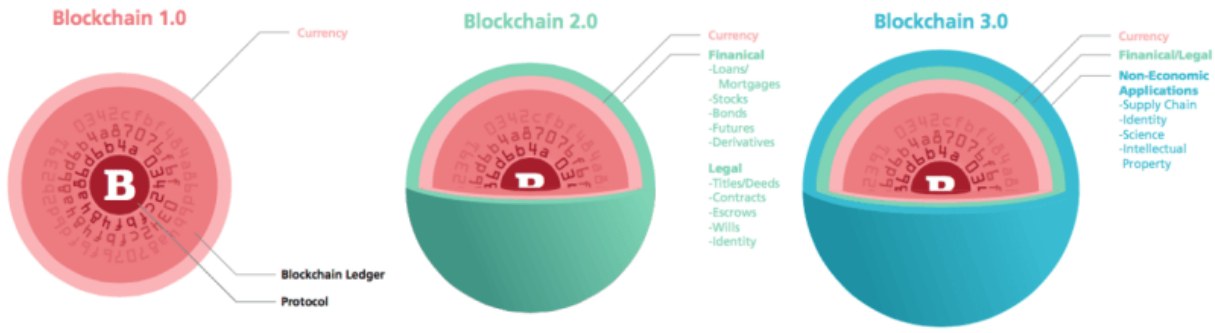


Figure 10: Blockchain generations (Singh, 2017)

6.1.1. Blockchain 1.0

Blockchain 1.0 corresponds to the first generation of blockchain strictly speaking as it appeared with the Bitcoin in 2009. The idea was to create a digital payment system using a decentralised digital currency. The objective was to avoid the costs of having a central

institution managing the currency and taking a percentage on transactions. Furthermore, Bitcoin allows to receive funds directly on a digital wallet and therefore reduces the classic transfer time.

The first generation finds itself useful for the financial industry mostly. Indeed, it ensures better efficiency and a less-costly way of doing financial transactions as it does not require a trustful third party. Payment, clearing and settlement activities are the first part of the industry that can be disrupted by the blockchain (Singh, 2017).

6.1.2. Blockchain 2.0

The second generation of blockchain started three years later, in 2012 and was focusing on assets and smart contracts. Indeed, the definition of blockchain 2.0 is broad. It includes every use that goes beyond a simple money ownership or transaction (Blockchain 1.0 scope) and is linked with the financial/economic or legal world. It covers among others: bonds, futures, loans, mortgages, smart properties or smart contracts. Whereas Blockchain 1.0 was decentralising money and payments, Blockchain 2.0 decentralises markets in a broader way. Any asset can receive value through the blockchain and therefore exchanges can be managed by smart contracts (Singh, 2017).

Smart contracts are contracts that are protected by the blockchain technology. It means that the contract is executed if and only if both parties respect their predetermined obligations. It can be used in a lot of legal or financial cases. For example, it could replace all notarial contracts that previously required the notary as a third-party trustful control that both parties respect their obligations. It could also validate the payment of the shipped product. Indeed, instead of having a bank that needs to secure the funds required to pay the transaction (and therefore having to pay for this third party), the blockchain could validate the payment when the shipment has been sent and received (Singh, 2017).

Another major change created by smart contracts technology is smart ownership. A good example of this shift is the digital diploma offered by schools and universities. Smart contract transforms the usual digital certificate every graduated student receives and that can be controlled by relying on a third party into something new.

Blockchain technology allows having immutable proof that can be public. Therefore, everyone can check if someone has a special certificate and it is totally secured and protected by the technology. It provides several advantages: no need for a third party to check the validity of a certificate, students do not have to give personal data to allow the control, no

intermediaries or central institution and students could also look for similar profiles for social inclusion purposes (Singh, 2017).

A concrete example of this smart contract already applied since 2017 is the MIT digital degree powered by the blockchain application Blockcerts.

6.1.3. Blockchain 3.0

This blockchain generation includes all applications that do not fit the scope of the two first generations. Therefore, it includes all non-economic applications of the blockchain. It ranges from government uses such as blockchain ID to civil usage like blockchain wedding by going through the protection of intellectual property thanks to timestamping.

One of the best-known blockchain 3.0 is Cardano, this blockchain and cryptocurrency solve four challenges of previous blockchains: Scalability, Interoperability, Sustainability and Governance. It features smart contracts in an innovative way and it follows a research-first approach for its development (Cardano).

Another promising third generation blockchain is Zilliqa which manages to process huge amount of transactions compared to previous blockchain generations. Indeed, Zilliqa can handle 100s and 1000s of transactions per second. In addition to that, this blockchain and cryptocurrency can deal with smart contracts deployment and execution at a very fast pace. Even more interestingly, the biggest the network is, the fastest the transactions are executed. This system is therefore ready to be applied at very large-scale equivalent to traditional transaction system such as MasterCard or Visa (Zilliqa, 2018).

These improvements are possible thanks to an innovative technology called *Sharding*. The network sharding concept claims to "*divide and conquer in parallel*". Indeed, it divides the network into different groups of nodes called *shards*. Then, each shard processes the transaction on its own and therefore, all shards can work in parallel. This faculty explains the linearly increasing pace of process correlated with the network size. Indeed, if the network is getting bigger, there will be more divisions and then more shards processing at the same time. Even if the idea seems simple, applying it is a real challenge Zilliqa managed to face. Indeed, three main issues appeared: Sybil resistance, shard creation and shard size. Zilliqa faced these problems with three solutions, respectively: keeping sybils in check, automated shard creation and choosing the right shard size by taking in consideration the probability of having a third of malicious nodes (Zilliqa, 2018).

There are many other third generation blockchains and many others to come. Here are few examples of existing ones: EOS, ArcBlock or Aion.

6.1.4. Blockchain 4.0

The fourth generation of blockchain technology is still oncoming. Therefore, there is not any widely accepted definition of what characteristics this new generation will encompass. Nevertheless, some companies already consider themselves as part of the fourth generation thanks to their innovations that go beyond the scope of the third generation. This section will analyse the most advanced and promising one: *Seele*.

6.1.4.1. Seele

According to Seele's definition of the blockchain's fourth generation, main highlights of the fourth blockchain generation are the heterogeneous forest network, the neural consensus algorithm, the on-chain and off-chain sharing and the value internet concept. Each of these features answers to an unsolved pain point of the previous generation or is an improvement of the already existing solutions. The following subsections will explore each of them: heterogeneous forest network, neural consensus algorithm, value transport protocol and finally quick value internet connection (Seele, 2018).

Heterogeneous forest network

A first innovation brought by Seele is its heterogeneous forest network system.

The first generations of blockchain work with a single chain which makes transaction and consensus easy to achieve. Nevertheless, it comes with different weaknesses as well. Firstly, the scalability compared to the demand for blockchain services is too weak. Secondly, it could create a congestion issue as many businesses can be on the same chain (if one of the business is requiring too many transactions per second, it creates congestion and slowdown in transaction performance). Finally, working as a closed network structure does not allow companies to make a connection with other chains which is a barrier to connectivity between different platforms (Seele, 2018).

These issues can be overcome by using multi-chains structures. There are different kinds of multi-chains structure with different pain points. A first option is a parallel chain structure, but it comes with the problem that each chain is preconfigured to face a certain need and is therefore not adapted to changing environments. A second alternative is to have the main chain with different "*side chain*". Indeed, it allows modification of the environment as side chains derive from business changes. On the other hand, side chain consensus is linked to the

main chain, so the consensus process can finally be concentrated on the main chain which leads to the typical issues of having a single chain system (Seele, 2018).

The heterogeneous forest network structure of Seele is the company's way of solving these issues. This concept acts as a classification system for the subnetworks (also called subnets) of the blockchain. The heterogeneous forest network organises the subnets in a hierarchical manner. As it can be understood by the name of this concept, the structure looks like a combination of trees.

The trunk is called the meta-chain and represents a global service. Each division depicts a business decision or a company characteristic.

Therefore, each branch is the representation of a certain scenario and a layer is the collection of these different scenarios. Small layers can benefit from the services provided by the upper levels. Each layer can be accessed, governed and controlled by a predetermined public that can differ from layer to layer. To cut a long story short, the heterogeneous forest network works as a tree where each separation is a segmentation of the possibilities and where each subnet can benefit from the service of the subnet to which it belongs with a final central subnet called the meta-chain (Seele, 2018).

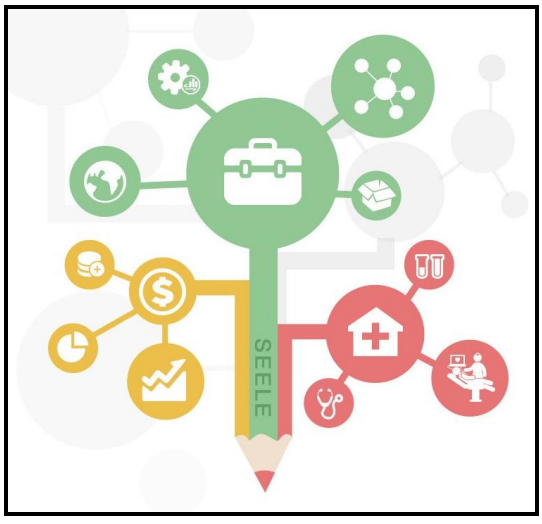


Figure 11: Seele's heterogeneous forest network

For example, the meta-chain could be all business services. The first segmentation (branches) could be marketing, finance, legal, human resources… Considering the marketing branch, it can be further divided into marketing per country: Belgium, France and Luxemburg. The next layer can be a division per product and so on. The final branch corresponds to a very specific possibility such as marketing for a specific product in Belgium in 2019.

This concept allows Seele to improve solutions provided by the three first generations of blockchain. Indeed, thanks to the segmentation system, it increases the security isolation and it avoids the issue of having one business using too many resources and therefore slowing down the transactions of another business. It improves the allocation of blockchain resources. In addition to that, the unification points within the tree give the opportunity for value exchange between subnets. Ultimately, the heterogeneous forest network offers high scalability to a large ecosystem of businesses (Seele, 2018).

In conclusion, the businesses with similar needs and features are part of the same group of subnets and benefit from the adapted resources, permission and level of security (Seele, 2018).

Neural consensus algorithm

A second innovation brought by Seele is the neural consensus algorithm.

To understand the neural consensus algorithm used by Seele, it is key to have a good understanding of the neural network system as well as of the practical Byzantine fault tolerance algorithm (Seele, 2018).

Neural network

The system behind neural networks can easily be understood through an analysis of its structure. As can be seen in the figure below, the neural network receives data (X_1 to X_5) that enters the input layer. After that, the data goes through the nodes (which can be compared to neurons). Each input is weighted based on its importance and is sent to the next layer. Finally, the neural network reduces the possibilities layer after layer and the output layer produces an output Y. The neural network is a predictive model that takes into consideration multiple inputs, weights them and produces a prediction based on the importance of each input (Saerens, 2018)

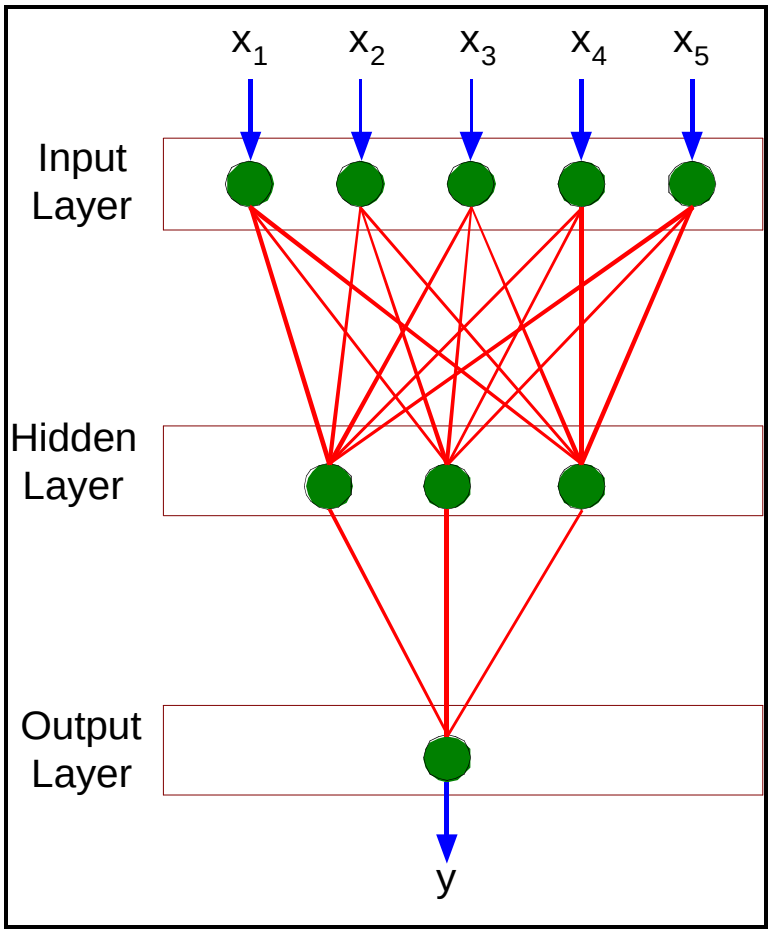


Figure 12: Structure of neural networks (Saerens, 2018)

Practical Byzantine fault tolerance algorithm

This algorithm was created as a solution to a specific byzantine difficult situation. Before going into technical details of the solution, here is a description of this hard position:

> *"Imagine that several divisions of the Byzantine army are camped outside an enemy city, each division commanded by its own general. The generals can communicate with one another only by messenger. After observing the enemy, they must decide upon a common plan of action. However, some of the generals may be traitors, trying to prevent the loyal generals from reaching agreement. The generals must decide on when to attack the city, but they need a strong majority of their army to attack at the same time. The generals must have an algorithm to guarantee that (a) all loyal generals decide upon the same plan of action, and (b) a small number of traitors can't cause the loyal generals to adopt a bad plan. The loyal generals will all do what the algorithm says they should, but the traitors may do anything they wish. The algorithm must guarantee condition (a) regardless of what the traitors do. The loyal generals*

should not only reach agreement but should agree upon a reasonable plan." (Lamport, Shostak, & Pease, 1982)

This allegory is really close to the blockchain consensus verification system. Each general is the representation of a node, messengers are connections between nodes, the objectives of the nodes is to determine the validity of the information that is proposed to the blockchain. The solution requires having at least two-thirds of the generals who are loyal. Therefore, if more than a third of the nodes are not acting correctly, no consensus can be reached.

To face this troublesome requirement, Seele has developed a *"ε-differential agreement"* (called EDA).

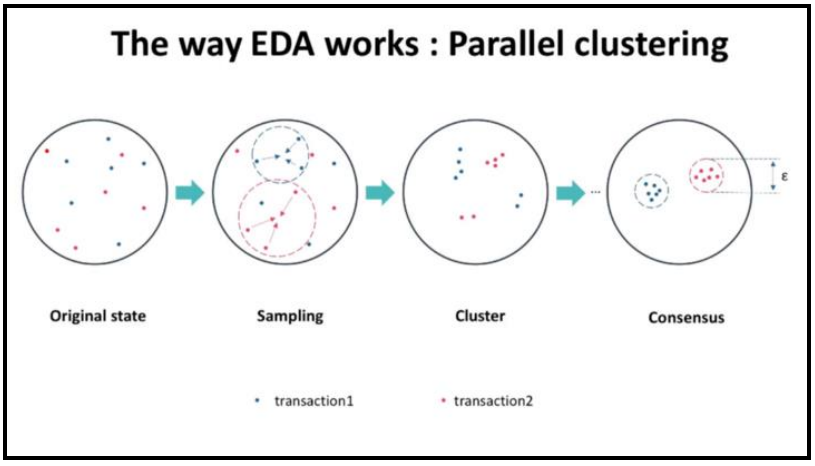


Figure 13: Seele's EDA system (Seele Tech, 2018)

As can be seen in the figure above, the EDA system is assembling closest nodes in the system (sampling phase to create clusters). The objective is to reunify nodes associated with the same transaction in order to, ultimately, reach a consensus faster.

This EDA shifts the agreement from a consensus issue to a request proceeding that is asynchronous. It increases the robustness and allows to have more than a third of the nodes that are bad actors. It is possible thanks to the fact that nodes can check inputs and use various sampling rates (Seele, 2018).

As a conclusion, the neural consensus algorithm developed by Seele offers various advantages. First, as aforementioned, the neural network system allows giving weight to the voting system on the blocks. Indeed, unlike previous blockchain generations with traditional 0 – 1 voting scheme, Seele's algorithm has a continuous voting process. Second, parameters can be adjusted to achieve an optimal efficiency level. Third, EDA does not require to select a head node nor to apply proof-of-work or proof-of-concept, therefore saving a lot of energy.

Fourth, Seede's algorithm is adaptable to different forms of blockchains and to *"Directed Acyclic Graph"* (DAG) which are structures that follow a certain direction (directed) and that are not cyclic (acyclic) (Seele, 2018).

Value transport protocol

Seele's third main innovation is called *value transport protocol*.

Previous blockchain generations faced issues that Seele's value transport protocol solves: interoperation ability and unfriendly naming convention. Indeed, each blockchain was created as a single entity that could not interact with others. In addition to that, as aforementioned, first blockchain generations use a serial number to identify data or transaction. This kind of combination (e.g. 2j7jd9fjd8jq9dkjGU8I9ikUmNunJ28hJk8) is not "*human-friendly*" as it is hard to read (Seele, 2018).

The value transport protocol invented by Seele is inspired by already existing protocol combined with the heterogeneous forest network (see Heterogeneous forest network for more details). Indeed, protocols are already used to get access to and share information. For example, the *Internet Protocol* (IP) is offering this naming service for the Internet. In addition to that, the *Uniform Resource Identifier* (URI) gives the opportunity for human users to connect with any kind of resource (Seele, 2018).

Seele has developed a specific naming mechanism called the *Uniform Asset Identifier* (UAI) that looks like this one (Seele, 2018):

CHAIN:\\edu.lsm.IB.thesis

In this example, "CHAIN:\\" is the default protocol header and it represents the meta-chain (= the "trunk") of the heterogeneous forest network. On the other hand, "edu", "lsm", "IB" and "thesis" are identification keys that allow the blockchain to go in the right direction at each segmentation layer. By making these choices, the blockchain can go down the hierarchy and find the relevant data required by the user. This solution allows the user to understand what he reads, and it gives the opportunity to make different branches exchange information which offers interconnectivity.

If a new subset of data is added, the information goes through the whole branch until it reaches the meta-chain that can validate the registration request. This process can be seen as one of the limits of this new concept; efficiency issue. Nevertheless, Seele has proposed four strategies to increase the value transport protocol efficiency (Seele, 2018):

1. A replacement strategy based on the frequency of access.
2. A replacement strategy based on the last access at a similar time.
3. A strategy based on both frequency of access and last access at a similar time;
4. A strategy based on a random replacement.

Finally, it is important to note that Seele developed a Value-HTTP (VHTTP) for Value Internet with the objective to optimise cross-chain access. The real added value of the VHTTP is that users of the Internet (HTTP users) can access the data of the VHTTP chain if they have permission to do so (Seele, 2018).

Quick value internet connection

The fourth major innovation Seele developed is the concept of *quick value internet connection*.

Blockchains have nodes all around the globe. This complex network creates network jitter (data package delay) and latency. Part of Seele's vision of the fourth generation of blockchain is an improvement of this situation. Instead of using the traditional internet protocols TCP and UDP, Seele developed the so-called *Quick Value Internet Connection* (Seele, 2018).

Before going deeper into this new concept, it is important to understand TCP and UDP protocols (Seele, 2018).

On the one hand, TCP stands for Transmission Control Protocol and is a simple protocol that ensures that the computer which sends the data create a direct connection with the computer receiver and maintains the connection for the whole duration of the data transfer. Once the transfer is done, the connection is interrupted until the next transfer. This protocol allows an efficient and reliable transfer of data. Nevertheless, the load is high as the connection need to be monitored at all time in case data must be transferred. An allegory can be made with a phone call; a direct connection is established for the duration of the data transfer (Seele, 2018).

On the other hand, User Datagram Protocol (UDP) is a protocol that requires the sender computer to send a package within the network which takes the responsibility to transfer the data package to the right computer receiver. It does not create a direct connection between the sender and the receiver and therefore reduces the workload compared to the TCP process. However, the network might fail in his role to transfer the data. It can be compared to a postal system; a sender gives a package to the network and in most cases, it is delivered to the receiver, but it might fail (Seele, 2018).

Seele is still blurry concerning the explanation of the QVIC. Indeed, if Seele's team manages to develop this technology, it would be a real game-changer for the data transmission world, so the company remains unclear with an explanation. Nevertheless, QVIC's objectives are to reduce package loss, network jitter and instability of the connection. It would combine the advantages of the UDP and TCP with a better network connection (like UDP) (Seele, 2018).

Seele did the first experimentation of this new concept and the results show great improvement in the data transmission. The company used nodes in three cities in China and in London to make the experimentation. The transfer of 1G of data was made with a rate of 1Mbps compared to 100Kbps for the TCP protocol and the QVIC reduced the confirmation time by 70%. As represented in the figure below, the transmission rate was 500% higher with the Quick Value Internet Protocol than with the Transmission Control Protocol (Seele, 2018).

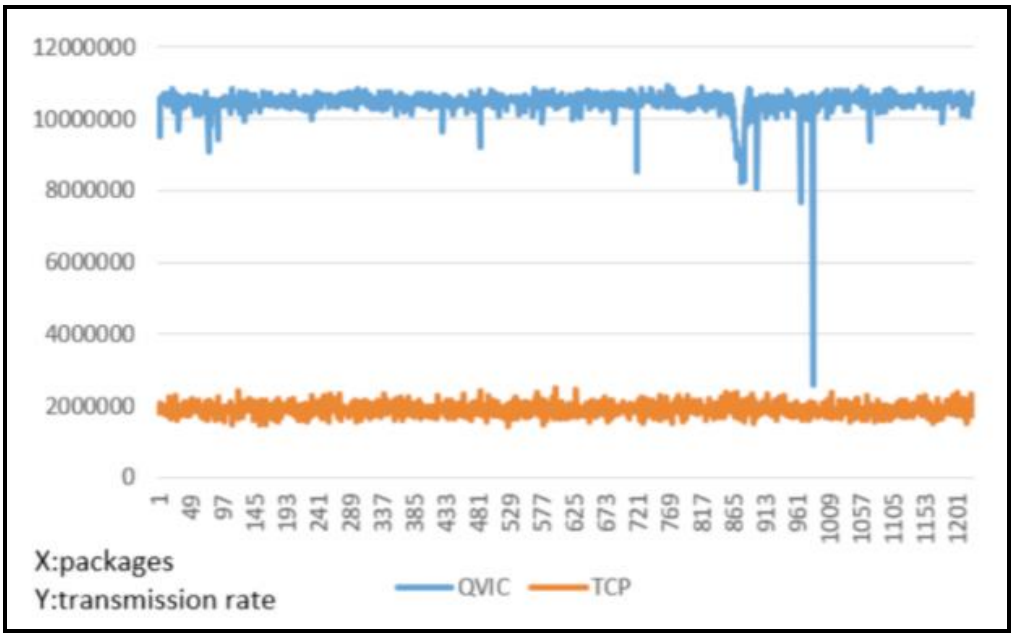


Figure 14: Transmission rate QVIC vs TCP (Seele, 2018)

7. Knowledge management

This section aims at defining the basis of knowledge management theory. It will later serve to explain the potential blockchain use in knowledge transfer in education. The section starts with an explanation of knowledge and processes. It continues with a quick overview of the main knowledge management cycles and models.

7.1. Knowledge

There are a lot of different and various definitions of knowledge. Nevertheless, it is often considered that knowledge is a "*justified personal belief*".

Knowledge management is all actions related to this knowledge. It is defined by King: "*Knowledge management is the planning, organizing, motivating, and controlling of people, processes and systems in the organisation to ensure that its knowledge-related assets are improved and effectively employed*." (King, 2007)

It is key to make a clear distinction between tacit and explicit knowledge (or knowledge-related assets). Tacit knowledge is part of people's mind and is "*either impossible, or difficult, to articulate*". Knowledge is typically tacit in nature as it is hard to put words on the knowledge. This knowledge is underutilised by organisations as "*the organisation does not know what it knows*" (O'Dell & Grayson, 1998). On the other hand, explicit knowledge is well-defined in an explicit form such as words, documents or data. Therefore, the real challenge of knowledge management is the tacit knowledge (O'Dell & Grayson, 1998).

There is another important segmentation of knowledge that separates the know what, how and why (O'Dell & Grayson, 1998).

The "*know what*" is the lowest level of knowledge. It encompasses being able to take a decision when there is a specific course of actions. For example, a pharmacist who gives specific drugs in response to a clear diagnostic (O'Dell & Grayson, 1998).

After the "*know what*" level, there is the "*know how*" stage. It includes a higher level of complexity in the treatment of the stimuli and understanding to provide the right course of action. The situation is unclear because of the noise around the relevant information. To get back to the pharmacist example, if the patient is feeling different symptoms and is not able to describe efficiently what he is enduring, the pharmacist will need the know-how knowledge to find the right solutions in presence of this significant noise (O'Dell & Grayson, 1998).

The highest stage of knowledge is the "*know why*" level. At this stage, the individual can take the right decision even in highly complex and noisy situations. It involves a good understanding of the causal relations, the interactive effect and previous exposure to experiences with situations that require "*know what*" knowledge. The "*know why*" knowledge can answer tough situations that deviate considerably from classic knowledge application and norms (O'Dell & Grayson, 1998).

As can be seen in the next figure, the evolution from noise (data stage), to know what (information stage), to know how (knowledge stage) and finally to know why (wisdom stage) involves a growing understanding of the data and an increasing range of context in which it can be used.

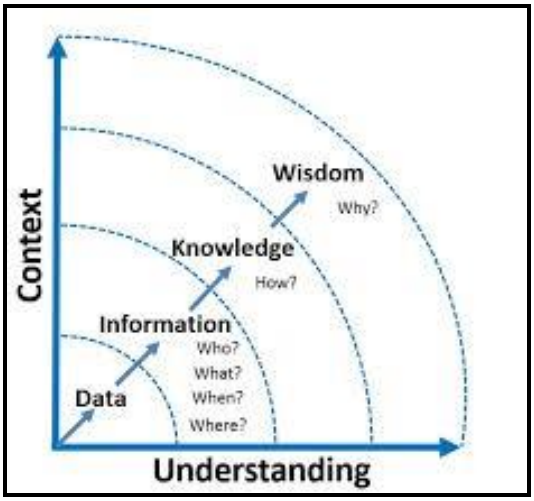


Figure 15: Evolution of knowledge (Boxley Group)

7.2. Processes and objectives

The knowledge management process includes many steps:

Figure 16: Knowledge management process based on (King, 2007)

As can be seen in the figure above, organisations acquire information by facing different situations. Then, knowledge is created based on the takeaways of the first step. After that, the knowledge is refined which means it is crossed with other similar experiences to extract the relevant reusable knowledge. Once the knowledge is refined, it needs to be stored for future usage. From this point, it is important not to let the knowledge unutilised in the database. It should be transferred and shared to pertinent new users. Finally, when the knowledge reaches the relevant users, it can be utilised (King, 2007).

Knowledge management goals are to utilise and leverage the knowledge-based assets to re-utilise best practices, improve behaviours, take better decisions and increase the performance. The summary of the knowledge management processes and their impacts on the rest of the organisational structure and results are depicted in the figure below (King, 2007).

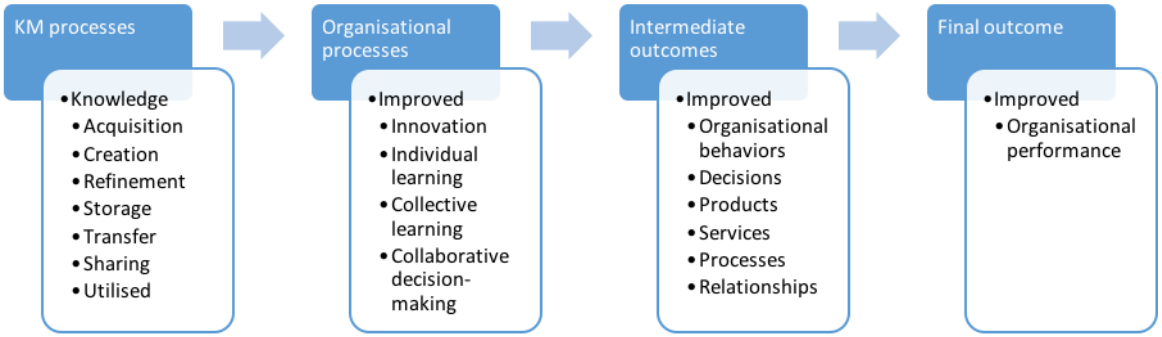


Figure 17: Knowledge management in organisations (King, 2007)

As can be seen, knowledge management processes influence directly organisational processes. As these processes improve many aspects of the business life, it improves intermediate outcomes for the organisation which ultimately increase the organisational performance.

7.3. Type of knowledge transferred in universities

As aforementioned (see Knowledge for more details), there are two kind of knowledge -tacit and explicit- and three levels of knowledge: know what, know how and know why.

Universities transfer a lot of explicit knowledge to their students through books, syllabi, courses, exercises… The amount of facts and figures transmitted from professors to students by any mean is considerable. On the other hand, there is less emphasis on the transfer of tacit knowledge (especially during the bachelor). Indeed, it is only through some experience sharing from certain professors or by doing a specific exercise (typically business presentations) that tacit knowledge is created in students' minds.

In addition to that, universities are doing their bests to make students "*know why*" actions happen. This level of knowledge concurs with a deep understanding of the concepts and the reasons behind each concepts. The student is able to apply them in many different and new situations. It really depends on the student's involvement to reach this level of comprehension and assimilation of the knowledge. Unfortunately, many students stop digging further into a course when they reach the "*know how*" level of knowledge. This "*know how*" includes an

understanding of the concepts and some situations where they apply. Outside of these previously seen situations, the student struggles to apply the concepts and is disturbed by new elements. Finally, the "*know what*" level is typically associated with a global understanding of the course and is usually not enough to validate a course. The student knows the main concepts but struggles to apply them in real-case situations.

7.4. Knowledge management cycles & application to university knowledge transfer

The objective of this section is to provide three main elements. First, a global explanation of major knowledge management cycles. Second, how they are applied in university and especially in the Université Catholique de Louvain. Third, how blockchain can improve these processes and to which extent. The blockchain use analysis will only be made on the Dalkir's integrated knowledge management model applied to UCL in order to avoid redundancies.

There is a multitude of knowledge management cycles that have been developed in the scientific literature. This section will only focus on four major ones that are already implemented in some organisations (so feedback and improvements were already made) and about which extensive literature exists.

7.4.1. The Meyer & Zack Knowledge Management Cycle

Meyer and Zack analysed the different steps of the development of a knowledge repository and summarised the information into a knowledge management cycle. The different stages of this refinery process are the following ones: acquisitions, refinement, storage & retrieval, distribution, and presentation (also called use) (Meyer & Zack, 1996).

1. Acquisition of information focuses on the quality of the raw data that gets into the process. Indeed, Meyer and Zack insist on the high quality of data that should enter the refinery in order to provide high-quality information at the end of the cycle
2. Refinement is the clean-up stage of the cycle, where most of the true added value is created. Meyer and Zack distinguish two kinds of added value: physical (typically a change of recipient) or logical (restructuring or indexing for example). The value creation comes from the transformation of raw data into "*readily usable knowledge objects*" and from the increased organisation of data storage which increases usability in the future.
3. Storage (or retrieval) is the phase creating the link between the refined information and the distribution to the end users. The storage can be physical or digital.

4. The distribution includes the delivery of the information to the end user as well as key information about the delivery (such as time, frequency and language).
5. Presentation or use is the final stage of the knowledge management cycle and where its success can be measured. Context is key in this phase as the user needs the right context to leverage the information he received. If he can't make use of the information, the knowledge management failed to deliver value.

The next figure summarises the Meyer and Zack knowledge management cycle. It comes with an example of information going through all steps (Meyer & Zack, 1996).

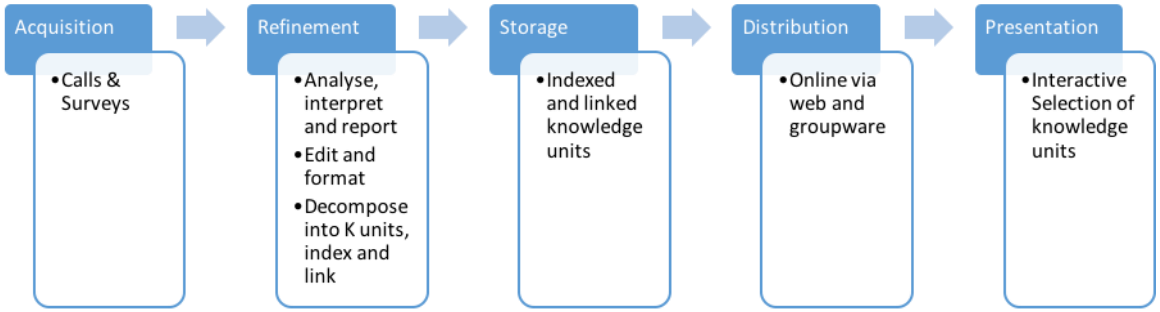


Figure 18: Meyer and Zack knowledge management cycle (Meyer & Zack, 1996)

Dalkir highlights two other elements that are not explicitly described by Meyer and Zack: feedback and continuous renewal. Indeed, Dalkir adds to the cycle an arrow for the presentation phase to the acquisition phase, emphasising on the importance of feedback. In addition to that, Dalkir focuses on the continuous renewal of information and refinement process to avoid obsolescence (Dalkir, 2005).

7.4.2. Application of Meyer & Zack cycle in the UCL case

Meyer & Zack describes five main steps in their knowledge management cycle. The university professors are handling the three first steps of the process. The first is the acquisition of a large amount of information. As UCL professors hold a PhD or are high-level professionals with a lot of business experience, they have acquired a lot of information. The second phase is a refinement to filter only the most relevant knowledge. This step happens when the professors gather the information they believe is the most relevant for the student's future. To do so, they determine some objectives for a course and then see what knowledge will be required to reach these targets. The final step handled by professors only is storage. This third step is often done through a physical tool such as books or syllabi. The objective is to prepare for the next step: distribution. In the university case, it is the moment where the

knowledge transfer happens from the teacher to the students. It can be done through courses, videos, books, syllabi, articles, etc. or a combination of these methods. The fifth and last step in the Meyer & Zach cycle is the use of the knowledge by the final user, here the students. This stage corresponds to a final exam and future uses after that.

7.4.3. The Bukowitz & Williams knowledge management cycle

According to Bukowitz and Williams, a knowledge management process framework should show how the organisation can create, keep up and utilise a certain amount of knowledge strategically chosen to create value. Through this knowledge management cycle, Bukowitz and Williams bring to the table two major changes: the addition of the learning phase and the decision to maintain or let information go (Bukowitz & Williams, 2000).

The next figure shows the Bukowitz and Williams knowledge management cycle (Bukowitz & Williams, 2000).

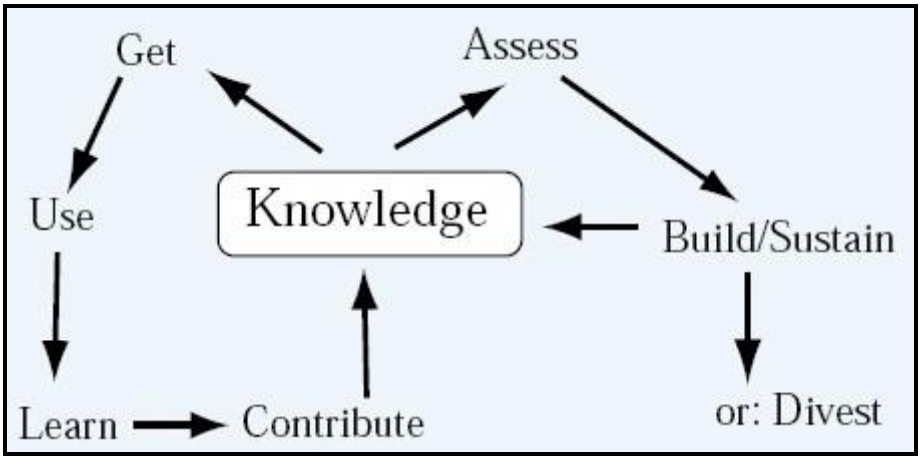


Figure 19: Bukowitz and Williams knowledge management cycle (Dalkir, 2005)

The Bukowitz and Williams knowledge management cycle in an organisation includes many stages (Bukowitz & Williams, 2000):

1. The first step, *get*, refers to seeking out the information that can be used by the end user to take the right course of action. Nowadays, the challenge is not anymore on how and where to find the information but more on how to find the relevant information in the gigantic amount of available data. It is also very important to note that the knowledge management system must offer the possibility for the end user to get in contact with the source of information. Indeed, it allows the invaluable tacit knowledge sharing.

2. The second step of the cycle is *use*. It encompasses the combination of information in order to promote innovation within the organisation. Bukowitz and Williams emphasise their model on the use of information to foster innovation for individuals and groups, even if the cycle covers a wider range of uses.
3. The third stage, *learning*, refers to value creation for the organisation by leveraging learnings. These learnings can come from past successes in the form of best practices or from failures in the form of key takeaways and lessons learned. The learning phase is crucial to deliver true value to the end user. Without the leveraging of learnings, the knowledge management cycle is only about warehousing content and not using it.
4. The final step in the individual loop of the Bukowitz and Williams cycle is the *contribute* step, it focuses on the user providing information to the cycle as well. Indeed, after having leveraged the content offered by others, the users have developed new content they shall share through the knowledge management system.
5. In the second loop of the knowledge management cycle, the emphasis is put on the organisation role in the process. The *assessment* is referring to the analysis of the available information. The first objective is to compare the available data with strategic future knowledge demands. The second one is to assess thanks to defined metrics the value created by the knowledge management process. Indeed, ensuring alignment of information with future needs and measuring the success of the system are keys.
6. The second phase of the organisational loop, *build and sustain*, is aimed at ensuring the viability and competitive advantage of the organisation in the long run. Indeed, a tactical failure of leveraging the right information at the right moment leads to a lost opportunity. But a strategic failure in identifying the relevant information to have and develop can lead to a loss of competitiveness and ultimately to organisational non-viability.
7. Finally, the *divest* step of the knowledge management cycle refers to a recurrent cost-benefit analysis of the information. Indeed, the organisation should always consider letting go of intellectual assets that are no longer creating value. Dalkir explained different ways of divesting these assets: patenting information, spinning off companies, terminating training or employees,…

On the one hand, the get, use, learn and contribute phases are tactical as they respond to market demand or opportunities. Indeed, the knowledge that goes through the process depends on the current market needs. On the other hand, the assess, build/sustain or divest stages are strategic as they are defined in advance, taking into consideration the macroenvironmental context. The strategic objective is to match the intellectual information available to the upcoming short-term demands (Bukowitz & Williams, 2000).

7.4.4. Application of the Bukowitz & Williams cycle in the UCL case

The Bukowitz and Williams knowledge management cycle is composed of two internal loops: an individual and an organisational one.

The individual cycle corresponds to the path of a student in his knowledge acquisition process. The first step is *get*: the student receives an important load of data from university courses. Then, he *uses* (step two) the most relevant part of this knowledge through exercises and he *learns* (step three) from his use of the information. Finally, he *contributes* (step four) to the knowledge through discussions, cross-courses link and knowledge sharing.

The organisational loop corresponds to the teacher journey. It starts with an *assessment* of the available information where the professors screen and filter information in order to keep only the most relevant for the course. It continues with a step where the teachers *build and sustain* a library of the most relevant information that will give the students an advantage on the market and that would best prepare them for their next career steps. Finally, teachers can *divest* as well. This last step relates to a cost-benefit analysis of the knowledge transferred to students and a re-focus on what creates the most value if it is necessary. It is usually done through feedback from students and from self-assessment from the professors. There is a responsibility for students to give feedback to professors so that they can know what was most interesting but the students do not have the long-term uses in mind yet. The professors, on the other hand, should have a more long-term business perspective and re-assess the content of their courses every year based on business changes.

7.4.5. McElroy knowledge management cycle

The McElroy knowledge management cycle is a process focusing on the link between knowledge production and integration. It also takes into consideration multiple feedback loops (McElroy, 1999).

McElroy defines two types of knowledge. The first is the subjective knowledge and it is stored in individual minds. The second is the objective knowledge, it can be stored in an explicit form (McElroy, 1999).

The McElroy knowledge management cycle is based on the principle of *Beliefs and Claims*. Knowledge use either leads to a success or a failure for the end user. If there is a match between the user's expectations and the information he gets, it will reinforce the existing knowledge which ultimately leads to a willingness to use it again. On the other hand, a single mismatch between expectations and reality lead to a readjustment (single-loop learning). If there are too many failures in a row, the users will doubt and finally reject the knowledge. This will result in new knowledge production and integration, it is double-loop learning (Argyris & Schon, 1978).

The global cycle is illustrated in the next figure.

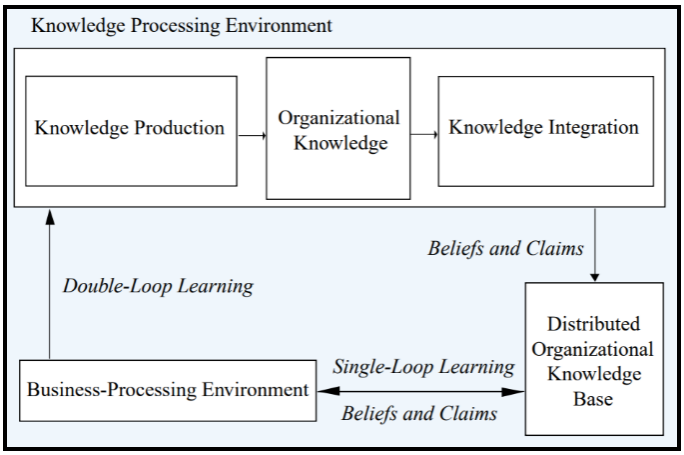


Figure 20: McElroy knowledge management cycle (Dalkir, 2005)

It starts with a problem claim formulation which is a first description of the knowledge gap. Then, there is a knowledge claim formulation that is made to validate the problem that occurred. After that, the knowledge claim must go through a knowledge claim evaluation process. There are two possible outcomes for the knowledge claim. Either it is validated and become new organisational knowledge (the second important phase of the knowledge management process), or it is set as a falsified (or undecided) knowledge claim. Then, organisational knowledge becomes distributed. It is the third step of the knowledge processing environment: Knowledge integration. This stage triggers new *beliefs and claims* which make the whole loop begin again (McElroy, 1999).

7.4.6. Application of the McElroy cycle in the UCL case

According to McElroy, knowledge production depends on the success or failure using some pieces of information that are beliefs or claims at the beginning of the process. The McElroy cycle is a loop composed of five steps.

In the UCL case, the three first steps are covered by university professors. Indeed, they formulate knowledge claims, they evaluate them, and they keep the validated claims as viable information. After that, professors enter the fourth step: knowledge integration. This phase encompasses the transmission of knowledge from the professors to the students; it is the knowledge distribution. It can be done through courses, syllabus, presentations, books or any other medium. The professor's objective is to make the students reach the course's learning targets thanks to the information transferred. Finally, based on that, some students might bring some beliefs and claims that ultimately close the loop and make the process start again (with a knowledge claim formulation). This last step is key in the university knowledge process. Indeed, most dedicated students can come up with innovative ideas that can change the current knowledge base. Then, they are invited to pursue an analysis of their claims thanks to further studies that could lead them to become a professor in the future. By doing so, they close the loop.

7.4.7. Wiig knowledge management cycle

According to Wiig, there are three main conditions for a business to succeed. It should have a product or service and customers, resources and an ability to act. The knowledge management cycle can have a great impact on this ability to act (Wiig, 1993).

Wiig's knowledge management cycle is made of four steps: building, holding, pooling and applying knowledge. They are not all perfectly independent and sequential as overlaps are possible (Wiig, Knowledge management foundations, 1993).

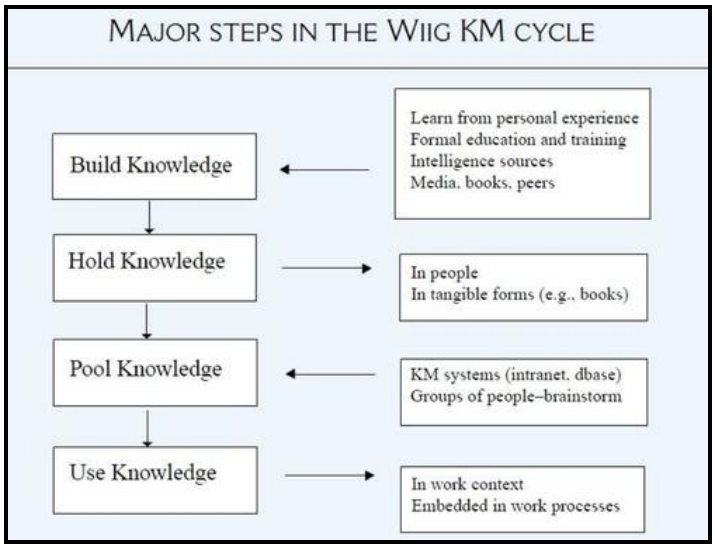


Figure 21: Wiig knowledge management cycle (Dalkir, 2005)

The first step, build knowledge, is separated into five main activities (Wiig, Knowledge management foundations, 1993):

1. Obtain knowledge
2. Analyse knowledge
3. Reconstruct or synthesise knowledge
4. Codify and model knowledge
5. Organise knowledge

The objective of this first phase (build knowledge) is to get organised knowledge out of raw data from different sources (Wiig, Knowledge management foundations, 1993).

The second step is to hold knowledge. It can be segmented in subparts (Wiig, 1993):

- *Remembering knowledge*, meaning that the individual has kept the knowledge in mind.
- *Accumulating knowledge* in a repository is targeting here the idea of storing the information in organisational memory.
- *Embedding knowledge* is the part that makes sure knowledge is part of businesses frameworks.
- *Archiving knowledge* meaning that a "*scientific library*" is created. Furthermore, archiving knowledge also encompasses the fact that irrelevant or falsified knowledge is taken out of the library.

The third step is to pool knowledge. This part can be seen as a process (Wiig, 1993):

1. It starts with the *coordination of knowledge*, an exchange between sources of knowledge to understand who knows what.
2. Then, the sources of information are *assembled* to create a library with references.
3. Finally, the information is available for the end user and the retrieval is made easy for him. The information can be access to a source of information (such as an expert in the field) or direct information (such as market analysis) from the library. This last step is called *access and retrieval.*

7.4.8. Application of the Wiig cycle in the UCL case

Wiig knowledge management cycle includes four major steps: building, holding, pooling and using knowledge.

University professors build knowledge thanks to their personal experience, formal education and pieces of training, scientific readings, books, peers, etc. Once the knowledge is built, they can hold it in two main ways: internally by having the knowledge in mind and externally by transmitting it in tangible forms (typically a book or syllabus). Then, university professors pool knowledge. This third step is subdivided into three parts. First, they coordinate the knowledge with their peers. Second, they assemble a library of knowledge that will be transmitted to the students. It should include references to the knowledge sources. Third, teachers transmit the knowledge and provide to the students access to the information so that they know how to retrieve the relevant information. After this knowledge pooling phase, the fourth step in the Wiig knowledge management cycle is the use of knowledge. It involves students using the acquired knowledge at a final exam and after that in future jobs or situations.

7.4.9. Comparison of knowledge management cycles

According to Kimiz Dalkir, there are three major steps in the knowledge management cycle that can be found in each of the aforementioned cycles: knowledge capture and/or creation, knowledge sharing and dissemination, knowledge acquisition and application. Between the first phase of knowledge capture and creation and the second phase of knowledge sharing and dissemination, an assessment of the knowledge content is done. After this phase, the knowledge content is contextualised to ensure it can be understood and used efficiently (third stage). Finally, the knowledge content can be updated through feedback and therefore links the third phase with the first one. Here is a visual representation of this integrated knowledge management cycle according to Dalkir (Dalkir, 2005):

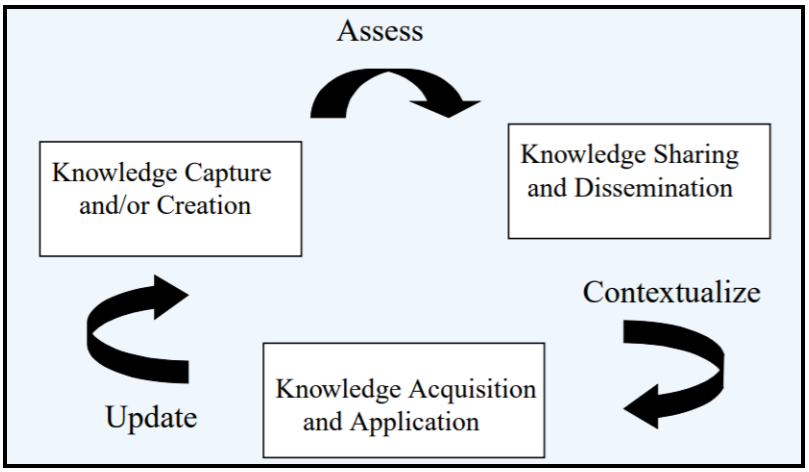


Figure 22: Dalkir's integrated knowledge management cycle (Dalkir, 2005)

7.4.10. Application of Dalkir integrated cycle in the UCL case

As aforementioned, Dalkir built up an integrated knowledge management cycle based on the fourth previously explained cycles. Her cycle is composed of three main steps that form a loop.

University professors start the journey with their knowledge capture and/or creation (step one). This step is done through their own studies and/or business experience as UCL teachers have a PhD or an extensive business experience. Once they have acquired sufficient knowledge, they assess it, decide what is worth sharing to the students and they disseminate the knowledge to them through a course (step two). According to Dalkir, students need to contextualize the knowledge received in order to acquire it and to be able to apply it in other scenarios (step three). The contextualization is done thanks to exercise and practical sessions where the students can use the knowledge in different situations. The objective is to understand all the links and actions related to the concept, to reach a "know why" understanding of the knowledge. Once the students have acquired the knowledge, they will use it and will be confronted with changes. Therefore, they will have to update the knowledge which closes the loop towards knowledge capture and/or creation.

7.4.11. Blockchain applications in UCL's Dalkir integrated cycle

This section aims at analyzing potential leads for blockchain use in the Dalkir's integrated knowledge management cycle applied to UCL. The objective is not to do a full analysis of these leads but only to identify them. There are three main potential leads identified in this section.

During the first step of the knowledge management process, blockchain could be used in the verification and validation of scientific articles. Indeed, for now, experts and professors

around the world form communities of practice and need to share the articles with people they know have the specific expertise. The process could be more efficient with the use of blockchain. A blockchain-based application could be used to provide an asynchronous worldwide-available verification tool of scientific articles. Experts around the world could search and review articles. This application could be based on a permissionless blockchain, allowing people with expertise but not part of specific communities of practice to have a word in the process. If the project is launched by UCL professors, it would offer important coverage for UCL.

During the contextualization phase done by the students, a blockchain-based tool could be used for the correction of the exercises by peers. Indeed, UCL professors often provide many exercises to their students. Then, students are doing some of them randomly (the amount depending on the student's involvement and comprehension) in order to get a full understanding of the concept in a different context. Unfortunately, quite often the solutions are not made available. Therefore, a blockchain-based application could be created for students. If a UCL student thinks he did an exercise right, he can upload it on the blockchain with some proves (link to the course or articles for example). If the other student of the course –the peers- validate the exercise, it is going to be available for all students to see. If not, the author student did a mistake seen by the peers and should redo the exercise. This tool would ultimately offer solutions to all exercises provided in a course. It could even push students to come up with extra exercises and solutions.

A third potential lead is in the update step at the end of the loop. When UCL students discover they need to update the knowledge, they should have a platform to propose changes but also to provide feedback if they believe knowledge should be added. For now, there is a feedback tool available to UCL students and they can always share their thoughts with the professor directly. Nevertheless, a blockchain-based application could provide a platform where students can share their feedback or propose new initiatives. These feedbacks need to be approved by the other UCL students to be uploaded on the blockchain. Therefore, there is a screening of the feedback done by the UCL students themselves. As a result, only the most relevant, interesting and globally approved feedbacks will be received by the professors.

7.5. Knowledge management models & application to university knowledge transfer

The knowledge management cycles described the activities in knowledge management. This section aims at providing a framework –a knowledge management model- for these activities.

Indeed, the knowledge management activities should be organized and coordinated in order to get all the added-value. To do so, this section will cover the most important and famous knowledge management models.

7.5.1. The von Krogh and Roos model of organisational epistemology

The knowledge management model of von Krogh and Roos is one of the first to make a distinction between individual and social knowledge. This model is adopting a connectionist approach. This perspective is considering that the brain is processing external information as a whole (and not linearly each information) but also creating its own data. As individuals in an organisation can share information, the knowledge is not only held in each individual but also on the connections between them (organisational knowledge) (Von Krogh & Roos, 1995).

According to von Krogh and Roos, knowledge is embodied in people. Therefore, there is no knowledge without a knower. Connections are key in preserving and sharing knowledge. This thinking is emphasised on a refined version of the model by von Krogh, Ichijo and Nonaka (Von Krogh, Ichijo, & Nonaka, 2000). Indeed, it highlights a model of enabling rather than knowledge management. Knowledge enabling is all the activities organized and actions taken in order to increase knowledge creation within the organisation (Von Krogh, Ichijo, & Nonaka, 2000).

7.5.2. Application of the von Krogh and Roos model in the UCL case

Von Krogh and Roos make a distinction between individual and organisational and knowledge only exists if there is a knower. Therefore, organisational knowledge is based on the connections between individuals and their personal knowledge. Based on this connectivity theory, university professors are knowers who transmit what they know to the students. It is the student responsibility to embody a maximum volume of information before the end of the connection. On the other hand, it is the responsibility of the professors to create a connection favourable to knowledge transfer and to create connections with other knowers (e.g.: other professors, book or article authors).

7.5.3. The Nonaka and Takeuchi knowledge spiral model

Another knowledge management model implemented in many organisation is the Nonaka and Takeuchi knowledge spiral.

After having studied the success of Japanese companies in their innovation and creativity processes, they found out that two ingredients were needed to produce innovation: "*the tacit/explicit spectrum of knowledge forms and the individual/group/organisational model of knowledge sharing and diffusion*" (Nonaka & Takeuchi, 1995).

According to Nonaka and Takeuchi, the knowledge conversion is not as linear. Indeed, as can be seen in the next chart, there are four main ways of knowledge conversion (Nonaka & Takeuchi, 1995):

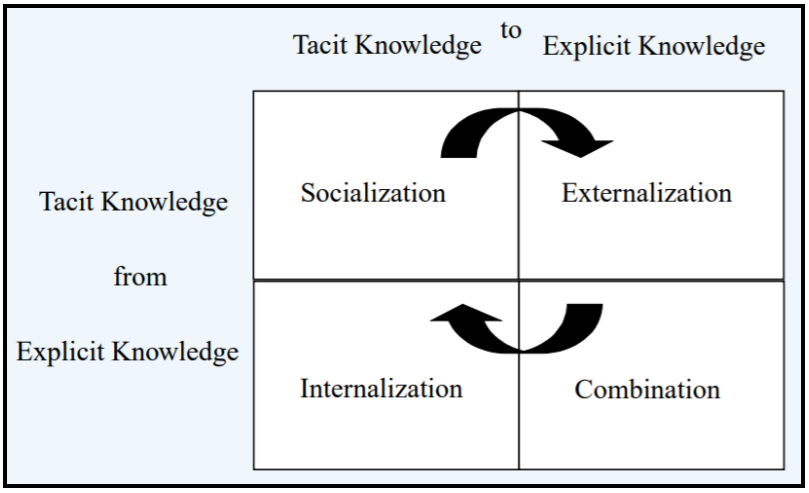


Figure 23: Nonaka and Takeuchi model of knowledge conversion (Dalkir, 2005)

Socialisation (tacit to tacit knowledge) refers to knowledge transfer through human discussions.

Externalisation (tacit to explicit knowledge) is the process through which an individual articulates his tacit knowledge in an explicit form (e.g.: writing down a model or draw a know-how process).

Combination (explicit to explicit knowledge), as its name implies, refers to a combination of explicit knowledge to form a summarised or more complete explicit knowledge. No knowledge content is created per se.

Internalisation (explicit to tacit knowledge) is referring to an embodiment of explicit knowledge. It is often compared to learning-by-doing.

The knowledge creation process begins with an individual having an idea and it continues with this person sharing the knowledge across the organisation. It is not a linear process. It is rather seen as a continuous knowledge spiral by Nonaka and Takeuchi. In order to ensure a good knowledge creation process, they determined five "*enabling conditions for organisational knowledge creation*" (Nonaka & Takeuchi, 1995):

1. Intention: willingness to reach the goals
2. Autonomy: individuals must be able to act autonomously to a minimum extent

3. Fluctuation and creative chaos: minimum interaction between the organisation and the external world and/or creative chaos
4. Redundancy: diversity of people working on an assignment (rotation of people or internal competition between teams for example)
5. Requisite variety: internal diversity to face complex issues

7.5.4. Application of the Nonaka and Takeuchi model in the UCL case

According to Nonaka and Takeuchi, there are four ways of transferring knowledge.

Firstly, socialisation is a transmission of tacit knowledge from a person to another one. The knowledge remains tacit. It is typically the case when professors transmit knowledge during physical courses, allowing students to understand and assimilate information.

Secondly, during courses, students are also doing an externalisation of the information given. Indeed, by taking notes, students are transforming the tacit knowledge received through oral explanations into explicit knowledge available on physical support.

Thirdly, the explicit knowledge can be transferred and remains explicit through combination. Both professors and students are combining explicit knowledge. On the one hand, professors are gathering a lot of information to condensate and create a course with a specific amount of explicit knowledge. On the other hand, students are taking knowledge from different explicit sources (notes, books, syllabus, articles mostly) to synthesise the relevant information.

Lastly, knowledge can be transformed from an explicit form into a tacit one. It typically happens when students embody, understand fully and study the knowledge offered on explicit supports at university.

Globally, university courses are juggling with the transformation of knowledge in all four aforementioned directions. Knowledge constantly changes support but should ultimately be tacitly mastered by the students. Once they have proved this knowledge acquisition through exams, they receive a degree that certifies it.

7.5.5. The Choo Sense-making knowledge management model

A third important knowledge management model is Choo's sense-making model. It brings a new point of view on knowledge management.

Choo's knowledge management model is based on three key elements: sense making (firstly introduced by Weick), decision making and knowledge creation. Each of these is influenced by an external action (Choo, 1998). Choo's model is summarised in the following figure:

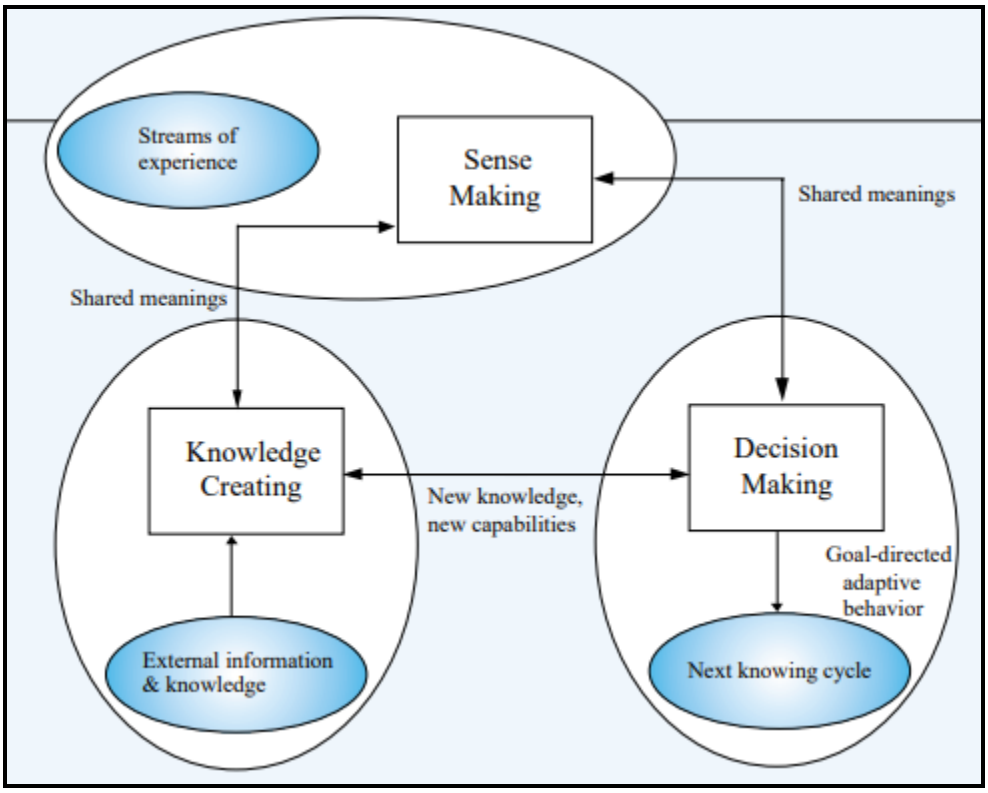


Figure 24: Choo's knowledge management model (Dalkir, 2005)

The sense-making phase as seen by Weick and used by Choo is the transformation of external information chaos into ordered processes thanks to interpretation shared by different individuals. Weick defines four integrated processes (Weick, 2001):

1. *Ecological change*: An ecological change is a change in the external environment of the organisation. This change triggers a shift in the information received by the individuals and therefore affects the internal processes of the organisation.
2. *Enactment*: This phase consists of a reorganisation of the organisation information. By creating its own rules and constraints, the organisation creates a systematic library of information.
3. *Selection*: This step involves a selection of the most relevant changes and therefore information for the organisation.
4. *Retention*: This final phase is the creation of a library of "*successful sense-making experiences*".

The knowledge creating phase is a phase where the individuals make a link between the current situations and the potential future courses of actions (thanks to dialogue and personal exchanges). People create new innovative solutions that feed the decision-making phase (Choo, 1998).

Then, the decision-making phase considers all options and take a decision based on the information received from the knowledge creating and the sense-making cycles. Finally, the organisation takes a final decision based on its chosen decision-making model (Choo, 1998).

7.5.6. Application of Choo's model in the UCL case

Choo's knowledge management model is based on three key elements: sense making, decision making and knowledge creation.

The sense-making part is done mostly by professors. Indeed, professors are subject to chaos of available information, they have to process it in order to convey a structured library of information. On the other hand, students receive a structured load of information. They have to understand and sometimes restructure the knowledge, but their starting base is not chaotic.

Decision-making is a capability professors teach students. Indeed, professors need to master the knowledge they teach and how to use it to take the most relevant and performant business decisions. After that, it is their roles to transfer both the knowledge and the tools to use it in order to encourage the students to do the decision-making process by themselves. Ultimately, students should be able to take the right decision based on the knowledge they have acquired. It is the main capacity tested during examinations.

Finally, the decision-making process, as well as the consequences (positive or negative), are an important source of knowledge for the decision-maker; here, the students. Indeed, based on their experiences taking a certain course of actions, students learn and create their own tacit background; knowledge for future situations.

7.5.7. The Wiig knowledge management model

A fourth and last model is described and analysed in this subsection: the Wiig knowledge management model.

Wiig' model relies on the principle that information is only valuable when it is structured. He makes a direct correlation link between structured information and the value of this knowledge. A common example of this model is based on the way the human being stores and organises knowledge. Human beings are organising their knowledge based on their uses and create a semantic network of information. In a semantic network, each branch can be explored further until the most relevant information is retrieved (Wiig, 1993). The next figure shows an example of a semantic network around the *university*. Once the user has seen the first layer (blue colour), he can decide in which branch the relevant information is located and go deeper

into the network (in this case, exploring the *courses* branch and reach the second layer in orange).

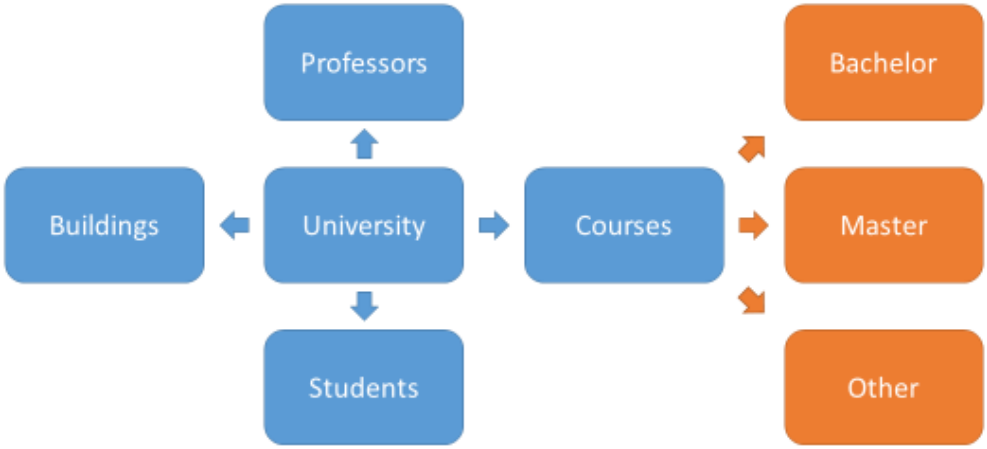


Figure 25: Example of a semantic network

According to Wiig, there are four elements that should be reunified to have a good systemic network (Wiig, 1993):

1. *Completeness*. This feature refers to the completeness of the information available; making sure there is no branch missing in the network. It is also key to make sure the user knows and is aware of the availability of the knowledge.
2. *Connectedness*. This characteristic refers to the links between knowledge objects. In a systemic network, each business object can be connected to many others as it is very rare to have independent objects. Therefore, a high volume of connections is proof of high network value.
3. *Congruency*. This feature refers to consistency. There should not be any misunderstanding, internal conflict or logical inconsistency within the network. It is really hard to have a perfect congruency, but the network should have a minimum level of consistency.
4. *Perspective and purpose*. This characteristic refers to specific knowledge associated with a limited event or for a very specific purpose. It should not be wrongfully generalised as it does not reflect an absolute truth.

Wiig's model is a refinement of Nonaka and Takeuchi's fourth quadrant – internalisation (see The Nonaka and Takeuchi knowledge spiral model for more details). Wiig developed a scale measuring the growing understanding and mastery of the knowledge from *Novice* to *Master*.

The scale is available in Appendix 1: Wiig knowledge management model: degrees of internalization (Wiig, 1993).

7.5.8. Application of the Wiig model in the UCL case

Wiig sees the knowledge transfer as an embodiment of external knowledge, a transformation from explicit into tacit knowledge. In his model, once the knowledge becomes tacit, it is structured as a semantic network.

In the case of professors-student knowledge transfer, examinations are meant to verify a good understanding of a certain group of subjects and therefore verify if the students have been able to develop a good semantic network of information in their minds. Indeed, the four factors of a good semantic network are key factors in the student assessment:

1. *Completeness*. The professor needs to make sure the student has a complete understanding of the course and that no parts are missing.
2. *Connectedness*. The more a student can make connections between knowledge objects, the more it shows he has a full understanding of the subject.
3. *Congruency*. The student should be consistent in his reasoning and should not show any internal conflict or present any misunderstanding.
4. *Perspective and purpose*. The student should not extrapolate or use certain information for the wrong purpose.

8. Blockchain use: Case of UCL

The previous parts focused on blockchain technology explanation (see Blockchain technology for more details) and a comparative analysis of knowledge management cycles and models between theories and university practices. The objective of this section is to determine where in these processes blockchain could be of help. Therefore, this part will develop different possibilities of blockchain implementation at the UCL. For each lead, a cost-benefit analysis will be done to determine the most promising and interesting one. The selected blockchain application will then be further developed in the next section.

8.1. Proposing new initiatives & offering feedback

8.1.1. Blockchain implementation

Indorse is a company that started to use the blockchain technology to create verified e-portfolio. The system will allow anyone to propose any claim and give a link that proves the claim afterwards, the other users can verify the claim in the same way verifiers check blocks of transactions. Thanks to this system, a verified e-portfolio is created (Torverkar & Moskowtiz, 2017).

Here is an example to illustrate this system:

Lucas enters the network and receives a minimum score that allows him to publish one claim (with a link to prove it). Lucas claims that he is graduated from the Louvain School of Management and give a link of the LSM website to prove it. Its score is now blocked, and random other users are chosen by the system to check whether the claim is correct or not. The claim enters now the so-called "*gestation period*" where it will be verified. This period ends when a given number of verifiers will have done their job.

Another user, Charles, receives a notification that he can verify Lucas' claim.

When a consensus is reached among the verifiers, Lucas' claim is validated and published. Lucas is rewarded by an increase of his score by one, meaning he can claim something else. Furthermore, he receives a reward for publishing something verified. The verifiers (including Charles) who were part of the consensus also receive a reward as they performed the job.

If a consensus can't be reached, Lucas will lose one point and will not be able to claim anything as he was at the minimal score. He will not receive any reward neither. On the other hand, the verifiers will.

In the case of *Indorse*, the reward is given in points that can be exchanged against the money earned by the website thanks to advertisements while the users were active (Torverkar & Moskowtiz, 2017).

There are multiple usages that can be done in this way of leveraging the blockchain technology. Following paragraphs will explore two important ones: feedback and initiative proposal tool and an e-verified stored portfolio (Grech & Camilleri, 2017).

Firstly, a system similar to *Indorse* based on an internal UCL blockchain could be used to ensure a way for students to give feedback to teachers, the faculty or the university. It can also offer a platform where students can propose freely new initiatives. Only the relevant and pertinent claims will be supported by other people in the network and will be published. This consensus-based filter serves as an assessment of the quality of the claims and ensures a non-abusive usage of the tool. Nevertheless, another layer of control would be desirable to avoid any abuse or finger pointing approved by a majority.

This system could be anonymous, offering a free space for students to speak and highlight important matters. It would give the opportunity for the professors and staff of the university to realise global feelings about its courses, organisation and management for example.

If the university decides to implement a system that is not anonymous, it could offer incentives for positive participation (either constructive feedback or good initiatives) such as discounts on sports cards or reduction on scientific books.

Secondly, a system like this one could be leveraged as a tool for students to publish their papers as well. Indeed, as explained in the example here above, a certain student can propose the publication of his work and pending on the verification by other students, it would be published. It could be used for courses where peer review assessment is performed. Every student would need consensus approval on his work to be published. Therefore, the author would have an incentive to do good work immediately as he could lose points by being blocked by the network. On the other hand, students would have to review the document should be impartial as well. Indeed, if a "judge" goes against the consensus, he will lose some points as well. If clear rules and instructions are determined in advance for the evaluation of the paper, this system could be particularly efficient.

This option can also be extended to student's work dedicated to other students. It can include synthesis, notes combination or any kind of data gathered for more efficient use. This option would offer a specific use of blockchain technology in any knowledge management cycle.

Considering Dalkir's model (Dalkir, 2005), a student would take on the responsibility of gathering data (potentially from different sources: syllabi, books, other syntheses, articles and oral courses). This first step is knowledge capture. Then, the student who decides to create a synthesis would need to filter the information and keep only the most relevant information. After that, he would enter the knowledge sharing and dissemination step where he shares the information with other students. Usually, this step is made without any checks and wrong information might circulate around the audience. A blockchain implementation at this step would ensure a higher quality of work shared. A 100% certification that the content summarises perfectly the information is impossible to reach but a filtering process where other students can interfere and approve or refuse the work would definitely improve the quality of published syntheses. In addition to that, thanks to the incentive system, students will think twice before publishing work which will increase quality from the very first step in the dissemination process.

Taking this thinking further, the incentive program could be sponsored by professors (e.g.: offering a bonus point for the top 3 students with most points), it would incentivise students to produce qualitative reports about the course and review thoroughly other reports. Some private parties (partner of the UCL or a specific program) could even take responsibility in this process. Indeed, a specific supply chain company could incentivise a really relevant course of the supply chain master in order to reach upcoming talents relevant to the firm's activities. It would be a new innovative way to make connections between future graduates and the private sector.

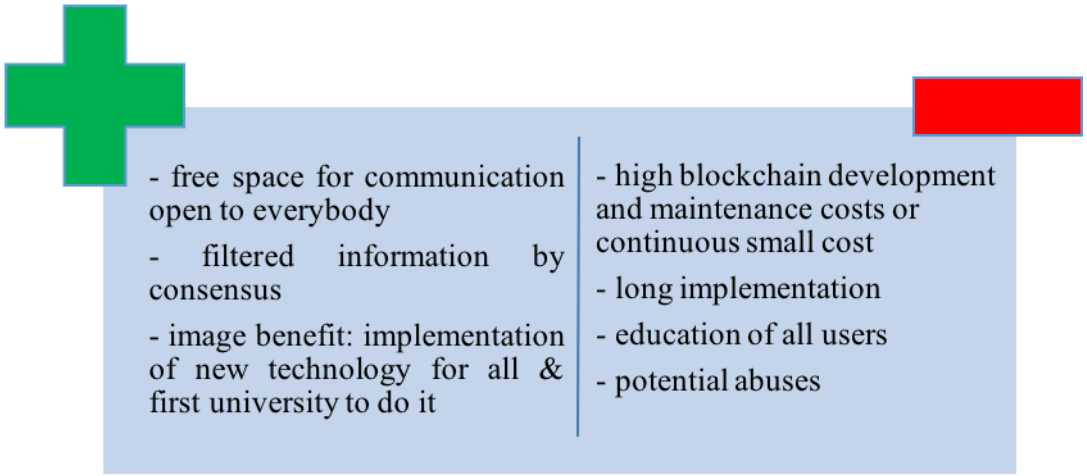
This blockchain use can also be related to the knowledge management models explored in this paper. Indeed, students that transfer the tacit knowledge received in a course and transform it into an explicit form is doing an *externalisation* according to Nonaka and Takeuchi (Nonaka & Takeuchi, 1995). With the same model in mind, any student who gathers multiple explicit sources of knowledge in order to create a synthesised result is doing a *combination*.

8.1.2. Feasibility

The first option, using this tool for feedback and initiatives, is the most feasible as the blockchain would be opened to any member of the university (students, professors and staff)

whereas, for the second option, access should always be limited to a certain number of selected people (that would change over time). Nevertheless, it would require an implementation of the tool, a test-phase with chosen educated users, global implementation and education for all users.

8.1.3. Cost-benefit analysis



On the cost side of the implementation of this tool, there are three options:

1. Rely on the Indorse application and depend on their evolving costs of usage and/or constraints like an advertisement (quantitative information is not publicly available).

2. Develop an internal blockchain for the UCL. Costs are very variable, they depend on the complexity of the application (here, pretty low), the location of developers (onshore, near shore or offshore) and the time of the demand (supply of talents being limited and demand to be really high as of mid-2019). Nevertheless, it can be estimated between 15 000 USD and 50 000 USD. After that, maintenance costs would include two or three developers at a cost of around 70-100 USD/hour/developer. It is important to note that these numbers are estimations and can vary over time.

3. Use the Ethereum blockchain and develop an autonomous agent for the UCL. The cost of using the Ethereum technology depends on the Ethereum cryptocurrency value and the request treatment time allowed. In this case, requests do not need immediate treatment (would cost 3 USD per publication if we consider the

Ethereum value at 300 USD) as twenty minutes treatment on average is totally ok for the university purpose. This would only cost 0.07 USD per proposal and less than 0.01USD per approval or refusal of users. Therefore, considering the proposal is sent to 100 users, 51 refusals or approvals are necessary to continue the process. It would cost less than 1 USD per full transaction. It is important to note that these numbers are estimations and can vary over time (Ryan, 2017).

8.1.4. Conclusion

Knowing that feedback and initiative proposal tools already exist and are implemented at the UCL, the benefits of implementing this blockchain application do not outweigh the important costs. Nevertheless, it is very important to mention that this conclusion would change if UCL were to adopt its own blockchain with a specialised development team. Indeed, in this hypothetical case, it would considerably reduce the costs (or share it with other purposes) without affecting the benefits.

8.2. Securing degrees & verifying their authenticities

8.2.1. Current situation

As of 2019, the degrees delivered by the UCL are given on physical support: paper. If the graduate wants to prove that he has effectively received his degree, he can show the certificate. If he needs to show further proof, as a simple piece of paper can easily be tampered with, he has to invite the verifier to call the university to check the information. This process can be long and fastidious for all the parties. Indeed, the graduate has to share some information with the verifier so that the verifier can prove to the UCL administrator his demand is legitimate. The graduate should also find the relevant UCL administrator that can confirm a degree has been delivered. The verifier needs to gather some information about the graduate, to call at certain hours the UCL administrator until reaching the person and then wait for a confirmation (or repeal). Finally, the UCL has to allocate this degree verification responsibility to one of its employees and to make sure he has access to the relevant information at any time.

Furthermore, a fake graduate with evil intentions could easily find ways to fake a verification process.

To cut a long story short, the process is really long, inefficient and not fully secure.

8.2.2. Blockchain implementation: Blockcerts

Fortunately, thanks to the advantages of the second generation of blockchain in non-financial applications, it is now possible to secure permanently degrees in a decentralised fashion. This system allows control by all parties the veracity of a degree very efficiently and without having a central institution managing the process. The current state of the technology makes it a possibility that has already been explored by MIT for its degree issuance. Indeed, MIT started to provide blockchain-based digital degrees to its new graduates. To do so, a company with open-source technology was created: *Blockcerts* (Grech & Camilleri, 2017).

The MIT Media Lab and Learning Machine have developed Blockcerts. According to Blockcerts itself, "*Blockcerts is an open standard for creating, issuing, viewing, and verifying blockchain-based certificates*" (Blockcerts, 2016).

The main objective is to give the opportunity to everybody to prove the possession and ownership of blockchain certificates while ensuring the protection of data and private information by preventing from using the third party and from tampering (Blockcerts, 2016).

As of mid-2019, Blockcerts is the only open standard that issues and verifies blockchain records. Its goal is to become the main world standard. To do so, it is open source. Indeed, by doing so, Blockcerts wants to avoid a standards war and a vendor lock-in which could be two major barriers on the way to reach a global standardisation and acceptation of Blockcerts (Blockcerts, 2016).

The only way that people own their personal data is by combining two conditions that Blockcerts meet (Grech & Camilleri, 2017):

1. Recipient ownership. It means that the owners of digital records have the key to prove their ownership. For example, a student can prove he has a UCL degree because he has the key to do so. He owns the key and can, therefore, decide to whom he wants to show proof.
2. Vendor independence. It means that the whole process should never rely on a single vendor. That is why Blockcerts is open-source so that the digital records can be migrated, shared and verified by any independent vendor.

The next figure, found on Blockcerts website, explains the whole process:

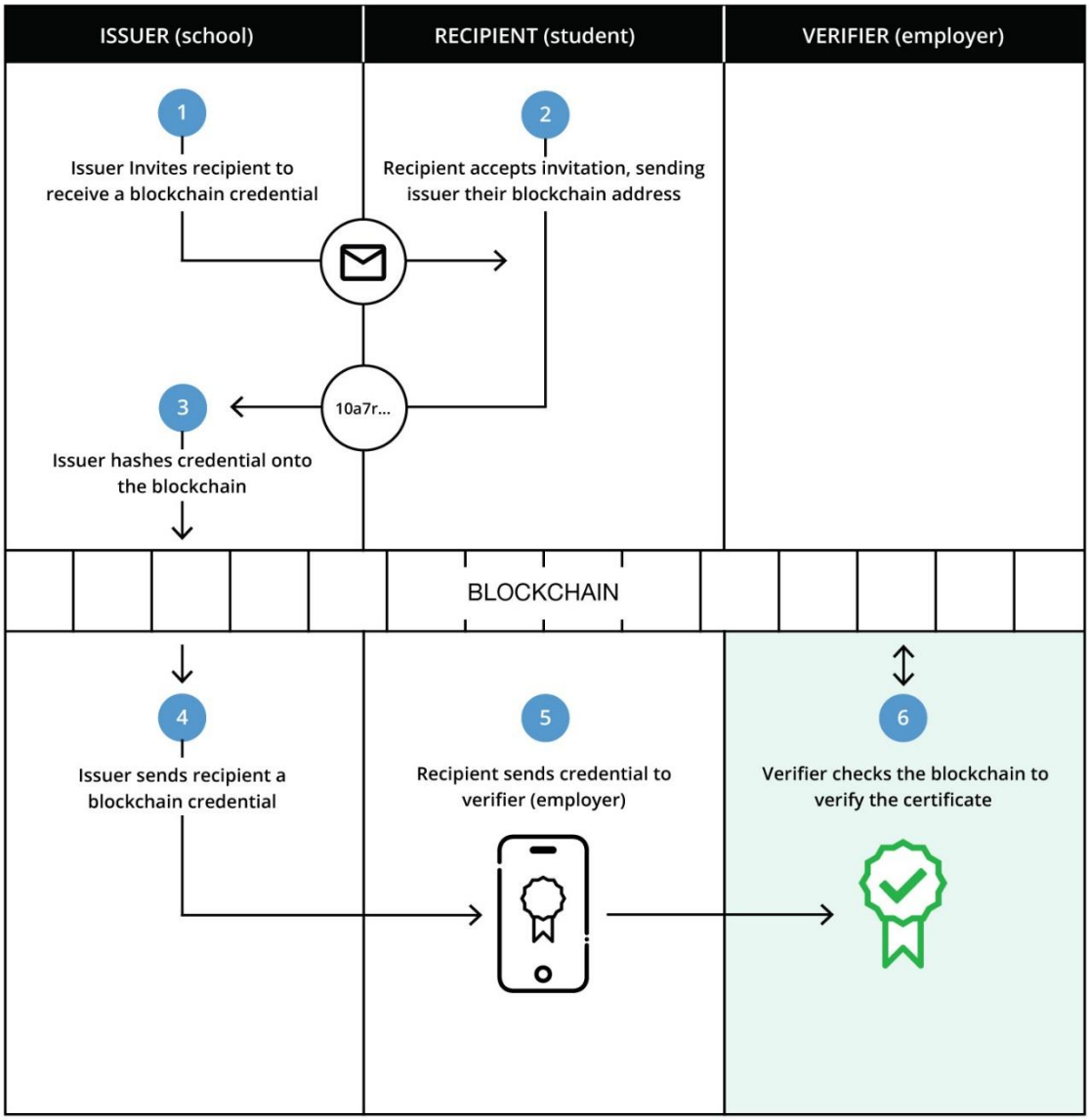


Figure 26: Blockcerts - How certificates are created, protected and checked (Blockcerts, 2016)

This process can easily be explained and illustrated in the case of an LSM student - Christophe- receiving a master's degree in business engineering:

1. The LSM sends an email to Christophe to congratulate him as he passed all his exams and to ask him his authorisation to receive blockchain address.
2. Christophe accepts right away, which directly sends the credentials to the LSM.
3. The LSM receives Christophe's unique blockchain credentials and adds it into the LSM blockchain. Only the LSM administrators can add graduates into the blockchain and certify a degree through the blockchain.

4. The LSM sends to Christophe his blockchain credentials. From now on, Christophe can share his credentials with any employer or party that want to verify he is graduated with a master in business engineering.

5. Christophe has entered the recruitment process at a company -P&G for the example- and he is asked to prove he is graduated from the LSM with a master degree in business engineering. Therefore, Christophe sends his blockchain credentials to P&G.

6. P&G recruitment team enters Christophe's personal blockchain credentials into the *Blockcerts*. Indeed, he received a master degree in business engineering from the LSM.

As can be seen, when the student has his digital certificate, he does not need the involvement of the school anymore. Indeed, to verify the certificate and prove ownership to any external party such as an employer, the student can use the blockchain.

The first real-case example of a Blockcerts use is the MIT degree certificate. Indeed, every degree issued by the MIT is now tamper-proof and verifiable thanks to Blockcerts. Few universities like University of Nicosia and of Birmingham quickly adopted the same technology (Grech & Camilleri, 2017).

Figure 27: MIT certificate issuance based on Blockcerts (Durant & Trachy, 2017)

As can be seen in the figure above, the degree delivered via Blockcerts is divided into three layers:

1. The presentation layer, showing a classic diploma received at the end of the degree.
2. The content layer that contains the public key. The public key is the blockchain credentials assigned to the document. It proves that the document is part of the blockchain. The credentials can be shared with any party to prove its authenticity.
3. The receipt layer, it serves as a receipt from the blockchain, a proof the certificate was added to the blockchain. The hash value assigned to the document is stored in this third layer. This hash value ensures that the document forms a block of the blockchain and is, therefore, secured by the whole blockchain system (see Block for more details).

8.2.3. Feasibility

The feasibility is extremely high in this situation as the technology has already been developed and is available open-source. In addition to that, Blockcerts has been created to be deployed as easily as possible so there is no need to have a full team of blockchain experts working on the project.

8.2.4. Cost-benefit analysis

The objective of this analysis is to determine if the UCL should implement the aforementioned solution. To take this important decision, an analysis of the advantages and disadvantages is made in this section.

8.2.4.1. Advantages

The implementation of Blockcerts for degree securitisation and verification at the UCL comes with many advantages for all parties.

For the university:

1. Image benefit. The UCL would be one of the first universities in the world and the first in Belgium to implement a blockchain-based degree. It would create press coverage around the event and it would show the UCL commitment to be a front runner in leveraging new technologies for education.
2. Security. The UCL would increase the security of its degree database by using blockchain.

3. Fraud reduction. Using blockchain-based certifications would reduce the number of UCL degree fraud considerably. Indeed, with the correct education of the users and communication towards companies or any third parties and with a faster and more efficient system, third parties will be inclined to perform more check. In addition to that, blockchain-based technology will discourage potential fraud.
4. Simplicity of verification. Once the blockchain-based degree has been given to the student, the UCL has nothing to do to ensure that the verification system is running. There is no need for a UCL employee having the responsibility to pick up the phone or answer email regarding degree veracity checks.
5. Efficiency. The steps one, three and four in the Blockcerts process can be automatised so that the university has no human actions to take in the whole process. It considerably increases efficiency for the university.
6. Reduced human input. One of the direct consequence of the previous advantage is the reduction of human input and, therefore, the reduction of costs.
7. Proof of issuance. In case it is ever necessary, the UCL can proof it issued a certificate to a graduate.
8. Revocation of certificate. If the university discovers post-graduation that a student has not abode with the UCL regulations during his studies (e.g.: post-graduation discovery that the student was impersonated by someone else during examinations to pass), the university can revoke a degree easily.
9. Possibility of providing renewable certifications. If the UCL offers some certifications that are only enforceable for a certain period of time and that needs to be renewed, the university can assign an end-date to a certification very easily.
10. Integrity and authenticity. Using a blockchain-based solution ensures integrity, meaning that the certificate has not been tampered with. In addition to that, it ensures authenticity, meaning that there is a connection between the UCL signature on the document and the hash saved on the blockchain. If a document is on the blockchain, it is an authentic document signed by a UCL administrator.

For the student:

1. Exclusivity. With this blockchain-based solution, each student will have the guarantee that his degree certificate is only provided to graduate students. It is not possible anymore to have fraud people taking advantage of the certificate without having done the whole curriculum.

2. Security. Thanks to this new solution, each student is ensured to have a secure link to his digital certificate. Losing the physical degree is not an issue anymore. In addition to that, it is impossible that the link to his degree is deleted from the blockchain (it would require every user of the software to delete this exact document, knowing that most users do not know each other and that there are thousands if not millions of users).
3. Independence. Graduate students do not need to rely on the UCL anymore to make a third-party verify the veracity of his degree.
4. Ownership. Each graduate student owns his credentials to the blockchain.
5. Control. Linked to the previous advantage, graduate students have full control of their credentials and can, therefore, decides who can access it.
6. Easiness of verification. Thanks to this new system, graduate students can easily give proof of degree reception and the third party –employers, other universities or any other third-party– can verify easily the information.
7. Privacy. As each graduate owns his credentials, he is the only person capable of giving the key to his certificate. Knowing that the blockchain is only a chain of scripted blocks without a key, other users do not know he has a certificate and his privacy is ensured.
8. Degree sharing. Thanks to the new solution, graduates can decide to share their degrees through different channels (mail, pdf doc download, LinkedIn, Facebook,…) very easily.

For the verifier:

1. User-friendly. The verification system that verifiers need to use is very simple and user-friendly, therefore making the task more interesting. Thanks to the user-friendliness of the system and the will of Blockcerts creators to make it available to anybody, no specific blockchain or IT qualifications are required to use the system.
2. Fast. Unlike the previous verification system, the Blockcerts-based solution is very fast. Indeed, once the verifier has the link to the system and the credential key, it takes less than 5 seconds for the system to verify the authenticity of the degree.
3. Independent. The verifier does not depend on the degree issuer (the university) to verify the authenticity of a degree. Complementarily, the verifier does not need much information or support from the graduate.

4. Available anytime. As the process does not require the participation of any other party, the verification can be done at any time (24/7/365).
5. Reliable. The verification system is reliable and will not refuse a verification for any possible reason.
6. Security. As the verification and authentication system is fully secure, the verifier can be sure that the degree has not been tampered with.

8.4.2.2. Disadvantages

Compared to the advantages, there are few disadvantages and they have little negative impacts.

For the university:

1. Implementation. The UCL would need to implement the new system. It is going to take time, efforts and investment. Nevertheless, thanks to the open-source Blockcerts system, the presence on the market of firms specialised in its implementation (like Learning Machine) and the fact that UCL benefits from highly qualified staff and professors, the disadvantage is limited.
2. Maintenance. The system would need maintenance to make sure updates are done properly and to ensure the security of the solution.
3. Education of employees. As the implementation of this system would be a major change in the degree securitisation and verification system, it will require an education phase to UCL employees. Indeed, it is key to make sure they understand at least globally how the solution work. Thanks to the focus on the user-friendliness of Blockcerts, there are not any technical prerequisites.
4. Education of students. After the staff education, students as well will need to be educated on how to access their blockchain-based degree but also on how to make a third-party verify it. A self-explicit learning material could easily be created and shared with graduate students at the relevant time.
5. Initial cost. The implementation of this system would come with an initial cost, mostly for the implementation. Indeed, the technology is open-source but needs to be implemented properly in the UCL technological ecosystem. Determining the real cost of this operation is hard as it depends on the UCL technological environment and on the rapidity of the implementation.

6. Storage of degrees. As the certificates are not stored on the blockchain (only the secure verification is), the university needs to keep a safe database of certificates issued. This should not be a major issue as it is already the case.

For the student:

1. System understanding. The students that are about to be or are already graduated need to understand how the system works for two main purposes. Firstly, for them to be able to check their degrees and share it. Secondly, they need to be able to send a rapid explanation (a link, a key and how to use the key on the website) on the verification to potential verifiers.
2. Degree storage. This disadvantage is very similar to the 6th disadvantage for the university. As the degree is not stored on the blockchain, the student needs to keep his degree safe. Nevertheless, thanks to the digital nature of the degree and the functionalities of Blockcerts to share it via email, Facebook, LinkedIn,…, it is easily kept safe. In addition, it is downloadable and even if it is accessed by someone with bad intentions, it is highly secure.

For the verifier:

1. Dependence on the graduate. Probably the major disadvantage for the verifier, it needs to receive the authorisation from the degree holder to verify the authenticity of the degree. Nevertheless, it is a way to ensure transparent verifications for all parties.
2. Understanding the system. The verifiers need to understand the verification process in order to effectuate the check. Considering it is very user-friendly and that the student would share a short "how to use" material, it should not be a major barrier.

8.4.2.3. Conclusion

Having observed the advantages for all involved parties, implementing a securitisation and verification blockchain-based system shows more advantages than disadvantages. Nevertheless, before taking the decision to advise such a change in the process, it is key to analyse if there are not any better technological or non-technological solutions.

8.4.3. Benchmark with other solutions

The purpose of this section is to determine if the blockchain-based solution is the best in the case of securitisation and verification check of UCL's degrees and certificates.

The table below shows the features of different solutions:

	Blockcerts	Digital Sigs	Badges	PDF	Paper
Human Readable	✓	✓	✓	✓	✓
Machine Readable	✓	✓	✓	✓	
Cryptographically Owned	✓				
Vendor Independent	✓		✓	✓	
Decentralized Verification	✓				
Tamper Evident	✓	✓			
Independent Timestamping	✓				

Figure 28: Comparison of ways to secure and verify certificates (Learning Machine, 2019)

In order to do this analysis, 7 features of securitisation and verification are used to compare the different options (Learning Machine, 2019).

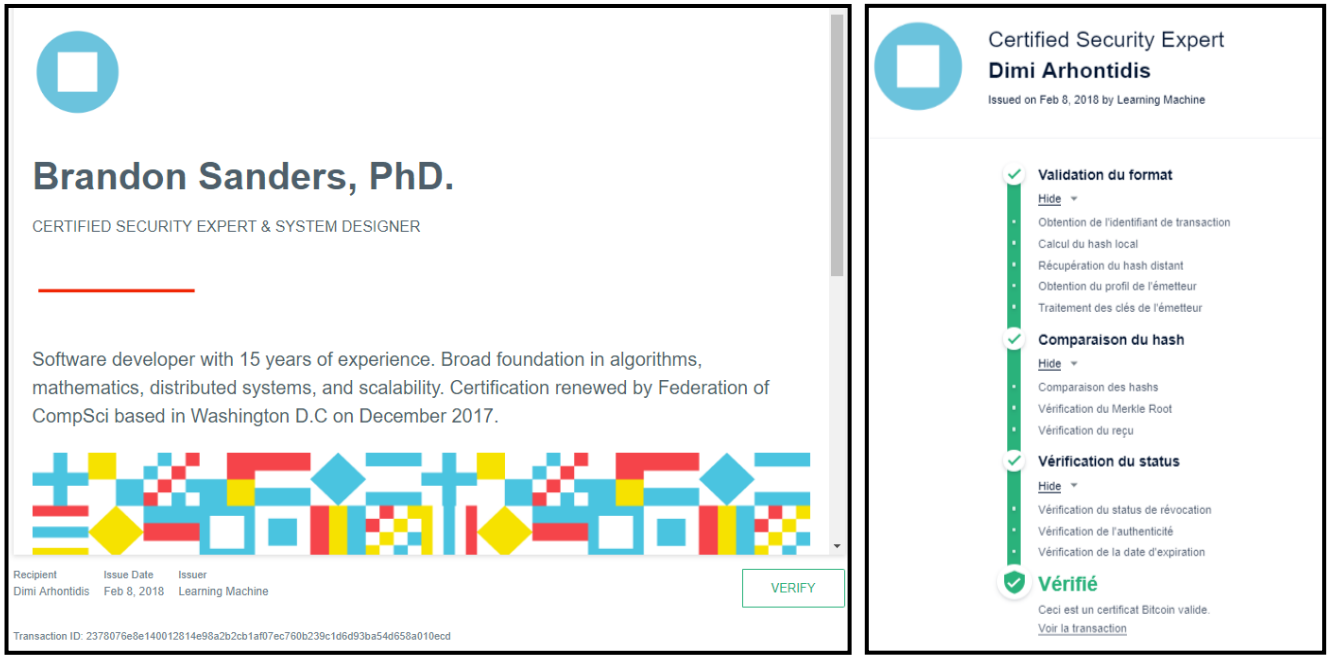
1. Human readability ensures that the document can be read by a human being. It is important in the UCL case as any verifier should be able to read the certificate.
2. Machine readability ensures that the document can be digitally read. It is also important in the UCL case as it is often difficult to give a physical version of the certificate to a verifier.
3. Cryptographic ownership refers to the ownership of the key to the document by the recipient of the certificate. It is key in the UCL-graduate case as the graduate should have the ownership of his document.
4. Vendor independence refers to independence towards the vendor organisation. Indeed, there is no dependence toward any blockchain or Blockcerts service provider. It is key for UCL as the university or the student do not want to depend on any third-party to do verifications (for students) or do their jobs (for UCL administrators).

5. Decentralised verification refers to the independence towards the issuing organisation. It is one of the main advantages in the UCL case, the student does not depend on the UCL and its constraints to verify his degree anymore.
6. Tamper evidence refers to the tamper-proof feature of the access to the certificate as well as the possibility to verify the key. It is primordial for universities such as UCL to make sure that they have the exclusivity of production of their degrees. Therefore, certificates should be tamper-proof.
7. Independent timestamping refers to the immutable proof that a certificate has been issued at a certain moment in time. None of the engaged parties can change that. It is very important for both students and UCL to have a record that a certificate has been given.

The only solution that can tick all the boxes is the Blockcerts option. Indeed, in the case of certificates that need to be secured and accessed permanently in a decentralised and secured fashion, Blockcerts appear to be the best solution. Therefore, it is recommended to go on with the project!

8.4.4. Real-life example

The user-friendliness of the application can be tested on the Learning Machine website. Here are a few screenshots of the process:



Figures 29: Blockcerts' verification process (Learning Machine, 2018)

As it can be seen on the first screenshot, the certificate shows the recipient of the certificate, the issue date as well as the issuing institution. The transaction ID is also part of the information available on the front page. The design of the certificate can be changed.

Once the user has clicked on the *verify* button, the verification process starts and the application shows the second screenshot. The verification process is composed of three main steps:

1. Format validation.
    a. The obtention of the transaction ID by the app (a combination of numbers and letters available on the front page).
    b. Computation of the local hash. The local hash is the hash associated with the certificate.
    c. Retrieval of the remote hash. The remote hash is the hash encrypted in the blockchain application, it is expected to be the same as the local hash.
    d. Issuing profile reception. Reception of information about the issuing party (the UCL in the university case).
    e. Issuing entity's key treatment. Using the key from the issuing entity to make sure the hash was encrypted in the blockchain by the issuing entity.
2. Hash comparison.
    a. Hash comparison. This step makes sure that the local and remote hashes are the same. By doing so, the application verifies that the certificate was indeed put in the blockchain by the issuing entity.
    b. Merkle root verification. See relevant part for more information.
    c. Receipt verification. This step consists of a check of the receipt included in the certificate with what is on the blockchain. Again, a match is required to validate the certificate.
3. Status verification.
    a. Revocation status verification. It is a check that the issuing entity has not revoked the certificate (e.g.: UCL realising a student has been cheating at his exams and revoking a degree).
    b. Authenticity verification. Check of the certificate's authenticity.
    c. Expiration verification. If the certificate has to be renewed, there is going to be an expiration date assigned to the certificate. This step verifies that the certificate is not expired.

The verification process might seem long but it takes less than 5 seconds.

8.4.5. Action plan

The road to a fully implemented Blockcerts solution for the whole UCL is long. This section will determine the milestones and steps to follow to reach such a result. The timing assigned to each step is hard to determine as it depends highly on the efforts, time and energy invested in the project.

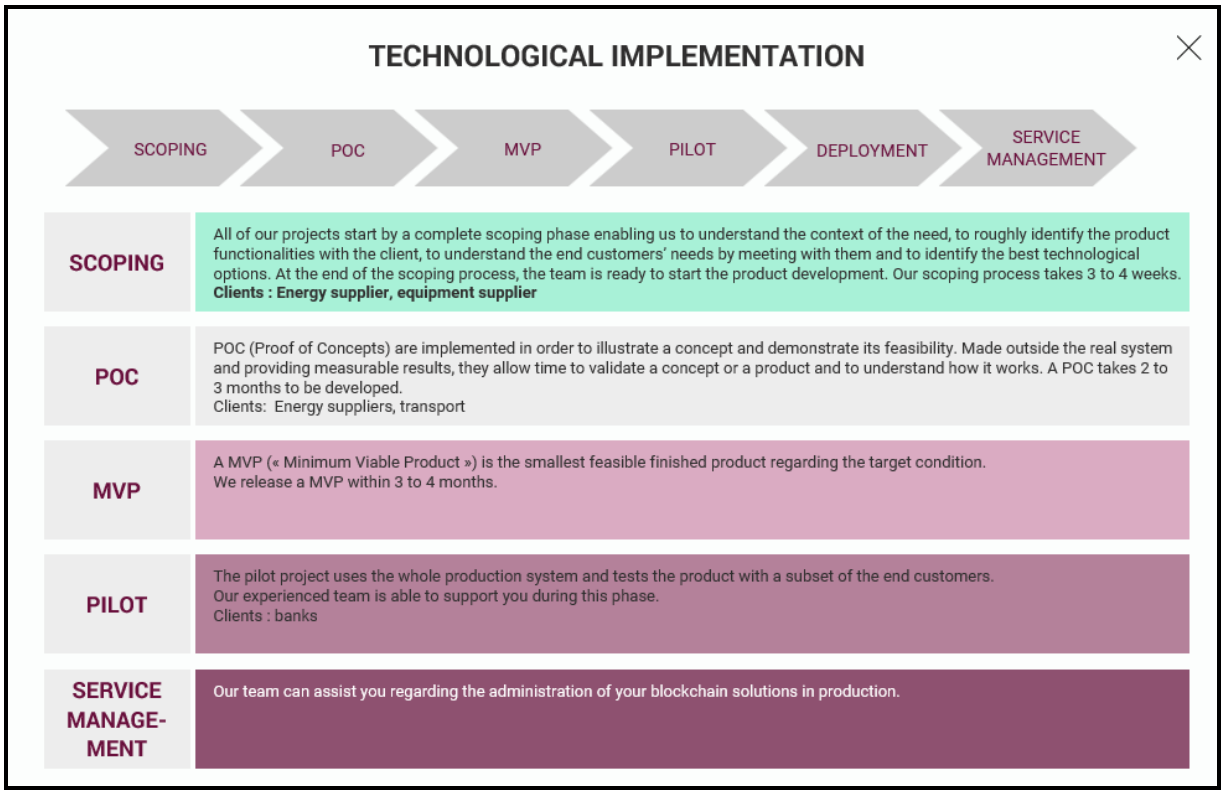


Figure 30: Sia Partners' Blockchain implementation phases (Sia Partners)

The figure here above summarises the main steps to implement a blockchain-based solution. It is composed of 6 main steps applied to the UCL case (Sia Partners):

1. Scoping. This first phase has for objective to fully understand the situation, environment, desired functionalities and main stakeholders. As stated in the name, the target is to estimate the scope of the project and what can and can't be done with the blockchain-based solution. In the UCL case, the objective is to meet the UCL administrators currently handling degree verification, to understand the functionalities they would like to see in the solution, what should be taken into consideration, etc.
2. Proof-of-concept. This second step serves as a testing phase to ensure that the application could work in the system. It is not yet used in the system itself but with

related information to make sure it works and deliver results. In the UCL case, it would be a testing phase with UCL administrators playing all roles: university administrators, graduate students and verifiers. The point is to get a maximum of feedback to build the minimum viable product.

3. Minimum viable product. This step aims at delivering a first version of the product, minimalistic in terms of functionalities and scale but that can already work with limited inputs. The objective is to have a product running as quickly as possible, even if it implicates that the product is really minimalistic. In the UCL case, it would be a small version of the blockchain application. UCL administrators would have to do the process with a small group of voluntary students and some fake verifiers. Again, the objective is to get a maximum of feedback.
4. Pilot. The product is used in the whole system but with a limited part of the end customers (here, graduates). The objective being to verify that the product works in its system and with real customers. In the UCL case, it could be a pilot phase where 30 to 50 students receive their blockchain-based certification. The communication between application developers, project manager and users (students, UCL administrators and verifiers) is key. Indeed, all users should provide full feedback on the user-friendliness, the understanding they have of the process, the advantages and disadvantages they observed, etc.
5. Deployment. If the pilot phase is successful, the project can move on to the deployment phase where the product is deployed to the whole system and for all customers. This would be a full deployment to all graduate students of UCL with a major communication.
6. Service management. This phase starts from the end of the deployment and can last indefinitely, it is the product maintenance phase. In the UCL case, it would be a part of the IT team dedicated to this application ownership and maintenance.

8.4.6. Risks

There are very few risks associated with this project.

A potential risk is potential upcoming regulations on Blockchain-based application. Indeed, blockchain being a new technology, regulators take the time to analyse it before publishing some regulations around it. Nevertheless, in this case, blockchain is not linked with financial

or sensitive information. On the contrary, it improves personal data protection for all graduates.

A governance risk might appear too if the project takes longer than expected and if the UCL governance changes in the way. This could be a major barrier, if not a stop, to the project. It is, therefore, key to integrating this project in the long-term digitalisation strategy of the UCL.

An implementation risk can occur as well. Indeed, either with an internal team or with an outsourced implementation team, there is a risk of failure if the right talents and resources are not pooled together.

Finally, strong technology advancement could be a game-changer for the project. Indeed, either if the blockchain technology benefits from major improvements non-implementable to the project or if a new technology shows up with even more benefits for securitisation and access to certificates, the project can be compromised. Nevertheless, this solution relies on new technology and improvements are shared on an open-source basis. In addition to that, for now, there are no new technologies with similar benefits appearing on the market.

8.4.7. Improvements

It is key to always looking forward to other improvements to make the solution even better, more efficient and complete. There is a major improvement that can be added to this solution, it is the subject of the next section.

8.5. Verification of an accreditation chain

8.5.1. Current situation

As of mid-2019, the accreditations chains for higher education institutions are all over the place in the European Union. Indeed, each country has its own regulations and regulators with different agencies, public or private, certifying different abilities of universities to deliver certain degrees under certain quality norms.

In this situation, any party who wants to verify the veracity of certification needs to go through a very long process including these checks:

- Verification that the institution effectively issued a certificate
- Verification of the quality of the institution based on its accreditations
- Verification with the accreditation entities that the institution has effectively received the accreditations

- Verification of the authority of the accrediting entities
- Verification that the accrediting entities are certified to give these accreditations

To illustrate this complex situation, here is an example of the Louvain School of Management (hereafter LSM). A future employer from Italy went through a recruitment process with a bright candidate from the LSM but he would like to make sure that the student's Belgian degree is true and of the highest quality. Therefore, he needs to perform these checks:

- Verification that the LSM effectively issued a master degree to the candidate
- Verification of the quality of courses given at the LSM based on its accreditations, including the EQUIS certification (UCLouvain)
- Verification with EQUIS that the LSM has really been certified
- Verification of the authority of the EQUIS expert who performed the assessment and ultimately gave the accreditation
- Verification that the EQUIS expert was certified to give the EQUIS accreditation to the LSM

8.5.2. Blockchain implementation

The blockchain-based solution that could disrupt the current situation is based on the same solution explained in the previous section.

The previous solution was securitising the relationship between the certificate issuer (e.g.: the university) and the recipient (e.g.: the graduate) as well as providing secured decentralised access to the certificate.

This solution is going a step further by including a second layer of security and certification. Indeed, the accreditor of a specific accreditation like EQUIS for universities would be included in the blockchain-based certificate. Therefore, when a verifier (e.g.: future employer of a UCL graduate) will perform the verification of the degree, he will receive a proof that the degree is authentic, valid and was given by the UCL but in addition to that, he will also have the proof that UCL was EQUIS certified.

8.5.3. Feasibility

The main issue with this innovative solution is the involvement of all parties. Indeed, for the UCL or any university that has already implemented the Blockcerts solution for their degrees, it is a minor update to add the accreditations on the system.

On the contrary, for the accreditors that have probably not implemented such a solution before, it takes more effort. If the accreditor can leverage the technology for itself and is ready to invest, the project can quickly become a huge success. On the other hand, if the accreditor is not interested in such technology for his accreditations, the UCL can't do it unilaterally.

To cut a long story short, the feasibility highly depends on the third-party.

8.5.4. Cost-benefit analysis

This solution presents the same advantages as the previous Blockcerts application (see Advantages for more information) and some extra ones.

For the university, as of mid-2019, it would be a world-first use of the blockchain so the image benefits would be even greater. In addition to that, it would show to all verifiers the UCL accreditations and give an extra proof of the quality of UCL courses.

For the students, the advantages are also amplified as the verifier would see the graduate's degree but also the university's accreditations.

The degree verifier would benefit from more information about the university, the information he can use or not. In addition to that, the verifier could be some potential students or third-parties that want to invest in UCL and would like to have proof of UCL's accreditations.

Finally, the accreditors would gain all the advantages mentioned for the UCL in the first Blockcerts section (one of the most interesting ones might be the renewal feature). Furthermore, it would strengthen the relationship with accredited schools.

On the other hand, it also shows the same disadvantages and some others. Indeed, it requires a necessary collaboration between the university and third-parties as aforementioned in the feasibility section. In addition to that, it would increase the application complexity which will lead to extra work on the development and maintenance sides.

In conclusion, if one or many third parties are willing to join the project, it could quickly become a success and highlight the UCL as a front runner on blockchain use in education.

8.6. Other uses in education

8.6.1. Managing intellectual property

Some companies are ahead with intellectual property management for the educational sector. Here are some examples and what they have to offer.

8.6.1.1. Binded

Binded is a company that is providing a copyrighting service for images using the blockchain technology. The clients of Binded are the photographers or owners of an image. They can upload their image on Binded. Then, a hash is assigned to this image and a timestamp of the date and time of the upload as well as the identity of the photographer or creator of the image are registered in the blockchain. Therefore, the author of the image can prove at any time that the image belongs to him. Indeed, nobody can tamper either with the date and time of the upload or with the data which is, in this case, an image (Binded).

Thanks to this interesting blockchain solution, images or photos of students in arts and photography could be saved and protected easily. It would protect the work of students at a low cost. On the long-run, this concept could be extended to other ideas of students from different faculties.

8.6.1.2. Ledger Journal

The Ledger Journal is an online journal at the University of Pittsburgh that publishes research articles about various topics including blockchain, mathematics and so on. The interesting characteristic of this digital journal is that it asks the author of each article to sign it with a blockchain digital signature. Furthermore, the Ledger Journal timestamps the publications so that both the content of the article and the authors are protected, they can always claim the article and the content can't be tampered with (Ledger Journal, 2019).

8.6.1.3. Bernstein Technologies

Bernstein Technologies provide a service using the same technology than the two previous ones but in the case of intellectual property. Indeed, this company provides digital security for copyrights or patents. Thanks to this system, the owner of a patent can publish it without revealing the precious content of it. Therefore, he can prove he is the first with this invention without having to divulge the content of the patent and he does not need a centralised system (Bernstein Technologies).

UCL's researchers or professors' greatest ideas could, therefore, be protected quickly and easily before a patent can be created. This would serve as first-round protection for the idea.

8.6.2. Capacity-currency transformation bank

This technique, also called "*learning is earning*" allows to transform the efforts of students into a currency. The blockchain records the learning experience of the user and follows its evolution in term of knowledge and skills. Therefore, the more efforts they put in their studies, the more they will earn a kind of digital currency. The standards of transformation

must be defined beforehand. Considering the current state of the technology and the constraints linked to the measurement of learning investment make this idea difficult to implement in short to medium term (Grech & Camilleri, 2017).

8.6.3. Future possibilities

This section explores potential future opportunities that are harder to implement on the short to medium term due to technological or non-technological concerns that are going to be explained at the end.

8.6.3.1. Smart contracts

Smarts contracts protected by the blockchain technology could be established between students and teachers. If one of the parties of the smart contract does not face its responsibilities, the smart contract will be terminated, and the party will not get the positive outcome expected.

8.6.3.2. Digital currency as driver

This system is close to "*learning is earning*" process but with teachers as an intermediary.

An internal digital currency can be used in a school to motivate students. If a teacher has the opportunity to offer a certain amount of this internal digital currency to students, these have an increased incentive of producing excellent work or participate extensively in class for instance. Afterwards, this internal digital currency could be used as tuition or even be exchanged against real currency for example (Grech & Camilleri, 2017).

8.6.3.3. Fairness of evaluation in teamwork

An effective and fair evaluation has always been an issue in the education sector. Especially when it comes to teamwork because the free-rider problem can occur. Indeed, one member of a team can ripe the benefit of the teamwork without having participated much in the process. Blockchain technology can partly help to fix this issue by applying a system like this one:

Each student of the team is assigned to a piece of work. Once it is done, he can upload the results on a platform via its unique personal account. The smart contract will review the personal work of the student, assess the performance and the results will be registered into blocks. In addition to that, the behaviours are also recorded to have proofs for the evaluation. Therefore, when the time of the evaluation will come, the blockchain network will take every student's opinion into account as each student is a node of the network. The outcome will then be a fair evaluation of each student's implication into the project. It is important not to lose sight of the teamwork side of the project and have a measurement of this KPI as well.

8.6.3.4. Teachers assessment

Teachers assessment based on student feedback is often subjective and does not really help professors improve. The blockchain technology could help teachers' assessment via smart contracts. Before the course even starts, each teacher could enter instructional activities into the blockchain system. During the time of the course, every educational activity will be recorded in the system. Therefore, at the end of the course, the smart contract can verify the consistency of the learning activities and be part of the assessment.

These smart contracts between the teachers and the school could use the same drive as smart contracts between students and teachers with an internal digital currency.

8.6.3.5. Potential drawbacks and issues

The future possibilities presented here above seem nice on a first approach, but they come with some issues as well that should not be forgotten.

First, it is very hard to assess essays or presentation through smart contracts without any kind of human intervention.

Second, the immutability of the system will ensure that the grades of students are not tampered with, but it also means that the right authorities can't change them afterwards even if it is for legitimate reasons. Nevertheless, they can upload a new document vouching for the invalidity of some information.

Finally, there are still some technical barriers while trying to implement blockchain technology in education. For example, the proof-of-work makes the school use a lot of energy (Grech & Camilleri, 2017).

9. Conclusion

The research aimed at identifying and analysing potential blockchain application leads for the education field and more specifically for the Université Catholique de Louvain. By analysing the few current pilot projects in universities around the world and thanks to the investigation for innovative ideas, this thesis has shown how the UCL can implement a blockchain-based application successfully and for its most interesting use. The most promising lead is a blockchain implementation for the securitisation of UCL degrees. It provides a decentralised, automated and secured way of giving ownership of the verification process to the graduates. Indeed, with this application, they do not depend on anyone to prove the authenticity of their degrees. In parallel, the UCL improves in efficiency, simplicity, reduces human inputs and costs and gain in image benefits. Last but not least, it is easier and user-friendly for company verifying the authenticity of a degree. In addition to that, it is advised to look ahead with the accreditations being secured on the blockchain as well. This would be a worldwide first use of the blockchain. Any verifier would be able to check the authenticity of a degree and at the same time discover or verify the accreditations received by the UCL.

While the methodology used showed limited details about the blockchain implementation steps and quantifiable information, it provided a broad scope of innovative ideas for blockchain use in education. This research clearly illustrates that UCL should move forward with a blockchain-based application implementation but it also rose the question of a more detailed action plan. This paper brought to light the best potential blockchain applications tailor-made for the UCL. It showed that the UCL should move forward with the implementation of a blockchain-based application for degree securitisation and verification, improved on the medium to long run by an accreditation securitisation.

Based on this work, practitioners might consider updating the information with the evolving potential of the technology and explore further the implementation details. In addition to that, applications developed in this thesis can excel out of the education scope, in business life. This is why some researches could be done on implementing the explained blockchain uses in other businesses, especially the ones working with a lot of renewable certifications. For example, an interesting complementary work would be to analyse the steps, timeline and costs of an implementation of a blockchain-based application for certificate securitisation in the accounting industry. Indeed, this field is one of the most regulated and it comes with renewable certifications. Therefore, advantages of the blockchain application would be multiplied.

10. References

Argyris, C., & Schon, D. (1978). *Organizational learning: a theory of action perspective.* New York: McGraw-Hill.

Bain, B. (2018, January 22). *What's in a Blockchain Name? SEC Demands More Than Investor Bait.* Retrieved from Bloomberg: https://www.bloomberg.com/news/articles/2018-01-22/what-s-in-a-blockchain-name-sec-demands-more-than-investor-bait

Baliga, A. (2017). Understanding blockchain consensus models. *Persistent*.

Bayer, D., Stuart, H., & Stornetta, S. (1993). Improving the Efficiency and Reliability of Digital Time-Stamping. (Springer, Ed.) *Sequences II*, pp. 329-334.

Bernstein Technologies. (s.d.). *Intellectual property for the digital age.* Récupéré sur Bernstein: https://www.bernstein.io

Binded. (n.d.). *Introducing Binded, the world's first copyright platform.* Retrieved from Binded: https://binded.com/about

Bitcoin Cash. (n.d.). *Peer-to-peer electronic cash .* Retrieved from Bitcoin cash: https://www.bitcoincash.org/#faq

Bitcoin gold. (n.d.). *Faq.* Retrieved from Bitcoin Gold: https://bitcoingold.org/faq/

Bitcoin Private. (n.d.). *FAQ.* Retrieved from Bitcoin Private: https://btcprivate.org/

Blockcerts. (2016). *Introduction.* Retrieved from Blockcerts: https://www.blockcerts.org/guide/

Boaventura, A. (2018, April 12). *Demystifying Blockchain and Consensus Mechanisms — Everything You Wanted to Know But Were Never Told.* Retrieved from Medium: https://medium.com/oracledevs/demystifying-blockchain-and-consensus-mechanisms-everything-you-wanted-to-know-but-were-never-aabe62145128

Boxley Group. (s.d.). *Knowledge management.* Récupéré sur Boxley Group: https://boxleygroup.com/solutions/know-solution/

Bukowitz, W., & Williams, R. (2000). *The knowledge management fieldbook.* London: Prentice Hall.

Cardano. (s.d.). *What is Cardano?* Récupéré sur Cardano: https://www.cardano.org/en/what-is-cardano/

Carson, B., Romanelli, G., Walsh, P., & Ahumaev, A. (2018, June). *Blockchain beyond the hype what is the strategic business value?* Retrieved from Mckinsey & Company: https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/blockchain-beyond-the-hype-what-is-the-strategic-business-value

Choo, C. (1998). *The knowing organization.* New York: Oxford University Press.

Coppola, F. (2016, July 21). A painful lesson for the ethereum community. *Forbes*. Retrieved from https://www.forbes.com/sites/francescoppola/2016/07/21/a-painful-lesson-for-the-ethereum-community/#663225bfbb24

Dalkir, Z. (2005). *Knowledge Management in theory and practice.* Elsevier.

de Rossi, L. M. (2018, November 28). *Blockchains and their imitators: efficiency or hype?* Retrieved from Bocconi Knowledge: https://www.knowledge.unibocconi.eu/notizia.php?idArt=20182

Douceur, J. (2002). The sybil attack. *International workshop on peer-to-peer systems* (pp. 251-260). Springer.

Durant, E., & Trachy, A. (2017, October 2017). *Digital Diploma debuts at MIT.* Retrieved from MIT news: news.mit.edu/2017/mit-debuts-secure-digital-diploma-using-bitcoin-blockchain-technology-1017?fbclid=IwAR23uubIl6-SH8Gzf2hOrWSxiH7VZuJeHxuc3K9DqicFERx8SwywHdeY630

Grech, A., & Camilleri, A. F. (2017). Blockchain in Education. (A. I. Santos, Ed.) *European Commission: Joint Research Centre*.

Haber, S., & Stornetta, S. (1991, January). How to time-stamp a digital document. (Springer, Ed.) *Journal of Cryptology, 3*(2), pp. 99-111.

Hammerschmidt, C. (2017, January 27). *Consensus in Blockchain Systems. In Short.* Récupéré sur Medium: https://medium.com/@chrshmmmr/consensus-in-blockchain-systems-in-short-691fc7d1fefe

Higginson, M., Nadeau, M.-C., & Rajgopal, K. (2019, January). *Blockchain's Occam problem.* Retrieved from McKinsey & Company: https://www.mckinsey.com/industries/financial-services/our-insights/blockchains-occam-problem

Iansity, M., & Lakhani, K. (2017). The truth about blockchain. *Harvard Business Review, 95*(1), pp. 118-127. Retrieved from https://hbr.org/2017/01/the-truth-about-blockchain

Investopedia. (2017, October 20). *Hash.* Récupéré sur Investopedia: https://www.investopedia.com/terms/h/hash.asp

King, R. (2007). Knowledge Management, a systems perspective. *International Journal of business systems and research, 1*(1), pp. 5-28.

Lamport, L., Shostak, R., & Pease, M. (1982). The Byzantine generals problem. *ACM Transactions on programming languages and systems*, 382-401.

Learning Machine. (2018, February). *Example Blockcerts.* Retrieved from Learning Machine: https://blockcerts.learningmachine.com/certificate/ab56912734bb5784bced00b7e0e82ac9

Learning Machine. (2019, January). *Badges and Blockcerts.* Retrieved from Learning Machine: https://www.learningmachine.com/badges-and-blockcerts/

Ledger Journal. (2019). *Ledger.* Retrieved from Ledger Journal: http://ledgerjournal.org/ojs/index.php/ledger?fbclid=IwAR0tZXR6CdojkUgjz8oFtPCc8oVMJKHKcwxLs6gQZqNmqtwdB5Z9N67pB94

McElroy, M. (1999). The knowledge life cycle. *ICM Conference on KM.* Miami, FL.

Merkle, R. (1987). A digital signature based on a conventional encryption function. *Conference on the theory and application of cryptographic techniques* (pp. 369-378). Berlin: Springer.

Meyer, M., & Zack, M. (1996). The design and implementation of information products. *Sloan management review, 37*(3), pp. 43-59.

Microsoft. (2017, March 30). *Ensuring Data Integrity with Hash Codes.* Récupéré sur Microsoft: https://docs.microsoft.com/en-us/dotnet/standard/security/ensuring-data-integrity-with-hash-codes

Morabito, V. (2017). *Business innovation Through Blockchain.* Cham: Springer International Publishing.

Nakamoto, S. (2008). *Bitcoin : A peer-to-peer electronic cash system.* Retrieved from Bitcoin.org: https://bitcoin.org/bitcoin.pdf

Nonaka, I., & Takeuchi, H. (1995). *The knowledge-creating company: how Japanese companies create the dynamics of innovation.* New York: Oxford University Press.

O'Dell, C., & Grayson, J. (1998, April 1). If only we knew what we know: Identification and transfer of internal best practices. *California management review*, pp. 154-174.

Panetta, K. (2017, August 15). *Top trends in the Gartner Hype Cycle for Emerging Technologies, 2017.* Retrieved from Gartner: https://www.gartner.com/smarterwithgartner/top-trends-in-the-gartner-hype-cycle-for-emerging-technologies-2017/

Panetta, K. (2018, August 16). *5 Trends Merge in the Gartner Hype Cycle for Emerging Technologies, 2018.* Retrieved from Gartner: https://www.gartner.com/smarterwithgartner/5-trends-emerge-in-gartner-hype-cycle-for-emerging-technologies-2018/

Panetta, K. (2018, June 27). *Assess Blockchain for GDPR Compliance.* Retrieved from Gartner: https://www.gartner.com/smarterwithgartner/assess-blockchain-for-gdpr-compliance/

Peters, G. W., & Panayi, E. (2016). Understanding modern banking ledgers through blockchain technologies: Future of trandaction processing ans smart contracts on the internet of money. In P. Tasca, T. Aste, & L. P. Pelizzon, *Banking beyond banks and money* (pp. 239-278). Springer.

Pettey, C. (2018, February 2018). *The Irrational Exuberance That is Blockchain.* Récupéré sur Gartner: https://www.gartner.com/smarterwithgartner/the-irrational-exuberance-that-is-blockchain/

Price, M. (2018, January 22). *SEC is scrutinizing overnight blockchain companies: chairman.* Récupéré sur Reuters: https://www.reuters.com/article/us-usa-sec-blockchain/sec-is-scrutinizing-overnight-blockchain-companies-chairman-idUSKBN1FB2XI

Quantalysus. (2018). *Choosing between Centralized, Decentralized, and Distributed Networks.* Retrieved from Steemit: https://steemit.com/cryptocurrency/@quantalysus/choosing-between-centralized-decentralized-and-distributed-networks

Rompel, J. (1990). One-way functions are necessary and sufficient for secure signatures. *STOC '90 Proceedings of the twenty-second annual ACM symposium on Theory of Computing*, 387-394.

Ryan, D. (2017, August 10). *Costs of a real world ethereum contract.* Retrieved from Hackernoon: https://hackernoon.com/costs-of-a-real-world-ethereum-contract-2033511b3214

Saerens, M. (2018). Artificial neural networks, SVM and feature transformation. UCL.

Seele. (2018). *Whitepaper: Building the internet of value for the future.* Retrieved from Seele.pro: http://seele-pro.oss-eu-west-1.aliyuncs.com/Seele_White_Paper_English_v3.1.pdf

Seele Tech. (2018, June 20). *Blockchain's New Brain: An Introduction to Seele's Neural Consensus Algorithm.* Retrieved from https://medium.com/seeletech/blockchains-new-brain-an-introduction-to-seele-s-neural-consensus-algorithm-9963749f03b5

Sia Partners. (n.d.). *Sia Partner leverages blockchain for your business.* Retrieved from Blockchain by Sia Partners: https://www.blockchain.sia-partners.com/

Simply Explained. (2017, November 13). Comment fonctionne une blockchain- Expliqué simplement. Retrieved from https://www.youtube.com/watch?time_continue=3&v=SSo_EIwHSd4&fbclid=IwAR1On06QFCLLDijNReiY52h3y_p-U78DKXXQLsqtJm1hdsOS7nw4CWiRImo

Singh, P. (2017, August 21). *Getting an insight of blockchain.* Récupéré sur DZone: https://dzone.com/articles/getting-an-insight-of-blockchain

Solat, S., & Potop-Butucaru, M. (2017). ZeroBlock: Timestamp-Free Prevention of Block-Withholding Attack in Bitcoin. *International Symposium on Stabilization, Safety, and Security of Distributed Systems.*

Suthar, A., & Patel, A. (s.d.). One Way Functions. Karagpur, India.

Swanson, T. (2015, April 6). Consensus-as-a-service: a brief report on the emergence of permissioned, distributed ledger systems. Retrieved from http://www.ofnumbers.com/wp-content/uploads/2015/04/Permissioned-distributed-ledgers.pdf?fbclid=IwAR0dDcfclVkI3FRysDTGb9eV04j1ZmrjGUWtRQQybpFWXWctGZDjqCOibVw

Torverkar, G., & Moskowtiz, D. (2017). *Indorse whitepaper.* Récupéré sur Indorse: https://indorse.io/static/media/Indorse-Whitepaper-v1.0.869d6b72.pdf

UCLouvain. (n.d.). *Accreditations et rankings.* Retrieved from UCLouvain: https://uclouvain.be/fr/facultes/lsm/accreditations-et-rankings.html

Von Krogh, G., & Roos, J. (1995). *Organizational epistemology.* New York: St. Martin's Press.

Von Krogh, G., Ichijo, K., & Nonaka, I. (2000). *Enabling knowledge creation: how to unlock the mystery of tacit knowledge and release the power of innovation.* Oxford: Oxford University Press.

Weick, K. (2001). *Making sense of the organization.* Malden, MA: Basil Blackwell.

Wiig, K. (1993). *Knowledge management foundations.* Arlington, Texas: Schema Press.

Wiig, K. (1993). *Knowledge management foundations: thinking about thinking. How people and organizations create, represent and use knowledge.* Arlington, TX: Schema Press.

Zilliqa. (2018). *About us.* Récupéré sur Zilliqa: https://zilliqa.com/about-us.html

11. Appendices

Appendix 1: Wiig knowledge management model: degrees of internalization (Wiig, 1993)

Level	Type	Description
1	Novice	Barely aware or not aware of the knowledge and how it can be used.
2	Beginner	Knows that the knowledge exists and where to get it but cannot reason with it.
3	Competent	Knows about the knowledge, can use and reason with the knowledge given external knowledge bases such as documents and people to help.
4	Expert	Knows the knowledge, holds the knowledge in memory, understands where it applies, reasons with it without any outside help.
5	Master	Internalizes the knowledge fully, has a deep understanding with full integration into values, judgments, and consequences of using that knowledge.