POLITECNICO
MILANO 1863

SCUOLA DI INGEGNERIA INDUSTRIALE E DELL'INFORMAZIONE

Laurea Magistrale in Ingegneria Gestionale

Potentials of Blockchain Technologies in Manufacturing:

Study of applicability of Blockchain technology in manufacturing: Blockchain typologies, manufacturing scenarios, application benefits and technology constraints.

Supervisor: Prof. Marco TAISCH
Co-Supervisor: Ing. Claudio PALASCIANO

Master of Science Thesis of:

Simone VACCA TORELLI

905294

Academic Year: 2018/19

This page is intentionally left blank

"So, the problem is not so much to see what nobody has yet seen, as to think what nobody has yet thought concerning that which everybody sees."

Arthur Schopenhauer.

This page is intentionally left blank

Acknowledgements

The process of writing this thesis has been both challenging and an invaluable learning experience. The writing of this thesis would not have been possible without the help of several knowledgeable and resourceful people, and I would like to take this opportunity to express my sincerest gratitude for their assistance.

First, I would like to show my deepest gratitude to my academic supervisor, Prof. Marco Taisch, and, in particular, to my co-supervisor, Eng. Claudio Palasciano, for giving me the opportunity to work on this thesis and for the feedbacks that I have received which have been highly useful in setting the structure and the direction of this thesis.

Lastly, I would like to express my sincerest gratitude and appreciation to my family and friends, for always supporting me and being there for me throughout all my studies.

Thank you!

Milan, December 2019.

This page is intentionally left blank

Abstract

This thesis analyses the possibility of application of the innovative Blockchain technology within Manufacturing, taking into consideration different application scenarios, the possible resulting benefits and the technological constraints.

Thanks to the diffusion of Bitcoins, which have gained great notoriety in recent years, the Blockchain has attracted the attention not only of researchers but also of investors who have begun to investigate the possibility of using this technology in other areas as well.

Therefore, in this thesis this technology is first examined from an informatics point of view to understand the basic working mechanism and to find out what are the motivations that make it so interesting and so versatile; then the phenomenon of the fourth industrial revolution, the so-called Industry 4.0, is investigated in order to contextualize the current production scenario and the technologies with which the manufacturing world is evolving; finally, the definition of a decision-making framework will make it possible to establish the applicability of the Blockchain within different industrial applications taking into account the main technologies with which it will have to interface, the requirements it will have to respect and the benefits it will bring.

This page is intentionally left blank

Abstract (Italian Version)

La tesi analizza la possibilità di applicazione della innovativa tecnologia Blockchain all'interno del Manufacturing, tenendo in considerazioni diversi scenari di applicazione, i possibili benefici risultanti ed i vincoli tecnologici.

Grazie alla diffusione dei Bitcoin, che hanno acquisito una grande notorietà negli ultimi anni, la Blockchain ha richiamato l'attenzione non solo di ricercatori ma anche di investitori che hanno iniziato ad indagare la possibilità di utilizzare questa tecnologia anche in altri ambiti.

Pertanto, in questa tesi viene dapprima analizzata questa tecnologia da un punto di vista informatico per capire il meccanismo base di funzionamento e per scoprire quali sono le motivazioni che la rendono così interessante e così versatile; quindi viene analizzato il fenomeno della quarta rivoluzione industriale, il cosiddetto Industry 4.0, al fine di contestualizzare al meglio l'attuale scenario produttivo e le tecnologie con cui il mondo del Manufacturing si sta evolvendo; infine, la definizione di un framework decisionale permetterà di stabilire l'applicabilità della Blockchain all'interno di diverse applicazioni industriali tenendo conto delle principali tecnologie con cui essa dovrà interfacciarsi, dei requisiti che dovrà rispettare e dei benefici che potrà portare.

This page is intentionally left blank

SUMMARY

Acknowledgements **4**
Abstract **6**
Abstract (Italian Version) **8**
Table of Figures **14**
Table of Tables **18**
Table of Acronyms **20**
1) Introduction to the Research **22**
2) Introduction to the Blockchain Technology **24**
2.1) What Blockchain Is **24**
2.1.1) History: from the Hash-Chain to the Bitcoin Block-Chain 24
2.1.2) Main Elements of a Blockchain 26
2.1.2.1) Centralised, Decentralised, Distributed systems 26
2.1.2.2) Blocks in the Blockchain 27
2.1.2.3) Mining 27
2.1.2.3.1) Rewards and Transactions Fees 28
2.1.2.4) Hash Value 29
2.1.2.4.1) Hash Algorithm: SHA256 29
2.1.2.5) The Timestamp 30
2.1.2.6) The Genesis Block 31
2.1.2.7) Digital signature: Public & Private Key Pairs 32
2.2) How Blockchain Works **34**
2.2.1) Stepping through key elements of Blockchain: 34
2.2.2) Network Propagation of the Blockchain 42
2.2.2.1) Block Size and Propagation Delay 43
2.2.2.2) Blocks Dissemination and Forks 44
2.2.2.3) Improving Network Propagation Speed 47
2.2.3) Fork Classes and Hard & Soft Types 47
2.2.4) Scalability and the Trilemma 49
2.2.5) Access Control 54
2.2.6) Consensus Mechanism 57
2.2. Unanimity in unreliable distributed systems: The Byzantine Generals Problem . 58
2.2.6.1.1 Illustration of the problem 59
2.2.6.1.2 Solutions to the problem 59
2.2.6.2 Consensus Algorithm 60
2.2.6.2.1 Classification of Consensus Algorithms 60
2.2.6.2.1.1) Proof of Work (PoW) 61
2.2.6.2.1.2) Proof of Stake (PoS) 65
2.2.6.2.1.3) Delayed Proof of Work (dPoW) 66
2.2.6.2.1.4) Delegated Proof of Stake (dPoS) 67

2.2.6.2.1.5) Leased Proof of Stake (lPoS) 68
2.2.6.2.1.6) Proof of Authority (PoA) 69
2.2.6.2.1.7) Proof of Reputation (PoRep) 69
2.2.6.2.1.8) Proof of Elapsed Time (PoET) 70
2.2.6.2.1.9) Proof of Space (PoSp) 70
2.2.6.2.1.10) Proof of History (PoH) 71
2.2.6.2.1.11) Proof of Stake Velocity (PoSV) 71
2.2.6.2.1.12) Proof of Importance (PoI) 72
2.2.6.2.1.13) Proof of Identity (PoId) 72
2.2.6.2.1.14) Proof of Retrievability (PoR) 73
2.2.6.2.1.15) Proof of Activity (PoAc) 73
2.2.6.2.1.16) Proof of Time (PoT) 74
2.2.6.2.1.17) Proof of Weight (PoWe) 74
2.2.6.2.1.18) Proof of Burn (PoB) 75
2.2.6.2.1.18) Ouroboros 75
2.2.6.2.1.19) Proof of Authentication (PoAh) 76
2.2.6.2.1.20) Proof of Devotion (PoD) 76
2.2.6.2.1.21) Byzantine Fault Tolerance (BFT) 77
2.2.6.2.1.22) Proof of Believability (PoBe) 79
2.2.6.2.1.23) RAFT 80
2.2.6.2.2) General comparison between consensus algorithms 81
2.3) Evolution of Blockchain 82
2.3.1) Directed Acyclic Graphs (DAG) 82
2.3.2) Smart Contracts 91
2.3.3) Side Chains 92
2.5) Blockchain Application Industries 94
2.4.1) Classification of Blockchain Application by Industries 94
2.4.2) Classification of Blockchain Applications in the Manufacturing Industry 99
2.4.2.1) Inbound & Outbound Logistic/Procurement 102
2.4.2.2) Product, Process & Technology Development 102
2.4.2.3) Operations 103
2.4.2.4) Sales & Marketing 105
2.4.2.5) Human Resource Management/Firm Infrastructure 106
2.4.3) Smart Contracts for Manufacturing 107
3) The Industry 4.0 Scenario 108
3.1) Industry 4.0 and the rise of Smart Manufacturing Systems 109
3.1.1) The Evolution of Industrial Production: from 1.0 to 4.0 109
3.1.2) Definition and Key Components of Industry 4.0 110
3.2) Design Principles 115
3.2.1) Interconnection 115

3.2.2) Information Transparency 116
3.2.3) Decentralized Decisions 116
3.2.4) Technical Assistance 117
3.3) Objectives 117
3.4) Benefits 120
3.5) Main Technological Pillars 123
3.5.1) Autonomous Robots 124
3.5.2) Big Data & Analytics 125
3.5.3) Cloud Computing 125
3.5.4) Industrial Internet of Things (IIoT) 127
3.5.5) Horizontal and Vertical System Integration 130
3.5.6) Simulation 130
3.5.7) Augmented & Virtual Reality 131
3.5.8) Additive Manufacturing 131
3.5.9) Cybersecurity 131
3.6) Requirements for Industry 4.0 133
3.7) Challenges 135
4) Potential Blockchain Applications in Manufacturing 138
4.0.1) Preliminary Considerations 138
4.0.2) Definition of a Framework for Assessing Potential Blockchain Application 139
4.1) Blockchain Key Functions for Manufacturing Applications 141
4.2) Classification of Blockchain typologies based on their Characteristics 148
4.3) Requirements for Potential Manufacturing Applications 151
4.4) Blockchain Typologies for Effective Manufacturing Applications 156
4.4.1) Blockchains for Internet of Things in Manufacturing Applications 157
4.4.2) Blockchains for Horizontal & Vertical System Integration in Manufacturing Applications 159
4.4.3) Blockchains for Big Data & Analytics in Manufacturing Applications 161
4.4.4) Blockchains for Augmented & Virtual Reality in Manufacturing Applications 162
4.4.5) Blockchains for Autonomous Robots & Vehicles in Manufacturing Applications 164
4.4.6) Blockchains for Cloud Storage & Computing in Manufacturing Applications 165
4.4.7) Blockchains for Additive Manufacturing in Manufacturing Applications 166
4.4.8) Blockchains for Cybersecurity in Manufacturing Applications 168
4.4.9) Blockchains for Simulation in Manufacturing Applications 168
4.6) Final Results for Potentials of Blockchain Technologies in Manufacturing 169
4.5) Further Conclusive Considerations 174
4.5.1) Blockchain Achieved Benefits for Manufacturing Application 174
4.5.2) Blockchain Solved Challenges for Manufacturing Application 177
4.5.3) Main Blockchain Future Implementation Challenges for Manufacturing 178

5) Conclusions.....182
Annex: Literature Review Research Methodology.....187
Bibliography 191

Table of Figures

Figure 1: Working Mechanism of a Hash Algorithm 24
Figure 2: Possible Typologies of Network Structure 26
Figure 3: Timestamp Effect on the Possible Event Occurence 30
Figure 4: Implication of the Genesis Block 30
Figure 5: Representation of Two Blocks with Two Different Hashes 34
Figure 6: Representation of a Replacing Activity on a Block 35
Figure 7: An Example of Simple Blockchain Consisting of Three Different Blocks 35
Figure 8: Effects of a Violation Attempt on the Original Blockchain 36
Figure 9: Effect of the Remining Activity on the Second Block 36
Figure 10: A Distributed Blockchain Owned by Two Different Nodes 37
Figure 11: Node B's Violation Attempt on the Distributed Database 37
Figure 12: Token-based Distributed Blockchain 38
Figure 13: Example of a Couple of Private and Public Key 39
Figure 14: Effect of Using the same Couple of Key on the same Message 39
Figure 15: Transaction Signature in the Blockchain 40
Figure 16: Representation of a Distributed and Signed Blockchain 41
Figure 17: Exchange of a Block between Two Nodes 42
Figure 18: Influence of Block Size on the Propagation Delay 43
Figure 19: Propagation of a Block over the Blockchain Network 44
Figure 20: Propagation of Two Different Blocks over the Blockchain Network 44
Figure 21: Representation of Two Partitions of the Network 45
Figure 22: Representation of a Detected Forking Event and coexistence of Two Partitions 46
Figure 23: Resolution of a Forking Event and Synchronization Starting 46
Figure 24: Normal and Rare Forkings 48
Figure 25: Representation on a Hard Fork Event 49
Figure 26: The Scalability Trilemma Represented in a Mechanical Logic 50
Figure 27: Directed Acyclic Graph Representation 54
Figure 28: Representation of the Logic for Access Control 55
Figure 29: Ordinary Block Production in PoS 67
Figure 30: Example of a Malfuctioning or Malicious Activities in PoS 68
Figure 31: Reaching the Limit of One-Third of Malevolent Node in PoS 68
Figure 32: PoAh Representation in the Blockchain 76
Figure 33: Phases in a Practical Byzatine Fault Tolerance 78
Figure 34: Simple Cyclic Graph 83
Figure 35: Directed Acyclic Graph 83
Figure 36: Blockchain-Similar Directed Acyclic Graphs 83

Figure 37: Forking Event in a Directed Acyclic Graph 84
Figure 38: Complex Directed Acyclic Graph 84
Figure 39: Tangle Directed Acyclic Graph 85
Figure 40: Couples on the same horizontal level are incomparable with each other but also some other pairs at different level, such as {b} and {g}, are also incomparable. 86
Figure 41: Double Spending on a Directed Acyclic Graph 87
Figure 42: Representation of Account Balance (on the left) and Fund Transfer (on the right) in Block-Lattice Data Structure 87
Figure 43: Events Representation on Hashgraph 88
Figure 44: Comparison Between Blockchain and Hashgraph 89
Figure 45: Round Creation and Election Starting 89
Figure 46: Election Mechanism for Reaching Consensus and Confirming Events 90
Figure 47: Representation of a Sidechain Network with Three Sidechains 93
Figure 48: Decentralization of Factory in Industry 4.0 with Blockchain. Adapted from (Rüßmann, et al., 2017) 100
Figure 49: Porter's Value Chain. Adapted from (Porter, 1985) 102
Figure 50: Single modular cells in SMSs. 113
Figure 51: Interconnection between cells in SMSs. 113
Figure 52: The whole physical system is represented and controlled at application level. 114
Figure 53: Design Principles for Industry 4.0 (Hermann, Pentek & Otto, 2016) 115
Figure 54: Main Technologies in Industry 4.0 (Rüßmann, et al., 2017) 124
Figure 55: Framework for the Assessment of Blockchain Application in Manufacturing (Author's Own Finding) 140
Figure 56: Focus on Functions in the Framework (Author's Own Finding) 141
Figure 57: Classification of Blockchain Functions (Author's Own Findings) 141
Figure 58: Focus on How Functions Satisfy Requirements in the Framework (Author's Own Finding) 147
Figure 59: Focus of What Blockchain Types Enable Certain Functions in the Framework (Author's Own Finding) 148
Figure 60: Focus of Which Requirements each Manufacturing Application Needs in the Framework (Author's Own Finding) 152
Figure 61: Application of the Results over the Whole Framework (Author's Own Findings) 156
Figure 62: Level of Integrability of Blockchain with Main Technologies of Industry 4.0 (Author's Own Findings)Table 21: Results for Potential Blockchain Application in Manufacturing (Author's Own Findings) 171
Figure 63: Level of Integrability of Blockchain with Main Technologies of Industry 4.0 (Author's Own Findings) 172

Figure 64: Potentiality of Application of Blockchain in Manufacturing with Each Technology in Industry 4.0 (Author's Own Findings).....173
Figure 65: Literature Review Research Process..... 189
Figure 66: Distribution of Documents over Years from 2009 and 2018..... 189
Figure 67: Google Trends Results regarding the Blockchain Keyword 189
Figure 68: Documents Classification based on Three Main Categories 190

This page is intentionally left blank

Table of Tables

Table 1: Comparison between different consensus algorithms 81
Table 2: Collection of Possible Definition of Industry 4.0 111
Table 3: Collection of Benefit of Industry 4.0 120
Table 4: Collection of Challenges of Industry 4.0 136
Table 5: Blockchain Functions Satisfy Manufacturing Requirements in Industry 4.0 (Author's Own Findings) 147
Table 6: What Blockchain Characteristics Enable Certain Functions (Author's Own Findings) 151
Table 7: Acronyms for Interpreting the Table 6 (Author's Own Findings) 151
Table 8: Potential Blockchain Manufacturing Application Obtained from the Literature Review (Author's Own Findings) 152
Table 9: Which Requirements Each Manufacturing Application Need – First Part (Author's Own Findings) 154
Table 10: Which Requirements Each Manufacturing Application Need – Second Part (Author's Own Findings) 155
Table 11: Blockchain Typologies for IoT Manufacturing Application (Author's Own Findings) 157
Table 12: Blockchain Typologies for Hor. & Vert. Sys. Int. Manufacturing Application (Author's Own Findings) 159
Table 13: Blockchain Typologies for Big Data & Analytics Manufacturing Application (Author's Own Findings) 161
Table 14: Blockchain Typologies for AR & VR Manufacturing Application (Author's Own Findings) 162
Table 15: Blockchain Typologies for Robots & Vehicles Manufacturing Application (Author's Own Findings) 164
Table 16: Blockchain Typologies for Cloud Manufacturing Application (Author's Own Findings) 165
Table 17: Blockchain Typologies for Additive Manufacturing Application (Author's Own Findings) 166
Table 18: Blockchain Typologies for Cybersecurity Manufacturing Application (Author's Own Findings) 168
Table 19: Blockchain Typologies for Simulation Manufacturing Application (Author's Own Findings) 168
Table 20: Results for Potential Blockchain Application in Manufacturing (Author's Own Findings) 171

Figure 62: Level of Integrability of Blockchain with Main Technologies of Industry 4.0 (Author's Own Findings)Table 21: Results for Potential Blockchain Application in Manufacturing (Author's Own Findings)..... 171
Table 22: Requirements distribution in potential Blockchain manufacturing applications. 184
Table 23: Most useful Blockchain architecture for Manufacturing applications 185
Table 24: Consensus Algorithm usage in potential Manufacturing application 186

Table of Acronyms

AGV	Automated guided vehicle
BaaS	Blockchain-as-a-Service
BGP	Byzantine General's Problem
BFT	Byzantine Fault Tolerance
C	Consortium Blockchain
CPS	Cyber-Physical System
dApp	Decentralized Application
dBFT	Delegated Byzantine Fault Tolerance
dPoS	Delegated Proof of Stake
dPoW	Delayed Proof of Work
fBFT	Federated Byzantine Fault Tolerance
H	Hybrid Blockchain
IIoT	Industrial Internet of Things
IoS	Internet of Services
IoT	Internet of Things
Lo	Logic-Oriented Blockchain
lPoS	Leased Proof of Stake
NT	Non-Tokenized Blockchain
pBFT	Practical Byzantine Fault Tolerance
Ped	Permissioned Blockchain
Pess	Permissionless Blockchain
PoA	Proof of Authority
PoAc	Proof of Activity
PoAh	Proof of Authentication
PoB	Proof of Burn
PoBe	Proof of Believability
PoD	Proof of Devotion
PoET	Proof of Elapsed Time
PoH	Proof of History
PoI	Proof of Importance
PoId	Proof of Identity
PoR	Proof of Retrievability
PoRep	Proof of Reputation
PoS	Proof of Stake
PoSp	Proof of Space
PoSV	Proof of Stake Velocity

PoT	Proof of Time
PoW	Proof of Work
PoWe	Proof of Weight
Pr	Private Blockchain
Pu	Public Blockchain
RAFT	Reliable, Replicated, Redundant and Fault-Tolerant consensus algorithm
RFId	Radio-frequency identification
Sc & De	Scalability and Decentralization
Se & De	Security and Decentralization
Se & Sc	Security and Scalability
SMS	Smart Manufacturing System
T	Tokenized Blockchain
Tr	Transaction-Oriented Blockchain
UAV	Unmanned aerial vehicle

1) Introduction to the Research

This thesis focuses on the potential application of the Blockchain technology in Manufacturing, taking into consideration several Blockchain typologies, many manufacturing scenarios, different application benefits and possible technology constraints. In particular, the objective is to have a full knowledge about how it would be possible to develop effective Blockchain solutions and the benefits that could be achieved by manufacturers.

The *main research question* of this master thesis is:

Considering different manufacturing scenarios, application benefits and technology constraints, how the Blockchain technology could be applied in the Manufacturing field?

The research question led to the construction of three introductory sub-questions for the researching activity that helped to answer "*if the Blockchain has reason to be applied in Manufacturing*", "*how the Blockchain could be successfully applied*" and "*in which scenario the Blockchain has the most relevant impact*" in order to demonstrate the applicability of the Blockchain technology in Manufacturing and thus replying entirely to the *main research question*.

In order to answer to these complex questions, the following structured approach is followed.

In *chapter 2*, there is an introduction to the Blockchain technology, and it is described precisely what the Blockchain is and how it works. All the main elements of this technology are analysed with the particular attention to the *Consensus Algorithms*, that are essential for giving specific characteristics to the Blockchain in terms of *Security*, *Scalability* and *Decentralization*, to the mechanisms of *Access Regulation* and *Permission Control*, which establish who can see the ledger and who can write on it respectively, and to the *Smart Contracts* functionality, which is very useful for executing automatic agreements in a network that works on its own without any intermediary or third party. Then, the state-of-the-art concerning the current Blockchain applications classified by industries is provided for generating insights and understanding possible future applications in manufacturing.

In *chapter 3*, the focus is moved to the fourth industrial revolution and the resulting Smart Manufacturing Systems. The evolution of the industrial production brought to Industry 4.0 and a definition together with the key components and main design principles are examined: the objective of this chapter is to describe what are the main requirements of this

phaenomenon by taking into consideration both the challenges and benefits for manufacturing and the nine technological pillar which are shaping the modern industry.

In chapter 4, the thesis studies a collection of potential cases of application in manufacturing and it is defined a reference framework for the analysis of implementation of Blockchain-based solutions for manufacturing. The functionalities allowed by the Blockchain technologies are conceived for clarifying how they satisfy the requirements of the manufacturing applications and are established which typologies of Blockchain are able to offer specific functions. Hence, it is proposed a classification of results by taking into consideration the different technologies with which the Blockchain must deal. Finally, some insights are generated on the results obtained and are delivered some future implementation challenges for Blockchain in manufacturing.

2) Introduction to the Blockchain Technology

2.1) What Blockchain Is

2.1.1) History: from the Hash-Chain to the Bitcoin Block-Chain

The first appearance of a Blockchain system dates back to 1991. It was the work described by two cryptographer, Stuart Haber and W. Scott Stornetta, in the attempt of implementing a system where document timestamp and authenticity could not be tampered.

Their work (Haber & Stornetta, 1991) had a structure different from the actual Blockchain System. However, they laid the basis for the modern Blockchain. Everything started with a modest problem:

"How to guarantee that a document is maintained untampered in term of timestamp and content?"

The simplest solution answered to this question in an unsatisfactory way: it was possible to send every document to a third company that stores the data in a "*Digital Safety Deposit Box*" which guarantee that not a single bit of the document was altered is both terms of timestamp and content.

Nevertheless, the aforementioned approach, raised up the privacy problem but, in particular, doesn't avoid the manipulation (or damage) of data during the transfer of data to the third party or memorization itself.

Hence, Haber and Scornetta developed a system in which initially a document is submitted to an algorithm of cryptographic hashing which produce a univocal ID for that document: every attempt in manipulating the data, will result in a tampered ID when the document is checked again with the same hashing algorithm.

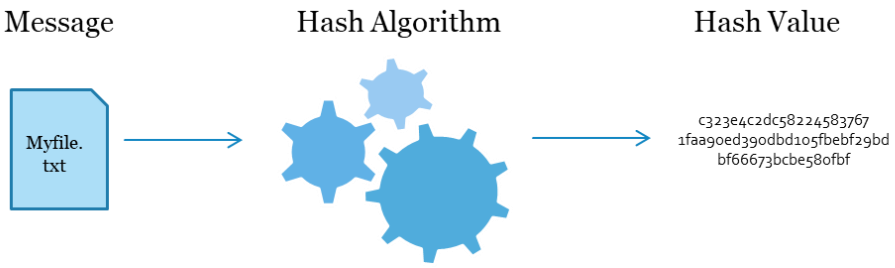


Figure 1: Working Mechanism of a Hash Algorithm

Then, they introduced the concept of digital signature, used for identifying in a univocal way the writer of the document. In this way, it was possible to send just the cryptographic hash to the digital service provider which digitally signs again the hash and stores this information in its private ledger.

At this point they effectively created the ancestor of Blockchain: while nowadays hashes are put inside a public ledger called "the Blockchain", in the '90 Haber and Stornetta understood that using the most important journals of that period was an excellent way to publicly share these hashes. But how did they do it?

In 1994, they launched Surety, a timestamp service which guaranteed the "Absolute Proof" of every digital document inside the digital databases which was composed by a "Hash-Chain" in which were collected all the hashes sent by clients to Surety. This created an immutable record of all Surety's hashes. No one was able to modify a single hash, but Surety.

How to guarantee that the Hash-Chain is not internally manipulated by the service provider? Every week, the overall amount of hashes inside the database was made public by creating a small section called "Notices & Lost and Found" in the New York Times. Surety published not all the hashes in the chain, but only a single hash of all the hashes collected inside the whole hash-chain. With this mechanism, it was impossible for everyone (likewise for Surety) to change the timestamp or the content of the documents sent to the company. The only possibly could be to produce more than 570.000 newspapers per day and diffuse in a speared way with a tampered hash in order to proliferate the counterfeit hash related to modified documents…

As affirmed also by Vitalik Buterin, cofounder of Ethereum, *"the more realistic attack vector would be to make fake newspapers with a different chain of hashes and circulate them more widely. Still very difficult though"*, this mechanism was very effective because an outbreak would require a very difficult attack with a lot of resources needed.

The first real appearance of Blockchain architecture was presented many year later the Haber & Scornetta's work. Under the pseudonym of Satoshi Nakamoto, this developer explained in its paper (Nakamoto, 2009) the Blockchain structure, taking inspiration from the Hash-Chain. Nakamoto proposed this block-based design as a core component of the crypto-currency Bitcoin which was deployed the following year.

2.1.2) Main Elements of a Blockchain

A Blockchain is nothing more than a distributed and immutable digital ledger system which contains a record of all the transactions occurred across the participants of the network.

2.1.2.1) Centralised, Decentralised, Distributed systems

When talking about a network, it is needed to refer to a collection of devices or system, that are called nodes, which are all together connected in order to share some data or resources between them. There are basically three main possible kinds of network which give

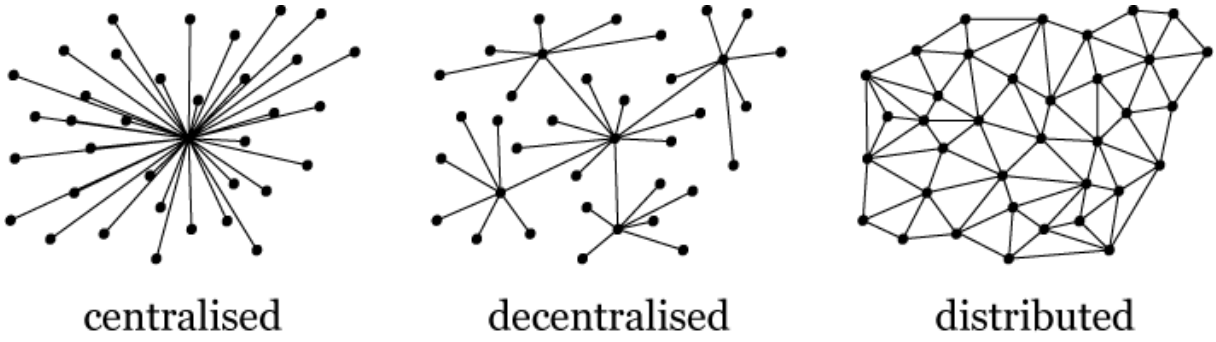


Figure 2: Possible Typologies of Network Structure

substantial differences to the entire structure:

- **Centralized Network =** a central node is responsible for maintaining the network. This node is the point of reference for every information shared between all the participants in the network. This structure has the critical issue of having a single point of failure: just a unique copy is stored in the network owner node (the central node). In addition to this, every single request coming from the rest of the network can be managed only by the owner and this leads to an access problem to resources because a high computational capability is required for a timely response. Notwithstanding, the network is considered more secure than the other configuration.
- **Decentralized Network =** in this network architecture, the main issue of the single point of failure is prevented. In fact, here multiple central nodes have a copy of the resources and in case of failure of a single or multiple node, data can still be accessible from all the others working nodes. Multiple central nodes mean also more computational power and higher throughput with less speed problems.
- **Distributed Network** = this is the case of absolute zero centralization: not a single node owns the network, and everyone have a copy of the resources with the ability to share them to other participants in the network. Here, the main issue become the security because every node is responsible of its data and therefore is able to spread counterfeit data. This is the underlining architecture behind Blockchain network.

In Blockchain network every user downloads a copy of the master ledger and interact with the all the participants in the distributed Blockchain network, sharing information and completing transactions. This configuration is necessary for guaranteeing an entirely decentralized system that ensures no dependence on each other and, in particular, eliminates completely the necessity of a third-party system.

2.1.2.2) Blocks in the Blockchain

Blocks are the main features introduced by Nakamoto while designing the public ledger network: they replaced the concept of documents used in the Haber & Scornetta work.

Behind the block there is the answer to the security issue and trust requirement of a distributed network.

Every Blockchain starts with the Genesis Block. Each block store inside this information:

1. **Index** = it is the position of the block in the chain. The genesis block has an index equal to 0. The following block will have an index of 1, and so on…
2. **Timestamp** = it is the record of when the block was created. It is of extreme importance because helps to keep the Blockchain in order and assure the past of a block.
3. **Hash** = it is a precise combination of letters and numbers and its alphanumeric value uniquely identifies data on the Blockchain. It represents the digital fingerprint of data.
4. **Previous Hash** = it is the hash of the previous block. Only the genesis block's previous hash is 0 because there is no previous block.
5. **Data** = each block can store a certain amount of data inside.
6. **Nonce** = it is the number used to find a valid hash because in order to find a valid hash it is necessary to discover a nonce value that will generate a valid hash when used with the remaining part of information from that block. This process is called Mining.

2.1.2.3) Mining

The process of determining the nonce value to be used for generating valid hashes is called Mining. The mining process starts with the value of "0" and this nonce is incremented by "1" until a Valid Hash is found.

A Valid Hash for a Blockchain is a hash that meets certain requirements defined for the Blockchain. For example, could be required that a hash, to be considered valid, needs a certain amount "N" of zeros at the beginning of the hash: only hashes with "N" zero in the beginning are considered valid and generate effective blocks for the chain (another requirement could be to find a hash value that is lower than the given difficulty target: the

mining mechanism does not change). In this instance, the number of starting zeros required represents the *difficulty* of the mining problem because the more zero are required, the more nonces need to be computed and verified before determining a valid hash. All this means that more computational power and more time are required for mining a new block: this mechanism is also known as *Proof-of-Work (PoW)*. Why does this matter?

It matters because it keeps the Blockchain immutable.

Considering having a Blockchain composed by three blocks: $\mathbf{1} \rightarrow \mathbf{2} \rightarrow \mathbf{3}$, and someone wants to change data on Block 1. This is what happens:

- Data are changed on Block 1 due to the manipulation attempt.
- Block 1's hash changes because data itself is used to calculate the hash.
- Block 1 becomes invalid because now its hash no longer has N leading zeros.
- Block 2's hash changes for the reason that Block 1's hash was also used to calculate Block 2's hash.
- Block 2 becomes invalid too since its hash no longer has N leading zeros.
- Block 3's hash changes for the reason that Block 2's hash was used too to calculate Block 3's hash.
- Block 3 becomes invalid, as its hash no longer has N leading zeros, and so on.

The required mining for all the blocks after the Block 1 depends on the difficulty introduced by the puzzle problem caused by the request of N leading zeros. Since new blocks are always being added, it's nearly impossible to mutate the entire Blockchain with standard computational system or, generally, with less than the 51% of the network's computing power.

2.1.2.3.1) Rewards and Transactions Fees

The Bitcoin Blockchain uses two different typologies of financial reward to incentivize users to mine the blocks. Rewards are given to the first miner that find a hash which meet the criteria set for the difficulty target: this miner is able to mint new Bitcoins (the number of yearly new Bitcoin is set by the Bitcoin protocol and decreases every year) and receive them when the block is effectively added to the chain. This is why in every block the first transaction is a coin-creation transaction: this enables to generate a *token-based Blockchain*. The reward for the block generation is used to incentivize faithful behaviours for the reason that the coin-creation transaction will only be valuable if it is accepted by others node which maintain the network. Together with the rewards, there are the transaction fees: when a user sends a transaction, generally another node in the network (i.e. a miner) will validate the block. Hence, some fees are included in the transaction and paid by the user for incentives other node to mine and validate its transaction: the higher is the fee, the higher will be the

number of miners interested in validating the transaction and thus the lower will be the confirmation time.

2.1.2.4) Hash Value

A hash is simply an alphanumeric string composed by several numbers and letter. Its alphanumeric value identifies data in a unique way and can be recognized as the digital fingerprint of data. A hash is generated through a hash algorithm which guarantee some properties for the hash:

1. Hash has a fixed length
2. Same data always maps to same hash
3. Different data always maps to different hash (within practical limitations)
4. A hash is easy to compute
5. It is infeasible to convert hash to data
6. A small change in data leads to a large change in hash

2.1.2.4.1) Hash Algorithm: SHA256

A hashing function takes data as input, condenses it, and returns a unique fixed length hash:

$$f\,(data) = hash\ value$$

The hash is used as a digital fingerprint of the entire block: in this case, the data is equivalent the combination of index, timestamp, previous hash, block data, and nonce.

$$f\,(index + timestamp + previous\ hash + data + nonce) = hash\ value$$

For instance, replacing the values for a genesis block it is possible to get:

f (0 + 1551621376000 + "0" + "This string is a few data example" + 3028) = 00028hs28sj1…

Bitcoin Blockchain uses the SHA256 Hashing Algorithm, which is one of the standard protocols for Secure Hashing Algorithm. It is the successor of the SHA160 which was designed by the United States National Security Agency and published in 1995 and was considered the main algorithm for hashing for decades. However, several researches has showed the weaknesses of SHA160 and encouraged a revaluation. (Stevens, Bursztein, Karpman, Albertini, & Markov, 2017) have recently released a paper for describing the first ever successful SHA160 collision, demonstrating that two different PDF files generate the same identical hash. Therefore, SHA256 is now the standard for hashing since its hash length is almost the double of the predecessor (256bit vs. 160bit). It has a number of different hashes equal to 2^{256}: this number far exceeds the number of grains of sand there are in the entire world…

For this reason, at the moment, it is infeasible to produce a collision with the actual available technology and then SHA256 is considered a very unquestionable hashing algorithm for guaranteeing the security inside a Blockchain architecture. Every manipulation will produce a different hash function and there is no possibility to find an alternative data, which produce the same output of the replaced one.

2.1.2.5) The Timestamp

The Timestamp is one of the core blocks properties that allow establishing the origin of transaction from a timing point of view. It solves the problem of guaranteeing that a certain event (or transaction, in the Bitcoin case) happened before a precise period: the timestamp, in fact, represents the time at which an event is recorded by a system and not the time of the event itself. Therefore, it is not possible to know exactly the moment in which transactions happened but only the timestamp in which the block was generated. However, generally a timestamp should be close to the time of the event and on the Bitcoin Blockchain it is possible to estimate it considering the average mining time (of 10 minutes). Still, there is no assurance about the exact timing and, in addition, when a transaction in made offline, there is no possibility to understand when it will be executed.

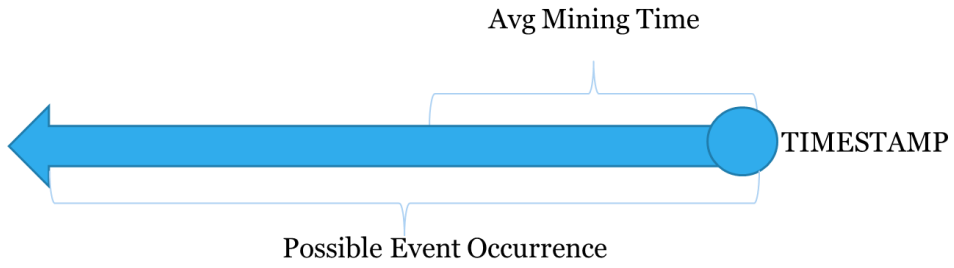


Figure 3: Timestamp Effect on the Possible Event Occurence

Hence, timestamp can guarantee only that an event is happened, for sure, before a certain data. It is curious that in the Bitcoin genesis block appears a reference to “The Times” of January 3rd, 2009. This was probably intended as a proof that the block was created on or after that data and not before: no one mined crypto values before the "C*hancellor on brink of second bailout for banks*".

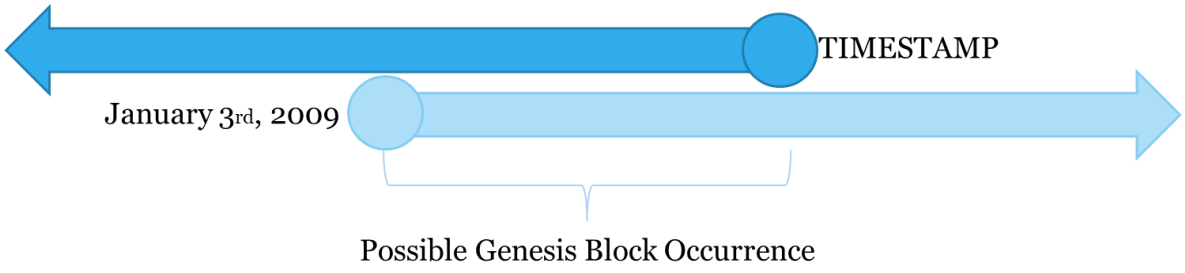


Figure 4: Implication of the Genesis Block

On the Bitcoin Blockchain, the timestamp is a sequence of characters and give date and time of day accurate to a second. Timestamp is encoded using the Unix Time format.

The Unix Time is the number of seconds that have elapsed since January 1, 1970 (midnight UTC/GMT). Many Unix systems store dates as a signed 32-bit integer (4 bytes), which might cause problems on January 19, 2038 (known as the Year 2038 problem): after that data, Unix timestamps will overflow, and the counter will restart from zero and all the succeeding blocks, in a Blockchain, will be invalid. This will happen also to the Bitcoin because the Blockchain header contains only 4 bytes, but, due to fact that Bitcoin are using unsigned integer, the expiration date is postponed by other 68 years. Several solutions are provided for the Year 2038 problem and the most compelling is the reallocation of some bit of the block for extending timestamp: this will require a modification of the Bitcoin protocol.

2.1.2.6) The Genesis Block

The Genesis Block, in whatever Blockchain, represents the first block of the entire chain. It is of extreme importance because inside it all the variables necessary to recreate the following blocks are defined. The block data structure cannot differ from a block to another in order to guarantee that the Blockchain works properly. The genesis block is the only one that has in the previous hash section a value equal to zero: this is a special condition which inform that this block has not any previous block to which make reference. Usually, in its original inception by Nakamoto, the genesis block has an index equal to 1. However, modern versions of Blockchain count the genesis block with 0. The explanation to this difference comes from the problem of "Unspendability" in the first Bitcoin block:

"The first 50 BTC block reward went to address 1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa, though this reward can't be spent due to a quirk in the way that the genesis block is expressed in the code (this may have been intentional)."

This is due to the fact that when a node in the Blockchain starts up, it initializes its copy of the block database alongside the genesis block and then begins the synchronization process. For some reason, Satoshi decided not to add the Coinbase transactions from the genesis block to the global transaction database. Thus, all the nodes in the network would reject the block. It is not sure if this was done on purpose or if it was simply an oversight, in any case, it is forever bound to its receiver. The only way to make the amount spendable should be to modify the current version of the Bitcoin Core client in which the genesis block is hard coded. Later Blockchains allow the possibility to use effectively the first genesis block considering it equal to the others. This difference is highlighted giving to the index of the genesis block a value equal to 0 and not 1.

Another peculiarity of the genesis block is that, in a Blockchain, only beyond this block there can be forks. No previous forks are possible. It is the only block which is present in all branches on the chain: for all other following blocks, it is not clear which branch will grow faster or if it has grown enough hence it is not sure if a block will end up in the actual Blockchain. Theoretically, even the second block could be challenged and modified by another longer subdivision of the chain. The genesis block is unique and every Blockchain have only one of it.

2.1.2.7) Digital signature: Public & Private Key Pairs

As stated by (Merkle, 1990), a digital signature is a one-way function which is easy to compute but whose inverse is very difficult to compute, with the capability to generate a prove of authenticity of a document. (Dods, Smart, & Stam, 2005) clarified that the digital signature is a function "f" that has a simple working mechanism: when the proprietary of a document "P" digitally signs a document "D", the mechanism of the digital signature will provide a value "S" which is the signature of the document. Any modification of "P" or "D" will change the value "S" if computed through "f".

$$Digital\ Signature = f_P(D) = S$$

In particular, a digital signature guarantees these following strong properties:

- Given any value "S", it is computationally impossible to find the original document "D" such that $f_P(D) = S$ (inverse function does not exist → $f^{-1}(S) = ??$).
- Given any document "D", it is computationally infeasible to find a different document "D*" such that $f_P(D) = f_P(D^*) = S$

In the digital signature, it is fundamental the role of the private and public key for generating a valid signature system (Hellman, November 1978). (Diffie & Hellman, 2006) explained the results of their work after years spent on the elaboration of the Diffie–Hellman–Merkle key exchange algorithm based on the Ralph Merkle's contribution to the invention of public-key cryptography which becomes later the basis for the Blockchain ecosystem: *Elliptic Curve Digital Signature Algorithm* is nowadays the cryptographic algorithm used by Bitcoin to ensure that transactions can only be executed by their legit owners.

ECDSA is an anonymous key agreement protocol that allows two parties, each having an elliptic-curve public and private key pair, to establish a shared secret over an insecure channel (the Bitcoin Network). This shared secret may be directly used as a key, or to derive another key. The key (private), or the derived key (public), can then be used to encrypt subsequent communications using a symmetric-key cipher.

With the ECDSA, the Blockchain promise the digital signature, based on the public key encryption and very few elements are needed:

- **Private Key**: this is a secret alphanumeric combination which is known only by the person who generated (generally randomly) it.
- **Public Key**: another alphanumeric combination which correspond univocally to the private key. This key must be calculated from the private key, nonetheless the opposite calculation is impossible (from the public key is impossible to get the private key).
- **Signature**: it is the hash result of the usage of a private key on a given transaction.

When a transaction is made, the owner of the transaction signs it with its private key: this generates the signature. It is then used its public key to verify that the original transaction generated exactly the same hash of the signature. In fact, only a couple of public and private key can generate the same signature.

Technically, in the Bitcoin's public key cryptography, it is used the SECP256K1 parameter to assure an efficient cryptography. Even if it was almost never exploited before Bitcoin, it recently became popular. This parameter, which is used for the elliptic curve domain, has several useful properties:

- It is constructed in a special non-random way which allows an efficient computation
- It is more than 30% faster than other curves
- SECP256K1's constants were selected in a predictable way, which significantly reduces the possibility that the curve's creator inserted any sort of backdoor into the curve.

Nowadays, this particular digital signature system is used not only by Bitcoin but also for other Blockchain like Ethereum, EOS, Litecoin, Dash, Dogecoin, Zcash.

2.2) How Blockchain Works

All the aforementioned elements analysed in the previous sections are just the basic foundation for a full working Blockchain system. Taking as a reference the first Nakamoto framework, on which is based the Bitcoin cryptocurrency, it is possible to fully understand the characteristics of those Blockchain systems and all the resulting pros and cons of this technology.

2.2.1) Stepping through key elements of Blockchain:

1) **SHA256 Hash**

   Every single data inside in the Blockchain is subjected to the SHA256 algorithm. Different information put in the block leads to different hash value. Same data will generate always the same hash: very small differences in data will generate big differences in the hash. Whatever kind of information, dimension, type, etc. we put in the block, results always in a hash of the same length. It is not possible to guess the original data behind the hash and is practically impossible, still not infeasible, to have to different data that generate the same hash (*Figure 5*).

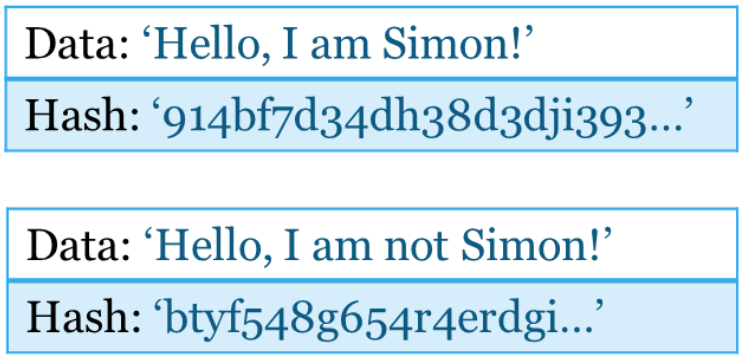


Figure 5: Representation of Two Blocks with Two Different Hashes

2) **Blocks**

   Inside a single block, data is formatted into different data section. Here a block ID number appear and classify each block in a unique way giving a chronological dimension to block. A nonce is put together the data field and very similarly to the previous step, all this information, the whole block, is passed through the algorithm which gives back a hash. Each hash must begin with a fixed number of zeros which is decided arbitrarily for proving that the block is effectively signed and is part of the Blockchain.

   Every attempt in replacing something in the block sections will generate a different hash (*figure 6*).

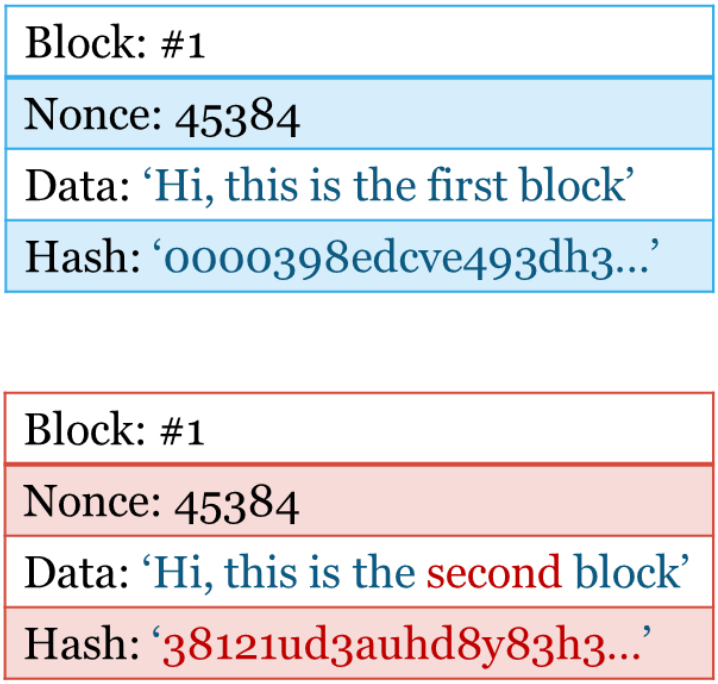


Figure 6: Representation of a Replacing Activity on a Block

3) The Blocks Chain

A Blockchain is a chain of these blocks that are linked together simply adding another block field: the previous hash section.

This section contains the hash of the previous block of the chain and so each block mentions the block before it. Only the genesis block, the first of the chain, contains as previous hash a bunch of zero in order to indicate that no block exists before it (*figure 7*).

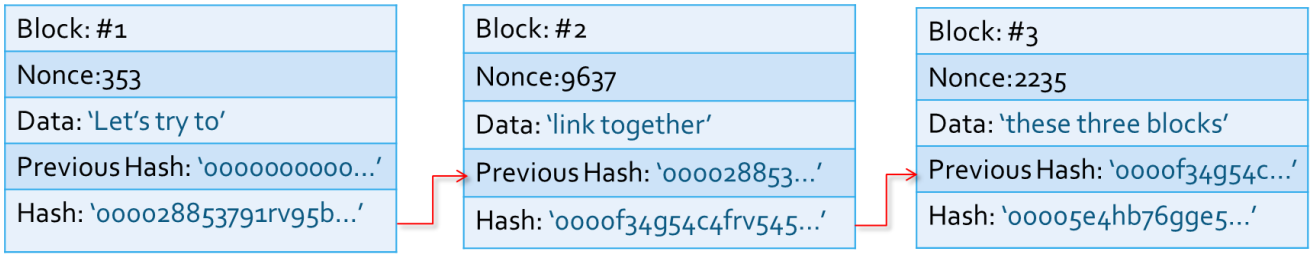


Figure 7: An Example of Simple Blockchain Consisting of Three Different Blocks

If something is changed in a block, it is always necessary to 'remine' the block (in order to validate it and get again the same number of zeros) but then it violates the hash contained in the following block generating a counterfeit Blockchain (*figure 8*).

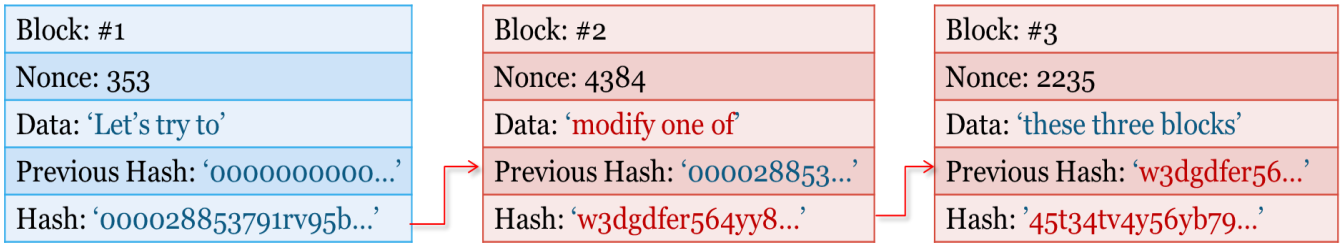


Figure 8: Effects of a Violation Attempt on the Original Blockchain

Even if the block is remined (a new nonce is obtained, the hash in the following block will not coincide and consequently need to be mined again also the following block and all the subsequent blocks present in the chain (*figure 9*).

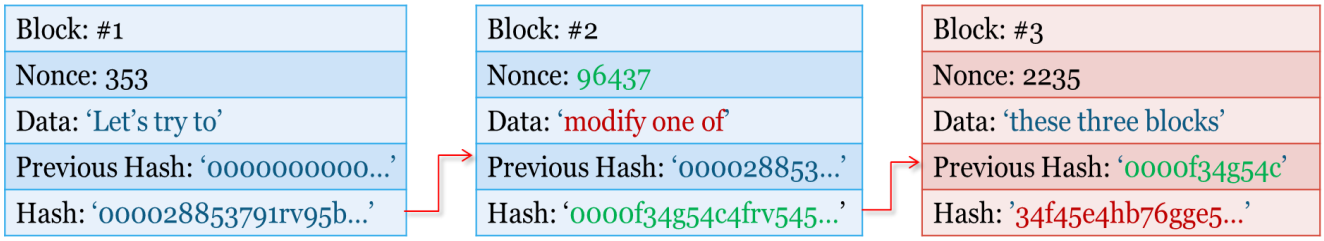


Figure 9: Effect of the Remining Activity on the Second Block

Consequently, every attack in the Blockchain violates the connection between all the following blocks and requires a massive computation effort for mining all the new blocks.

4) Distributed Blockchain

In a distributed Blockchain is possible to spot if a Blockchain in effectively modified in a certain point.

Every node shares the entire ledger in which is contained the Blockchain. The higher the number of nodes, the higher is the number of copies of the distributed ledger (*figure 10*).

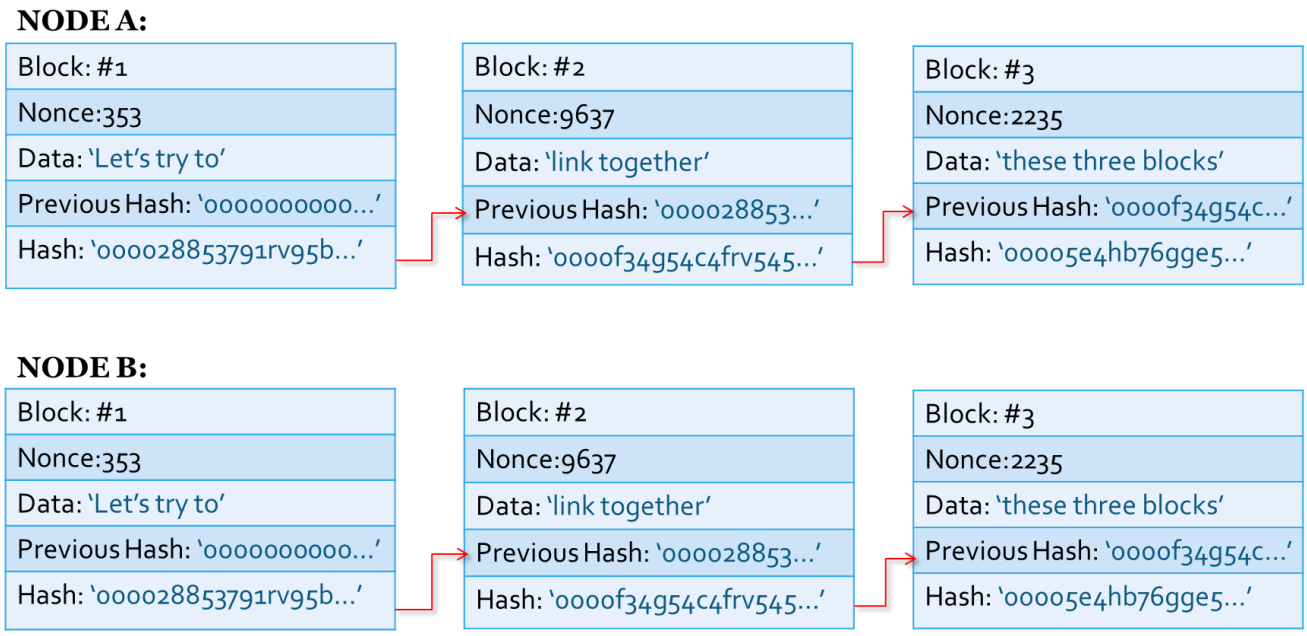


Figure 10: A Distributed Blockchain Owned by Two Different Nodes

When a node modifies a block, even if it is able to remine all the following blocks in the chain, just observing at the last hash in its Blockchain, it will not agree with the one contained in the others Blockchain and thus it will be an evident attempt of manipulation of data. Of course, in the distributed network will win the copy of the ledger that is shared by more nodes. This leads to the problem of the 51% power (*figure 11*).

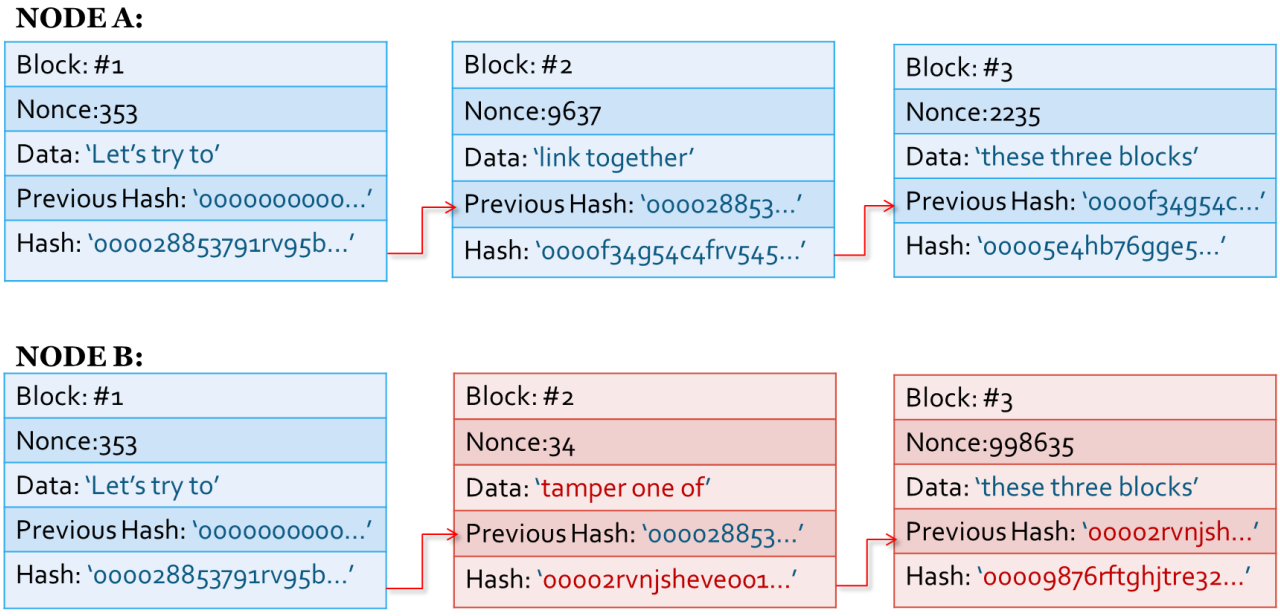


Figure 11: Node B's Violation Attempt on the Distributed Database

5) Token-Based Distributed Blockchain

Until now, anything in the block refers to tokens, coins or something similar to this. Hence, it is introduced a token transaction system with an additional Coinbase section inside the blocks and some data fields used for users' transactions (*figure 12*). The economic value of token is referred to the value of the virtual coin. Every block contains a set of different transaction in which a certain amount of token is transferred from a peer to another: the first transaction is generally a coin-creation transaction (i.e. the one that generates new coins/tokens for the Blockchain), the following transactions refers to the coins that are transferred by users inside the network. Any kind of modification in term of token or peer always mismatches the hashes of the blocks.

In the Blockchain is not present an account balance but are just stored all the transaction inside the entire network. This leads to different problems: does a peer have the amount of token it is transferring? How can be sure that a coin is not double spent?

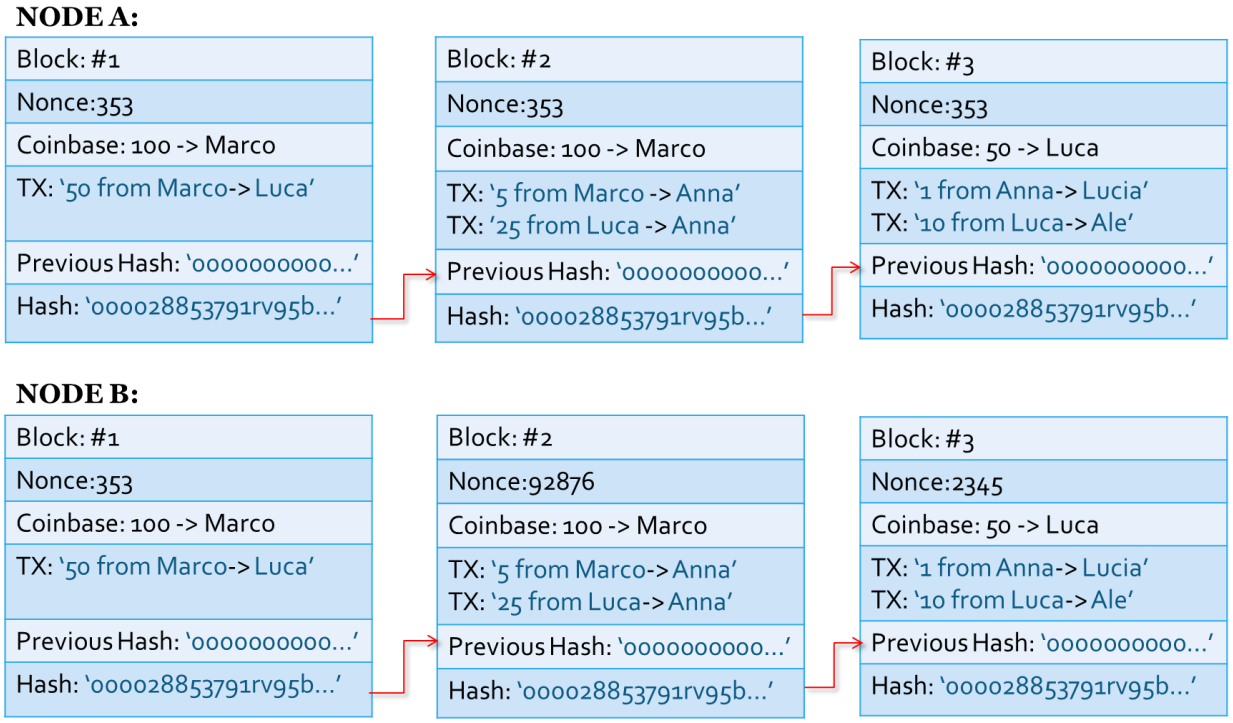


Figure 12: Token-based Distributed Blockchain

6) Public & Private Key Pairs

Until now, a Blockchain done like this would make possible that someone make a transaction on behalf of someone else: everyone would be able to add a new block and create transactions of his favour. In addition, the identity of every node is completely public and there is no possibility to cover it. An effective protection to these problems is made thanks to another cryptographic primitive: the public & private key pairs.

A private key is an alphanumeric combination of a fixed length and is known only by the owner of the key. Every private key is computed through a hash algorithm, which generates a unique related private key and is not possible to go back to the private key starting from the public one. Of course, private key must be kept private; the public one can be shared to everyone.

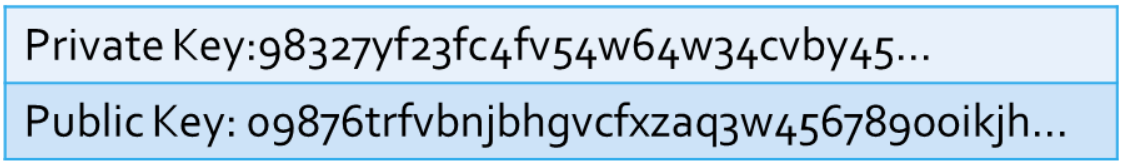


Figure 13: Example of a Couple of Private and Public Key

7) Message Signature

The couple of keys is used for the message signature and, in the Blockchain, is used to sign transaction inside the blocks. Taking a message or a transaction, and computing it in the hash algorithm, through the private key, is possible to get a unique hash, which represents the message signature. Then, when this message signature is shared to someone else together with the original data, with the same algorithm, but this time using the public key, it is possible to verify the owner of the data just putting original data in the hash algorithm. The application of the public key and of the private key on the same data, gives always the same digital signature. This proves the authenticity of transactions inside the Blockchain. Everyone is then able to check the authenticity of a message, just knowing the public key of the message owner.

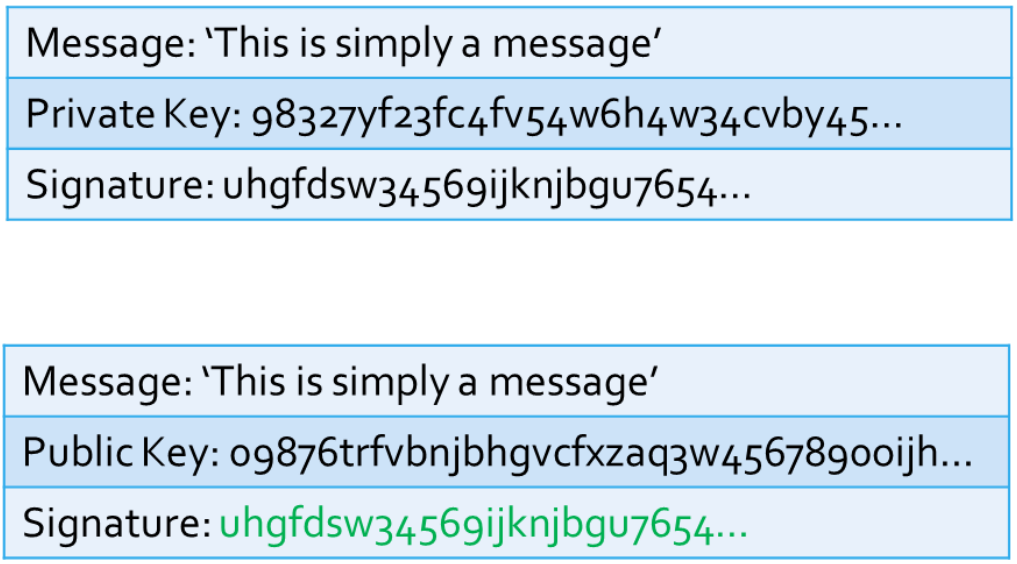


Figure 14: Effect of Using the same Couple of Key on the same Message

8) Transaction Signature

Instead of having a message, in the block we have a structured data field used for putting transactions. Each transaction contains just three information: the public key of the sender, the public key of the receiver and information regarding the transaction involved (e.g. a token transmission). The sender simply uses his private key to digitally sign the whole transaction obtaining a signature. Sending the whole message (the transaction) and the related signature, whoever is able to verify the genuineness of the transaction computing the message with the public key of the sender and comparing the two signatures obtained: they must be exactly the same. Blocks with tampered signature are automatically rejected by the system and never added to the chain.

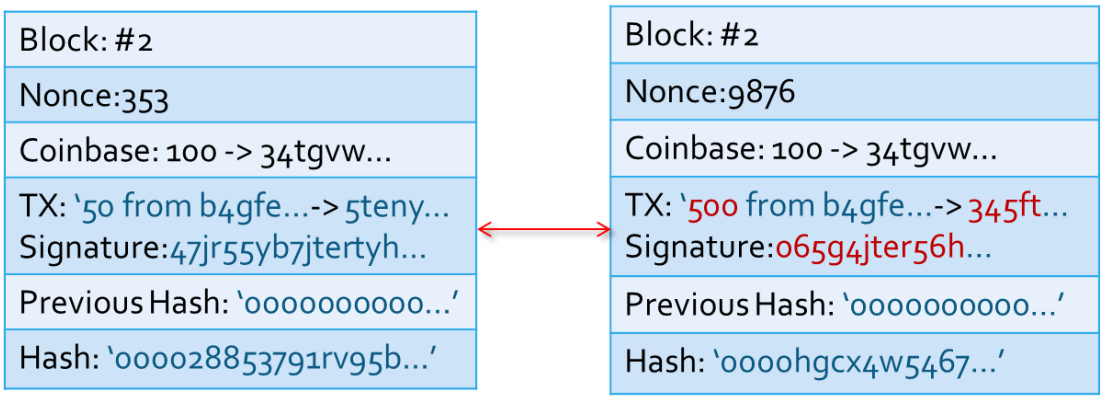


Figure 15: Transaction Signature in the Blockchain

9) Signed Blockchain

The final structure of the Blockchain has the same data sections of the step #5 but with an additional field, which is the signature field. In the blocks, just public keys are shown. This structure, like before, avoid the possibly of tampering any transactions but assure also that only genuine transactions are put inside the blocks. Even if a block is mined with not genuine transaction, just looking that the transactions signature is possible to identify which transactions are invalid. Only owners of private keys can generate valid transactions inside the blocks, and everyone can check them (*figure 16*).

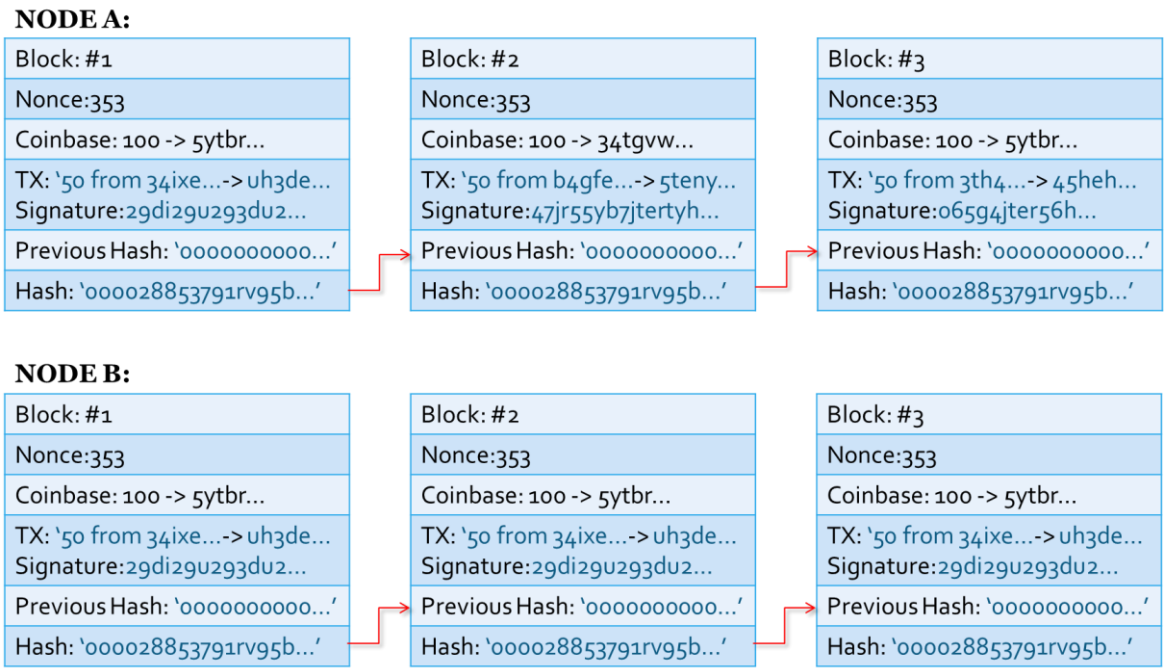


Figure 16: Representation of a Distributed and Signed Blockchain

10) Final Outputs Analysis

The Blockchains, as already design, has gained so much admiration for these reasons:

- The data is cryptographically stored inside
- It is not owned by a single entity, hence it is decentralized
- The Blockchain is immutable, so no one can tamper with the data inside
- The Blockchain is transparent, so one can track the data if they want to

These reasons furnish the three main properties of the Blockchain Technology which become the main pillars for the spreading of the Blockchain technologies:

- Decentralization
- Transparency
- Immutability.

2.2.2) Network Propagation of the Blockchain

In the first conception of Blockchain, the Bitcoin one, the network on which run the Blockchain is composed by homogenous nodes without any coordinator within them (Decker & Wattenhofer, 2013). Since the Blockchain is permissionless and, so, fully decentralized, each node has to keep a copy of the entire ledger with all the transactions and has to verify the correctness of new ones. This process is able to run in a complete absence of trust between nodes thanks to both the mechanisms of the digital signature and the proof of work.

When dealing with the network, it is necessary to clarify the topology of it: several DNS servers, which are kept by volunteers, maintain up the entire network and when a node ask for joining into the network they provide all the information needed, returning also a complete set of all the other nodes participating in the network. After the connection to the network, a node establishes who are its neighbours and attempts to retain a minimum number of open connections with other nodes all of time. In the first connection, the new node queries and obtains the newest Blockchain ledger and download an entire copy of it locally. Then every node starts updating and synchronizing its copy of the ledger with only new blocks with new transactions. In the network, the information regarding blocks & transactions is not directly shared to every node every time otherwise too many messages would be exchanged between nodes resulting in a lot of replicas of them (a node may receive the same message by different nodes). To avoid harmful congestion, when a new block is announced or discovered, a node communicates it by sending an "*inv message*" to neighbours: in this message is contained all the set of transactions hashes together with blocks hashes that have been already verified. Only when a node discovers information that it does not have yet then will ask to the inv message sender node the needed information by using the "*getdata message*" (*figure 17*).

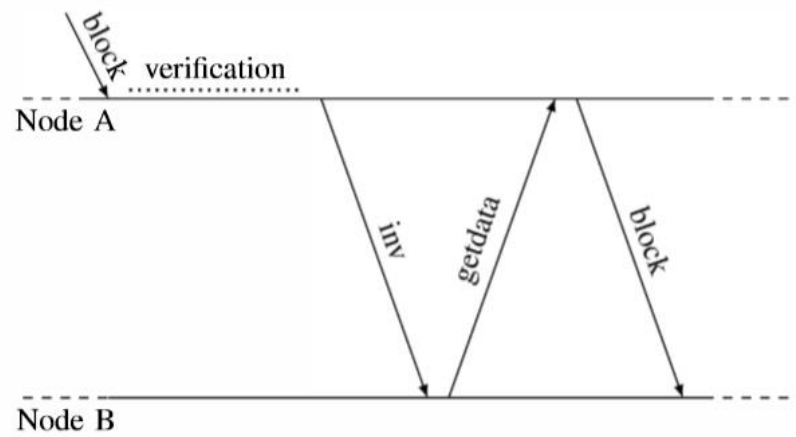


Figure 17: Exchange of a Block between Two Nodes

Of course, this broadcasting mechanism implies some *propagation delay* in the network, delay made of two different components: the *verification time* of the block or transaction summed with the *transmission time*. It is evident that the transmission time is composed by the three steps necessary for delivering successfully a block, while is less evident how these three components impact the whole transmission time. Inv messages and getdata messages weigh around just 61 bytes while an entire block could range from 500kB to 1MB: so, the impact ratio is about 1/8196 to 1/16393 and practically the propagation time is occupied for the 99% by the block delivery. This is enough for affirming that the transmission time is practically composed and depended on the block size and thus the speed of the network and the latency of it.

2.2.2.1) Block Size and Propagation Delay

The size of a block and the propagation delay in the network are correlated. The bigger is the block, the higher is the influence of the transmission time over the overall propagation delay. Since the verification time is nearly constant and does not depend on the kB of the information, it is possible to calculate the *Delay Cost (s/kB)* which the ratio between the seconds necessary for the block/transaction propagation and its relative size. (Decker & Wattenhofer, 2013) measured and analysed data regarding a sample of 10000 Bitcoin blocks discovering that, until a block size of 20kB, the delay costs more because the verification time has a higher impact over the whole propagation time, while for blocks larger than 20kB the Delay Cost is constant, and each kB adds 80ms of delay. Therefore, it is very effective to send blocks with a size higher than 20kB. Oppositely, transactions with size lower than 1kB, are very sensible to the verification time because the necessary overhead for the verification impacts far more on the size.

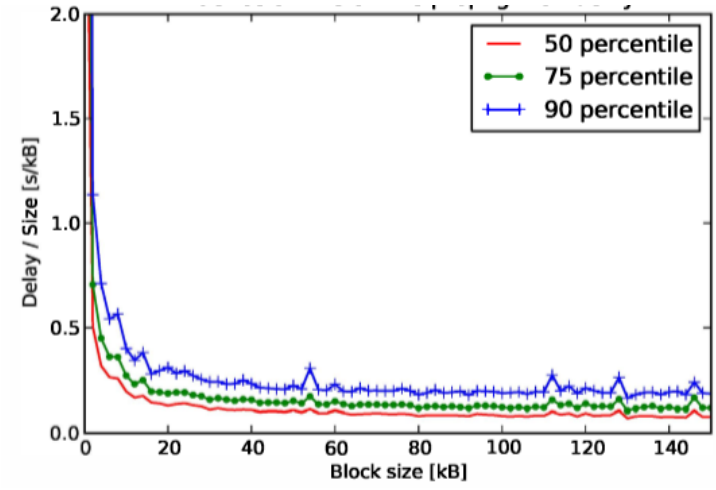


Figure 18: Influence of Block Size on the Propagation Delay

2.2.2.2) Blocks Dissemination and Forks

During the normal blocks dissemination inside the network executed by nodes, only valid transaction and confirmed block can spread over the net: everything which is proved to be invalid (wrong transaction, double spending problem, invalid signature, tampered block, etc.) is automatically rejected by nodes and not forwarded anymore (*figure 19*).

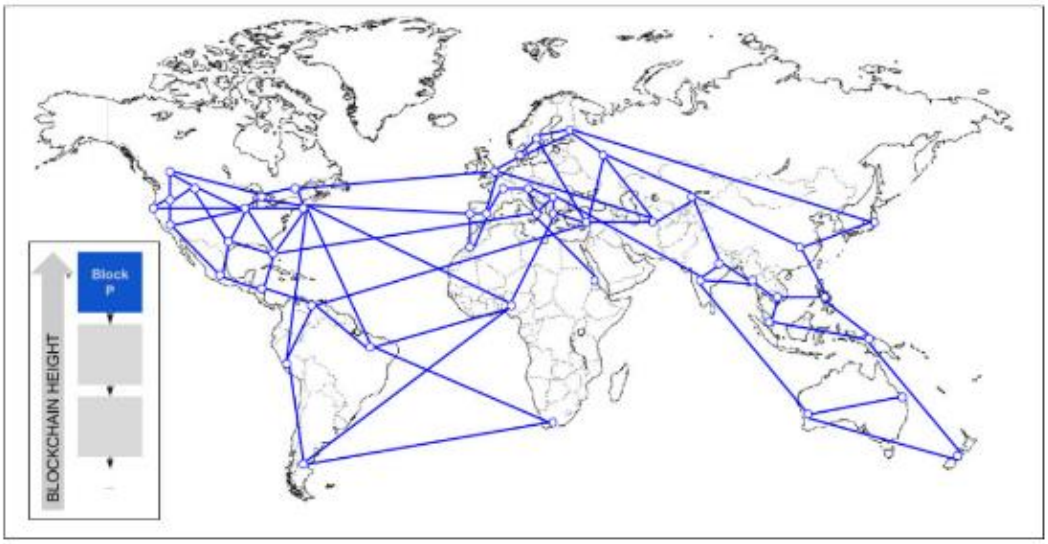


Figure 19: Propagation of a Block over the Blockchain Network

However, often may occur that simultaneously in the network starts to spread two different valid blocks because two diverse nodes discover and validate a new block. In this situation the network is rapidly split into two partitions: every partition contains the Blockchain until the height "*h*", which is the index of the last block in the Blockchain, hence contains all the blocks till the h^{th} block (the latency of the network does not permit to distribute instantaneously the new block to all the nodes, hence two blocks can be shared in the same period) (*figure 20*).

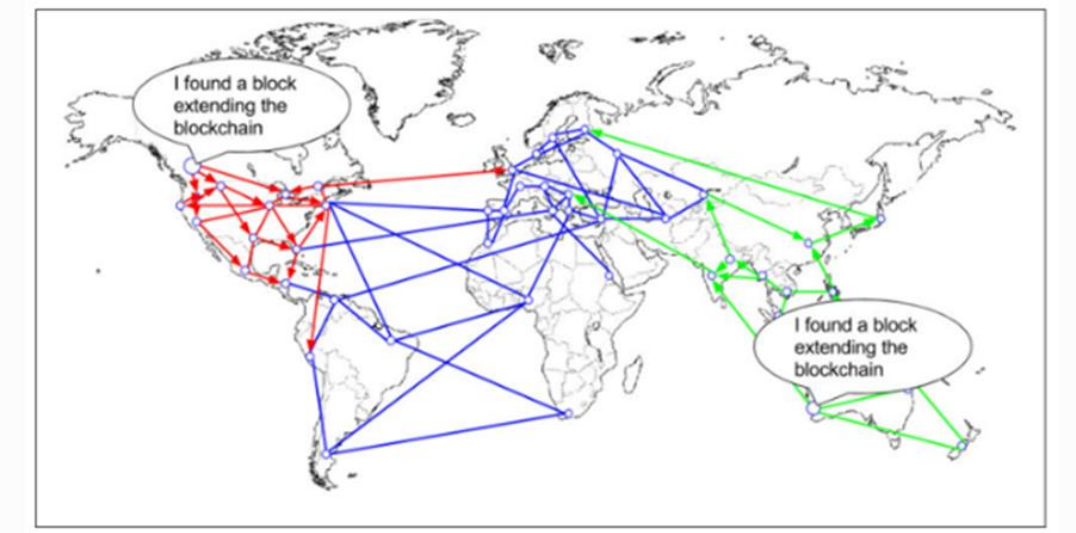


Figure 20: Propagation of Two Different Blocks over the Blockchain Network

If no other blocks are found yet, the network remains in this situation for a while. It is important to note that only the boundaries nodes between the two partitions are conscious about the presence of two conflicting blocks because these nodes on the border do not diffuse the diverse block in the other partition (note: this happens equally for the transactions propagation).

This propagation system, on one hand, has the pros of contrasting a malicious node by preventing the diffusion of malevolent transactions or blocks, on the other hand, has the cons of create a time window in which double spending attacks are not detected and a user could be defrauded (precise explanation of the phenomenon in the *paragraph 2.2.6.2.1.1*). When on the same network there are contemporary two different valid Blockchains, the correct definition for this situation is *Forking Event (figure 21)*: two (rarely more than two) partitions of the network (composed by a different number of nodes), due to the structural latency of the network, hold different Blockchains.

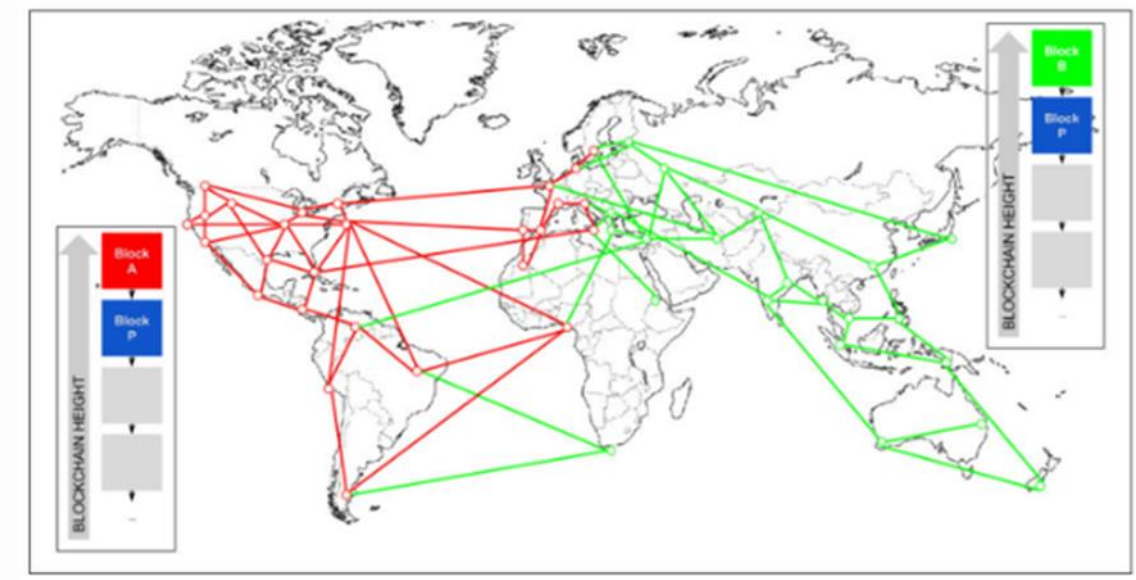


Figure 21: Representation of Two Partitions of the Network

A fork persists until a newer block which extend one of the two Blockchain is found. When this block is found, it is broadcasted to all the nodes of the network which check the block: if the block extend the chain, nodes will accept it and maintain the ledger otherwise if the block extend another chain, then it means that the Blockchain which is hold by that node is not the longest one and thus it is discarded. All the nodes with the oldest Blockchain will query the longest chain which is considered the main one. At the end of this process, all the nodes are updated and synchronized (*figure 22*).

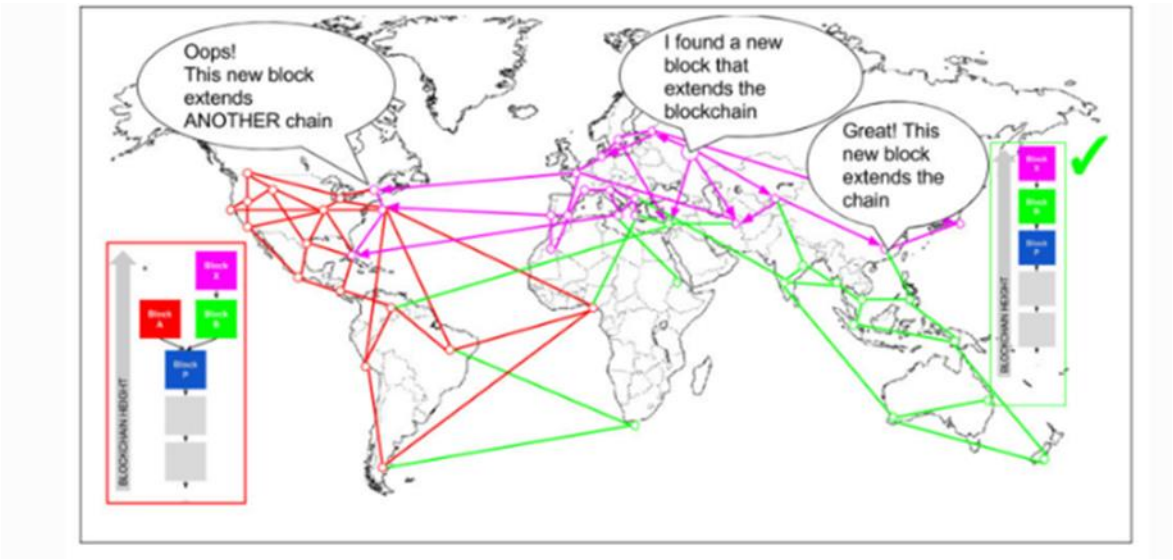


Figure 22: Representation of a Detected Forking Event and coexistence of Two Partitions

Every time an event of fork has occurred, the network has wasted time and computational power because many nodes have worked uselessly on an obsolete version of the chain. Hereafter, the lower is the probability of forking, the higher will be the speed of the network in generating blocks. Good and efficient Blockchain must have fork probability very low (note: forking cannot be eliminated in traditional Blockchain since it is structurally expected).

Figure 23: Resolution of a Forking Event and Synchronization Starting

2.2.2.3) Improving Network Propagation Speed

Considering the structural characteristic of an original Bitcoin Blockchain, its protocol has some limits on which depends the fork rate. Modifying several parameters, as suggested by (Decker & Wattenhofer, 2013), it is possible to speed up the information propagation in the network:

1. Reduce Verification Time: similarly to Segwit (*paragraph 2.2.4*), it is possible to reduce the time necessary for a block verification. Verification time is function of the block size (*previous paragraph*): the higher is the size, the more time is needed to find a proof-of-work for that block and, in addition, it is necessary to validate all the transactions inside the block. If the propagation of the block is done immediately after its validation and not after the verification of all the transaction, the block will spread faster in the network.
2. Routing Block Enhancement: if the broadcasting mechanism is modified and the inv messages are sent immediately after the validating of a block, the getdata messages for block will immediately be sent and queued till the new block is mined. Even if blocks will be broadcasted prompter, malicious node could trick the network by sending lots of inv messages without broadcasting then any block and letting other nodes waiting for them (however the impact could be low, and it is already possible by creating millions of fake transactions and publicising them to the net).
3. Increase the Connectivity: reducing the physical distance between nodes, by introducing a central communication hub, will speed up the propagation of messages and thus blocks and transactions. This solution may be the less effective and may obviously create some degree of centralization in the network.

2.2.3) Fork Classes and Hard & Soft Types

It the previous paragraph, it was clarified the origin of the phenomenon of forking. However, in every Blockchain, the reasons behind a fork could be very different because not all the forks are equal. First of all, it is important to recognize two different classes of forks:

1) Consensus Splitting: this corresponds to the primary reason behind a forking event and it is due to the simultaneous discovering of two different blocks in the same time. A forking event is normally a rare event and hence *normal occasional forking* may last only for one block (e.g. the fork persists only for the block 2). In very rare situation, the forking event can last for more than one block (e.g. the fork persists for block 2-3-4-5) and a *rare extended forking* survives for several blocks (note: it can happen in situation in which the network latency is very high and becomes difficult to agree on one out of the two Blockchains: in this case the two chains continue to be extended until one becomes longer much earlier than the other) (*figure 24*).

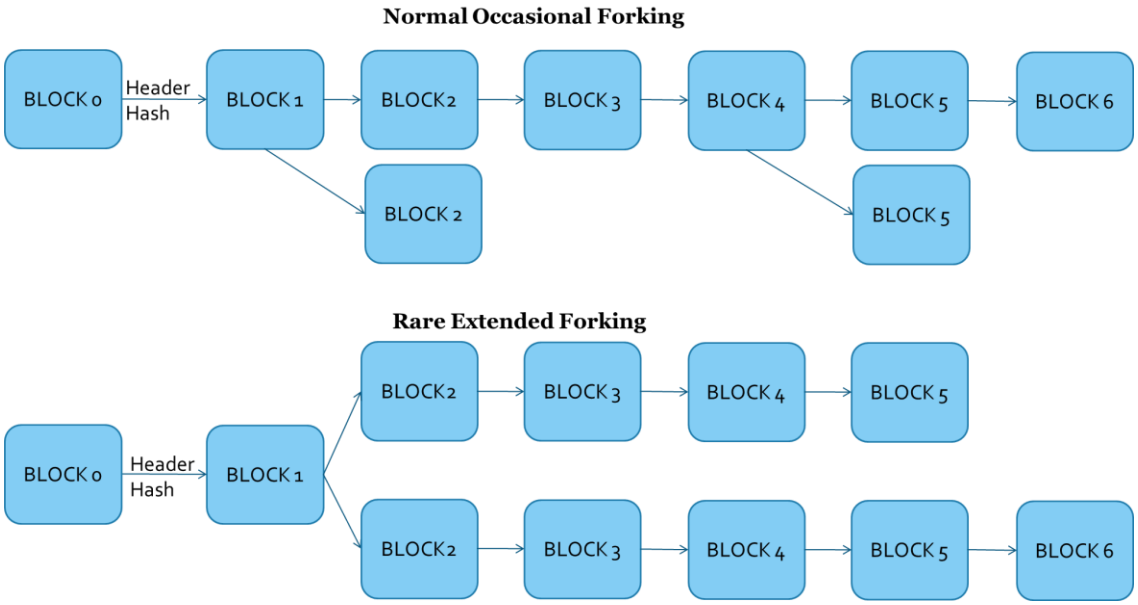


Figure 24: Normal and Rare Forkings

2) Protocol Rules Changing: the previous kind of fork events could be considered aleatory since there is no possibility to predict exactly when it happens and, generally, they are temporary. Instead, the second kind represents a well-defined and permanent event in which the protocol of the Blockchain is changed in order to add new features, enhance some functionality or just change a code rule. The effect of these choices could be different:

- **Soft Forks** are generated when the protocol update is retro compatible with previous versions. Even if some nodes do not update to the newer version, they are still able to validate and verify transactions. Non-updated nodes suffer just of the inability to achieve new functionalities and so a gradual upgrading is required. An example of soft fork could be an upgrade in the block size.

- **Hard Forks** are stricter because they require all the nodes to update. Whoever is unable to update, cannot continue to generate blocks or transactions because they will result no more valid and rejected by the network. The shorter, not valid version, of Blockchain will exist until every node is updated: from this moment, only the new version of Blockchain will continue its growth. For instance, every change in the consensus algorithm require a hard fork (*figure 25*).

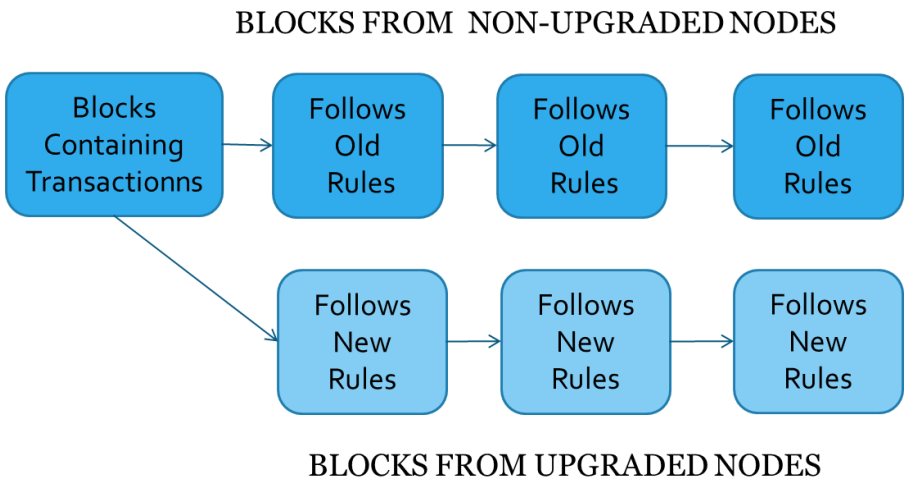


Figure 25: Representation on a Hard Fork Event

2.2.4) Scalability and the Trilemma

In order to fully understand how the Blockchain works, it is necessary to introduce the Scalability problem and the subsequent Trilemma. A more in-depth analysis to this problem is provided in the paragraph 2.2.6 and all the consequent solution are investigated later through an explanation of the different consensus mechanism. Therefore, in this section is introduced a brief description of the problem together with an overview of the main scaling solutions.

As already mentioned in the initial paragraph 2.1.2.1, Blockchain technologies are decentralized systems that are trying to improve many industries, which are based on the traditional centralized systems. To effectively disrupt actual systems and to become a practical solution, Blockchain must be able to scale and to speed up consensus mechanism in order to validate more transactions increasing the number of transactions per second. The actual Blockchain throughput is in fact very low if compared to other centralized systems (e.g. Visa can verify thousands of transactions per second while Bitcoin only less than ten).

However, enabling scalability of a Blockchain is difficult because every solution has to face off an important trade-off called the Scalability Trilemma (*figure 26*). When dealing with the development of a Blockchain system it is necessary to consider three main variables:

- **Security**: distributed networks must deal with a large variety of attacks (e.g. the 51% Attack, DoS Attacks, Sybil Attack, etc.) and contemporary must be fault-tolerant which means that the system is able to stay up even if some nodes of the network fails.
- **Decentralization**: even if the core characteristic of Blockchain is decentralization, network must be censorship-resistant allowing anyone to participate without preconception or unbalancing (e.g. absolute decentralization may create opportunistic behaviours, for example the selfish mining, in which nodes rise up coalitions which control the network in a centralized way): assuring decentralization without an authority is a hard job.
- **Scalability**: the network should be able to increase its capacity with the increasing of the dimension of the network.

Figure 26: The Scalability Trilemma Represented in a Mechanical Logic

The Trilemma affirms that is possible to choose only two out of these three characteristics when developing a Blockchain. For example, both Bitcoin and Ethereum allow both Security and Decentralization but they are not able to scale and thus their processing speed remains very low: this is due to the fact that full decentralization and high security levels require a distributed consensus of the state of the Blockchain which then needs a huge amount of time.

Therefore, in the recent years, immense efforts were made on the research of an effective Scaling Solution: still no solution is able to solve the Trilemma and then every combination of

these three variable permits to have some key strength that fit differently the application fields. It is possible to classify the different types of scaling solution into four main classes:

1. **First Layer "On-Chain" Solutions**: these kinds of solutions act directly on the codebase of the Blockchain (henceforth "On-Chain"). Usually the core characteristics of the Blockchain are modified in order to enhance the features of the Blockchain. For instance, some on-chain solutions consist in the increasing of the block size limit adding more transactions in a block (and hence making higher the TPS), some other solutions reduce the block creation time making easier the reaching of consensus. However, the main outcome of these typologies of solutions is the generation of Hard Forks (detailed information in the *paragraph 2.2.3*), required for the structural modification of such Blockchain's variables. To this first class of solution three main scaling types belong:
    - **Segregated Witness**: one of the first upgrade for the Bitcoin protocol was Segwit. This modification changes the data structure of a block by removing the signature data for each transaction. Without the signature more space is available and more transactions can be added inside a block. Of course, the elimination of the signature will eliminate the integrity check for Bitcoins creating huge issues for every user in the network: therefore, the signature is not eliminated but is simply placed outside the block and shared together with it.
    - **Sharding**: proposed to be implemented on Ethereum, this solution consists into dividing the Blockchain into smaller and more manageable parts (the "shards") which operate in parallel: instead of having a Blockchain limited by the speed of each individual node, Sharding allows to have a fragmented network in which each shard works independently from the others but still having a Blockchain functioning with the sum of all its parts.
    - **Hard Fork**: when it is necessary to modify a Blockchain while it has been already developed and in operation, the only valid solution is to create a hard fork (both the two previous solutions require this procedure to work properly). The new portion of the Blockchain is, in fact, forked-away with the implemented structural changes in the code base (e.g. Litecoin and Bitcoin Cash are both fork off the original Bitcoin network) allowing a new Blockchain with enhanced features and, often, higher transaction per second.
2. **Second Layer "Off-Chain" Solutions**: oppositely to on-chain solutions, these ones try to solve the scalability problem by creating secondary protocols built on the top of the main Blockchain and thus creating a second layer for the Blockchain. Here

transactions are removed by the main chain and located to the second layer chain obtaining two main benefits: there is saving of space and reduced network congestion. There are three main types belonging to this class and represents three solutions adopted by different Blockchains.

- **Lightning Network** (Poon & Dryja, 2015): it consists in a scaling solution which allows the creation of private off-chain channels that enable instantaneous transactions with small fees: a transaction does not need to be shared to the public Blockchain network if the two involved parties decide to close the channel. Built on top the original Bitcoin Blockchain, this solution moves all the transactions off the main chain reducing the heaviness of the network: hence, also micropayments are allowed because the speed and the costs of the network are improved.
- **Raiden Network**: similarly to the Lightning Network, this off-chain solution permits the users to establish private channels without involving the main Blockchain. It has been implemented on top the Ethereum Blockchain.
- **Plasma**: this solution creates some *child chains* that are originated from the *parent Blockchain*, which is the main one, and each of them works separately from the others, managing its own transactions, connecting its own nodes but still counting on the original parent chain. Security is hence set by the original Blockchain while the efficiency is augmented. One additional benefit is the possibility to set specific rules and variables for each child chain letting possible to process specific category of transactions by each sub-chain, still relying on the security of the same network system.

3. **Scalable Consensus Mechanism**: all the previous scaling mechanisms are, basically, the first attempt in improving the efficiency of the original Bitcoin Blockchain still using the same Proof-of-Work consensus algorithm. The second generation of solution are more sophisticated and involve the generation of specific ad-hoc consensus mechanism with the exact objective of improving the Blockchain scalability. In this case, three main classes of consensus algorithms were developed by different Blockchains and all of them are worthwhile solutions to the scalability problems (note: a deeper analysis of consensus algorithm is proposed in *paragraph 2.2.6.2*):
    - **Delegated Proof-of-Stake**: it is a consensus mechanism where some nodes are delegated to validate transactions of the network. The delegation is given based on the token hold by each node. The number of delegated nodes can vary a periodically changed; can be set by the system administrator and some strict rules regulate if a node is performing well enough or is behaving

correctly. When some misbehaviours are identified, delegated nodes are kicked out of the network and replaced. This consensus algorithm is considered partially centralized but creates a Blockchain, which runs faster than traditional PoW Blockchains.

- **Proof-of-Authority (PoA)**: it is an algorithm based on the reputation. Some nodes in the network, whose identities are clear and verified, are responsible for the validation process. The high number of TPS must deal with the problem of identities, which are necessary for the process, and thus PoA suits well in private or permissioned Blockchains.
- **Byzantine Fault Tolerance**: as clarified in the *following paragraph 2.2.6.1,* every distributed system, and so every Blockchain System, has to deal with the Byzantine Generals Problem in order to guarantee the consensus inside the network. The Byzantine Fault Tolerance is the capability of the system to achieve this objective even if in the system there are some faulty components. Several versions of BFT currently exists:
    - Practical Byzantine Fault Tolerance = it is a variation of the BFT that allows very high computational work with small increases in latency. It works like an asynchronous system in which a primary node deals with several backup nodes in order to reach the consensus through the majority (e.g. Hyperledger and Zilliqa use this consensus algorithm)
    - Federated Byzantine Agreement = this BFT version is able to reach consensus within a system using quorums or part of them. The quorum is nothing more than the minimum number of nodes needed to reach consensus over the total number of nodes in the system: then the quorum could be subdivided into different slices which contains at least two nodes. This voting system allows reaching consensus rapidly without the need of a majority of consensus but only of a minimum of trusted nodes.
    - Delegated Byzantine Fault Tolerance = this last type consists in a subdivision of nodes into two typologies: the delegated nodes and the ordinary ones. Exactly like a democracy, delegated works on behalf of ordinaries: delegated nodes are randomly chosen in order to verify and validate transactions sent by ordinary node.

4. **<u>Scalable Distributed Ledger</u>**: Blockchain systems are based on a data structure composed by several blocks linked together in order to generate a distributed architecture. When the distributed ledger technology is maintained while the data structure is modified, it is possible to rely on different information technologies which provide an alternative solution to Blockchain while performing in the same way: these are the *Directed Acyclic Graphs (figure 27)*. In these systems the transactions are not ordered and do not need to be processed in a chronological way: all the transactions can be virtually be processed together in a single instant while the linear data structure is then able to order all the flows of data in an topological way (Kahn, 1962). In the recent years, four different typologies of DAGs were proposed to solve the scalability issue of Blockchain systems and are further analysed in the *paragraph 2.2.6.2* (i.e. IOTA, Hashgraph, Spectre, Byteball).

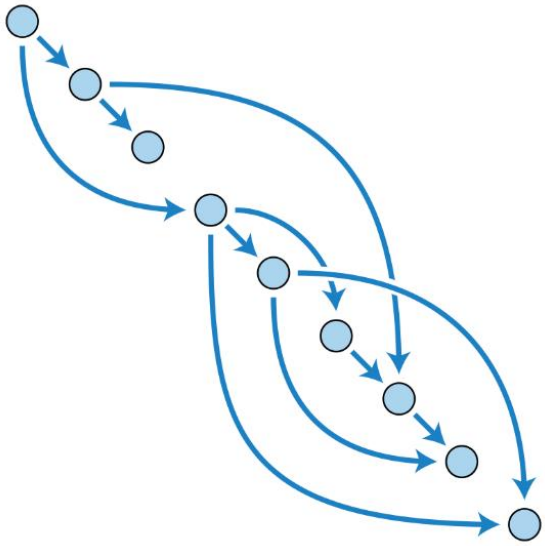


Figure 27: Directed Acyclic Graph Representation

2.2.5) Access Control

Together with the consensus mechanism, the Blockchain access control represents a main variable that permits a practical differentiation between Blockchains. Access control, in fact, creates a huge difference between Blockchains, giving some very specific characteristics that fit in very different applications. For a proper classification of access control, some question should be asked:

1) **How many copies of the ledger?** This main question poses the difference between a traditional ledger system, a simple database, and a distributed ledger system, a Blockchain. When only one copy of the ledger exists, then the system is based on a traditional ledger, otherwise when there are many equal copies of the ledger, then the

system is based on a distributed ledger. Blockchains allows to have a decentralized structure in which all the peers share a copy of the ledger, information is immutable and contemporary transparent.

2) **Who can see the ledger?** If only an owner group can join in the Blockchain, seeing all the information, sending transaction and validating blocks, then the Blockchain is *Private*. In this configuration the ledger is permissioned and shared only privately. The Blockchain is fully closed and only exact participants inside the network are allowed. The system is centralized under one organization which controls the right to view and send transactions.

   Otherwise, if anyone can read the Blockchain, another question is needed since there are two similar typologies of Blockchain that are part of this category.

3) **Who maintains the integrity of the ledger?** When both owner and validated users can participate in the Blockchain, the Blockchain is *Permissioned*. In fact, in this case, even if the ledger is shared publicly, it is still permissioned and only authorized nodes can modify it. This establishes a decentralized trust in a network of known participants because only Selected nodes (validators or trusted nodes) participate in consensus procedure.

   Otherwise, when any user can read but also participate actively in the Blockchain system, the Blockchain is *Public*: the ledger is permissionless and publicly shared. This is the opposite situation of Private Blockchain: Public ones are fully open and anyone in the network can read and send transactions participating in the consensus procedure.

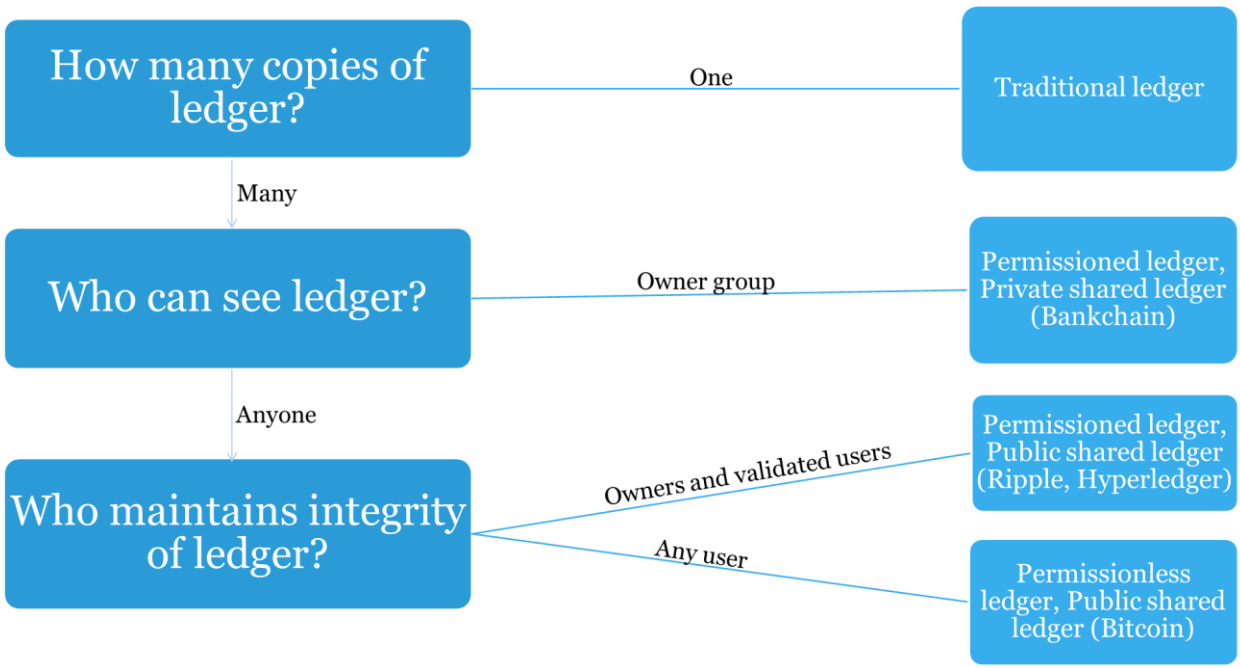


Figure 28: Representation of the Logic for Access Control

These three structures have some advantages and disadvantages are each of them is more suited for a particular usage.

Starting from private Blockchains, since they limit the access to data, they are used in sectors in which the confidentiality of information is mandatory. These Blockchains are normally faster the public ones because with only few authorized participants in the network, less time is needed to reach the consensus. Therefore, higher transactions per second rate is achieved. A private Blockchain is also more scalable. In accordance with the trilemma (*paragraph 2.2.4*), that affirms that only two out of three characteristics can be chosen in a Blockchain (security, decentralization, scalability), since the private Blockchain is highly centralized, both security and scalability are simply granted. In fact, the network can increase its capacity with the increasing of the transactions number (they are faster because consensus is prompter). However, even if private Blockchains are externally secure (if the Blockchain is isolated from the outside, no one can hack it), they are internally insecure (if an authorized node tries to subvert the network, since the dimension is smaller than public Blockchain, bad actions require less effort). thus private Blockchains require trust between authorized internal node. The credibility of a private Blockchain relies, in fact, on the reliability of authorized participants. In addition, a private Blockchain is by definition centralized and thus it is not possible to achieve the decentralization, one of the key features of Blockchain systems.

Public Blockchains have different advantages: first of all, they are trustless because oppositely to private ones, they can work very well even if there is no trust between participants. The network can be considered secure anyway thanks to different consensus algorithm. These Blockchains can be effectively external secure because an attack, in order to subvert the entire network, will require huge efforts. Finally, public Blockchains are fully open and transparent and this feature is very useful for a lot of applications, because information can be verified by everyone. Main disadvantages are both speed and scalability. Differently from the private one, they are usually slower and in order to achieve an acceptable level of scalability, huge efforts in developing an effective and enough faster consensus algorithms are needed.

Hence, based on the advantages and disadvantages of them, each access control generates a kind of Blockchain that fits better in different applications field. However, even if the majority of use cases can deal with these three configurations, sometimes a hybrid solution, which combines different pros and cons, is needed because it provides several benefits from the different access control. However, only off-chain mechanism can generate such kind of Blockchains (*paragraph 2.3.3*).

2.2.6) Consensus Mechanism

In every centralized system, the main authority node is responsible for the maintaining and updating of the database in which information is collected. This node is the only one which is accountable for the control of all the flows of data: it has the full power concerning data modification (i.e. it can decide which data can be added, deleted, updated, etc.) and it bases its decisions on the set of rules and polices that it has autonomously set before. This means that all the other nodes in the network can only have a restricted access to data and must ask for a permission granted by the central authority.

The situation is completely different when dealing with a decentralized system: since there is not a single authority responsible for the system, each node in the network oversees the administration of the network generating a self-regulating environment. *As already mentioned in the paragraph 2.1.2.1*, a Blockchain has a distributed network architecture and usually involves a number of participants, from hundreds to thousands (and even more in public Blockchain), who maintain up the ledger, process transaction and mine & verify blocks. In this highly dynamic situation, the status of the Blockchain changes continuously (even different public shared ledgers coexist in every moment) and thus requires a certain attention because several problems arose in this system configuration:

- It is necessary that all the participants in the network agree to the ledger without a central authority and that *only one* correct version exists in a certain moment.
- It is necessary that all the sent transactions, by every participant, are real and authentic.
- It is necessary to regulate how decisions are taken in the distributed network.
- It is necessary to deploy some techniques to defend the system from *attacks*.

Consequently, in a Blockchain network a *consensus mechanism* is compulsory: it is a safe instrument which ensures, firstly, that all the transactions happening on the network are genuine and, secondly, that and all participants agree unanimously on the status of the ledger. All the Blockchain rules are hard-coded into the Blockchain protocol which reveals exactly which consensus mechanism is used and permits to ensure that everyone uses the same Blockchain enabling a "trustless network". In addition, without a virtuous consensus mechanism, a Blockchain is at risk of numerous attacks.

Hence, a consensus mechanism has several functions that can be summed up into five different main points:

- It solves the issues on having a single ledger status, achieving a unified agreement between nodes in the network

- It prevents the double-spending problem thanks to the validation of only authentic and valid transaction in the public ledger
- Every consensus mechanism is able to align in different ways the interest of participant giving an economic incentive to good behaviours and punishing bad actors
- Anyone can verify the underlying source code of the consensus mechanism participate in the verification process (each protocol has its own rules)
- It ensures that a Blockchain is fault tolerant and hence both reliable and consistent.

There are many ways to reach consensus, nevertheless they are nothing more than different solutions to the Byzantine General's Problem (BGP), introduced in the next section.

2.2. Unanimity in unreliable distributed systems: The Byzantine Generals Problem

In every Blockchain it is essential to reach an agreement concerning what it is exchanged amongst the different participants: indeed, a unanimous consensus is necessary for accepting transaction, for distributing a unique ledger and for regulating decisions concerning to certain events occurrence or attacks detection.

The unanimity in unreliable distributed system is a topic already discussed in the "Byzantine Generals Problem", problematic that was named by (Lamport, Shostak, & Pease, 1982): this dilemma is referred to an issue of distributed computing systems, which consists in a network condition where nodes may fail or where there is imperfect information about a node failure. This problem requires developing a fault tolerant computer system, which produces the so-called Byzantine Fault Tolerance. The BGP is just a general, yet wider, formulation of the Two Generals Problem (Gray, 1978) which was the first computer communication problem to be proved to be unsolvable (Akkoyunlu, Ekanadham, & Huber, 1975): consequently, also the BGP is proved to be unsolvable and thus some realistic expectation must be considered while dealing with such type of systems. The problem of obtaining Byzantine consensus was mathematically formalized by Robert Shostak: he proved that for n=1 faulty computer, no fewer than 3n+1 computers in total were needed for any algorithm that could guarantee consensus, demonstrating its result using an algorithm based on two rounds of message exchanges that started guaranteeing consensus with a minimum of four computers. Then, Marshal Pease generalized the result algorithmically showing that 3n+1 computers are sufficient as well as necessary for every n>0 faulty computers.. Finally, Lamport, demonstrated that if messages could be digitally signed, then only 3n are needed: their aggregated results were published in the paper (Pease, Shostak, & Lamport, 1979).

Only few year later, (Lamport, Shostak, & Pease, 1982) published the metaphor of Byzantine Generals: this allegory was used to describe the situation in which an unreliable computer

system must agree on a defined strategy for avoiding the system's failure by narrating the problem through the story of several byzantine generals who needed to coordinate the timing of an attack on an enemy by exchanging messages carried out by some messengers.

2.2.6.1.1 Illustration of the problem

A group of generals, each commanding a fraction of the Byzantine army, has surrounded a city. The generals have to formulate a plan for attacking the city and they must decide whether to attack or retreat: it is fundamental that every general agrees on a common decision because only with a coordinated whole-army attack the city could be defeated, or a joint retreat could be effective and save the entire Byzantine army.

In addition to this first problem, it is known that some disloyal generals may not vote truly for the attack strategy and they can also modify the message coming from other generals. Therefore, not all the messages exchanged by the messengers are reliable and also not all the messengers are loyal: some may be traitors too. Hence, both messengers and other generals could falsify a message.

Another issue is related to the enemy: it can simply kill some messengers preventing the communication between generals or can capture a messenger and replace him with a fake messenger to transmit fake messages.

2.2.6.1.2 Solutions to the problem

Two different solutions, based on iterative algorithms, were originally described in the paper and used to reach an *iterative consensus*:

- One solution, in case of forgeable messages, showed an algorithm with which it is possible to assure a consensus on the attack only if the number of traitorous generals is less than one third: are always needed 3n+1 general to avoid that n traitors nullify the attack strategy.
- The second solution, in case of unforgeable messages (a general's signature cannot be altered, and anyone can verify the authenticity), permits to reach consensus even with one third of traitorous generals: are needed 3n generals to solve the problem in case of n traitors.
- Advanced solution was later introduced in 1999 by Miguel Castro and Barbara Liskov who presented the "Practical Byzantine Fault Tolerance" (PBFT) algorithm.

2.2.6.2 Consensus Algorithm

To solve the Byzantine Generals Problem, consensus algorithms are used in order to provide a Byzantine Fault Tolerance otherwise it could be impossible to guarantee that two nodes in the Blockchain are using the same data.

Basically, consensus algorithms rely on *two main concepts*:

- Each node in the Blockchain (i.e. each Byzantine General) must invest some resources in the network (i.e. must put a consistent amount of *Solidus*, Byzantine money) or must solve a very difficult puzzle (i.e. must find a keyword before signing a message) in order to show its interest in the maintaining of the chain (i.e. their involvement in the attack strategy formulation). This idea assures that anyone who refuses to put some kind of effort (money or time) is suspected of behaving not correctly and, on the other hand, make difficult for a betrayer to act unfairly (this will lead to the first two typologies of consensus mechanisms: the *Proof-of-Work* and the *Proof-of-Stake*).
- In the Blockchain ledger, all the previous communication cannot be tampered and must tracks each node's transaction (i.e. the messages coming from a General cannot be modified by someone else because are signed and verifiable). This is guaranteed by the chained structure of blocks and the presence of hash values of both senders and receivers.

2.2.6.2.1 Classification of Consensus Algorithms

Hence, behind every Blockchain there is a consensus algorithm. It is not possible to find an algorithm that fits every Blockchain because no consensus algorithm is perfect: each of them has several strengths and several weaknesses and therefore the choice of an algorithm depends on the precise utilization of the Blockchain. Until today, very little has been written about when it is better to deploy a specific type of consensus and, from the literature, there is even less information about how to classify kinds of consensus. Accordingly to a research from (Hays, 2018), it is possible to propose a classification based on two different main variables that characterize dissimilar algorithms.

The first variable, which represents the y-axis, is the *degree of centralization*. It goes from "centralized", which means that trust into someone or into an organization is needed to add something to the Distributed Ledger (i.e. Private and Permissioned Blockchains), to "decentralized", which oppositely means that everyone has the access to the Blockchain ad is able to send transactions (i.e. Public Blockchains). The second variable, which represents the x-axis, is the *degree of externality*, which ranges from "high external anchor", which means that the consensus mechanism requires some external resources to make decisions within the

network (i.e. time, computational effort, tokens, money, assets, etc.), to “no external anchor”, which means that no external resources are required.

It this way, it is possible to identify four different classes of consensus algorithms. Each category has several pros and cons and, in addition to this, in each category every algorithm has several benefits that distinguish it from the others. It is not a surprise to discover that no algorithm has excellent performance in every kind of benefit and often to each benefit corresponds a specific outcome. Therefore, in the following paragraph, a detailed description of the most diffused consensus algorithm is provided: such explanation analyses algorithms evaluating some common variables, identifying also all the defects or limits that every consensus algorithm produces.

2.2.6.2.1.1) Proof of Work (PoW)

PoW Algorithm is the first Blockchain Consensus Algorithm formulated by Nakamoto in its Bitcoin Blockchain. Even if it is still considered secure, it is nowadays recognised as a legacy technology due to the presence of so many recent alternatives more efficient which make very difficult to see a new Blockchain based on PoW (even Ethereum is switching from PoW to PoS). The reason behind this phenomenon reside in the PoW working mechanism.

A PoW Algorithm, *as already explained in the paragraph 2.1.2.3*, is based on the mining system generated by the algorithm: to reach the consensus, every miner, with a random process, tries to find the solution to the mathematical puzzle in order to generate a valid block to be added to the Blockchain. This computation is very costly and time consuming and a huge amount of trials are required on average before a valid proof is generated. This is the reason why this kind of consensus is classified as a “High External Anchor” because a large amount of computational power (i.e. CPU hardware together with electric energy) is necessary to maintain up the entire Blockchain. Consequently, the first main issue of the PoW algorithm is that the entire network consumes *huge quantities of energy* and the *overall hardware equipment* have been estimated to cost around $400 million per year (Aste, 2016). In addition, the more miners entry in the network, the more difficult becomes the solution for the proof of a block (note: difficulty is automatically set by the protocol and vary with the number of miners) and thus the energy a miner have to spend to validate a block constantly increases.

Second, the PoW algorithm has several disadvantages that include different *Attack Vectors* that malicious nodes can exploit (Gervais, et al., 2016):

- **Race Attack**: this type of attack happens when a cheater sends a transaction to the receiver (typically a merchant) with the payment together with a conflicting

transaction which spends the coin to himself to the rest of the network. The second conflicting transaction is then mined and accepted by the network, which adds the block into the Blockchain. (Karame, 2012) affirmed that the Bitcoin Protocol allows a high degree of success by a cheater when performing a race attack and recommended to disable incoming connection and to choose specific outgoing connections as solution for this PoW algorithm problem.

- **Finney Attack**: it consists in a fraudulent double-spending: an attacker generates a block, which contains a transaction between two owned addresses. Then, with the same sending address, he sends a transaction to a receiver (again, a merchant). After the payment, the merchant checks for a few moments the authenticity of the transaction and complete the bargain (e.g. sends the goods to the cheater) but then the attacker broadcasts his previous block to the network which then takes the precedence over the transaction to the merchant, tricking him. Even if this attack cannot be eliminated with some precautions, some miner hash power is required, and a specific sequence of events must occur.
- **Vector 76 Attack**: it could be considered a mixture of the previous two types of attack. This attack combines the two previous techniques for generating a double spending which frauds the receiver. Vector 76 is very effective but very rare: if fact, three conditions are necessary for an attack to go well (i.e. merchant accepts payment after only one confirmation, the receiver node allows incoming transaction while using a static IP address). Also, when the attack is not successful, the attacker has invested uselessly on the generation of a block, which required time and energy (and thus money).
- **Alternative History Attack**: this typology of attack requires a high hash rate and a risk of significant expense in wasted electricity to the attacking miner but works even if the receiver waits for several "N" confirmations. The cheater propagates to the receiver and to the network the transaction, which pays the merchant while mining an alternative Blockchain fork in which a counterfeit double-spending transaction is included. The receiver waits for "N" confirmations from the network before trusting the transaction but then, if the attacker has found more than "N" blocks, he broadcasts his fork to the network and gains its own tokens. However, it may happen that the attacker is not able to generate "N" blocks on time and continue to extend his fork with the hope of catching up the rest of the Blockchain which becomes longer: if he is not able to do this, the attack fails and the attacker has waster a lot of energy while paying effectively the merchant. It has been calculated (Rosenfeld, 2014) that the success probability is function of the hash rate of the attacker and the number of confirmations that the receiver waits for trusting the transaction.

- **Majority Attack (51% Attack)**: this is the extreme generalization of the previous attack. When an attacker has more than one half of the network computing power (i.e. the attacker hash rate is >50% of the network hash rate), the Alternative History Attack has a 100% probability of success whatever is the number of confirmations required by a receiver. It is very easy for the attacker to get the controls of the entire Blockchain since he can generate blocks faster than the network and send whatever transaction on it. The increasing of the number of confirmations will increase the resource cost of performing the attack: this fact can potentially make the 51% Attack unprofitable of simple require too much time for being effectively used in practise. A solution to avoid this attack consists in preventing mining pool from reaching a hash power higher than 50% (or higher than a set value) by modifying appropriately the Blockchain protocol. However, it has been demonstrated (Decker & Wattenhofer, 2013) that due to technical inefficiencies in the network, caused by latency between nodes, the effective computational power of a PoW network system is never exactly the 100% of its resources and thus even a lower share of the overall network computational power is enough for an attacker to revert the Blockchain and get the control of it (e.g. they demonstrated that the Bitcoin computational power is effective only for the 98.20% and then a >49,1% is necessary and sufficient for an attacker). (Milutinovic, He, Wu, & Kanwal, 2016) confirmed this result suggesting also some stringent thresholds for mining pools and hence, eventually, for avoiding a mining attack although, later, (Ba, 2019) demonstrated that since the information propagation in the network is very variable, it is not possible to assure if a selfish-mine attack is successful or not.
- **Denial of Service (DoS) Attack**: these kinds of attacks occur when an attacker sends too much data to a node which make it too busy to process transactions. Different protections are needed to prevent different DoS attack and must be well encoded in the Blockchain protocol: good protocols foresee almost the totality of the possible attacks. Even if many protections are set, the Blockchain is still vulnerable to newer and more sophisticated Denial of Service Attacks.
- **Sybil Attack**: it consists in the attempt of the attacker of introducing in the network nodes which are directly controlled. When an important number of malicious nodes is introduced in the network, the probability to connect to them becomes very high. As stated by (Douceur, 2002), the attacker can subvert the system of a peer to peer network getting a large influence on it: the attacker can refuse to send selected transactions, can disconnect a peer from the network, can falsify the network as seen by a peer (i.e. a peer connected to malicious nodes sees a completely different and tampered Blockchain), can slow down the network allowing other double spending

attacks, etc. The system vulnerability depends on the easiness of introduction a new malicious node in the network. To prevent these attacks an authentication mechanism is needed; when this is not possible (e.g. in Public Blockchain) the consensus mechanism could just make these attacks more difficult limiting the number of outbound connections between nodes while maintaining incoming connection unlimited (these actions limit and prevents the possibility to create an extensive harmful sub-network).

- **Selfish Mining**: this problem was originally formulated by (Milutinovic, He, Wu, & Kanwal, 2016). It consists in a mining strategy where miners choose accurately when to submit blocks to the public chain instead of submitting immediately: this is done in order to let the other miners to work uselessly on obsolete chains, thus increasing the selfish miner's part of mining revenues. This kind of outbreak does not generate only an unbalanced and unfair reward between miners but also produce network latency and increased electricity costs. However, selfish mining has a limit: it could be considered a zero-sum game because if practising selfish mining is more remunerative than honest mining then everyone is incentivized to do it but with a whole-network selfish mining all the advantages will disappear letting only the harmful consequences. In fact, accordingly to Paul Sztorc, with selfish mining "you end up right back where you were before". To prevent this problem, (Heilman, 2014) proposed a useful and necessary defence mechanism that penalizes the profitability of selfish miners using an unforgeable timestamp to punish miners who withhold blocks.

Third, another main PoW problem is the *Scalability* of the Blockchain itself. Scalability, defined as the capacity for a system or network to grow in size and manage increasing demand (Bondi, 2000), on a PoW limits the amount of transactions per second that the network is able to process. This limit is structurally settled by two main factors which are established by the PoW protocol: the *average block creation time* is nearly around 10 minutes and if a block can contain only a limited number of transaction (e.g. commonly are put ≈2000 transactions) then only a certain amount of transaction can be processed in a second (i.e. TPS is limited); the *block size* is limited to 1 MB and again no more transactions can be added and processed every second (note: the reason behind this limit was to contain the possibility of DoS attacks). Hence, the PoW consensus mechanism is a limit itself for the scalability of the Blockchain because it requires long times to validate block for reaching consensus, discouraging a mass adoption of the Blockchain and then increasing the transaction fees too much when the network is very congested. Several typologies of solutions are adopted in different Blockchain to increase the scalability possibility and each of them generally tries to solve the Scalability Trilemma: *as already mentioned in the paragraph*

2.2.4, numerous are the proposed solution to the Trilemma and each of them use a specific consensus algorithm.

Pros: secure and steady; well-known; widely and for a long time used.

Cons: very slow; low throughput; high energy consumption (expensive).

2.2.6.2.1.2) Proof of Stake (PoS)

The Proof of Stake, originally introduced by (Aste, 2016), could be considered the as the first alternative to the Proof of Work, settled in order to solve the main issue of the high computational power required. In fact, when dealing with such type of algorithms, the consensus is reached through different stake mechanisms and the creators of the next block (i.e. the block *minters*) are chosen with a random selection that take into consideration a certain stake: that stake could be based on the wealth or the age (or a combination of both) of each node belonging to the network (the stake is generally nothing more than the ratio between the owned tokens and the overall tokens available in the network). It is evident that in a PoS system the blocks are not created by a hard mining work but are generated by selected nodes, which have invested in buying tokens in the network rather than acquiring computational power. With this mechanism, it would be very costly to attack the network because it is necessary to own a high stake before making an attack: for malicious nodes, this attempt could cost their entire investment because in the case of forking event, block minters have to spend their tokens choosing which fork to support and, assuming that most minters will pick up the correct fork, validators who voted for a tampered fork would lose their stake. This voting system could be more or less secure by setting a quorum to different levels; some PoS algorithms may require simply the majority (51%), even if in this case an attack will cost less it will still be far more expensive than a 51% on a PoW Blockchain, others may necessitate a two-thirds majority or an unanimously consensus (100%). However, PoS has some weaknesses and several critics were made to it. First of all, it is evident that nodes with higher stakes are more important and their probability to mint blocks receiving rewards is higher and thus the system appear more centralized than a PoW (in addition to this, riches get richer, i.e. important nodes increases their importance by time). An attempt to solve this problem is made by introducing a time variable that multiplies the tokens: bigger and older coins have greater probability to be elected as minters but once a stake of coins has been used they restart from time zero allowing every nodes to participated fairly in the Blockchain and increasing again the degree of decentralization. The second problem in a PoS, similarly to PoW, is the possibility of two different attacks:

- **Nothing-at-Stake Attack**: this problem arises due to the lack of mining power needed for generating blocks: the block minters could easily vote every fork in the Blockchain and build following blocks on top of each Blockchain forks because from a financial point of view they will collect transactions fees of whatever fork will prevail and it costs nothing for a validator to validate blocks on multiple forks (there is no more proof of work). This attack would allow double spending attempts, disrupting the consensus mechanism.
- **Fake Stake Attack**: this kind of attack threatens the stability of the network by making a node crashing. In this situation, an attacker without much stake, or sometimes without stake at all, is able to fill the computing resources of another node (i.e. disk or RAM memory are saturated) with useless garbage data. This is possible due to an inadequate validation process in the consensus protocol that for speeding up the process does not verify network data before employing valuable machine resources.

Different solutions to these problems modify the consensus algorithm introducing a hybrid PoW system together with the PoS one; other solutions introduce a timestamping system based on a Proof of Activities or develop new consensus Proof of Burn algorithm starting from the original PoS.

Pros: energy efficient (compared to PoW); the 51% attacks are more expensive.

Cons: risk of centralization; Nothing-at-Stake and Fake Stake Attacks; rich get richer problem; harder scalability.

2.2.6.2.1.3) Delayed Proof of Work (dPoW)

dPoW consensus algorithm was developed by (Komodo Platform, 2018) and consists in a hybrid method which create a secondary Blockchain based on a primary Blockchain. The dPoW can take the security advantage provided by the hashing power of the underlying Blockchain (i.e. the Bitcoin one) while reaching the consensus on the secondary one. The working mechanism is quite simple: two different kind of nodes reside in a dPoW network, the normal nodes and the notary ones. Normal nodes are necessary to validate blocks inside the dPoW Blockchain through a PoW (or even a PoS) consensus system. Notary nodes, which are elected by the dPoW Blockchain main stakeholders, are responsible of the notarization of confirmed blocks from the secondary Blockchain to the main primary Blockchain. Every time a block is generated on the dPoW Blockchain, its hash is added to a Bitcoin transaction and it is signed by the notary nodes: in this way a list of all the dPoW block hashes is written inside the Bitcoin Blockchain. A Delayed Proof of Work consensus system permits to achieve an

increased security, thanks to the computational power of the underlying PoW Blockchain, while increasing the efficiency on the secondary Blockchain (e.g. by using less complex PoW algorithm or energy efficient PoS). Moreover, a dPoW Blockchain can create additional value to another Blockchain by providing same Bitcoin security without paying its transaction costs (i.e. another Blockchain using dPoW can the attacked to the secondary Blockchain which is subsequently linked to the Bitcoin Blockchain).

Pros: increased security; more efficient; economically cheaper.

Cons: only PoW and PoS can be used.

2.2.6.2.1.4) Delegated Proof of Stake (dPoS)

The dPoS was designed by Daniel Larimer and used for the first time in the BitShare Blockchain (BitShares Foundation, 2015), implemented also in other high speed Blockchain such as Steem and EOS. The dPoS algorithm differs a lot from the PoS one. Here, every node which owns tokens in the network (i.e. every stakeholder) does not vote for the validity of transaction nor blocks: each node instead votes in order to elect some delegates for the blocks' validation on their behalf. These delegates, which are chosen periodically, are responsible for managing transactions and generating blocks. Hence, the algorithm runs in two different steps: firstly, the group of *witnesses* (i.e. block producers) is nominated; secondly, a scheduling for the block production is generated (every witness has a dedicate time slot for producing a block: if it is not able to produce a block on time it will skip its turn and when a delegate continuously misses its block or publishes invalid transaction, it is kicked out and replaced by another better delegates). The tiny number of nodes responsible for generating blocks make possible to reach the consensus very rapidly and efficiently: however, the network depends on several nodes and thus, partially centralizing the creation of blocks the Blockchain results less decentralized. The security of the Blockchain is created by the separation between nodes who vote for delegates and who generate blocks. Greaten token holders, that like in PoS have higher stake, can be malicious but cannot generate blocks: they can vote for some malevolent nodes risking their tokens, but then other trustful nodes must choose also that malevolent nodes. So, it is more difficult to coordinate an attack in the network: the Blockchain is considered fully secure until two-third plus one delegated are honest. In fact, in an ordinary block production, every witness produces a block:

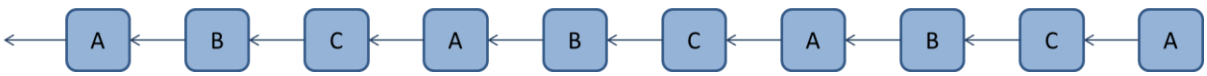


Figure 29: Ordinary Block Production in PoS

When up to one-third of the nodes is malicious or malfunctioning, only a minority fork is created and then the longest chain will prevail, and bad nodes are replaced (e.g. node B is replaced after two invalid blocks):

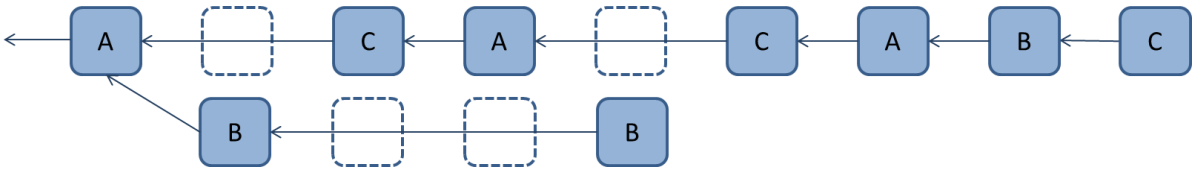


Figure 30: Example of a Malfuctioning or Malicious Activities in PoS

Exceeded the limit of one third of malevolent nodes, which is a very rare event that requires an extremely difficult coordination between malicious stakeholders and witnesses, the Blockchain becomes unstable an attack becomes possible:

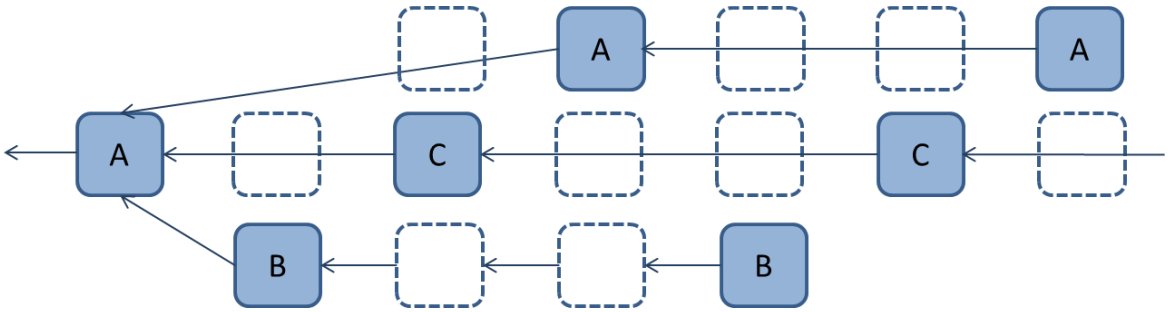


Figure 31: Reaching the Limit of One-Third of Malevolent Node in PoS

Hence, election mechanism makes secure the entire network while providing high speed and efficiency and making possible a scalable Blockchain: the number of witnesses can be, in fact, regulated based on the number of nodes in the network.

Pros: faster and cheaper transactions compared to PoS; scalable; energy efficient.

Cons: partially centralized.

2.2.6.2.1.5) Leased Proof of Stake (lPoS)

It is an alternative version of PoS which was deployed on the (Waves Platform, 2016) and it is an attempt to enhance the original PoS. The lPoS algorithm permits to each node which holds some tokens to participate in the next block generation without computing it directly. In fact, every user can lease its tokens to other nodes increasing the chance to become a selected node with high stake. Some nodes, called *full nodes*, stay in the network in order to be only

selected as block minters, other ordinary nodes, which does not generate physically blocks, choose to which full nodes leasing its token. Similarly to dPoS, in this algorithm can be recognized a certain delegation mechanism still remaining, in practise, a PoS Blockchain.

Pros: greater economic incentive to all nodes.

Cons: higher risk of coalition between malevolent nodes.

2.2.6.2.1.6) Proof of Authority (PoA)

The Proof of Authority is a consensus algorithm based on the reputation of nodes: here block validators do not stake their token but their reputation. Some truthful entities are necessary for selecting arbitrarily the different validating nodes (i.e. the authorities). It is a very suitable solution for private and permissioned networks because the identity of authority nodes must be obviously well-known in order to check their reputation. Since the number of validators is limited and chosen ex-ante, the PoA Blockchain is very scalable and efficient for large network. Even if every PoA algorithm differs from the others but they all need three different conditions: several valid and reliable nodes, difficulty to become an authority (reputation is made through investment and time) and standard authority selection (rules for being a validator must be equal to everybody). PoA is considered a faster but secure version of PoW and a more scalable solution than PoS but, anyway, in accordance to the scalability trilemma, it lacks decentralization.

Pros: secure; scalable; high throughput.

Cons: centralized; validators cannot be anonymous.

2.2.6.2.1.7) Proof of Reputation (PoRep)

PoR algorithm is a variant of PoA. It was recently deployed by (GoChain Foundation, 2018) and the consensus depends on a reputation of the participants which ensure a secure network. Reputation here is a relative concept: only the nodes (which here are generally represented by companies) with a reputation level important enough can be voted and can become an authoritative node (i.e. a block validator). The reputation is rated with two factors that are the *economic valuation* (the higher the value of a company, the higher is the reputation) and the *brand name* (the more important is the brand, the higher is the reputation). Obviously, in a business environment the reputation is very high and so it is critical for authoritative nodes to maintain their high reputation, avoiding dishonest behaviours since they would face significant financial and/or brand consequences if they attempted to cheat in the network. A PoR system can run also in public Blockchains and an

economic incentive is given to every authoritative node that generates blocks (i.e. they earn tokens).

Pros: secure; scalable; high throughput.

Cons: reputation is very crucial (51% attack could be easily executed by authoritative nodes).

2.2.6.2.1.8) Proof of Elapsed Time (PoET)

It is used by Hyperledger Sawtooth for the first time (The Linux Foundation, 2018). In this algorithm each node in the network participate in the block generation. Every node needs to wait for a random time period and the first node that complete the designated waiting time has to create the next block. Only the node with the shorted sleeping time can produce the block broadcasting then all the necessary information to the network. Every time a new block is discovered the process is repeated. Naturally, the PoET consensus, in order to work properly, needs that all the participants honestly get a random time and not a shorter one only for generating the following block and, then, the selected node effectively has to wait the sleeping time. These mechanisms are guaranteed by Intel SGX, a tool developed in 2016 by Intel which permits the assigning of a waiting time to each requesting nodes in a protect environment (called *enclave*) and thus electing a leader for the generation of the following block in the chain, like in a fully trusted lottery. Such consensus guarantees a fair and verifiable Blockchain but requires some hardware investments in order to run the scripts needed for participating in the system and thus only permissioned nodes can effectively join in the network. This algorithm is also called *Proof of Luck* and was rigidly defined in their paper by (Milutinovic, He, Wu, & Kanwal, 2016).

Pros: fully decentralized (to all permissioned nodes); secure; verifiable; adequate throughput.

Cons: require expensive hardware.

2.2.6.2.1.9) Proof of Space (PoSp)

PoSp was originally formulated by (Ateniese, Bonacina, Faonio, & Galesi, 2014) in a paper in which was described a method for substituting a proof given through a computational effort with a proof guaranteed by a memory allocation. Later (Dziembowski, Faust, Kolmogorov, & Pietrzak, 2015) developed a specific algorithm which suits Blockchains application. The PoSpace is comparable to PoW except for the utilization of storage rather than the computation: the working mechanism consists in a piece of data that is exchanged between a prover and a verifier. The prover receiver this data and the verification process takes place in

its hardware: if the prover has not allocated a certain amount of space then it could be not possible to complete the task given by the verifier. However, it could be not manageable to send large quantities of data between prover and verifier, since this algorithm must be used as a verification process in a network of nodes, therefore, instead of large data, hard-to-pebble graphs are exchanged by them which require low data to be sent but large memory to be computed and rapid and efficient verification time (Paul, Tarjan, & Celoni, 1976).

Pros: lower computational effort is required; memory space is cheaper than computing power.

Cons: it is more difficult to give incentives based on memory rather than computing power.

2.2.6.2.1.10) Proof of History (PoH)

Introduced by (Yakovenko, 2017), PoH algorithm supports a PoS Blockchain by modifying its working mechanism, increasing the overall network throughput without compromising security but permitting also the scalability of the network. It works thanks to the PoH algorithm which is able to verify the ordering and the timing of every transaction inside the network. In this system, some nodes are elected as *Leaders* and their roles is to organize all the other users' messages and send them to other *Verifiers* nodes which executes every transaction and publish a confirmation. These confirmations are then used for the PoS consensus mechanism which then confirm the correct sequence of transactions and generate blocks. After a block is generated the process is restarted by electing new *Leaders*. This additional layer of proof for transactions timestamping, allow to avoid the synchronization of nodes inside the network: since all the transactions are already sorted (and this sorting in unique and hashed-based) the block creation require less coordination effort and thus a speedier but secure verification process is obtained.

Pros: very high throughput; secure.

Cons: higher level of trust in the PoH algorithm layer is required.

2.2.6.2.1.11) Proof of Stake Velocity (PoSV)

This algorithm was proposed by (Ren, 2014) and it is based on the main PoS but with a key difference: every time it is necessary to calculate the stake in order to reach the consensus, the age of token is taken into consideration not in a linear way (like in the original PoS algorithm) but with a non-linear aging function which incentivize the regular staking and advantage younger tokens. This modification encourages the participation of nodes in the

network not only with the ownership (i.e. Stake) of tokens but also with the activity (i.e. Velocity) in the network.

Pros: fairer and more active network.

Cons: same of PoS.

2.2.6.2.1.12) Proof of Importance (PoI)

The PoI is an algorithm introduced by (NEM Foundation, 2018). The PoI is the working mechanism underlying NEM Blockchain and it is used for determining which nodes in the network can be chosen for adding the blocks to the chain. Unlike the PoS, the PoI is more wide-ranging since it takes into account how a node globally supports the network. If in a PoS the probability of adding a block are proportional only to one factor (e.g. if a node owns the 15% of tokens it will have the 15% of chance of generating the next block), in a PoI not only tokens are considered but also the number of transactions and the activity of a node in the network. In this way, the more a node is active and contribute to the network, the more it demonstrates its involvement in the Blockchain and thus has a higher important and deserves to *harvest* the next block. The process of adding a new block is called *harvesting*: this procedure, in fact, gives more incentive to the nodes (i.e. the *harvester*) which collect as many transactions to the block as possible.

Pros: better evaluation of stake than PoS.

Cons: risk of activity speculation (nodes may send and receives back dummy transactions only in order to increase their activity score).

2.2.6.2.1.13) Proof of Identity (PoId)

Implemented by (Mannabase Incorporated, 2018), this form of consensus does not rely on computing power nor capital of money: it relies on people. This means that the Proof of Identity, equally called Proof of People, aims at creating a Blockchain between trusted people in which the distributed ledger is shared only between these people and the trust is possible thanks to possibility of recognizing clearly the identity of a person and distinguishing every person from the other.

Pros: very simple.

Cons: can work only in small and private Blockchain.

2.2.6.2.1.14) Proof of Retrievability (PoR)

Starting from the theory of (Milutinovic, He, Wu, & Kanwal, 2016), Blockchain application of the Proof of Retrievability are proposed by (Miller, Juels, Shi, Parno, & Katz, 2014) and are nowadays used in Parmacoins. This kind of algorithm, the PoR, uses as a proof a file system. A prover sends to a client, that has the role of verifier, a target *file*: if this *file* is valuated as intact then the consensus between these two nodes is established. PoR requires not only some computational resources for check the integrity of the *file* but also some storage resources. This file system created through the PoR algorithm could be useful for reaching a consensus also in decentralized computing or file storage system (e.g. Cloud applications).

Pros: Blockchain can be used for Cloud solutions.

Cons: both computational and storage resources are required.

2.2.6.2.1.15) Proof of Activity (PoAc)

The Proof of Activities is a consensus algorithm that was proposed in a paper by (Bentov, Lee, Mizrahi, & Rosenfeld, 2014) that was created starting from the original Bitcoin PoW. PoAc can be considered as a hybrid algorithm between PoW and PoS. In order to reach the consensus in the network, the algorithm starts with the PoW: in this phase a mining process between various mining nodes takes place and results in the generation of a new block. Until now, the block is empty because it contains only a header and the miner's address. At this point the algorithm switches to the PoS. The second phase consists in the selection of several validators that are asked to sign the found block. The validators are chosen based on their stake, hence, the more token they have the higher is their chance to be selected. Only once all the validators sign the block it is considered valid and added to the Blockchain and only now it contains all the transaction in it. May happens that sometimes some validators are not able to sign the block on time and therefore the block is casted off because incomplete: the next mined block is used, and the process is restarted. In this PoAc algorithm the fees for all these activities are divided between all the nodes which have participated in the process (i.e. the mining nodes and the validators ones). It is evident that the algorithm is very long and complex because it requires a double proof given by exactly two different Proofs (i.e. of Work and of Stake): consequently, it is one of the most secure algorithm for consensus and, differently from PoW, the probability of a 51% attack is almost zero because two conditions are needed: a successful attack would necessity contemporarily both 51% of computing power and the majority of stake in the system by the exactly same group of nodes. The Proof of Activity, thanks to its hybrid nature, is able to furnish the benefits of both PoW and PoS while also sharing their cons.

Pros: more secure; lower storage space and network communication issues than PoW.

Cons: still requires large amount of resources for mining; nothing-at-stake attack may persist.

2.2.6.2.1.16) Proof of Time (PoT)

The PoT has been developed by (ChronoLogic, 2018). It is proposed as a solution for Blockchains in order to solve the problem of lacking the time-based functionalities of transaction scheduling. This protocol offers a decentralized scheduling for transactions through an off-chain network of nodes that are called Timenodes: they are incentivized to operate thanks to the presence of transactions fees. The logic of this algorithms allows complex operations which are based on the timing of transaction (e.g. decentralized application or smart contracts).

Pros: permits time-based transactions.

Cons: requires external off-chains.

2.2.6.2.1.17) Proof of Weight (PoWe)

It is used by Algorand and it is an algorithm derived from the canonical PoS. It was published for the first time by (Gilad, Hemo, Micali, Vlachos, & Zeldovich, 2017) and could be considered as a generalization of the Proof of Stake: in fact, if in a PoS network the probability of generating a new block depends on a specific stake which is calculated from the tokens in the network, in the PoWe different weighted values are used. These values are calculated and assigned to each node in the network through a Byzantine Agreement (see *paragraph 2.2.6.2.1.21*) protocol: this protocol is made up of two phases which consist in several phases in which firstly the protocol reduces the problem of reaching the consensus on few options and then agrees on a block which could be a proposed one or an empty block (i.e. the process aborts on the approval of the proposed block). This complex algorithm permits to solve the main issues of the original PoW which are the waste of computational resources and the scalability problem.

Pros: high scalability; high throughput.

Cons: long and critical assignment of weight for reaching the consensus.

2.2.6.2.1.18) Proof of Burn (PoB)

The Proof of Burn is a method for reaching the consensus is an alternative way to PoW. The idea behind this algorithm is very simple: instead of using several expensive computational resources for mining a block, it is sufficient to invest some money sending coins (i.e. burning them) to a verified un-spendable address. This is a simple method for substituting the consuming of resources (which are consuming energy and hence money) with just money: in fact, the more money is burn (similarly to PoW, the more computing power is allocated) the higher is the probability to be selected for mining the following block. The original idea came from (Slimcoin, 2014) which described the first mining mechanism without powerful hardware.

Pros: environmentally friendly solution.

Cons: same as PoW.

2.2.6.2.1.18) Ouroboros

Ouroboros is a Blockchain protocol based on PoS and developed by (Kiayias, Russell, David, & Oliynykov, 2017) with the original objective of guarantee high security to the network while attempting to reach a scalable Blockchain. Ouroboros works in a different manner than original block based Blockchains: here the protocol works in a dynamic and synchronous way, proceeding in time slots which correspond to blocks. Then these slots are grouped into epochs and before an epoch starts, a committee elects a sequence of block producers for the slots within that epoch and the probability of being chosen as a producer is proportional to the number of tokens owned: after the block is produced the committee has to elect the following committee for the successive epoch.

Pros: higher throughput, higher scalability, higher security (note: compared to PoW).

Cons: not mature: it is still open to some attacks (e.g. 51% attack).

2.2.6.2.1.19) Proof of Authentication (PoAh)

This consensus algorithm, proposed recently by (Deschamps, Saturno, & Pertel, 2017), has the objective to create a Blockchain which is really "lighter", namely less resources-required, in order to be compatible with all the devices, even the smallest and most portable ones. The procedure for the PoAh is extremely simple and short: as usual, transactions generated by the participant in the network are combined into blocks but before a node broadcast its block, it signs it using its private key. Hence, in this Blockchain the blocks are modified as shown in the image, with the data field of the PoAh.

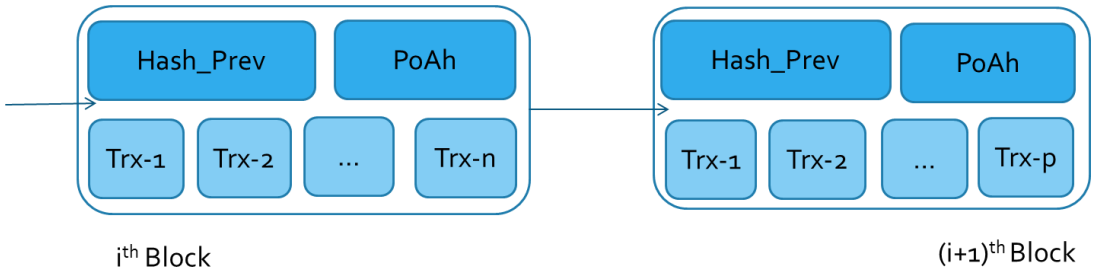


Figure 32: PoAh Representation in the Blockchain

In the network are present some trusted node that are responsible for the block validation: they role is to evaluate the signature of the block by checking the authenticity it. After the signature validation, also the MAC value of the node if tested and only when the authentication is considered successful the block is shared to the entire network, otherwise the block is dropped. Every time a node successfully authenticates a block, it increases its trust score: only the nodes with a certain trust score in the network are qualified to be trusted node.

Pros: lightweight Blockchain; faster and more scalable than PoW Blockchain; resource-constrained devices can be used.

Cons: the security of the network relies only on trusted nodes.

2.2.6.2.1.20) Proof of Devotion (PoD)

The PoD is a consensus protocol developed by the research (Nebulas Team, 2018). The Proof of Devotion is similar to the Proof of Importance (*see paragraph 2.2.6.2.1.12*) since they both utilize a ranking system for determining which nodes can be a block validator but here the eligibility is given by the *influence* a node has (based on the propagation of transaction and the liquidity). The algorithm starts by selecting only the top nodes in network; then these nodes demonstrates their involvement paying a deposit for proposing as block validator and randomly the algorithm chooses a set of validators. This set of validators participate in voting

round and only if more than two third of validator agree on a block it is added to the Blockchain. This set of validators is hence dynamic and changed for every block.

Pros: high security; better evaluation of nodes commitment than PoS.

Cons: same as PoI.

2.2.6.2.1.21) Byzantine Fault Tolerance (BFT)

In the *paragraph 2.2.6.1*, it was introduced the Byzantine Generals Problem, a typical situation which occurs easily in many systems in which a certain degree of coordination is needed. Blockchains, which are decentralized ledgers system and thus are not controlled by a central authority, require some kinds of coordination expedients in order to overcome the typical problems and class of failures that belong to the BGP (already mentioned in the previous paragraph). When a consensus mechanism is able to guarantee a solution to the Byzantine Generals Problem, then is called Byzantine Fault Tolerant.

Due to the high scalability (they are proposed as scalability solution, already explained in the *paragraph 2.2.4*) and high throughput that this kind of consensus algorithm are able to provide, different versions of Byzantine Fault Tolerance algorithm were development in the recent years:

- **Practical Byzantine Fault Tolerance** (pBFT) is one of the first solution proposed by (Castro & Liskov, 1999) and it optimizes the consensus protocol in order to make it tolerant to Byzantine Faults. pBFT provides a state machine replication (i.e. replicas are identical nodes in the network) that tolerates malicious nodes assuming that there are only independent node failure and only altered messages sent by precise nodes. The system consists in a set of nodes that are well-organized: one is the leader (e.g. node 0) and the other ones are called backup nodes (e.g. nodes 1, 2, 3). In the system is requested that all the nodes communicate with each other because this is the only way for honest nodes to come to an agreement, using a majority rule, about the state of the system. The complex communication between nodes, that could be seen as a waste of resources and time, is necessary in order to prove that messages effectively come from a certain node and that are genuine. There is a limit for the system to tolerate malicious nodes: they must be no more the one third of all the nodes in the network and hence the more nodes are present, the more the network is secure. The number of replicas R, that are necessary in a replica set |R|, for a given number of f faulty nodes is equal to: $|R|=3f+1$. The pBFT algorithm acts in four phases:
    1. A client sends a request to the primary node to demand a service operation

2. Primary node broadcasts it to all the backup nodes
3. Backup nodes execute the request and send back a reply
4. Client waits for *f+1* replies from the nodes with the same results (where f is the max number of potential faulty nodes).

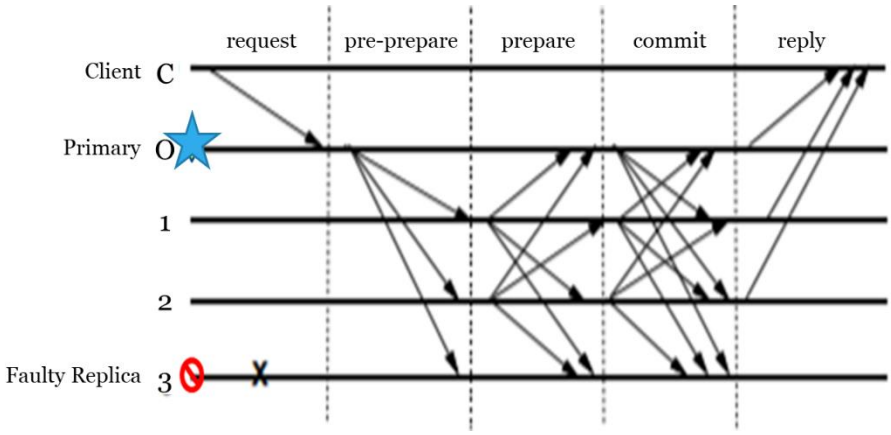


Figure 33: Phases in a Practical Byzatine Fault Tolerance

All the malicious nodes and messages are individuated in the network until the limit of one third of malicious nodes. After every step (which could be a block added to the chain), the primary nodes are checked for integrity and could be changed with other ones. Currently pBFT is used by Hyperledger Fabric which has a few numbers of preselected primary nodes on a private network.

Pros: High transaction throughput.

Cons: Centralized; fits private/permissioned Blockchain; does not scale well (in comparison to the following Byzantine protocols).

- **Federated Byzantine Fault Tolerance** (fBFT), also called *Federated Byzantine Agreement*, is a modification introduced by (Mazières, 2016) that improves considerably the performances of a Blockchain. The fBFT reaches and agreement on a status update (e.g. a new block added) using several *slots,* i.e. partitions, on which nodes at each consensus round must agree. This protocol uses *quorum slices* that represents subsets of *quorums*. A quorum is a set of nodes needed to reach an agreement in a distributed system: quorum slices are subsets of quorum that are able to convince a particular node about a certain statement. The main advantage of this consensus protocol is that a node does not need to trust the entire network but only its slice: the intersections and overlaps of quorum in the network permit an agreement. Then, in the fBFT there is a federating voting. With this method the protocol reaches an agreement on statements which are made by participants and a

four-steps voting process permits to easily converge on a result, that could add or reject a new block to the Blockchain.

***Pros*:** very decentralized; very scalable; low latency with high throughput**.**

***Cons*:** differently to pBFT, in fBFT each participant has freedom in selecting whom to trust; the network is open to nodes joining in a permissionless setting rather than having a permissioned node list.

- **Delegated Byzantine Fault Tolerance (dBFT)** is another version of BFT that primarily enables a large scaling solution. In this algorithm, formulated by (Zhang E. , 2014), not very differently from the DPoS, all the nodes in the network elect a group of consensus nodes and from this group a node called *speaker* is chosen casually while the rest of nodes in this group assume the role of *delegates*. It is responsibility of the speaker node to generate a new block using the transactions that are waiting to be added. After a block is generated, it is passed to delegates which validate it and approve the transactions. All the delegate must broadcast and compare their blocks in ore to verify that they all have the same hashes and only if more than two third of delegates are honest and agree on the new block it is added to the Blockchain. With this algorithm it is possible for a Blockchain to resist in case of the speaker is malicious, the delegates are malicious or both (always maintaining more than two third of honest nodes in the network).

  ***Pros*:** very fast scalable**.**

  ***Cons*:** partially centralized.

2.2.6.2.1.22) Proof of Believability (PoBe)

This typology of consensus algorithm aims at facing the problem of centralization which the Proof of Stake protocol originally has. The PoB developed by (The Internet of Services Foundation, 2017) is able to maintain a good compromise between safety and throughput; using a sharding system (*see paragraph 2.2.4*) the Proof of Believability can deliver high performance while providing resiliency against misbehaviours. This solution is based on an approach called “intra-shard believable-first” that works by dividing all validators nodes into two groups: a *believable league* and a *normal league*. The validators inside the believable league are considered believable and therefore they firstly process transactions very quickly but then a sample of transactions is verified in a second phase by normal validators in order to check and assure the genuineness of transactions. The probability to be elected as believable validators is proportional to several factors that effectively assure their good behaviour in the network. In addition, the low latency in block generation is provided thanks to the subdivision of believable validators in tiny groups and letting only one validator per group to produce a block per time. The dimension of these shards is calculated taking into

consideration the believability score of each validator: the higher is the score, the smaller will be the group (since trust is higher). When a believable validator is detected as misbehaviour, it is automatically defrauded of all tokens and its reputation is loss. The two different leagues can run in different consensus scheme and, in fact, the normal league is based on the PBFT (see *previous paragraph*) in order to achieve a good scalability with the thousands of normal validators.

Pros: more decentralized than PoS; higher throughput than PoS.

Cons: security still depends on believing several nodes.

2.2.6.2.1.23) RAFT

The Reliable, Replicated, Redundant, and Fault-Tolerant consensus algorithm, i.e. RAFT, was advanced by (Ongaro & Ousterhout, 2014) as an alternative to Paxos, a family of protocol used in a network of unreliable participant for solving the consensus issues (Lamport, The Part-time Parliament, 1998). Paxos was used to achieve consensus among a distributed network of nodes that communicate asynchronously one or more nodes propose a value to the algorithm and if the majority of the systems that are running Paxos agrees on the proposed value then the consensus is reached. RAFT is safer than Paxos and even able to provide additional features. It uses an elected leader for reaching the consensus: in the network every node can be *leader* or *follower* and during an election phase a *candidate* ask for becoming a new leader. This leader is randomly chosen between candidates and it becomes responsible for the updating of the network with all the transactions received by the network by sending messages to other nodes: it is equally responsible for adding new block to the chain and broadcasting to the network. For remaining in the status of leader, the node must send constantly and heartbeat message otherwise a new election phase is executed and rapidly a new leader is elected.

Pros: simpler but safer than Paxos protocols, more vulnerable than PoW.

Cons: used in small private and permissioned Blockchains; not scale easy.

2.2.6.2.2) General comparison between consensus algorithms

As already mentioned in *paragraph 2.2.6.2.1*, each consensus algorithm has several strengths and several weaknesses and therefore the choice of an algorithm depends on the precise utilization of the Blockchain: every algorithm has several benefits that distinguish it from the others and no algorithm has excellent performance in all the three components that concern the scalability trilemma.

Therefore, the table 1 compare 26 consensus algorithms that have been analysed in the previous paragraph, helping to understand their characteristics and assigning the couple of most appropriate key variable from the Scalability Trilemma (*paragraph 2.2.4*).

Table 1: Comparison between different consensus algorithms

Consensus Algorithm	Permission Control	Security (Se) Level	Decentralization (De) Level	Scalability (Sc) Level	Trilemma
PoW	Permissionless	High	High	Low	Se & De
PoS	Permissionless	Medium	High	High	De & Sc
dPoW	*Both*	Medium	Medium	High	De & Sc
dPoS	Permissionless	Medium	High	Medium	De & Sc
lPoS	Permissionless	Medium	High	High	De & Sc
PoA	*Both*	High	High	Medium	Se & De
PoRep	*Both*	Medium	High	Medium	De & Sc
PoET	*Both*	Medium	Medium	High	Se & Sc
PoSp	Permissionless	High	Medium	Medium	Se & Sc
PoH	*Both*	Medium	High	Low	Se & De
PoSV	Permissionless	Medium	High	High	De & Sc
PoI	*Both*	High	Medium	Medium	Se & De
PoId	*Both*	Medium	High	Low	Se & De
PoR	Permissionless	High	Low	Medium	Se & Sc
PoAc	*Both*	High	Medium	Medium	Se & De
PoT	Permissionless	High	Low	Medium	Se & Sc
PoWe	Permissionless	Medium	High	High	De & Sc
PoB	Permissionless	High	High	Medium	Se & De
Ouroboros	*Both*	Medium	Low	Medium	Se & Sc
PoAh	Permissioned	Medium	High	High	De & Sc
PoD	*Both*	High	Medium	Medium	Se & De
pBFT	*Both*	Medium	High	Low	Se & De
fBFT	*Both*	Medium	High	Medium	De & Sc
dBFT	Permissioned	High	Medium	High	Se & Sc
PoBe	*Both*	Low	High	Medium	De & Sc
RAFT	Permissioned	Medium	Medium	Low	Se & De

2.3) Evolution of Blockchain

Since its conception in 2009, the Blockchain has grown and evolved relentlessly. During its evolution, the main innovations have attempted to improve this technology trying to increase its performance, in terms of throughput and decentralization, and to provide new features seeking to make this technology more attractive for different applications.

In particular, the main efforts were spent on improving the consensus mechanism originally proposed by the Bitcoin protocol. Indeed, there are numerous and growing proposals for alternative algorithms with performance and features that are superior to the original ones. An attempt was also made to adopt new structures with which to construct and link the blocks to each other through the use of alternative data structures such as DAGs (*paragraph 2.3.1*).

One of the greatest innovations was then brought by Smart Contracts (*paragraph 2.3.2*), which allowed the Blockchain to equip itself with features that no technology could ever guarantee at the level of security and automation and which therefore only the Blockchain could satisfy.

Then several ideas tried to make the Blockchain more usable and scalable through Sidechain based on off-chain transactions (*paragraph 2.3.3*).

A more accurate explanation of these innovations is given in the following paragraphs.

2.3.1) Directed Acyclic Graphs (DAG)

Building a distributed database on a Blockchain, literally building it on a long chain of blocks structure, leads to a very rigid architecture from which is not possible to move without breaking security rules. In fact, it is not possible to place a new block in a position, which is different from the last one, as no forks are considered valid until a certain branch is defined the main one and all the transactions have to be added in a severe and chronological way. However, a different kind of architecture could be used for generating a more efficient Blockchain, with higher speed and increased reliability, while maintaining the same benefit of it (transparency, decentralization, immutability): DAG, directed acyclic graph, is a data structure used for ordering information in a topological way rather than a pure mere chronological one based just on timestamps. In a DAG every transaction, which is added, is able to confirm one or more previous transactions, creating a sort of *tree* between all the hashes placed in the network.

In literature, a directed acyclic graph is a particular kind of directed graph without any cycles (Thulasiraman & Swamy, 1992). It is very simple to understand DAG's properties starting with a common non-directed cyclic graph (*figure 35*):

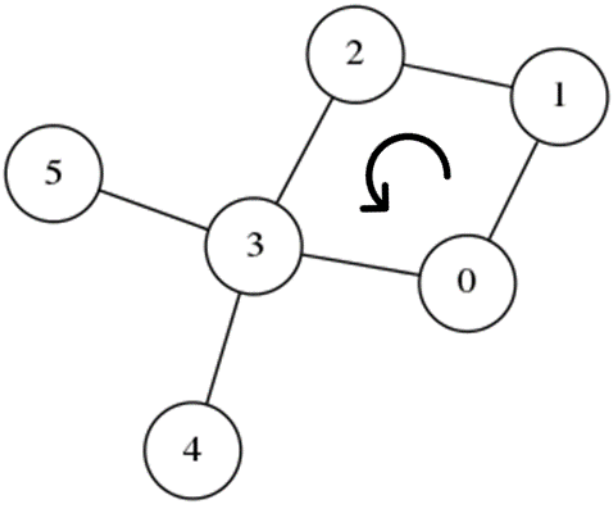


Figure 34: Simple Cyclic Graph

In this graph, the nodes are connected to each other but, in particular, nodes 0, 1, 2, 3 are connected together in a cyclic way: information can be passed from node 0 to 3 and returned back to node 0 without any node comes across more than once. In case of an acyclic graph, this phenomenon is not possible, and the graph does not have any circle for different reasons: it is *not possible to close* the circuit with a certain number of nodes or the information is *directed* and it does not permit to any information to come back to the previous node. The previous example could be modified in a DAG as follow (*figure 35*):

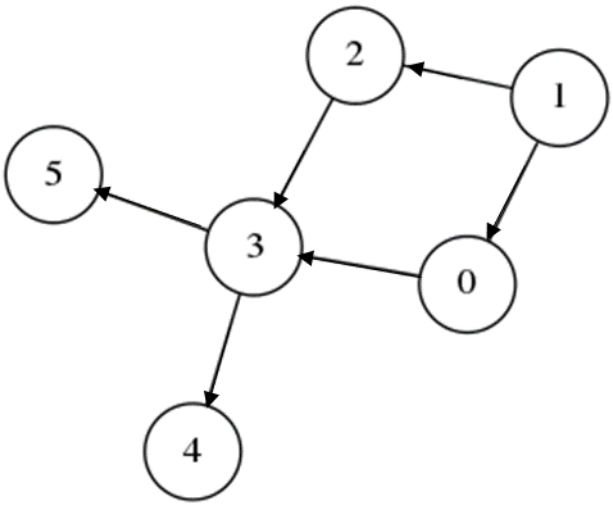


Figure 35: Directed Acyclic Graph

When there is not a path that can return the information back to the previous node, the graph assumes a structure that could be similar to a Blockchain under a forking event.

Figure 36: Blockchain-Similar Directed Acyclic Graphs

The Blockchain generally produces some forks but after a time period only one single branch survives, and the time used for the generation of blocks on the other shorter branches is wasted.

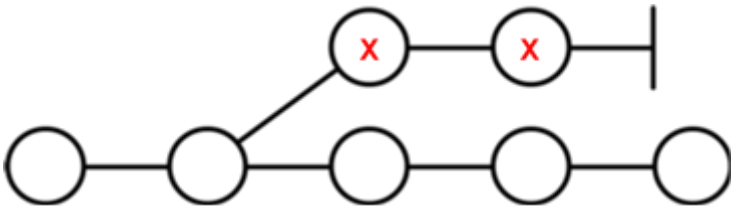


Figure 37: Forking Event in a Directed Acyclic Graph

Only using DAGs it is possible to allow the existence of multiples chains of blocks which coexists and are interconnected without forming any kind of cycles with previous parent blocks. With this configuration every chain of blocks can in parallel exist with the other because the information, and thus, the transactions are directed and ordered in a topological way.

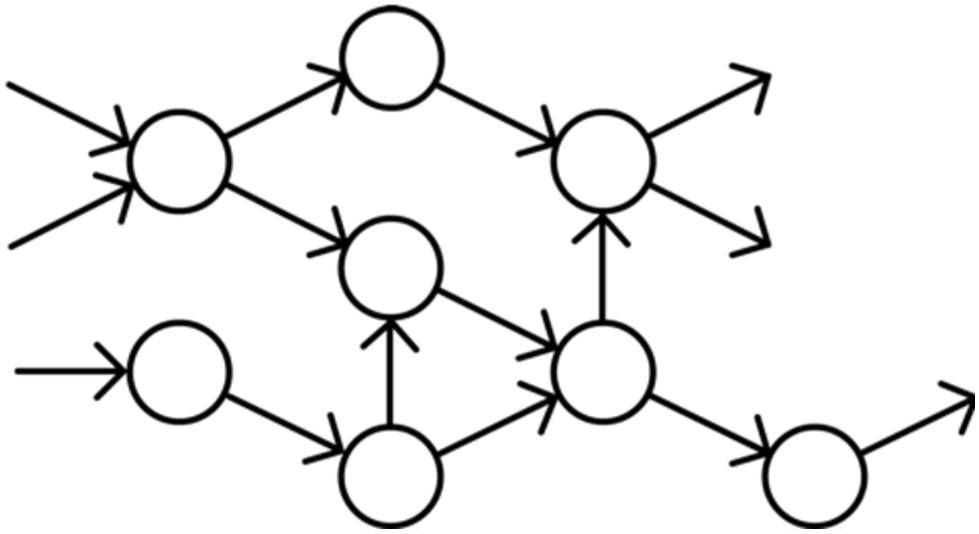


Figure 38: Complex Directed Acyclic Graph

This solution is evidently able to increase the potentiality of block linkages on multiple chains, permitting a greater scalability with also a throughput higher than linear Blockchains and less wasted time in validating blocks on eliminated branches. The architecture of Blockchain is deeply modified since there is no more a single chain of blocks but a sort of net of blocks that form a "*Block-Net*" (hence it should not be correct to talk about Blockchain if the underlying technology are the Directed Acyclic Graphs). Currently this solution is under development and it is not clear if it could be considered as secure as a common Blockchain but yet different projects are running with very innovative consensus protocol that must be profoundly modified in order to reach an agreement on blocks in such DAGs. Currently, the main Directed Acyclic Graph consensus protocols are:

- **Tangle**: proposed in a paper by (Popov, 2018) the Tangle is the consensus algorithm for the DAG used by IOTA Foundation. Instead of storing the transaction in blocks, all the transactions that are sent by different nodes are part of the Tangle graph, which is in practise the real ledger for the system. Every time a new transaction is added, it must approve two previous transactions making them connected together by the hashes.

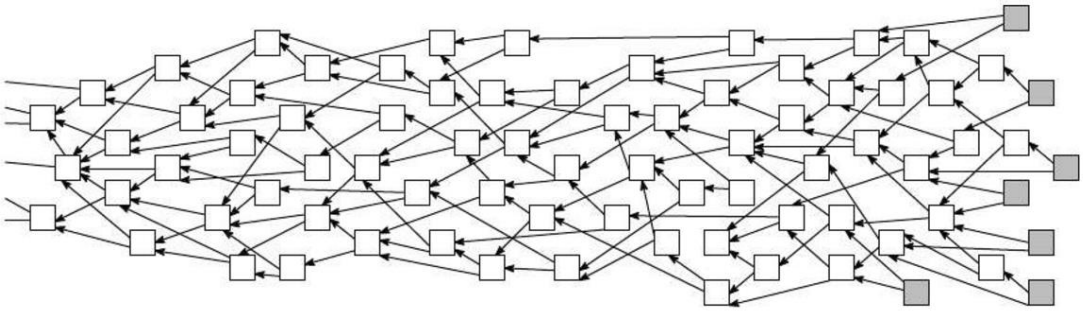


Figure 39: Tangle Directed Acyclic Graph

Similarly to the Blockchain, also here is present a genesis transaction which is indirectly approved by all the subsequent transactions in the graph. The mining mechanism changes because nodes here, in order to issue a transaction, must just put some effort in order to approve the other previous transactions: again, a small cryptographic puzzle is used for generating a nonce that is able to concatenate the hash of transactions. Of course, it is not possible to approve invalid transactions because the conflicting ones when detected by nodes are automatically discarded and cannot be added. Due to the fact that not every node can see contemporary all the transactions in the network and thus it is not able to check if all other nodes have already approved the same transaction, a consensus algorithm is used for giving a confidence level to transactions; so when a transaction is approved by a large number of nodes it has a higher confidence than the others and has the precedence on all the other conflicting transactions. In the paper is shown that this protocol reduces the confirmation times for transactions while improving also the security of the network. However, possible attack vectors are also documented in a Tangle network, in particular, if theoretically a single node is able to generate more than one third of the whole network transactions[1] it could convince the other nodes that its hacked transactions are valid. Therefore, the Iota Foundations itself, which is convinced that this problem is computationally unfeasible when the transaction volume is very high, introduced a centralized node called "Coordinator" which is responsible of checking the transactions and avoiding possible attacks in this growing phase of the network.

[1] This derives from the Byzantine setting in which no more than one third of nodes should be malevolent, *see paragraph 2.2.6.1.2*

- **ByteBall**: similarly to the Tangle (*see the paragraph above*), this decentralized system, deployed by (Churyumov, 2016), was developed in order to obtain a storage of tamperproof data, using typical storage units organized in small block of information linked to each other by hashes, but in this case the DAG, which establish a set of links

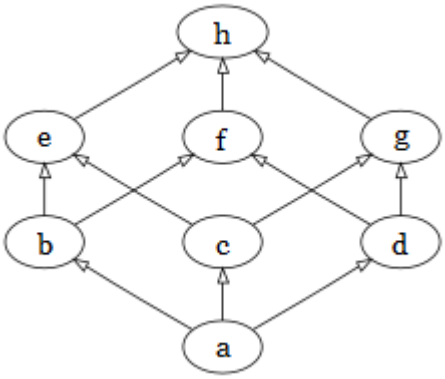


Figure 40: Couples on the same horizontal level are incomparable with each other but also some other pairs at different level, such as {b} and {g}, are also incomparable.

between different storage units, is able to determine a *partial order* between all the information while adding, differently from the Tangle, the "*main chain*" within the Directed Acyclic Graph establishing, in this case, a *total order* amongst single chains. In the order theory of mathematics (Simovici & Djeraba, 2008), the partial order of a set of elements is a property which gives to a binary relation over two elements reflexivity (each element is comparable to itself), antisymmetry (no two different elements precede each other) and transitivity (the start of a chain of precedence relations must precede the end of the chain). Hence, in case of partial order between two transactions within the DAG it is possible to compare them and establish an order but not for every pairs of transaction in the graph. Total order, instead, differs from partial order because every pair of elements is comparable.

This partial order property is very common in DAGs since it is not possible to assign an ordering between every couple of transactions. Hence, Byteball introduced an important novelty with the main chain for the reason that it allows to define an ordering between transactions: in fact, all the transaction which are inserted earlier on the main chain are believed earlier in the total order. Thus, in case of double transactions it is very easy to check which prevails because the transaction that comes earlier is deemed valid while all the others are void.

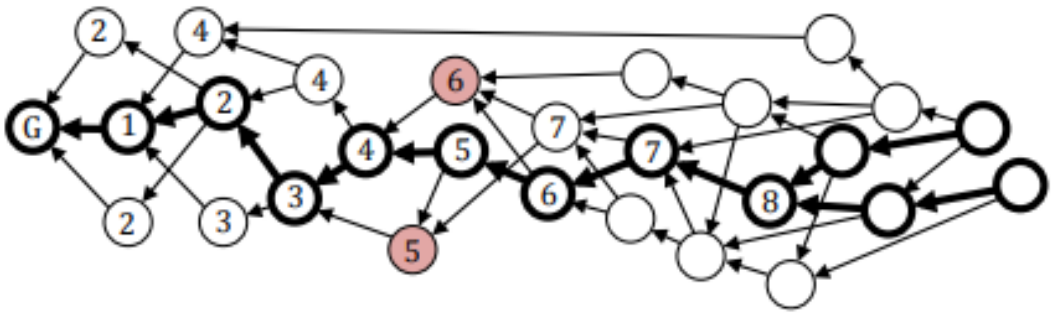


Figure 41: Double Spending on a Directed Acyclic Graph

In the *figure 41*, two transactions (the red ones) are creating a double spending problem but the transaction on the bottom wins because it is related to the main chain index #5 while the other is related to the main chain index #6 which is subsequent. The main chain is stated in a deterministic way based on the positions of transactions in the DAG and the transactions on which it is made upon are generated by well-known non-anonymous users called *witnesses*. These witnesses are included in a list that is shared amongst the nodes of the network and are elected based on strict security rules defined by the protocol. So, the consensus is generated thanks to the presence of some authoritative nodes responsible for the generation of main chain transactions which validate several previous transactions together with their hashes: such authorities could be reputable people or companies with a long-established reputation, interested in keeping the network safety. Another fundamental feature of the Byteball algorithm is the presence in the system of oracles that are necessary for any smart contract functionality in DAGs.

- **BlockLattice**: BlockLattice is the data structure on which is constructed the Nano cryptocurrency. This architecture was published by (LeMahieu, 2015) and differently

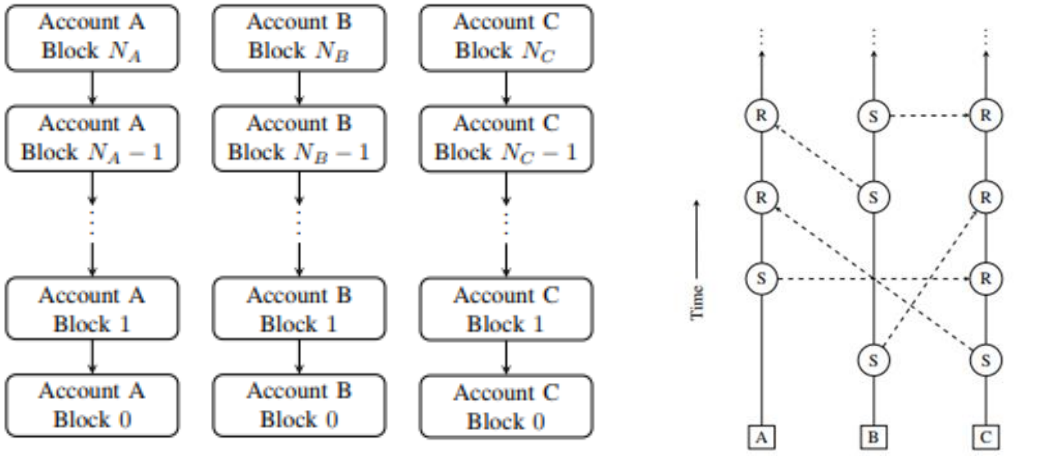


Figure 42: Representation of Account Balance (on the left) and Fund Transfer (on the right) in Block-Lattice Data Structure

revious algorithms, here the consensus is achieved by means of balance-weighted vote on conflicting transactions: it means that when two opposing transactions appear on the network, a representative node creates a voting survey about that block and receives votes by different nodes in the network and the results are then weighted with the number of coins of each vote (thus it is very difficult to receive many votes by many big stakeholders) and the losing transaction is discarded. This mechanism is possible thanks to the block-lattice structure in which each account in the network owns its personal Blockchain and it is responsible for the updating of it. Only the involved Blockchains of the transaction, hence the sender and the receiver ones, are updated immediately while the rest of the block-lattice is asynchronously refreshed.
The interconnections between Blockchains create the DAG. The peculiarity of this system allows an almost infinite scalability since every node is responsible to keep its own Blockchain and a very fast network with high throughput because single nodes are responsible for mining the new added transactions in a block. However, the network is vulnerable to different attack vectors and one in particular, the Penny-Spend Attack, where an attacker just creating cheap and numerous transactions is able to waste the storage resources of nodes, is an issue to be taken into account while deploying such systems.

- **Hashgraph**: the Hashgraph has been developed by (Baird, 2016). This innovative protocol is used for a data structure very different from the classical Blockchain: here, instead of having data stored in blocks, there are several *events* which contains several transactions, the timestamp of the event and both the hashes of the two parent events: the *self-parent* and its *other-parent*.

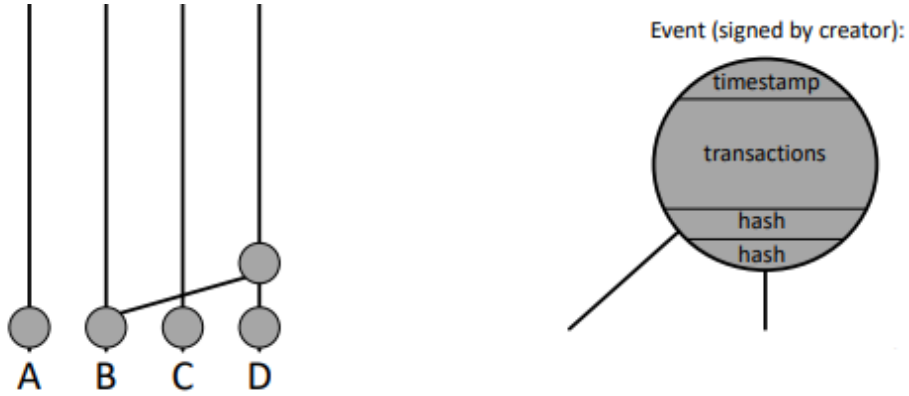


Figure 43: Events Representation on Hashgraph

The events are shared between nodes through a *gossip protocol* which is responsible for spreading the information randomly amongst all the different participant in the network starting from the neighbour nodes and hence creating the *graph of hashes*.

The events are ordered through the timestamp contained in them and then are validated through a specific consensus protocol. Consensus is purely based on the connection graph (which is by construction a Directed Acyclic Graph) and does not require additional effort from the nodes of the network. Initially the Hashgraph is divided into different rounds and the criteria for starting a new round is topological: when a new added event can have paths for more than two third of the nodes of the population within the previous round, a new round starts. The connection is checked by going up the hashes of the event.

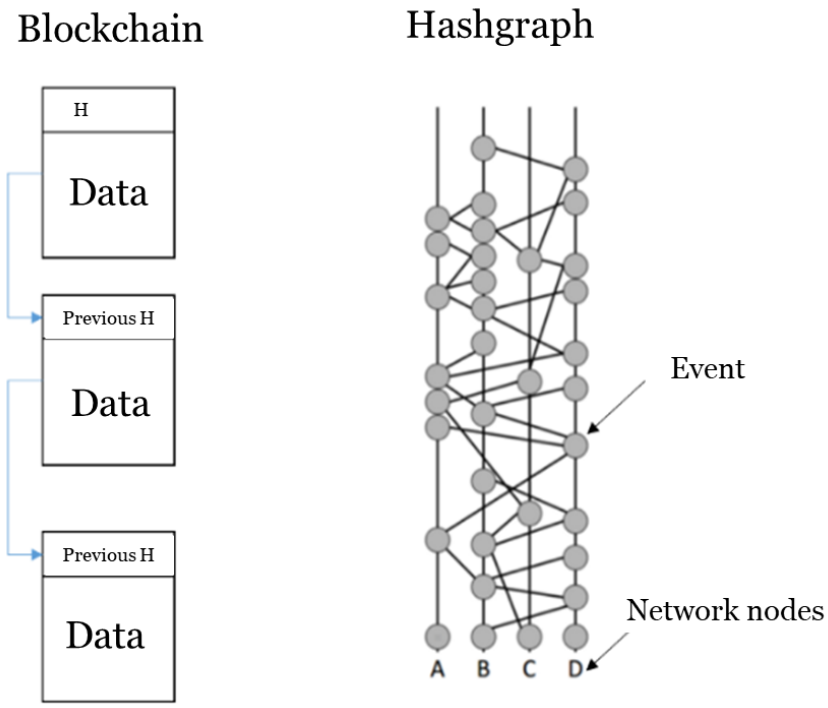


Figure 44: Comparison Between Blockchain and Hashgraph

Whenever a new round has started, the first events of the current round are considered and begin an election about one first event of the previous period per time: when it is possible to highlight an entirely downward path from more than two third of the first nodes of the current period with the first node of the previous period.

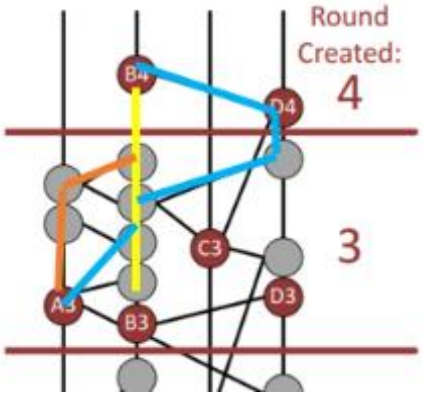


Figure 45: Round Creation and Election Starting

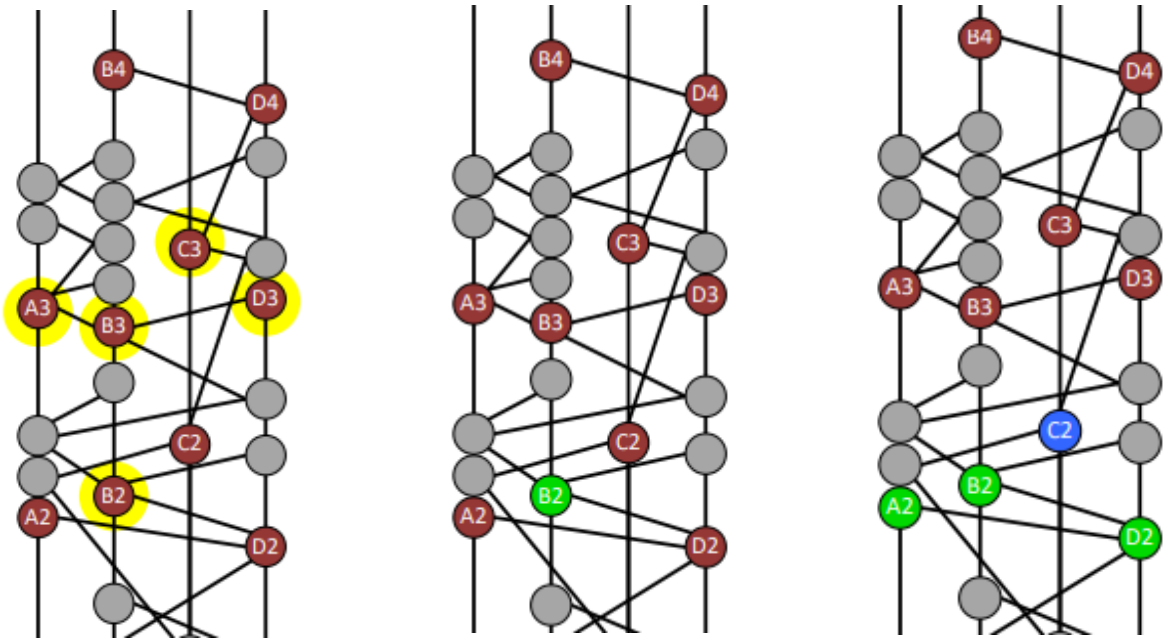


Figure 46: Election Mechanism for Reaching Consensus and Confirming Events

When the election gives a positive result, the events are confirmed and the consensus is reached otherwise it remains unconfirmed until new events, which provide new paths, are added. This consensus mechanism permits an incredibly high transaction per second which is only limited by the bandwidth of the internet on which the Hashgraph is running. However, one of the biggest limits is the actual permissioned structure in which all the nodes are known, and the identity is the main protection against possible attack. No additional security mechanisms are put into practice and hence and this represents a big limit for scalability in case of public applications of Hashgraph.

- **Holochain**: it was presented by (Harris-Braun, Luck, & Brock, 2018) as a solution for the scalability Blockchain issue. Holochain uses a multiple ledger system owned by each node in the network: every participant manages its own chain by adding data or sending transactions interacting with other peers. These multiple chains can merge or split, and several interactions may occur thanks to a peer-to-peer networking for processing and reaching consensus between users. This system hence permits to any device, even a smartphone, to own its chain-based ledger system.
- **Spectre**: in a paper proposed by (Sompolinsky, Lewenberg, & Zohar, 2017), it was described a scaling solution that uses a combination of DAGs and Proof of Work in order to reach a scalable consensus (SPECTRE stands for: Serialization of Proof-of-work Events: Confirming Transactions via Recursive Elections). Differently from PoW Blockchain, where blocks added to the chain contain only a single hash from one parent block, in Spectre blocks are created in parallel and connected by multiple

parent hashes through a Directed Acyclic Graph. The consensus is reached through an algorithm which, using a recursive voting system, confirms “parent block with most following children”, similarly to the concept of “the longest chain wins”. The algorithm itself is able to decide between conflicting transactions allowing a very high throughput with a high security level.

2.3.2) Smart Contracts

The first idea of smart contract was proposed in 1994 by Nick Szabo who originally defined a protocol to carry out computerized transactions that automatically execute the terms of a contract: this was the first example of smart contract and it was initially intended for the sale of financial assets such as derivatives and bonds.

His work is the basis of the current functioning of smart contracts: in fact, recently this technology has been made possible thanks to the use of software programs which, by inserting information blocks in the form of transactions within the blocks contained in the Blockchain, allow execution automatic smart contracts. They operate in an if-then-else logic, enabling the deployment of transactions once the terms stipulated in the contract, which are coded directly inside the smart contract, are met. Since they are based on the Blockchain, they mainly enjoy three foundational properties: they are self-verifiable, self-executable and tamperproof.

In fact, these pre-programmed rules permit the self-executions of contracts without the need of any intermediary and for this reason it is possible to affirm that smart contract guarantee that for any given input there will be a known set of outputs. It is the underlining Blockchain technology, upon smart contract are deployed, that guarantees the working mechanism of these intelligent agreements that are hence able to connect the decentralized ledger to the different decentralized applications (dApps) that run and communicate through the Blockchain by means of different functions that are possible thank to smart contracts.

Each application is then able to use numerous smart contracts, even simultaneously, making it possible to carry out various activities such as the sale of an object or service, sharing a post or comment and much more, finding use in many different sectors and with numerous features that open up to diverse innovative possibilities or business models. All this is made possible thanks to the various advantages that smart contracts offer, and which can be enclosed in five key points that are:

1) *Autonomy*: once stipulated, they can be activated by themselves without anyone that have to verify or activate them. They are able to provide the outputs for which they have been programmed automatically.
2) *Immutability*: all the information on which they are based is immutable and also transparent (in the case of public Blockchains) and does not allow the modification of the agreements nor their elimination.
3) *Security*: since they are based on decentralized Blockchain ledgers, it is not possible to obtain the outputs without certain inputs having been attained into the Blockchain, nor to modify or manipulate the results of these contracts in any way.
4) *Accuracy*: in addition to being automatic, they are also extremely precise as they are able to produce specific outputs when certain precise conditions occur, eliminating any risk of human error.
5) *Trust-less and intermediary free*: they are able to work even if there is no mutual trust between the authors of the contract and it is also not necessary to involve any intermediary for their operation or verification.

2.3.3) Side Chains

Sidechains are an alternative off-chain solution (*see paragraph 2.2.4*) for Blockchain that aim at increasing the scalability of standard Blockchain technology.

The Sidechains are an innovative mechanism by which the Blockchain technology tries to evolve in an attempt to solve its scalability problems. The basic mechanism of operation of a sidechain allows to move transactions, and therefore tokens or other digital assets, from a Blockchain to another secondary one, to be eventually placed back in the original Blockchain if necessary: this simple and intuitive mechanism allows to supply promising functionality to a Blockchain.

By transferring information from a Blockchain to its Sidechain, of course, it is not possible to actually transfer information or value from one chain to another but simply it is possible to link certain values (concretely, hashes) from a main "parent" Blockchain, in which these values are blocked and momentarily technically no more available, to a secondary "child" Blockchain, in which such hashes can be transformed and processed independently of what in the meantime happens in the main Blockchain.

This therefore allows unprecedented interoperability between Blockchains, as even completely different architectures become perfectly compatible when they are implemented

through diverse Sidechains, thus allowing a massive scalability of the Blockchain. Furthermore, it is possible to combine Blockchains that execute different functions (payments, smart contract, asset transfer ...) and therefore operate with different logics and algorithms, allowing to prefer speed, security, decentralization for each different Blockchain without compromising the operation of none and thus achieving optimization at a global level.

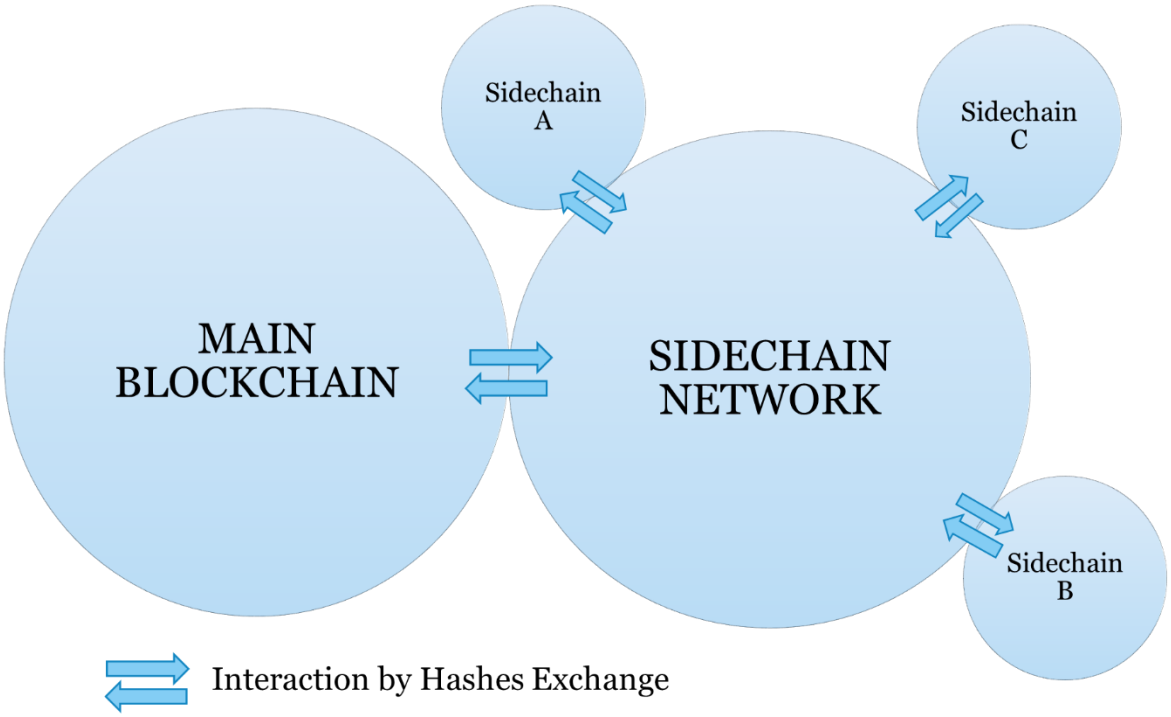


Figure 47: Representation of a Sidechain Network with Three Sidechains

2.5) Blockchain Application Industries

The Blockchain technology has many diverse usages and new applications of this technology are incessantly introduced across different industries. Therefore, it is interesting to study some recent use cases amongst different businesses, creating an overall classification of applications fields, before exploring more in deep the potential usages of Blockchain for the manufacturing industry, understanding at that point to what extent it is impacted by this technology in comparison to the other businesses.

2.4.1) Classification of Blockchain Application by Industries

A) <u>Banking, Finance & Insurance</u>

This is probably the sectors that has been the more exploited by the Blockchain technology thanks to the potential of this technology to transform and reshape completely the banking and financial industry.

According to (Holden, 2018), the implementation of Blockchain in this sector will enable banks and financial institutes to save up to $27 billion by the end of 2030 on international transactions, reducing costs by more than 11%. However, this is only one of the many ways in which Blockchain will affect the financial industries allowing institution to save billions of dollars with the distributed ledger technology.

Some different example of Blockchain application in this sector may be:

- *Global Payments*
- *Insurance*
- *Syndicated Loans*
- *Trade Finance*
- *Automated Compliance*
- *Asset Rehypothecation*
- *Custody and Proxy Voting*
- *Equity Post-Trade*

B) <u>Supply Chain</u>

Considering a supply chains at a global level, they can support every item from raw materials to finished and packaged consumer goods. Blockchain technology is still able to improve efficiency and traceability and to reduce unfair behaviours even in the most technological advanced supply chains. For instance, according to (Sluijs, 2017), in the container industry the paperwork, which could be substituted by Blockchain technology, can account for almost half of the cost of transport. *Cost saving* is not the only reason which push towards Blockchain adoption; in fact, according to a study conducted by (Oceana, 2013) in the USA, the seafood is mislabelled up to the 87% of

the time generating *frauds* or *errors*, while according to (Schipper & Cowan, 2018) the mica is frequently sourced from *illegal* mines by child laborers.

Moreover, many sectors like luxury, electronics and pharmaceuticals are susceptible to *counterfeiting* product due to lack of traceability.

Hence, it is possible to recognize three kind of properties that Blockchain could guarantee in the supply chain context which are:

1. Traceability: it increases operational efficiency by tracking and representing the companies' supply chains.
2. Transparency: it creates trust by providing data like certifications and claims and by opening to everyone the access this information that does not need to be certified by third parties and may be updated and validated in real time.
3. Tradability: Blockchain technology allows to create tokens connected to assets, building a digital identity over physical object and creating shares that represents its ownership. So, similarly to stock exchange, assets could be traded through these tokens and the ownership may change and be transferred without the physical moving of the asset.

Some different example of Blockchain application in this sector may be:

- *Reduce Counterfeiting*
- *Product Recalls*
- *Enhancing Supply Chain Transparency & Process Tracking*
- *Regulatory Compliance & Reporting*
- *Enable Efficient Ownership & Licencing*

C) Energy

Blockchain has the capability to renovate also the energy sector and energy companies, from utility providers to oil & gas enterprises, agree about its transformative impact. Indeed, in the recent years, the energy industry run into numerous innovations such as rooftop solar, smart metering, electric vehicles, etc. and now the distributed ledger technology, with the deployment of smart contract, is disrupting the sector. It is able to permit a high degree of system interoperability opening to a very wide set of application for energy and sustainability: according to a recent report from (PwC & Stanford Woods Institute, 2018) there are more than 65 developing Blockchain applications for the environment since the Blockchain technology has capability to track the chain of custody for grid material and it is a unique solution for renewable energy distribution: the main benefits from its adoption are the reductions of costs, the increased transparency for stakeholder

(without compromising privacy) and, last but not least, the environmental sustainability.

Some different example of Blockchain application in this sector may be:

- *Peer-To-Peer Energy Trading*
- *Wholesale Electricity Distribution*
- *Electricity Data Management*
- *Commodity Trading*
- *Oil & Gas Resource Exploration, Storage and Transportation*
- *Utility Providers*
- *Refined Resource Management and Sale*

D) <u>Real Estate</u>

Even the real estate industry could benefit from the Blockchain technology. It may enhance the different typical operations of this sector by means of automation, tokenization and access to real time info. Nowadays, the typical systems employed are independent from each other and difficulty interconnected impeding the interoperability between different real estate networks. The distributed ledger technology can reduce costs and enhance transparency together with an increase of data accessibility and a reduction of human error, offering solution that optimize actual processes and also eliminating the third-party mediators. Indeed, even if in the real estate industry the know-how and the advice of experts remain decisive, there will be huge changes in all the administrative tasks like document and securities processing, accounting processes and liability management.

Some different example of Blockchain application in this sector may be:

- *Asset Tokenization*
- *Asset Management and Real Estate Funds*
- *Land Titles and Deed Records*
- *Property Sale and Title Assignment*
- *Investor and Tenant Identity*
- *Real-Time Accounting*
- *Payments and Leasing*

E) <u>Government & Public Sector</u>

The public sector and the government may take enormous advantages from the usage of Blockchain becoming more modern and efficient. Governments can employ this technology for dealing with complex challenges like the transparency and accountability that always need to be clearly demonstrated, the public request for improving performances as well as reducing costs, etc. Contemporary governments

may become more flexible and secure, making lean and efficient many public functions and promising different benefits such as a safe storage of citizen & business information, a decrease of manual activities and expensive processes, an elimination of chances for corruption or abuse and a general intensification of trust in the government and in the whole public systems: indeed, a distributed ledger-based system can create a digital government that protect data and modernise processes, reducing wastes, fraud and abusive actions generating an increase in trust thanks to the innate properties of Blockchain technology. In addition, the public administration benefits from Blockchain technologies since it enables a secure and efficient tracking and management of digital identities, offering to many digital identities issues a solution in which identity can be, in a safe way, univocally identified and cannot be refused nor tampered. Indeed, with Blockchain-based systems the identity authentication would be done through an irrefutable verification by means of digital signature based on public key cryptography, enabling different useful applications.

Some different example of Blockchain application in this sector may be:

- *Smart Cities*
- *Validation of Education and Professional Qualifications*
- *Tracking Vaccinations*
- *Tracking Loans and Student Grants*
- *Payroll Tax Collection*
- *E-Residency*
- *Immigration & Biometric Identity*

F) <u>Healthcare & Life Science</u>

Another sector that the Blockchain will probably exploit is the healthcare one: in the last decades, the trends in this industry observed the centralization of data systems together with the regulation of health data with a focus of digitalizing them through different Electronic Medical Record service providers. However, all the stored information kept by healthcare providers do not interact with pharmaceutical firms no other stakeholders in the health environment. This lack of interoperability generates different issues rising up several troublesome situations when, for instance, a patient demands for medical services from other healthcare providers, when the author of a clinical test desire to validate the medical data of its participants or when pharmaceutical firms put effort in assuring the authenticity of drugs in the markets.

Hence, due to the inability to share medical records in a safe way, patients are requested to spend time and resources in redundant medical care (e.g. repeated tests) while in emergency occasions doctors may not have a full visibility over the medical history of the subject, exposing to inappropriate treatment. In addition, considering

the drug traceability, it is critical to prevent the diffusion of counterfeit medicines which create huge risk every time ingredients are altered or in illegal proportions due to the risk of even fatal side effects.

Some different example of Blockchain application in this sector may be:

- *Secure Management of Electronic Health Records (EHRs)*
- *Patient Consent Management*
- *Drug Traceability*
- *Data Security in Clinical Trials*
- *Decentralization & Interoperability of Medical Data*

G) <u>Media, Music & Entertainment</u>

Blockchain is useful as well in the entertainment industry: digital piracy, duplication of digital items, violation of intellectual property, etc. are frequently and common in these sectors. Applying this technology may finally help to prevent all these issues. For example, in the music industry, distributed ledger technology may rationalise ownership rights and help deliver correct payment for artists' work while conveying transparency to the whole industry.

Some different example of Blockchain application in this sector may be:

- *Digital Piracy Reduction*
- *Intellectual Property Safeguard*
- *Protection of Digital Contents*
- *Distribution of Authentic Digital Collectibles*
- *Music & Video Royalty Management*

H) <u>Manufacturing</u>

Blockchain has the potentiality to be applied in a wide range of manufacturing areas from the procurement and strategic sourcing to the plant operation and quality controls: this technology enables new way of doing manufacturing businesses: therefore, since the objective of this thesis it to explore the applicability of Blockchain to manufacturing, an accurate analysis is performed in *following paragraph 2.4.2*.

Some different example of Blockchain application in this sector may be:

- *Protecting & Monetizing Critical Product/Process Intellectual Property*
- *Authentication of IIoT devices*
- *Simplifying & Safeguarding Quality Checks*
- *Configuration Management*
- *Advancing Machine as a Service*
- *Enabling Machine Controlled Maintenance*
  Improving Trust in Products through Public Data

2.4.2) Classification of Blockchain Applications in the Manufacturing Industry

One of the greatest potentials of Blockchain technology to deliver business value, is in the manufacturing field (Dieterich, et al., 2017) and, indeed, it is essential to comprehend how Blockchain technology can contribute for the next evolutional step of current traditional factories which may transform them into the future smart factories (i.e. smart manufacturing systems) which are, by design, more flexible to adapt to production requirements and more efficient regarding the management of resources.

Digitalization, in the recent years, is a phenomenon, which is spreading all over the world, and the manufacturing sector too is quickly becoming more and more digitalized and interconnected. In the factories of the future, there will be a sharing of data between a complex network of machineries, parts, products, and value chain members together with equipment providers and logistics companies. In fact, this interconnection will not affect only the supply chains with suppliers, strategic sourcing, procurement, etc. but also every area of the manufacturing including machine-level monitoring, maintenance, prototype protection, etc. enabling totally new manufacturing business models. Traditional databases are not always the right solutions to all the previous tasks and while looking for a solution, manufacturers should start considering the Blockchain: the distributed ledger technology is well suited for facing the challenge of sharing data safely inside and outside the factory walls, offering great benefits in environment where there is no trust between parties that need to share, store or capture critical data.

Considering that one of the main pillars of Industry 4.0 involves the collection of data whenever it is possible, the analysis of Blockchain technology as a possible interconnection method is very appropriate. In fact, nowadays data collection is done through systems which permits to acquire, process and exchange data with tools and devices installed in suppliers' factories or owned by customers. Therefore, the reaching of a high level of connectivity is a key objective which is aimed by the Industry 4.0 paradigm through making usage of aforementioned innovative technologies (e.g. Big Data, Analytics, Cloud, IIOT, etc.) that enable an autonomous communication between thousands of industrial devices distributed all over the factories and on the internet.

This process, which is enabled by new technologies, pushes toward the evolution of the current communication paradigm, that is based on a cloud communication architecture or an internet service-oriented architecture, enabling a new industrial network in which all the parties and involved in the information exchange exactly like a Peer-to-Peer environment (f*igure 53)*.

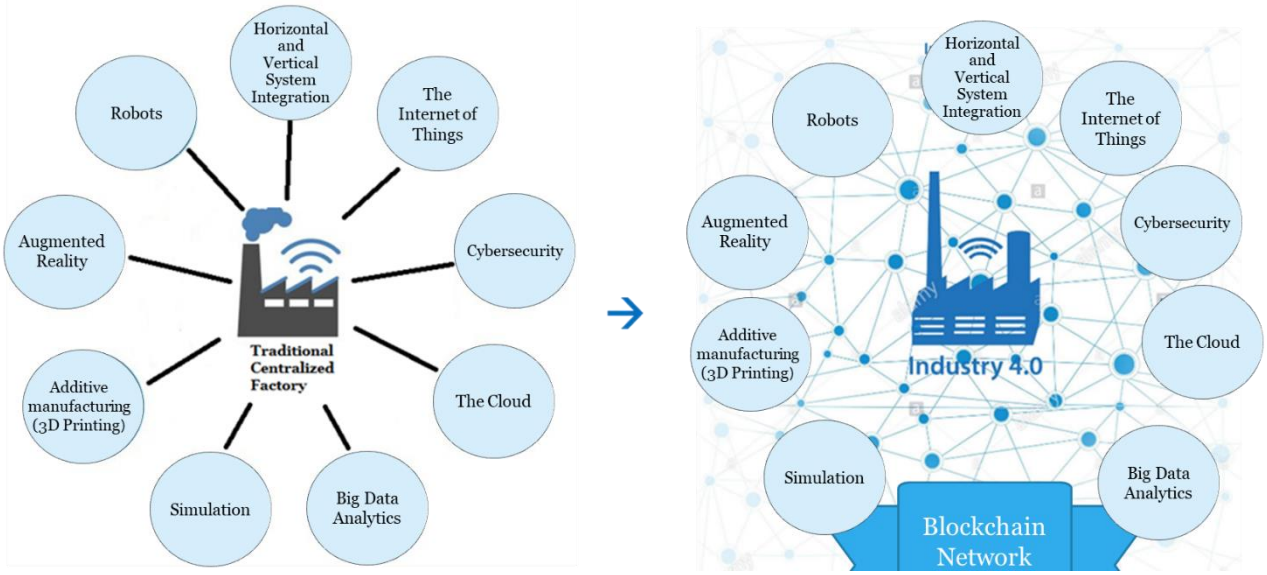


Figure 48: Decentralization of Factory in Industry 4.0 with Blockchain. Adapted from (Rüßmann, et al., 2017)

Hence, Blockchain may be considered one of the most promising technologies in the industrial sector owing to its potentiality in the creation of distributed networks and its capability to deal with the current industrial challenges (*analysed in paragraph 3.5*).

Most of the abovementioned difficulties can be handled by the Blockchain because it is possible to exploit the potential of the decentralized ledger in order to store all the accomplished transactions in an immutable way.

Supply chains, foundational elements of every manufacturing business, were the first that had made use of distributed ledger systems thanks to an approach of aggregating transactions, regarding values or assets exchanges, into blocks in order to enhance the overall supply chain efficiency by refining supplier order accurateness and simplifying traceability letting manufacturers to meet delivery dates and increasing product quality thus selling more.

Nevertheless, supply chains are just one of the first applications of Blockchain in manufacturing: the reason why Blockchains started in this context is due to a structure based on transactions which is very similar to the digital currency one in the financial sectors. Originally, first generation of distributed ledgers were not suitable for other industrial applications due to a limited network scalability and interoperability with low processing speed. Only recently, with new consensus algorithms under development, it is possible to increase the verification speed thus improving network efficiency and reducing computing costs.

With the recent efforts for improving the Blockchain performances, it is becoming possible to use together IoT and Blockchain technology opening to the possibility of creating a connected network of devices for the factory of the future. However, this interaction requires some standards for communicating and transmitting data: only if a defined standard will be universally accepted, it would be possible to reach higher levels of interoperability, security and transparency compared to the ones of actual systems; until that moment many Blockchain may remain in the proof-of-concept phase.

Recently, for instance, the (Trusted IoT Alliance, 2019), a project between several technology leader (like Cisco Systems, Bosch, Siemens, etc.) and different startups, has started with the intention of developing an open source standard for the integration between Internet of Thing and Blockchain technology with a particular focus on the deployment of an interface for smart contracts that will permit to move data seamlessly within and between Blockchain enabled systems. For now, this application focuses on supply chain, but it is envisioning the creation other applications for supporting undisputable documentation and trusted hardware proof of identity: after established a proper standard, it should be adopted by factories inside their HW and SW in order to make the most of Blockchain technology.

It is noticeable the contribute of BaaS (Blockchain as a Service) for simplifying the Blockchain's implementation inside the companies since originally distributed ledgers are self-managed so firms must customize the database's capabilities but also manage and host the node locally or in the cloud. Instead, the Blockchain as a Service is able to provide the same features while also adding other tools for facilitating management and deployment at scale: this is a great possibility for all those manufacturers with limited technical skills or which are lacking ad-hoc technical infrastructures.

It is possible to classify the Blockchain applications for manufacturing on the basis of the type of activity in which the technology is affecting the processes. All the following examples can be grouped into different categories representing various typical activities within a factory that are performed for creating value for customer. Therefore, the *Porter's Value Chain* could be a useful tool for mapping some of these Blockchain application in manufacturing; here is provided a more detailed description of the only categories involved in such applications for manufacturing in *figure 49*.

Figure 49: Porter's Value Chain. Adapted from (Porter, 1985)

Some different cases of Blockchain application in manufacturing, grouped using the Porter Value Chain, may be:

2.4.2.1) Inbound & Outbound Logistic/Procurement

- **Enhancing Track & Trace – Supply Chain Management**

  Blockchain can be used, as already explained in *paragraph 4.1*, for supply chain management thanks to the possibility to share data precisely and safely in an easy way even in complex supply chains.

  Distributed ledger systems have immutable and tamperproof digital record of any material, item and subcomponent exchanged by firms creating endwise visibility and thereby a source of truth to all the participants. These advantages are very important when supply chains have many participants with different IT systems or if there is not trust among members or a frequent need to involve new ones.

2.4.2.2) Product, Process & Technology Development

- **Protecting & Monetizing Critical Intellectual Property**

  The protection of Intellectual Property is extremely critical in the manufacturing world. It is not only a matter of costs, but it is crucial to take decisions regarding the choice of building internally parts or to outsource the production of them with the risks linked to the sharing of sensitive models and patents.

  In this context, Blockchain can help in preventing the steal of Intellectual Property and prove the ownership to the right patent holder preventing eventual disputes.

(Bernstein Technologies, 2019) is a recent example that developed an online service for permitting users to register Intellectual Property rights into a public Blockchain by creating a certificate which demonstrates the presence, integrity and rights of the IP.
Blockchain can do even more: it is a solution for helping companies to protect and control Intellectual Property when monetizing digital assets for instance in cases where machines, connected to the distributed ledger, produce parts with digital project documents stored in the ledger. In this case, the firm owner of the projects can exploit a licencing model for monetize the information that was made available to the company which is producing the part through the Blockchain itself.

- **Authentication of IIoT devices**
  With the fourth industrial revolution, a large number of devices and sensors are invading industries and manufacturing. But with the arrival of IoT it becomes critical to create a network in which the integrity of the data that is exchanged through the devices is guaranteed, even because these data are collected for subsequent big data analysis. So, to provide a network in which IOT devices are authenticated, monitored and through which information can be exchanged in a secure and immediate manner, the combined use of the Blockchain with IOT becomes fundamental. A recent example is (Xage, 2019) a Blockchain-protected cybersecurity model for industrial operations which provide a security layer for industrial IoT.

2.4.2.3) Operations

- **Simplifying & Safeguarding Quality Checks**
  Another objective for smart manufacturers of tomorrow, consists in increasing the value for customers and this could be accomplished with distributed ledger to support quality control. In fact, it is not easy nowadays to show a complete documentation to clients regarding the quality of production processes and materials used because it would require some expensive third parties that provide an IT infrastructure that guarantee a certain degree of transparency: Blockchain is a good solution for assuring quality. Moreover, inbound logistics could be supported by Blockchain thanks to the registration on a distributed ledger of all the quality control checks and production process data about an inbound part. It is necessary for a manufacturer, in this case, to implement an automated quality check that writes measurement directly into the Blockchain thereby creating a database containing a univocal tag for each item with its production history, modification and quality control supporting an access to data to multiple parties that can reduce or eliminate inbound quality control by assessing the checks that the supplier has performed. In addition to this, a manufacturer by using original equipment with Blockchain technology will be able to cut any intermediary ensuring automatically authenticity thanks to the certificate capability

of the distributed ledger. So, in manufacturing Blockchain can prove not only the origin of parts but also verify that parts meet some appropriate specifications.

- **Configuration Management**

  Blockchain can be used for creating, on an immutable ledger, a list of all the components, settings, parts versions, software firmware etc. of a unique product, creating and managing respective certificates of functionality or performance. In this way, the configuration would be stored securely and permits to be transparently verified: any mismatch between components will be easily detected.

- **Advancing Machine as a Service – MaaS**

  The Blockchain technology is an enabler for the innovative machine as a service (MaaS) pay-per-use model in which machines and equipment, instead of being sold to the manufacturer (i.e. final user), are charged by the machine provider (i.e. supplier) proportionally to the output that the equipment has generated. For instance (Steamchain, 2019), instead of selling an industrial labelling machine, it would be feasible to sell working hours (€/h) or even ask for a payment for a fixed number of labels processed (€/# labels processed). By using a MaaS model, the benefits for manufacturing firms are remarkable since they can avoid large initial investments and can even effortlessly upgrade or downgrade equipment to exploit the latest technology or to save money when lower performances are enough or the machine is not needed and so it is not working: therefore, it becomes evident that this new pay-per-use model may increase the production flexibility of companies.

  Nowadays first adoptions of this model are limited to very basic and easy measurable applications (e.g. industrial labelling machine) but the distributed ledger technology may permit more elaborated MaaS applications like the intellectual property protection (e.g. in case of additive manufacturing), the documentation management and even the performance tracking. Through the usage of a distributed Blockchain ledger, it is possible to generate a usage record which turns into a smart contract allowing a machine to automatically pay for services. For example, properly recording operational parameters onto a Blockchain, like an overall machine utilization together with consumables usage, machineries can autonomously send payments to the supplier for the utilization that the manufacturer has requested also allowing the machines user to activate/deactivate particular features on demand.

- **Enabling Machine Controlled Maintenance – Better Tracking of Maintenance Work**

  New maintenance approaches can rise with the Blockchain technology, generating automated service agreements and shorter maintenance times. Such kind of innovations are of extreme importance for the future development of manufacturing

since they are able to manage the complex circumstances that arise from the technological progresses of very advanced production machines.

For simplifying the maintenance in outsourcing, the distributed ledger can be used for registering service agreements and saving all the documentation regarding the history of each device creating a sort of digital twin onto the Blockchain which allow the automatic execution and payment of scheduled maintenance.

In fact, a machinery can request automated maintenance work or even a replacement part by generating a smart contract that trigs a service request: the payment is processed automatically after the completion of the maintenance which is detected directly by the machine.

Hence, documentation about the maintenance history is appended to the Blockchain improving the reliability of equipment and facilitating the monitoring of equipment. Eventually, when the maintenance if performed by team internal to the company, the record in the Blockchain serves as a proof to equipment suppliers that the maintenance was done in accordance with the set requirements in order to check warranty and guarantee agreements.

Finally, documents could be used for making easier the sales of used machines causing new product life cycle scenario, normally shorter, that will encourage manufacturers to upgrade their equipment more recurrently.

2.4.2.4) Sales & Marketing

- **Improving Trust in Products through Public Data**

  Blockchain is an essential technology when it is necessary to earn the customers' trust. Fraud in manufacturing, especially in the food sector, is a widespread and harmful phenomenon for both industries and customers. For this reason, producers who want to protect themselves must option to expensive third-party certifications. However, there is no reason why the customer should not be informed about the production processes and raw materials used: indeed, client autonomously should be able to access and verify this information regarding products is going to purchase. A decentralized ledger technology may allow information to be shared without any worries about manipulation or cancellation. Therefore, the customer could become faithful with respect to his supplier thanks also to the possibility of checking his supplier history in a few seconds: Blockchain-based loyalty programs could increase revenues while also reducing supplier management costs. Finally, a strong customer loyalty is especially important for expensive goods purchased overseas, food and medicine. Typical examples for this application are TradeLens used by Maersk (IBM & Maersk, 2019) and Provenance (Provenance Organization, 2019) used by Unilever,

Bridgehead Coffee, Panificio Pontino, etc. (Project Provenance Ltd., 2019), two Blockchains for guaranteeing the origin and quality of products.

2.4.2.5) Human Resource Management/Firm Infrastructure

- **Securing Critical Data/Logs**

  Blockchain could be simply used for creating a secure data log, that is simply a register internal to the company which save all the information regarding, for instance, company assets, employees' activities & timesheets, expenses record, internal events, etc. which is not possible to modify in any way and thus creating a tamperproof register useful for every manufacturing company, from the smallest company to the biggest world-wide enterprise.

2.4.3) Smart Contracts for Manufacturing

Smart Contracts are very important for manufacturing because Blockchain technology is helping industrial processes to reach the automation while involving several different companies. A Smart Contract (*as already explained in paragraph 2.3.3*) consists in a computer program that is able to accomplish certain agreements that are established by different parties: when a series of some specific conditions occur, a Smart Contract performs definite actions automatically accomplishing the conforming clauses.

Hence, in manufacturing with a Smart Contract it is possible to control both physical and digital items through an automatic program that runs in accordance to specified legal terms. The power of such kind of codes resides in the data, on which external services of the real world depend, that is stored inside the Blockchain. These external services, that are called "*oracles*" are those responsible for checking real world conditions (e.g. inspect if an asset is arrived undamaged) and then write the information on the distributed ledger. This operation may activate a Smart Contract that, triggered by a conditional statement, reads information on blocks and write new ones (e.g. a property exchange is written inside the Blockchain whether certain agreements conditions are met between two firms).

There are different types of oracles based on the interaction with the external world:

- *Software Oracles* manage the information that is available online: data come from web sources that is collected and then analysed by the oracles which extract the needed information and use it for the Smart Contract (e.g. price of acquired items; position of trucks related to logistic processes; temperature of a stored product).
- *Hardware Oracles* are able to use information directly from the real world, for instance by using RFiD sensors as a data source, IoT devices connected to the factories, and so on.
- *Inbound Oracles* enclosure data from the exterior world (i.e. from info sources that have not contact with the Blockchain) into the distributed ledger (e.g., price of an item, that can be procured automatically when it reaches set price).
- *Outbound Oracles* permit smart contracts to deliver info to the external world (e.g., when a certain object is confirmed to be received properly, then a payment is sent automatically).

3) The Industry 4.0 Scenario

Within the definition of Industry 4.0, there are actually several sectors that are preparing to improve their organisations in order to increase productivity, reducing costs, improving the quality, flexibility and reliability of the systems. Mainly, this is made possible by so many new technologies, like Internet of Things, Cyber-Physical System, Big Data Analytics, Cloud Computing, etc. that are revolutionizing the way of doing business by introducing new business models and opening up to new scenarios and opportunities.

The manufacturing industry is one of the main sectors which can be transformed by the fourth industrial revolution and that can benefit from the new advantages offered by adopting new design principles and new technologies. Indeed, it is thanks to these new advantages that the fourth industrial revolution began, by giving life to what are today called Smart Manufacturing Systems where the key principle of enabling connectivity between industrial units, machines and equipment, suppliers and retailers, together with the other supporting industries, generated a smart network over the whole manufacturing value chain increasing the overall efficiency and profitability.

The creation of this smart and interconnected network supports in automating operations, thus increasing the profitability of production systems thanks to the increase in flexibility and productivity combined with the reduction in costs: consequently, it is reshaping manufacturing business models creating opportunities for manufacturers that can become more competitive.

To achieve this goal, however, it is necessary to carry out a correct integration of many systems and technologies across all over the network; this generates complications related to information exchange and connectivity between the entities involved creating security and trust difficulties, together with reliability, traceability and agreement automation issues within the manufacturing value chain.

The Blockchain technology may address several of these challenges thanks to its features that permit to create a safe and shared register of information on which is possible to reach a distributed agreement that allow useful manufacturing applications.

The following part of this thesis is organized as follows: this *chapter 3* provides background information about Industry 4.0 Smart Manufacturing, specifying benefits, challenges and requirements; paragraph 4.1-4.4 discuss a framework for proposing specific Blockchain typologies for supporting effective manufacturing applications while paragraph 4.5 and 4.6 show the result of this process and then conclude the thesis.

3.1) Industry 4.0 and the rise of Smart Manufacturing Systems

The term "Industry 4.0", referred to the fourth industrial revolution, was presented publicly for the first time in 2011 at the Hannover Fair under the initiative of the German government for a high-tech project in order to enhance the competitiveness of the manufacturing industry by facilitating better performances, lower costs and higher quality in various fields of industry. This phaenomenon is often referred to as the creation of the *Smart Factory* or the *Smart Manufacturing Systems* where different emerging technologies are integrated and developed in order to collaborate for the abovementioned common goals. Industry 4.0 has been headed by three further industrial revolutions and is considered the succeeding revolution which is happening right now in the industrial sector.

For understanding clearly how manufacturing got here, what the *definition of Industry 4.0* really is and what the *key components* behind it are (*paragraph 3.1.2*), it is necessary to define a timeline which illustrates the *evolution of manufacturing and industrial sector* (*paragraph 3.1.1*) from the end of 18th century to today.

3.1.1) The Evolution of Industrial Production: from 1.0 to 4.0

1. **The First Industrial Revolution**

   Everything started in Britain, around 1760, with the introduction of mechanical machines, powered by steam engines and water, in substitution of manual work production inside well-organized production facilities throughout a process which has intensified for the entire 19th century. The term "factory" started spreading at that time and many industries benefited from it, in particular the textile, which was the first to adopt it, and the agriculture, developing immensely the British economy.

2. **The Second Industrial Revolution**

   It dates back to 1870 and regards the electrification of factories: the introduction of electric-powered machines helped in increasing the production rates transforming the manufacturing sector involving also transformation in the organizational model of labour (e.g. Taylorism). Indeed, the mass production became the milestone for industries defining the key characteristic of that historical period. Many existing technologies was introduced into industries, like telegraphs and railways: in particular, the second one contributes reciprocally to the revolution thanks to the mass production of steel. This period was also affected by important innovations in chemistry which were put inside the industry contributing in its development.

3. **The Third Industrial Revolution**

   With the end of the World War II, with a development that has grown until the 1970's, industries assisted to the third industrial revolution who earned the title of "the digital revolution" due to the introduction of digital technologies. The key aspect was

the switching from analogic to digital systems as a result of the development of advanced electronics & computers together with IT technologies that enhanced the development of automation of production processes.

4. **The Four Industrial Revolution**

   The fourth industrial revolution is a new phase for manufacturing systems and is still being under definition since many academics and researches are disputing to define appropriately this phaenomenon.

   The key concept behind this fourth stage is that Industry 4.0 brings the manufacturing processes to a new high level of automation by introducing personalised yet flexible mass production by means of the most innovative technologies.

   In this scenario, machines start operating autonomously or in a strict collaboration with people making the production field independent and able to collect and analyse data while eventually give advises upon information.

   Manufacturers are becoming able to communicate with computer, not only to operate with them, and in the fourth revolution, thanks to the quick evolution of ICT technologies, real and virtual world become more and more mixed creating an environment where machines can communicate with each other (Internet of Things) and with people (Internet of People) by creating the Cyber-Physical Production Systems.

3.1.2) Definition and Key Components of Industry 4.0

The original definition of Industry 4.0, more precisely, of "Industrie 4.0" was proposed by the "Germany Trade and Invest" and it explained the main points of this current trend in manufacturing in the paper (MacDougall, 2014):

> *"Industrie 4.0" refers to the technological evolution from embedded systems to cyber-physical systems. Put simply, Industrie 4.0 represents the coming fourth industrial revolution on the way to an Internet of Things, Data and Services. Decentralized intelligence helps create intelligent object networking and independent process management, with the interaction of the real and virtual worlds representing a crucial new aspect of the manufacturing and production process. Industrie 4.0 represents a paradigm shift from "centralized" to "decentralized" production – made possible by technological advances which constitute a reversal of conventional production process logic. Simply put, this means that industrial production machinery no longer simply "processes" the product, but that the product communicates with the machinery to tell it*

exactly what to do. Industrie 4.0 connects embedded system production technologies and smart production processes to pave the way to a new technological age which will radically transform industry and production value chains and business models (e.g. "Smart Production System").

This is only one of the proposed definitions for Industry 4.0 and, unfortunately, not all the definitions of it are the same since this term comprehends many different aspects that what someone considers a definition, some others will not. Therefore, in order to understand Industry 4.0 truthfully, the *table 2* presents a collection of several definitions from which is possible to understand all the common aspects of this wide and complex phaenomenon:

Table 2: Collection of Possible Definition of Industry 4.0

Definition of Industry 4.0	Author
"Industrie 4.0 is a collective term for technologies and concepts of value chain organization. Within the modular structured Smart Factories of Industrie 4.0, CPS monitor physical processes, create a virtual copy of the physical world and make decentralized decisions. Over the IoT, CPS communicate and cooperate with each other and humans in real time. Via the IoS, both internal and cross organizational services are offered and utilized by participants of the value chain".	Hermann's definitions of Industry 4.0
Industrie 4.0 is a German-government-sponsored vision for advanced manufacturing. The underlying concept of Industrie 4.0 is to connect embedded systems and smart production facilities to generate a digital convergence between industry, business and internal functions and processes. Industrie 4.0 refers to a fourth industrial revolution (following water/steam power, mass production and automation through IT and robotics) and introduces the concept of "cyber-physical systems" to differentiate this new evolutionary phase from the electronic automation that has gone before.	Gartner's definition of Industry 4.0
Industry 4.0 refers to the fourth industrial revolution. After mechanisation (Industry 1.0), mass production (Industry 2.0) and automation (Industry 3.0), now the "internet of things and services" is becoming an integral part of manufacturing. Industry 4.0 technologies have the potential to create extraordinary growth opportunities and competitive advantages for Germany as a business location. Experts forecast that businesses will be able to increase their productivity by about 30 percent using Industry 4.0.	BDI's definition of Industry 4.0
Industry 4.0 is the next phase in the digitization of the manufacturing sector, driven by four disruptions: the astonishing rise in data volumes, computational power, and connectivity, especially new low-power wide-area networks; the emergence of analytics and business-intelligence capabilities; new forms of human-machine interaction such as touch interfaces and augmented-reality	McKinsey's definition of Industry 4.0

systems; and improvements in transferring digital instructions to the physical world, such as advanced robotics and 3-D printing.	
Industry 4.0 is a collective term for technologies and concepts of value chain organization. Based on the technological concepts of cyber-physical systems, the Internet of Things and the Internet of Services, it facilitates the vision of the Smart Factory. Within the modular structured Smart Factories of Industry 4.0, cyber-physical systems monitor physical processes, create a virtual copy of the physical world and make decentralized decisions. Over the Internet of Things, Cyber-physical systems communicate and cooperate with each other and humans in real time. Via the Internet of Services, both internal and cross-organizational services are offered and utilized by participants of the value chain.	SAP's definition of Industry 4.0
Industry 4.0 is a term applied to a group of rapid transformations in the design, manufacture, operation and service of manufacturing systems and products. The 4.0 designation signifies that this is the world's fourth industrial revolution, the successor to three earlier industrial revolutions that caused quantum leaps in productivity and changed the lives of people throughout the world.	European Parliament's definition of Industry 4.0
Industry 4.0 is the current trend of automation and data exchange in manufacturing technologies. It includes cyber-physical systems, the Internet of things and cloud computing. Industry 4.0 creates what has been called a "smart factory".	Wikipedia's definition of Industry 4.0

The *table 2* clearly demonstrate that a universal accepted definition of Industry 4.0 still does not exist and probably this term could not be yet defined definitively because, due to the fact that the 4th industrial revolution was predicted ex-ante and not discovered ex-post (was presented publicly by the German "Industry 4.0 Working Group"), there is still room for additional evolution and so companies, researchers and institutes are still shaping the future of Industry 4.0.

Therefore, the main difficulty at an academic level is to define all possible Industry 4.0 scenarios that may arise from this industrial revolution; indeed, scientific research is interfered whether a clear definition misses (Koomey, Turner, Stanley, & Taylor, 2007).

It is for this reason that is interesting to analyse how this revolution is modelling the actual factories, which are turning into *Smart Manufacturing Systems*, and understand what are the main components that characterize these new firms. Obviously, it is important to compare these components in relation to the *objectives* and *requirements* of the manufacturing systems, in order to not have only a conceptual framework derived from a literature review but a practical reference architecture for forecasting the evolution of

companies and for suggesting possible technological applications (e.g. Blockchain in manufacturing).

It all started with the development and integration of different elements like the *smart machines*, *intelligent warehousing system* and *production facilities*, that all together created the *cyber-physical production systems*, that incorporated different functions like inbound & outbound logistic, design & engineering, marketing, etc. into the production operations (Ji & Wang, 2017). According to (Liao, Deschamps, Freitas Rocha Loures, & Ramos, 2017) it is possible to identify different classes of components that could be then grouped into three different levels that are the *Physical level*, the *Smart Connection and Communication level* and the *Application level* that represent the key components for the Industry 4.0.

1. **Physical level:**
   This level is the basic requirement for a smart manufacturing system. It is constituted by smart & multi agent cells which contains a set of sensors & actuators, communication technologies and other infrastructures like robotics arms, smart meters etc. *(figure 50)* that enable the interconnection of those smart and modular cells. Sensing and communication module (e.g. WiFi, Bluetooth…) implanted into equipment and tools allow for a smart production with intelligent and online features that are also self-adaptive (e.g. automated processing temperature, on-line quality control…). These features open to the era of intelligent monitoring and decisions for smart operation: some example are the (Davis & Edgar, 2019) with an integrated and self-aware plant assets with several sensors and the (Brewer, Sloan, & Landers, 2019) with a smart tracking system by means of wireless devices with GPS or RFiD for materials and products tracking inside the entire production system. Under those example it is possible to identify a plant system that provide information in a visual way to all the stakeholders involved in the production processes, supplying different attributes that are taken for granted at physical level by the paradigm of Industry 4.0 like adaptability, autonomy and interconnect ability. The smart attributes of physical level allow smart manufacturing systems to be connected and to evolve by itself.

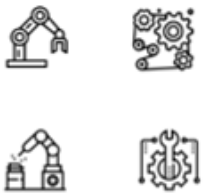


Figure 50: Single modular cells in SMSs.

2. **Smart Interconnection and Communication level:**
   In the middle between the physical level and the application level (the cyber one), there is the interconnection and communication level which enable the manufacturing to reach a connection by using low energy and high efficiency communication network. All the devices, sensors, machine and

Figure 51: Interconnection between cells in SMSs.

even people are connected together *(figure 51)* moving from the IoT, stepping through the Internet of People to the Internet of Everything by exploiting different communication technologies: this level contains many standards like WiFi, IPV6, 4G/5G, RFID, Bluetooth, GPS, etc. In this level, the attributes that constitutes it, embrace real-time, synchronized integrated networks of RFIDs and wireless sensor network merging IoT into company systems and businesses: the smart factory can be easily attained by the communication technology.

3. **Application level:**

In the intelligent factory, not only the physical part should be considered but it should be taken into account how the hardware and software levels are integrated with each other, establishing a connected physical and cyber world that forms a new intelligent, open & constantly evolving production platform (*figure 52)*. All this opens up to new scenarios such as cloud-based simulation, prediction analysis and intelligent decision making based on large data, etc. Naturally the autonomous Smart Manufacturing Systems are proposed putting to side of the human wisdom the most modern technologies: for instance, (Hong-Seok & Ngoc-Hien, 2015) proposed a cloud based SMS for machining transmission in which the "advanced information and communication technology such as cognitive agent, swarm intelligence, and cloud computing are used to integrate, organize and allocate the machining resources", continuing for a metaphor in which production systems are equated with living biological organisms whose characteristics of self-adaptation, self-diagnosis and self-repair are inspired by nature; (Kaestle, Fleischmann, Scholz, Haerter, & Franke, 2016), instead, deepens the integration of miniaturized sensors and printed communication technologies into machines and products to melt together virtual and real world counterparts and establishing a self-learning control application in order to "increase process robustness as well as process flexibility and thus allowing for instant product changes with an ideal lot size of one".

Figure 52: The whole physical system is represented and controlled at application level.

All these applications for reaching autonomous operations provide different value which include visualization, cognitive ability, self-organizing ability, self-healing ability and self-decision ability.

3.2) Design Principles

In order to properly identify and designate a factory as Smart Manufacturing System derived from the Industry 4.0, it is necessary to be sure to embrace some common principles: therefore, it is useful to originate some *Industry 4.0 Design Principles* for defining the boundaries of what is inside this industrial revolution and what is still not. The reason behind this researching activity is to define some "how to do Industry 4.0" principles for supporting the identification of possible scenarios for manufacturing companies in which new technologies (e.g. Blockchain) could be then implemented.

The main reference for this paragraph is (Hermann, Pentek, & Otto, 2016), a recent work of literature review for the Institute of Electrical and Electronics Engineers with thousands of citations in the academic literature.

The results obtained gave rise to four design principles as showed in *figure 52* and further analysed in the following subchapters; that suggests an endorsement for the Blockchain technology whose main properties, *as already explained in paragraphs 2.2.1-10*, are Decentralization, Transparency and Immutability (i.e. Security).

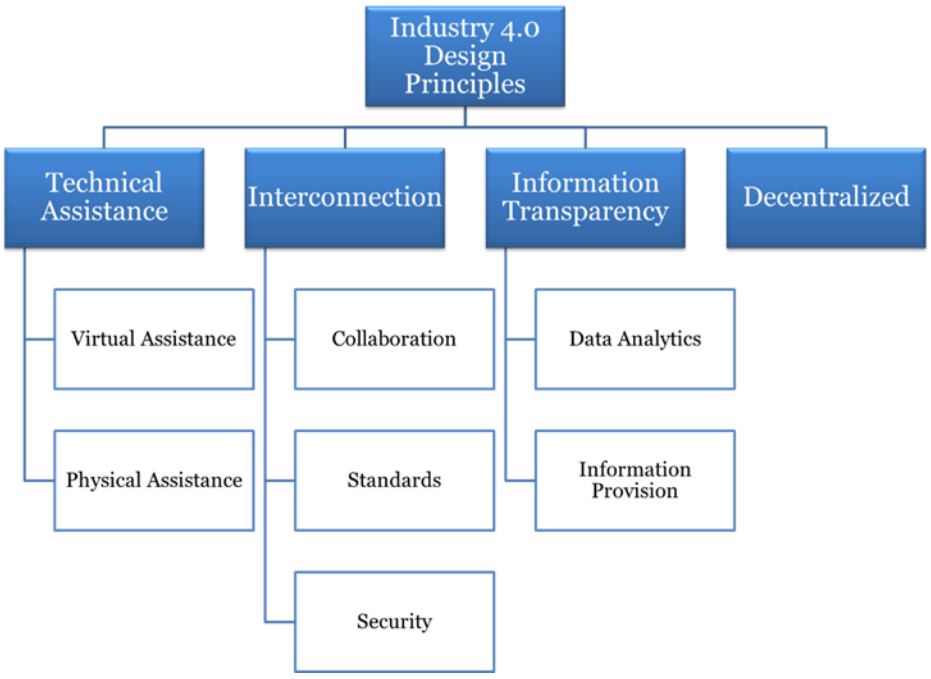


Figure 53: Design Principles for Industry 4.0 (Hermann, Pentek & Otto, 2016)

3.2.1) Interconnection

With the fourth industrial revolution has born what is called *Internet of Everything* (IoE) since all the kind of machines, devices, sensors and people are interconnected together forming the *Internet of Things* [IoT concept was introduced as early as 2010 by (Giusto, Iera, Morabito, & Atzori, 2010) presenting this subject as an emerging topic in the wireless

technology arena, emphasizing the importance of a pervasive presence of a high variety of devices able to interact and cooperate with each other for reaching common goals] and the *Internet of People* [IoP becomes an essential paradigm for exploiting IoT and getting the maximum from the concept of IoE (Santos & Villalonga, 2015)].

Interconnection is a design principle which required three key aspects: *collaboration*, *standards* and *security* (i.e. cybersecurity). As stated by (Schuh, Potente, Wesch-Potente, & Hauptvogel, 2013), the IoE generates interconnected objects and people which will be able to share information on the basis of three forms of collaboration: human-human collaboration, human-machine collaboration, and machine-machine collaboration. However, for connecting this multitude of elements is essential the presence of common communication standards since only with them a degree of combination between machines from different vendors will give enough flexibility to the system otherwise incommunicability will rise in wide and complex systems (Zuehlke, 2010). Finally, as already mentioned in the previous paragraph, the need for cyber-security will increase in such contexts since with a growing number of participants in the Internet of Everything, harmful attack to production facilities will be more and more pushed by monetary or political interests (Lu, Qu, Li, & Hui, 2015).

3.2.2) Information Transparency

The second design principle directly comes from the first one: objects and people interconnected together with the fusion of physical and virtual world (i.e. Cyber-Physical Systems), require a new form of information transparency (Kagermann H., 2014). In fact, new conscious information about the context is indispensable for making appropriate decisions by the Internet of Everything participants when a virtual copy of the physical world is created by the digitalization of productions sites (e.g. for the physical wolrd, information regarding the position of tools, the conditions of machines, and so on; for the virtual worlds, information about 3D drawings, simulation models, electronic documents, and so on).

Therefore, when dealing with the analysis and management of the physical world, becomes necessary to collect information from sensors and interpret it: for creating transparency, all the results from analytics must be enclosed in the systems that are accessible to all the participant in the network (Gorecky, Schmitt, Loskyll, & Zuhlke, 2014). In addition to transparency, also real-time is a feature of great importance for decision making processes, in particular for the third-generation cyber-physical systems, as already mentioned in the previous *paragraph 3.2.6* by (Bauernhansl, Hompel, & Vogel-Heuser, 2014).

3.2.3) Decentralized Decisions

This third design principle is a consequence of the combination of the first two ones: decentralized decisions are made possible by the transparency of information and the

interconnection: cyber-physical systems enable from a technical point of view the control of the physical world (Lee E. A., 2008). All the decision makers can take advantages by this since they can combine together local with global information for taking better decision as well as increasing global productivity. Decentralized decisions allow participant to become almost autonomous in accomplishing tasks as long as interferences of conflicts arise: in this case, critical tasks are assigned to high level decision makers.

3.2.4) Technical Assistance

Finally, the last principles, explain how is changing the role of people inside a smart factory. From modest machines' operator to operational decision maker for flexible problem solving: this is a direct consequence of the increasing complexity of production sites. As already explained, the establishment of new cyber-physical systems will be necessary for developing the industry 4.0 paradigm; with an increasing number of network connections and decentralized decisions, operators will need assistance systems for collecting and visualizing information in a clear, aggregated and simplified view in order to assure that problems are noticed and solved in short period and decisions are taken in an fully-informed way (Gorecky, Schmitt, Loskyll, & Zuhlke, 2014). As stated by (Miranda, et al., 2015), the interconnection between people and things is mainly supported by smartphones and tablets while wearables will be fundamental soon in the future (Williamson, et al., 2015).

Another aspect regarding technical assistance consists in the physical support of humans by robots which will be able to support several tasks unpleasant or debilitating for people: in this collaboration between humans and robots, people must be properly trained while robots should be programmed in order to be able to interact efficiently and securely with operators (Awais & Henrich, 2013).

3.3) Objectives

Putting these design principles all together, with Industry 4.0 we allow people, advanced manufacturing hardware, and sophisticated software, to collaborate effectively to optimize operations and automate manufacturing processes.

At that point, it is essential to understand in which direction is moving the manufacturing industry, what it is looking for and what are its main goals, for correctly proposing effective solutions that are valuable and supportive for businesses. Hence, it is fundamental to start from a literature review in order to identify main objectives and to propose an aggregation or clustering of them since a universal aggregation of objectives for manufacturing has not yet been set.

This paragraph followed a structured approach that stepped through different authors for the definition of some general goals. Preliminary, starting from a paper of (Bititci, Suwignjo, &

Carrie, 2001) which developed and evaluated a strategy for grouping in manufacturing systems the performances based on cost, quality, transportation and adaptability, and moving a step_further with a mapping of the key objectives proposed in the manufacturing plant configuration stage by (Lee, et al., 2017), which proposed a classification scheme for performance metrics for smart manufacturing encompassing agility, resource usage, and sustainability under the sensor-empowered assembling equipment and controller software condition, finishing with an independent, self-remedying and aware strategy anticipated by (Feeney, Frechette, & Srinivasan, 2015) (mainly focused on the item design), it is possible to present a probable aggregation of key objectives for modern manufacturing systems identifying three main categories: *Autonomous Lean Operation*, *Sustainable Value Added* and *Win-Win Partnership*.

- **Autonomous Lean Operation:**
  The fundamental objective for building up self-governing lean Smart Manufacturing Systems is to expand the productivity & autonomy of production systems.
  It is important to build up an assessment framework that thinks about the changes in processing because of autonomy. SMSs empower the user to assess self-ruling procedures against conventionally managed processes. Besides, it is important to describe the constraints of management and autonomy to better incorporate various factors (such as KPIs with resources and activities) into the framework structure. Hence, dynamical targets can be set, and new qualities of self-governance can be considered. Self-ruling SMSs (Park & Tran, 2014) contain the capacity of responding to exceptional and unexpected events.
  Some management strategies are required to reduce the threats regarding the planning of activities. Independent SMSs should consider the firm's activities under the lean thinking, integrating Artificial Intelligence and managerial technique. This target principally centres around the combination of rising technologies and management.
- **Sustainable Value Added:**
  Since manufacturing firms are being impacted by a growing complexity cause by a fast-changing requirements in the global market, companies need to establish a worldwide value creation network for satisfying the great list of requirements: (Oertwig, Jochem, & Knothe, 2017) proposed to establish the shaping of a worldwide value creation network where the design and control of partner relations for a monetary, ecological, and social assessment of items, services, and value chains are considered and managed efficiently.
  Moreover, (Brown, Amundson, & Badurdeen, 2014) affirmed that accomplishing sustainability in manufacturing requires a comprehensive view spreading over item

design, production processes and systems, and the whole supply chain: especially, it was proposed a value stream mapping technique for identifying the area of weaknesses and potential areas of improvement for reaching an effective sustainability in the modern manufacturing. Hence this goal for the most part centres around sustainability and value added included in the overall SMSs lifecycle.

- **Win-Win Partnership:**
  In self-sufficient operation situations, a definitive target of Smart Manufacturing Systems is to make an ongoing and constant collaboration where the whole lifecycle of SMSs is more successful than the total of all its individual parts. Win-Win Partnership depends on the autonomous lean operations, sustainable value added, data, and information sharing to accomplish multi-partner and SMSs co-improvement.

As a result of the combination of the design principles and these key objectives, (Mohamed & Al-Jaroodi, 2019) showed how Smart Manufacturing Systems become able to offer advanced capabilities proposing a list of technical skills which affect the manufacturing industry after the transformation enforced by the fourth industrial revolution. In fact, a smart factory becomes capable to:

1. Automate more tasks using customizable and adaptive devices and machines.
2. Incorporate new manufacturing processes, and technologies.
3. Reduce human interaction with the machines via digital sensing, controls and automated decisions.
4. Improve measurement and monitoring procedures using precision devices.
5. Enhance response times for more accurate control of processes.
6. Collect and store real-time data across all areas of the manufacturing plant continuously.
7. Elevate analysis capabilities using the collected data and advanced data analytics models.
8. Introduce intelligent algorithms using available data to allow the system to make autonomous decisions.
9. Reduce the reliance on humans for monitoring and decision making.
10. Provide better maintenance and repair operations based on predictive analysis of operational data.
11. Create safer and more comfortable working environments.
12. Enable the creation and utilization of new business models in manufacturing.
13. Facilitate the integration of different technologies, models, sectors, and organizations in the manufacturing industry.

3.4) Benefits

Keeping in mind the above-mentioned advanced capabilities achieved by Industry 4.0, it is worth setting and focusing on the benefits that Industry 4.0 will convey to the industries: the future manufacturing sector include various opportunities regarding profitability and growth, improving the competitiveness of companies.

As stated by (Nunes, Pereira, & Alves, 2017), investing in smart manufacturing system for the fourth industrial revolution, in fact, will mean deep changes in each aspect of organizations' value chain, from the products development processes, marketing, after sales services, to operations, logistics, quality assurance and so on. Smart factory requires together with its development also smart logistics and smart networks, creating an entire future smart infrastructure: it is from this new infrastructure that several benefits and profits will arrive (Vila, Ugarte, Rı´os, & Abellán, 2017).

With smart manufacturing, for instance, the usage of innovative production technologies will mainly increase the firms' flexibility with benefits regarding the dynamic allocation of resources and capacity, less wastes and consumes, shorter setup time, the reduction of production complexity and constraints. All this can be translated into quicker, less expensive and easier productions processes. Even if it is key, flexibility is only one of the many dimensions that is impacted by Industry 4.0, since numerous benefits regard the simplification of business processes, the reductions of labour costs and inventories, the creation of a more transparent logistic supply chain, the optimization of global forecasts, the better satisfaction for customers and so on. The *table 3* shows different benefits that the new factory will take advantage of, and it is supportive for the creation of some main benefit categories for Industry 4.0.

Table 3: Collection of Benefit of Industry 4.0

Benefits of Industry 4.0	Author
- Advanced planning and controlling with relevant, real-time data - Rapid reaction to changes in demand, stock level, errors - Sustainable manufacturing/ resources efficiency (materials, energy, people) - Higher quality, flexible production - Increased productivity - Ad-hoc reaction to market changes - Personalization of products - New level of customer satisfaction - Increase in competitive advantage by the successful digital business model implementation and technology creation - Costs and wastes reduction - Safer work conditions - New workplaces - Work-life balance	Ekaterina Uglovskaia (2017)

- Increase in revenue - Innovative company's image	
- Reduction of overproduction and waste - Reduction of energy consumption as energy intensive tasks can be done when there is overproduction. Use of energy recovery for the whole system. - Reduction of waste especially in the product development phase - Reduction of transportation and travel effort - Saving of natural resources - Contribute to the environmental dimension of existing manufacturing plants	M.W. Waibel et al. (2018)
- Logistics cost : Changes in logistics cost savings in terms of transport, warehousing, inventory carrying and administration costs - Delivery time : Changes in delivery improvements, cycle time, lead time - Transport delay Changes in amount of delayed shipment - Inventory reduction : Changes in inventory volume - Loss/damage : Changes in amount of lost and/or damaged goods from damage, theft and accidents - Frequency of service : Changes in utilization rate (load factor), frequent intervals - Forecast accuracy : Changes in demand uncertainties - Reliability : Changes in logistics quality in terms of transport, inventory and warehousing e.g. perfect order, scheduled time deliveries - Flexibility : Changes in planning conditions e.g. percentage of non-programmed shipments executed without undue delay - Transport volumes : Changes in total transported freight volume - Applications : Suitable applications for digitization in logistics processes	Yasanur Kayikci / (2018)
- Decentralized and digitalized production, where the production elements are able to autonomously control themselves - The products will become more modular and configurable, promoting mass customization in order to meet specific customer requirements - New innovative business models :, value chains are becoming more responsive, increasing competitiveness through the elimination of barriers between information and physical structures - Digitization consists in convergence between physical and virtual worlds and will have a widespread impact in every economic sector. - The main driver for innovation, which will play a critical role in productivity and competitiveness. - Transforming jobs and required skills : avoid what is known as technological unemployment, redefining current jobs and taking measures to adapt the workforce for the new jobs that will be created - New competencies and it is necessary to create opportunities for the acquisition of the required skills through high quality training	T. Pereira et al. (2017)
- Workers will have a much greater share of doing complex and indirect tasks such as collaborating with machines in their daily work; - Workers will have to (1) solve unstructured problems, (2) work with new information, and (3) carry out several non-routine manual tasks. - Reinforcing physical abilities such as strength or fine motor skills and lowering the physical work related strain by using exoskeletons, positioning devices, robots or automation of monotonous tasks; Lowering the required short-term memory effort by visualizing detailed and on demand information (users obtain relevant information when he/she needs it and in a form that he/she can comprehend it); Reducing the number of errors made on the shop floor by real-time observation of the process and skill-/ability based work instructions	Hugo Karre et al. (2017)
- Large increase in all operational efficiencies with the use of data levering to improve processes	McKinsey and Company

- Industry 4.0 is seen as one of the major drivers for the growth of revenue levels, even as its implementation will also require significant investments by businesses. - logistics and statistics are generated and collected in an automated manner, so responses are faster - the growth it stimulates will lead to a 6% increase in employment over the next ten years	(2015)
- Increased productivity : The automotive industry alone, productivity is expected to increase by 10–20%, once Industry 4.0 is fully implemented - the growth it stimulates will lead to a 6% increase in employment over the next ten years	BCG study (2015)
- Increased productivity: operational efficiencies will increase by an average of 3.3% annually for the following five years leading to an average annual reduction in costs of 2.6%. - Revenue will increase faster and higher than the costs incurred to automate or digitise the manufacturing process in terms of Industry 4.0. - with Industry 4.0 concepts and methods applied, logistics and statistics are generated and collected in an automated manner, so responses are faster	Koch et al. (2014)

3.5) Main Technological Pillars

The great benefits and the overall success of Industry 4.0 is mainly grounded on the technological innovation both hardware and software that affected the Information and Communication Technology field. In the literature, the technological pillars on which the Industry 4.0 is made upon are grouped in many different ways by different academics and organizations; furthermore, the technologies involved vary significantly with the year in which the technological pillars are individuated and the sector in which the research is conducted.

For instance, (Hermann, Pentek, & Otto, 2015) identified only four main components for the 4th industrial revolution: *Internet of Things*, *Internet of Services*, *Cyber-Physical Systems* and *Smart Factory*, considering some technologies, such as *Big Data* and *Cloud Computing*, only data services which operates on the data that are provided by the Industry 4.0 environment sustaining that they could not be considered independent component of it (they are consequences, not causes).

Recently, (Mohamed & Al-Jaroodi, 2019) focused on just six key technologies: *Industrial Internet of Things* (IoT) for connecting different manufacturing machines and devices in a network; the *Internet of Service* (IoS) for providing services for manufacturing systems and organizations through the Internet; *Manufacturing Cyber-Physical Systems* (CPS) for facilitating interactions between the cyber world and the physical manufacturing world such as machines and robots, by providing continuous monitoring and control services; *Cloud Manufacturing* for providing on demand scalable computation, data storage, and advanced smart services for different manufacturing-related applications; *Fog Manufacturing* for low latency support, real time control, location awareness, better mobility and security support, and streaming support for manufacturing applications and *Manufacturing Data Analytics* for offering intelligent decisions based on gathered manufacturing data and enhancing manufacturing processes.

Differently, the Boston Consulting Group published a research (Rüßmann, et al., 2017) in which is provided a complete description of nine key technological foundation (f*igure 51)* shaping the Industry 4.0 still considering *Internet of Things* an independent component but considering *Cyber-Physical System* a consequence of those technologies and judging the *Smart Factory* as a result, an output, of the application of Industry 4.0 components on the traditional factories. Since this description is well updated, in line with the actual trends and also used as a reference by many other authors, it is now provided the aforementioned classification together with different concrete example from several selected case studies.

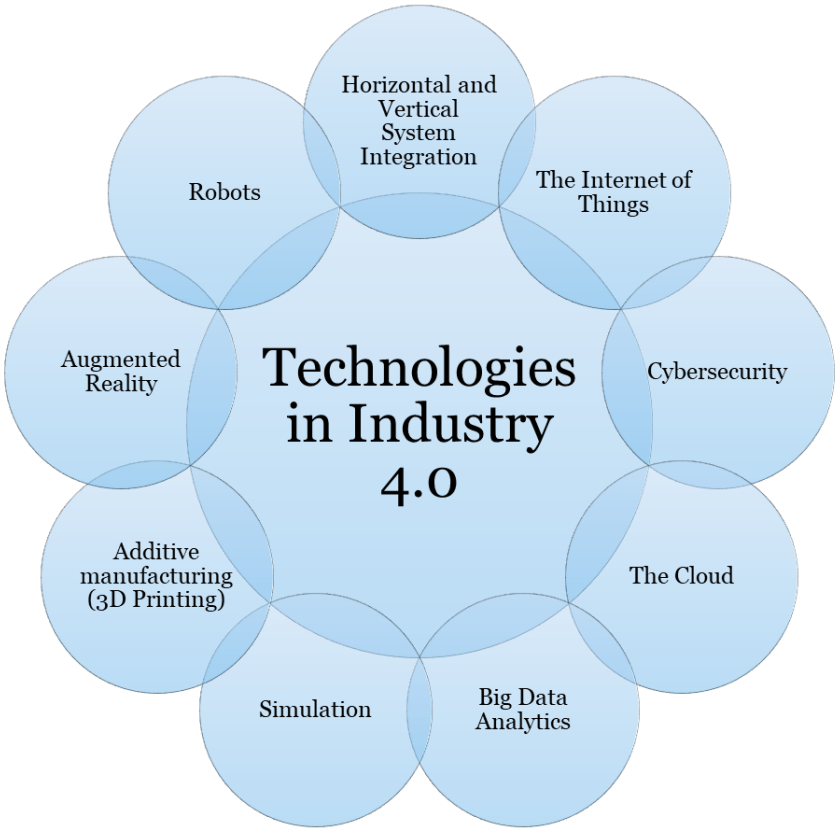


Figure 54: Main Technologies in Industry 4.0 (Rüßmann, et al., 2017)

3.5.1) Autonomous Robots

In the manufacturing field, robots are already used for many applications. Generally, the main reason behind the utilization of robots is their usefulness in executing complex tasks that a human cannot perform easily. With the Industry 4.0 their usage will increase since constant improvements in designing industrial robots, already applied in production, logistics and distribution, are making them less complicated to be programmed and controlled enabling a human-robot cooperation (that is the reason why is growing the usage of the term "cobot").

Nowadays, numerous human-robot interfaces create a close cooperation between them. The operator, which still has an important roles for enabling the connection between robots inside a greater production system, will provide necessary information to the system by just giving the instructions and commands to the robots inside it: autonomous robots will interpret command autonomously performing automatically the needed tasks (no more need to be deeply programmed: movements, load/unload operations, etc.) reaching even more lean manufacturing objectives (Hedelind & Jackson, 2011).

Advanced companies are introducing new technologies in the robotic field: KUKA, one of the leader companies in robotics, developed a light mechanical robotic arm, the LBR iiwa, capable of adaptive assembly. This robot is able to work in strict contact with human, collaborating with them and learning by the human itself what and how to behave. In addition, with the connection to cloud systems, it can document all the performed tasks, check for error or missing steps or parts and eventually optimize all its jobs with the usage of analytics (Bahrin, Othman, Azli, & Talib, 2016).

3.5.2) Big Data & Analytics

Big data is one of the hottest topics and takes one of the most important role for the 4th industrial revolution (Yin & Kaynak, 2015): in recent years a lot of companies has investing in big data project, analytics are considered a top priority and it is requiring large investments, also for the next years. Big data, from one side, is introducing new digital technologies and is creating new techniques for actual manufacturers, but from the other side, are the improvements in the firms' technological capabilities that are pushing to the usage of big data itself thanks to a *behavioural trend* for data collection (the number of sensors or devices generating data has increased, the number of online devices, i.e. IoT, is increased and, in general, whenever possible data are being collected in all the possible ways), and a *technical trend* consisting in the availability of more (and cheaper) computing power together with more (and cheaper) storage capacity than before.

The new high level of data accelerates the companies' competitive advantage by the increase of productivity, innovation and thus competition since with analytics it is possible to solve challenges both at organizational and operational level with the monitoring, measuring and managing in a better way. Big data could be used in different ways and in various areas: analysing large datasets, it is possible to get insights about customers while using data coming from manufacturer datawarehouses, analytics are useful for fault prediction and hence for lowering error probability (Ji & Wang, 2017) and also for generating predictive algorithms for decreasing harms before many damages happen (Seele, 2017).

Henceforth, in nowadays manufacturers, from the smallest to the largest, the increasing level of data will encourage companies to achieve mainstream business practices by increasing their capacity and infrastructure development.

3.5.3) Cloud Computing

The Cloud Computing, thanks to the Internet technologies, permitted to offer different IT resources, both processing capabilities and storage capacity, with a scalable approach to a multitude of clients enabling the as-a-service paradigm. This virtualization of resources, no more physically present on site, brought to several advantages to companies facilitating

management and administration, automating procedures and integrating companies alongside the supply-chains. There are three delivery model of Cloud Computing identified with three service models:

- *Software as a Service (SaaS):* consists in a series of software applications and services that a user can access on-demand thanks to internet technologies with a flexible & measurable approach and through an economic compensation based on the actual consumption (e.g. through a web-browser-like interface, CRM, Finance & Accounting, ERP, BI & Analytics, etc.);
- *Platform as a service (PaaS):* it refers to a set of environments user can access, on which applications can be developed and executed (e.g. developing and testing platforms, operative environments, App Marketplaces, etc.). These environments are supplied by a provider, based on pre-set SLAs, with a measurable and scalable approach, through an economic compensation based on actual consumption.
- *Infrastructure as a service (IaaS):* it refers to an on-demand, consume-based, consumption model, based on a scalable, elastic and measurable approach, focused on IT infrastructural resources (e.g. CPU capacity, Network and Computing, Backup), which are provided by a supplier or by an internal ICT Management Office, based on pre-set service level agreements.

Beside these three service models there are also four main deployment models which represent different configurations for providing cloud computing services in the Industry 4.0 context:

- *Private cloud*: it is when Cloud infrastructure is owned by a single firm and is only used by that same firm. Firm possesses complete control. It can be the case of a big company with many branches, who does not want to buy cloud services from a third-party provider: so, can decide to create its own private cloud, whose clients will be all the different branches. This permits to have a full privacy on company data and processes.
- *Public cloud*: it is when Cloud infrastructure is owned by an external organization providing Cloud services to customer firms: control is in the hands of an external vendor (e.g. Amazon Cloud).
- *Community cloud*: it is when the control of the cloud infrastructure is shared among various actors (various partners): hence this solution is in between the two previous models. It is similar to a private cloud that may be shared by different companies that operate in the same district and that do not trust public cloud: they create a

community cloud with single data centre and data will be available just for those enterprises; however this model is not very common.

- *Hybrid cloud*: this is considered more a configuration than a deployment model. In this case, there is a connection, an integration between the private cloud and the public cloud. It is used when some external cloud services are needed and must be joined together with the pre-existent private cloud infrastructure.

The Cloud paradigm is increasing in importance in the 4th industrial revolution due to its *benefits* (Haug, Kretschmer, & Strobel, Cloud adaptiveness within industry sectors – Measurement and observations, 2016): higher speed of the service even if firm reduces the customization (moving from IaaS to SaaS); reduction of investment costs even if company has lower control (moving from Private Cloud to Public Cloud), higher service scalability, lower management complexity of Data Centre, lower investments needed for comparable solutions, higher flexibility & timeliness, better continuity of service & system reliability, higher measurability & costs control, functionalities always updated. All those benefits for companies adopting Cloud can be synthesized in four main economics principles (Liu, Wang, Wang, Xu, & Jiang, 2019):

1. Cost reduction (no initial licencing costs, no HW infrastructure, lower implementation costs, free updates, no maintenance costs; XaaS models permit to reduce the Total Cost of Ownership, especially for first years)
2. Improvement of cash flows
3. Minimization of financial and business risk
4. Maximization of revenues opportunities.

3.5.4) Industrial Internet of Things (IIoT)

Together with Big Data, IoT is another very important topic for Industry 4.0, so important that according to (Kagermann, Helbig, Hellinger, & Wahlster, 2013) is the IoT that applied in the manufacturing process together with the Internet of Services ["IoS consists in the selling of services via Internet by service vendors: these services are offered and combined into value-added services and accesses by users via various channels" (Buxmann, Hess, & Ruggaber, 2009)] has originated the 4th industrial revolution. IoT simply consists in physical objects connected through a network, which change their behaviour based on the data they receive and send. These objects are defined "Smart Objects" since they have these characteristics (not necessarily all of them):

- *Self-awareness*: they can identify themselves & know their localization and can also make self-diagnosis.

- *Interaction*: they can be able to meter (distances, temperature, electricity, etc.) but also detect or sense things and objects around themselves. Finally, according to these measures, they can take action.
- *Processing/elaboration*: According to what they sense, they can detect their specific status.
- *Communication*: they can communicate with both people and other objects. The most diffused technology for enabling the communication of smart object is the RFId (the Radio Frequency Identification is a technology for the automatic identification of objects in radiofrequency, using electronic labels called tags. It is over 70 years old and applications are more and more widespread. RFId allow automatic tag reading, multiple reading, data transfer, information security, storage capacity, reading/writing, robustness, small dimensions, reusability, sensors…).

IoT are assuming a crucial role in business innovation, in particular in the industrial sector, because they are altering the industry structure exposing companies to new opportunities and threats: smart objects generate a new nature of the "things" that thanks to their "expanded capabilities of smart, connected products and the data they generate that are ushering in a new era of competition" (Porter & Heppelmann, How smart, connected products are transforming competition, 2014). In particular, expanded capabilities mean enabling new functionalities like:

- *Monitoring*: because sensors and external data sources enable the comprehensive monitoring of the products' condition, the external environment, the products operation and usage. Monitoring also enable alerts and notification of changes
- *Control*: software embedded in the product or in the product cloud enables control of product functions, personalization of the experience.
- *Optimization*: monitoring and control capabilities enable algorithms that optimize product operation and use in order to enhance product performance, allow predictive diagnostics, service and repair.
- *Autonomy*: combining monitoring, control and optimization allows autonomous product operation, self-coordination of operation with other products and systems, autonomous product enhancement and personalization, self-diagnosis and service.

Because they allow to generate a huge quantity of data, and so get a great competitive advantage, companies nowadays are investing a lot on smart objects, in lot of different areas from *Smart Home* to *Smart Grid*, however they have a wider diffusion inside the factory: through their usage a traditional factory becomes a *Smart Factory* and with the use of machines sensitive to the context in which they operate, it is possible to automatically detect

real-time information, communicate and make decisions. With Smart Factory it is possible to include within the planning decisions other criteria beyond the mere production of machinery, such as energy efficiency and the optimisation of the loads from the profile of energy costs over time enabling new approaches of production planning. These devices in a factory can be used to for:

- *Production*: machinery preparation, support to operators, production progress monitoring, better planning/production scheduling (e.g. the production of complex product, which may have up to hundreds of components, can be simplified by the reading of RFid tag on each item and visual support to guide the operator in the assembly phases in order to reduce time and errors).
- *Maintenance*: allowing a preventive or predictive maintained. (e.g. Mueller industries uses vibrations and ultrasound for predictive maintenance and ai for learning algorithms to make diagnoses.
- *Quality control*: better control of production/assembly activities, higher support to human operators, with reduction in errors. (e.g. Pirelli uses cameras for the identification of potential bugs and AI for self-learning algorithms (Imaging & Machine Vision, 2018)).
- *Material handling*: product movements monitoring, management and monitoring of handling systems, like AGV (e.g. in Goglio, each container employed in handling activities has an RFid tag (Internet4Things, 2017), which is associated to the container contents allowing a reduction in production errors due to incorrect picks and movements).
- *Job safety monitoring*: of the workers position and movements within the factory, identification of environmental hazards conditions.
- *Energy management*: consumption monitoring, integration with other use case (e.g. Polibol monitors temperature, level of brightness and co2 concentration to improve the safety and the wellness of workers and to benefit also in terms of product quality thanks to the volatile organic compounds).

In conclusion, in manufacturing the usage of IoT permits to make more agile and integrated the business operations accomplishing a competitive advantage on the whole supply chain; the IoT capabilities of the firms will be “critical in the future because frequently connected with operation agility and effective decision making” (Akhtar, Khan, Tarba, & Jayawickrama, 2018).

3.5.5) Horizontal and Vertical System Integration

All the above-mentioned technologies contribute to the creation of an *Industrial Network* in which a lot of devices collects data, the Big Data, making it available through the Cloud to the participants in the network for optimizing the coordination between members and improving the overall system performances. This is a framework that is necessary for the creation of the Smart Factory: the coordination mechanism is constituted by Vertical and Horizontal System Integration.

Vertical System Integration involves the flexibility and reconfigurability of systems inside the factory and all these systems must be fully integrated to each other in order to achieve agility and elasticity; Horizontal System Integration refers to the complete integration and interconnection of partners within the supply-chain. When these two System Integrations are enabled, it would be possible to integrate every physical object into each other through smart networks in manufacturing systems designed for being self-organized structures: in addition, systems which exploit cloud technologies may enable vertical partners connections for integrating together their shared platforms. In this scenario, all the process and product flows could be displayed, shared and tracked by all the members of the supply-chain (Wang, Wan, Zhang, Li, & Zhang, 2016).

3.5.6) Simulation

The Simulation is a digital tool that supports the production-related activities by diagnosing the manufacturing environment optimizing the design of production systems. It can deal with complex system in very competitive business environment by "planning the operations, having the knowledge and information and accurate estimation about the system by using the engineering capacity" (Weyer, Meyer, Ohmer, Gorecky, & Zühlke, 2016). Indeed, simulation models can execute investigation dynamically on production systems with the usage of real time data supporting the strategic planning: so, from data acquired by system, it is possible a real time optimization on operations (Uhlemann, Lehmann, & Steinhilper, 2017).

This became possible thanks to one important component of Industry 4.0: the Cyber-Physical System which consists in the combination of physical and virtual world (Kagermann, Anderl, Gausemeier, & Schuh, 2014). According to (Bauernhansl, Hompel, & Vogel-Heuser, 2014), Cyber-Physical System has evolved in time: first generations only included identification technologies for unique identification (e.g. by means of RFId) and a centralized service was responsible for storage and analytical purposes; the second generations started using both sensors and actuators in a very basic way while only in the third generation of Cyber-Physical Systems, they started to be equipped with different sensors & actuators with fully network compatibility and with storage & analysis of data capabilities.

3.5.7) Augmented & Virtual Reality

The *Augmented Reality* is a technique used for generating an innovative yet improved experience in the real-world environment by the enhancement of real objects through specific computer and software tools which are able to receive visual, auditory, haptic and olfactory inputs and to generate in output a modified reality, provided to a person who is involved in an exciting immersive experience (Kipper, 2013). In the *Virtual Reality* instead, the output of this computing process is so preponderant that a person is completely inserted in an artificial world without having more perception of the physical environment around (Hardiess, Mallot, & Meilinger, 2015).

These technologies become more and more applied in the manufacturing sector since they enhance the human-machine interaction. Together or independently, Augmented and Virtual reality could be used in many application simply combining the physical object with computer graphics: they allow the remote control of machine or other components, they help in prototyping and designing 3D models, they assist operators in complex assembly tasks, they inspect components and systems for helping with the maintenance, they support the verification of quality requirements assuring high level testing; many other applications are still under development (Ong & Nee, 2013).

3.5.8) Additive Manufacturing

The Additive Manufacturing technique, frequently recognised also with the more common term “3D Printing”, consists in the process of making parts directly from 3D models using a layer-by-layer production steps (main diffused techniques are powder bed fusion, wire/powder fed system) instead of the traditional machining, milling, drilling, etc. processes.

The advantages of Additive Manufacturing are remarkable: product lots becomes smaller allowing the production of unique and customized products, less raw material is needed with the advantage of having less stocks, there are less wastes and scraps, systems reduce their lead time increasing the mass customization maintaining an agile configuration (Conner, et al., 2014). As confirmed by (Frazier, 2014), Additive Manufacturing permits to obtain just-in-time production systems thanks to the subsequent speed, flexibility and versatility.

3.5.9) Cybersecurity

Cyber-Physical Systems, Internet of Thing, Cloud Computing and in general the connection between an increasing number of smart factories generate Cybersecurity issues. This is a component of Industry 4.0 which cannot be eliminated but must be considered when dealing with those technologies enabling the industrial revolution. Cybersecurity in an outcome that may have negative impact on the business environment causing serious damages in case of

attacks. It is necessary to prevent possible attack by creating robust defence systems analysing all the previous attack types and training employees against possible cyber-attacks.

Cybersecurity is a component necessary for further developments of Industry 4.0 and the deployment of solutions will impact on the overall costs for the companies. However, the total costs for the potential negative impact of possible cyber-attacks would be even higher for, hence a security program and strategies must be seriously taken into account by every firms (Thames & Schaefer, 2017).

3.6) Requirements for Industry 4.0

Mapping the exact requirements of smart manufacturers is the underlying assignment for every planner, advisor, and producer in the design and development phases of each Smart Manufacturing System and a precise identification of SMSs' necessities is the essential duty to be completed for manufacturers.

The concept of Industry 4.0 is largely based on six main requirements that represent a general framework for developing smart manufacturing systems (Hermann, Pentek, & Otto, 2015). These requirements help in comprehend more precisely the Industry 4.0 needs that are:

1. **Interoperability**: it is a significant enabler of Industry 4.0 where organizations, cyber-physical systems and humans are connected and communicate over the Internet of Thing and of Everything. A key achievement factor will be standards, as long as they will permit CPS to communicate amongst different manufacturers: hence, interoperability means that all entities inside the plant (equipment, material handlers, assembly stations, products…) are able to communicate with each other through an open but safe network.

2. **Service Orientation**: cyber-physical systems and humans provide many services that could be offered (both internally, within the same manufacturing unit, and externally, beyond the manufacturing unit's borders) over the internet and be exploited by other participants: this allow a plant to offer its functionalities as an encapsulated web service, transforming a plant into a service-oriented architecture. Hence, it is the ability to offer the functions of the manufacturing processes as a set of services.

3. **Decentralization**: the ability of different manufacturing systems to make decisions on their own. That means giving autonomy, resources and responsibility to all the entities inside the network and requires avoiding the use of centralized controls. Although manufacturing systems can take advantage of other central services and systems like cloud manufacturing and fog manufacturing, they still need to be able to make their own decisions locally to effectively continue their operations.

4. **Real-time Capability**: it is necessary that data is collected and analysed in real time: the condition of the plant should be always tracked and examined (e.g. a plant respond to the failure of a machine and redirect products to another one). It is hence required the ability to immediately collect and analyse manufacturing data in order to conduct the right actions timely, enabling accurate controls of machines operations and real time adjustments. This requirement is mainly related to internal manufacturing processes: an SMS should be able to identify defect and issues (e.g. the failure of a machine in production line) and eventually

delegating tasks to other operating machines, hence contributing to the flexibility and optimization of the production system.

5. **Modularity**: it corresponds to the flexibility of changing, expanding, and enhancing individual modules to meet new requirements in the existing manufacturing processes or to build new ones. Systems in a plant should follow a plug and play logic, hence should be designed for modularity in order to flexibly adapt to fluctuating requirements by simply replacing or expanding single modules. Consequently, these systems can be effortlessly adjusted in case of seasonal instabilities or changed product features. Also, new modules may be identified autonomously and can be used directly via the Internet of Everything thanks to standardized SW and HW interfaces.

6. **Virtualization**: it implies that cyber-physical systems can have a monitoring role over physical processes: with sensors, it is feasible to link to a virtual plant the real one, permitting the execution of simulation models. Consequently, a virtual duplicate of the physical world is created, including the condition of all CPS and forecasting many cases of failure providing also additional info for managing the increasing production complexity. With simulation, an SMS becomes able to monitor existing objects in the surrounding environment and to develop insights for the improvements of production operations.

Achieving these principles is the key to a successful implementation and deployment of useful and highly beneficial smart manufacturing applications. Thus, it is important to consider the specifics of these principles in the design of these applications and find suitable techniques and technologies that can facilitate the seamless integration across all smart manufacturing applications components.

3.7) Challenges

The requirements analysed in *paragraph 3.6* show the existence of some needs that must be satisfied for the effective development of the Industry 4.0 and that may impede its current development. Thus, similarly to the analysis of benefits (*paragraph 3.4*), it is necessary to carry out a study on the current challenges and problems arising from the implementation of the principles of the Industry 4.0: indeed, by understanding the main Industry 4.0 difficulties, it is possible to recognize how to face those critical challenges that arise with the fourth industrial revolution. However, a full list of all the possible challenges which is fronting the manufacturing development is, of course, not realizable since many different situations may generate different conditions very specific for each case study: yet, it is feasible to recognize the most common and relevant challenges currently faced by typical industrial scenarios.

Starting from what (Pereira & Romero, 2017) affirmed, the application of the design principles of Industry 4.0 (*paragraph 3.2*) poses, first of all, some technological challenges that have a considerable influence on many dimensions of the current manufacturing industry and it is therefore necessary, as (Zhou, Liu, & Zhou, 2015) says, even before starting an implementation of these principles, to develop a common strategy that involves all the players in the value chain in order to reach an agreement regarding security problems and architectural standards. Furthermore, numerous authors support the idea that this current process of development and implementation of the Industry 4.0 will be a lasting and difficult path that may take a decade or even more to be completed. This new manufacturing era will involve various aspects that will range from scientific and technological challenges to economic, social and even political difficulties.

From an organizational point of view, for example, one of the biggest challenges for companies that want to ride the wave of innovation, is the preparation of their workers who have to face constant and profound changes that modify their way of working and their duties: this require new skills (e.g. problem-solving skills, failure analysis, expertise with new technologies, etc.) and new qualifications that are not immediate to achieve. In fact, mainly regarding the use of new technologies, it will be necessary to gain experience for the activities of collection, processing and visualization of manufacturing process data (Unger, Börner, & Müller, 2017).

However, the biggest challenges regard the technological innovations with the advances in digital transformation and the development of interconnectivity that play a key role in every company. In fact, as can be seen from the design principles and requirements of the Industry 4.0, the fourth industrial revolution consists in proposing a new way of doing manufacturing that is very close to the complete digitalization of all the physical processes of a company with

the integration of all the partners of the value chain in a digital ecosystem. So, even if the industry is bringing numerous benefits and must be seen as an opportunity, it is necessary to consider all the difficulties and face a multitude of factors: only by recognizing the problems will it be possible to adopt a strategy compatible with the revolution in progress and to arrive at a new kind of global and networked manufacturing enterprise that works on big data and analytics for responding quickly to changing conditions and can also pursue long term opportunities for customers and companies. According to McKinsey, a large number of companies, especially the medium-small ones, do not seem willing to respond quickly and decisively to the digital transformation due to the many barriers they face.

The *table 4* provides an outlook of the main challenges of implementing Industry 4.0.

Table 4: Collection of Challenges of Industry 4.0

Challenges of Industry 4.0	Author
- Cyber Security: With the increased connectivity and use of standard communications protocols that come with Industry 4.0, the need to protect critical industrial systems and manufacturing lines and system data from cyber security threats increases dramatically. - Manufacturing Specific Big Data and Analytics: It is a challenge to ensure high quality and integrity of the data recorded from manufacturing system. The annotations of the data entities are very diverse, and it is an increasing challenge to incorporate diverse data repositories with different semantics for advanced data analytics. - Investment Issues: Investment issue is rather general issue for most of new technology-based initiatives in manufacturing. The implementation of all the pillar of industry 4.0 requires huge amount of investment for an industry. -Reduction of the development and innovation periods. High innovation capability is turning into an essential success factor for many companies - Individualization sales. Over the time, the buyers have gained the chance to define the conditions of the trade. This trend leads to an increasing individualization of products. It is called “batch size one” - Flexibility. Due to the characteristics of the markets is essential flexibility in the production - Decentralization. To deal with the new framework requirements, faster decision-making procedures will be necessary. Therefore, organizational hierarchies need to be reduced - More sustainability. The aim is an economic and ecological efficiency in the production, due to the increase of the prices for resources as well as the social change in ecological aspects	Saurabh Vaidya et al. / Procedia Manufacturing 20 (2018)
- Uncertainties about financial benefits due to a lack of demonstrated business cases justifying investments - No strategy to coordinate actions across different organizational units - Missing talent and capabilities, e.g. data scientists - A lack of courage to push through radical transformation - Cybersecurity concerns with third-party providers	Dennis Kü sters et al. (2017)
- Automation difficulty: The manufacturing equipment will be characterized by the application of highly automated machine tools and robots. The equipment will be able to flexibly adapt to changes in the other value creation factors, e.g. the robots will be working together collaboratively with the workers on joint tasks - Job reduction: The current jobs in manufacturing are facing a high risk for being automated to a large extent. The numbers of workers will thus decrease. The remaining manufacturing jobs will contain more knowledge work as well as more short-term and hard-to-plan tasks. The workers increasingly must monitor the automated equipment, are being integrated in decentralized decision-making, and	T. Stock and G. Seliger (2016)

are participating in engineering activities as part of the end-to-end engineering - Decentralization: The increasing organizational complexity in the manufacturing system cannot be managed by a central instance from a certain point on. Decision making will thus be shifted away from a central instance towards decentralized instances. The decentralized instances will autonomously consider local information for the decision making. The decision itself will be taken by the workers or by the equipment using methods from the field of artificial intelligence - Additive manufacturing implementation: it is increasingly deployed in value creation processes, since the costs of additive manufacturing have been rapidly dropping during the last years by simultaneously increasing in terms of speed and precision. This allows designing more complex, stronger, and more lightweight geometries as well as the application of additive manufacturing to higher quantities and larger scales of the product but requires a high level of integration with all the activities of the value creation, from designing and engineering to the physical manufacturing.	
- Horizontal integration through value networks - Vertical integration - Life cycle management and end-to-end engineering - The human being as a conductor for added value	Samuel Nilsen and Eric Nyberg (2016)
- Intelligent Decision-Making and Negotiation Mechanism: In smart manufacturing system needs more autonomy and sociality capabilities as key factors of self-organized systems whereas the today's system has 3C Capabilities i.e. lack autonomy in the systems - High Speed Industrial Wireless Network Protocols: The IWN network used today can't provide enough bandwidth for heavy communication and transfer of high volume of data but it is superior to the weird network in manufacturing environment - System Modelling and Analysis: In system modeling, to reduce dynamical equations and conclude appropriate control model, systems should be modelled as self-organized manufacturing system. The research is still going on for complex system - Modularized and Flexible Physical Artefacts: When processing a product, Equipment for machining or testing should be grouped and worked together for distributed decision making. So, there is a need of creating modularized and smart conveying unit that can dynamically reconfigure the production routes	Wan et al. (2016)

4) Potential Blockchain Applications in Manufacturing

4.0.1) Preliminary Considerations

The rapid progression in information technologies combined with evolutions in industrialization methods, have given rise to the fourth industrial revolution that led to the creation of SMS.

The advent of the Industry 4.0 has promised revolutionary benefits for the new generation of manufacturing systems (*paragraph 3.4*), not only significantly changing the way of producing but also radically transforming and restructuring both horizontally and vertically the whole value chain with the help of technologies coming from the digital transformation (*paragraph 3.5*) that has influenced also the offered products and services.

The advanced digitization within the new manufacturers led us towards an ecosystem so that the product is manufactured through a worldwide network of factories, supply chains, customers and other interconnected service providers (e.g. logistic services, retailers, customer care centres, etc.): this ecosystem becomes highly automated with the development of smart factories that create multiple opportunities for producers and even new business ideas. Naturally, an entire automated and interconnected system exposes to multiple risks, in particular related to the Internet of Thing world whose connectivity is not safe by definition, since a very large number of objects is deployed and it is not possible to check every time every device, exposing them to possible attacks and hence making the entire network vulnerable.

Under the guidance of Industry 4.0 revolution, for the effective development of smart manufacturing systems, there are several requirements (*paragraph 3.6*) that need to be satisfied where security is always essential and must be guaranteed for manufacturers (e.g. no interoperability is effective whether the open network is not safe; decentralization is not achievable if attacks can take control over the network; virtualization is useless if information inside the cyber world are tampered and mismatch the physical world; etc.). Only achieving the industry 4.0 requirements it is possible to successfully implement and deploy smart manufacturing application and exploit truly the Industry 4.0 benefits: hence security techniques are, for sure, needed for an effective system integration between smart manufacturing components.

Blockchain is a promising technology in this sense: it is able to provide security, trust, data integrity and decentralization, without involving any other third party, to cyber-physical systems of smart manufacturing companies, ensuring that smart factory can perform autonomously and safely their innovative processes (e.g. automatic ordering of necessary spare parts, exploit benefits of predictive maintenance, accomplish regulation of energy

consumption for smart energy saving, send reliable information all over the network for forecasting production demands, identify forthcoming faults in the supply chain before they occur, etc.) and truly exploiting the benefits of the actual industrial revolution throughout the different application enabled by such a technology (*paragraph 2.4.2*). Hence, Blockchain can potentially allow an innovative optimized, flexible and efficient business model where security and trust are guaranteed to all the stakeholders involved.

The security offered by Blockchain technology is essential for an automated industry and all the participants involved, from the manufacturers to the final customers, are honestly interested in the information that is exchanged and stored in the network: for instance, it is very commonly recognized how great is the concern about finding traceability info regarding products for every customers, from the final user to each client in all the steps of supply chains.

There are many different features that the Blockchain technology can offer for the manufacturing and they come from key characteristic of this technology itself (*paragraph 2.2*): first of all, the consensus mechanism required permits to reach an agreement amongst all the participants that are inside the network and are demanding to store and share blocks, and hence information, in a decentralized but still secure, and accepted by everyone, modality; secondly, all the block are linked together through cryptographic functions assuring also that the agreed information is untampered; thirdly, all the actors inside the network can benefits from the absence of a third intermediary party.

Hence with Blockchain, every entity involved in the manufacturing network (i.e. a person, a group of people, an organization, a device, a sensor, a robot, a software, etc.) can take part in the recording process and check for information shared all over the interconnected ecosystem in a very transparent way: they can collaborative produce detailed ledgers of transactions and activities, establishing trust and reliability on a shared ledger that represents the history of all the activities and processes done.

4.0.2) Definition of a Framework for Assessing Potential Blockchain Application

From the literature review, it is evident that the Blockchain is a technology that can be useful for different scenarios within the industry 4.0.

The purpose of this thesis, which is to study the applicability of Blockchain technology in manufacturing, considering the different types of Blockchain, the various manufacturing scenarios, the benefits of applications and the technological constraints, led to the development of a framework for the assessment of potential Blockchain applications: the framework takes as its input the results of the literature review of *chapter 3* in which 44

potential application cases were identified and for which the requirements (i.e. the 6 key requirements of Industry 4.0, *paragraph 3.6*) of these applications were investigated.

Parallelly, from the literature review of *chapter 2*, 5 main functionalities have been identified together with 22 sub-functionalities that are allowed by the innovative Blockchain technology based on its technical operating characteristics. These functionalities, useful for satisfying the previously identified requirements of Industry 4.0, have allowed to attribute for each application in manufacturing the functionalities of Blockchain useful for their development.

Finally, by clarifying from a technological point of view the characteristics of the Blockchain with the variation of 5 fundamental parameters, it is possible to explain which type of Blockchain is more suitable for the supply of these features, thus allowing finally to correlate each manufacturing application with the type of Blockchain required.

The framework adopted is illustrated in *figure 55*.

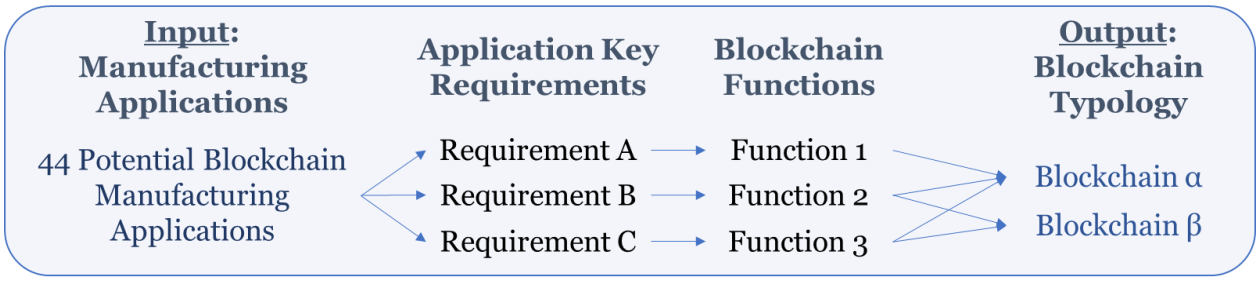


Figure 55: Framework for the Assessment of Blockchain Application in Manufacturing (Author's Own Finding)

4.1) Blockchain Key Functions for Manufacturing Applications

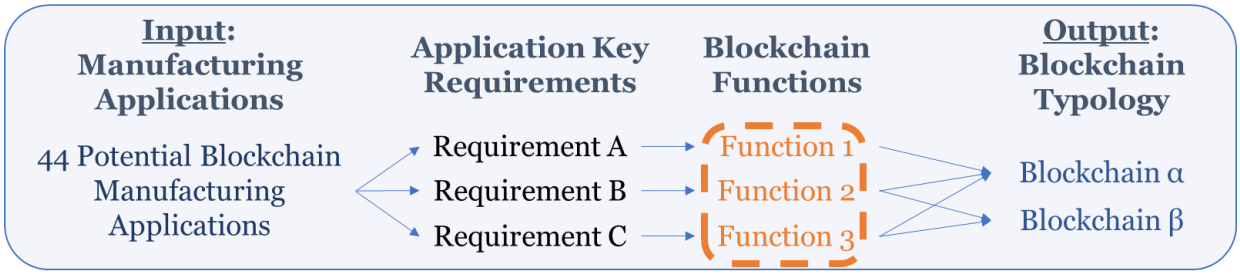


Figure 56: Focus on Functions in the Framework (Author's Own Finding)

The different features that the Blockchain technology could bring to different businesses come from the large versatility of this technology and its adoption modalities: thus, it was essential a study that focused on those functions which have a key role for manufacturing applications.

Starting from the results of the technological literature review of *chapter 2* concerning the Blockchain technology, it is possible to classify the Blockchain Functions into five main categories: *Security*, *Identity*, *Smart Contracts*, *Controls* and *Integration*. For each of these categories, some sub-functions are identified that are still related to the parent categories and permit to indagate deeply several diverse useful applications that are generated from the characteristics of the main function. *Figure 57* represents the classification of Blockchain Functions.

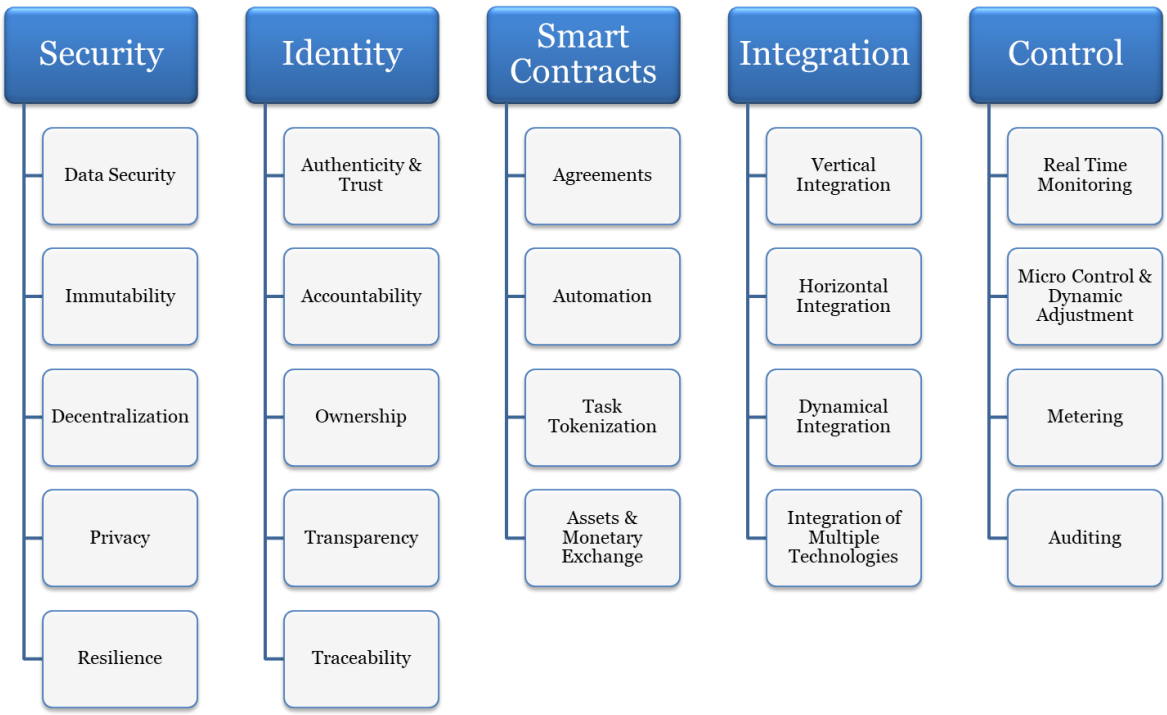


Figure 57: Classification of Blockchain Functions (Author's Own Findings)

1) Security:

The key function of Blockchain is the safety assurance that it can provide to make protected the systems on which it is applied. Security is the primary function which is crucial in many scenarios and also relevant for many manufacturing application, in particular when applied in smart manufacturing systems. There are five sub-functions that explain the Security function for Blockchain:

A. *Data Security:* in the Blockchain ledger, data reliability and consistency is secured by structured cryptographic and hash functions which make impossible to append incomplete information in the system or to send invalid transaction or duplicated data or whatever manipulated information: all the wrong data is rejected by the system and never stored. So, it is not possible to force the system to behave in an incorrect way or to modify its conduct and it is impossible to insert in the ledger information which has not been approved by the consensus algorithm.

B. *Immutability*: once approved by the consensus process, information is protected and recorded forever inside blocks in the ledger; it is not possible to modify nor delete the data that are already inside the Blockchain and neither change the timestamps related to when the transactions were sent, and blocks were added.

C. *Decentralization:* thanks to the consensus algorithm it is possible to reach an agreement between multiple parties that do not trust to each other. This decentralization allows for the elimination of intermediary third parties since an authoritative control is no longer needed. By eliminating a central authority, there is no possibility to control the network singularly; also, the current practice of third parties collecting personal data or manipulate under request or for other interests, which generate the risk of security breaches and poor reliability of information, is no longer a problem.

D. *Privacy:* since data inside blocks is encrypted through cryptographic hash functions, when the decryption rules are kept secret to those who are not permitted to access to the information, the data privacy is guarantee still maintaining the access to the ledger open to everybody, also permitting the Blockchain to continue its operations without any further intervention.

E. *Resilience:* for the reason that the ledger is distributed across multiple locations in the network, the entire Blockchain can continue to operate even if one or more parts of the network go down, fail or are attacked by malicious entities. In addition to this, if a party leaves a network, none of the data it has dispatched on the Blockchain will be lost and hence the Blockchain databases are stored in multiple nodes and have not one single point of failure, on the contrary of many centralized systems.

2) Identity:

Another peculiar function enabled by the Blockchain, and often required in SMSs, is the Identity concept that permits the user to benefit of different functionalities:

A) *Authenticity & Trust*: this is the second key functions for Blockchain applications, and it consists in the creation of a trusted network between nodes that do not trust and do not even know each other. The underlying mechanism of Blockchain permits, through the digital signature, to enable the authentication feature that identify a distinctive node. The non-repudiation of the signature is fundamental for authenticating the information and the agreements inside the Blockchain: an entity in the network cannot be substituted by anyone else (i.e. cannot sign transactions on behalf of another one), the digital identify cannot be stolen and an information cannot be untrue nor neglected by anyone.

B) *Accountability*: the mechanism of digital signature inside the Blockchain is crucial for signing blocks and every time a block is added to the chain, it is already signed by its author. Therefore, every node in the network is responsible for the information that it is sending on the ledger and there is no possibility to maintain unsigned the data or to append information, related to processes, activities, transactions, etc. that are not pertained to anyone: each block has an author who is accountable for the information delivered to the Blockchain.

C) *Ownership*: the usage of Blockchain for digital identities permits to express the concept of property on every object, such as machines, tools, systems, etc. and on every digital item, like a project, a design, a patent, etc. thanks to the authentication functions which is guarantee by univocal hashes. Every node in the network has its own hash on which are related some other hashes that are associated to specific physical & digital elements: hence, when their hash is revealed on the network, they could be univocally accredited to a specific owner that is recognized by its identity.

D) *Transparency*: it is one of the most appealing function, but it seems somehow in contrast with the concept of privacy already mentioned: however, Privacy and Transparency coexist onto the Blockchain and offer two useful functions for its users. Since transactions of each public address are stored in blocks that are open to viewing, using an explorer it is feasible to look for every transaction carried out by a specific address. This is the concept of transparency. Of course, every user can obtain more than one public address and avoiding revealing the public identity, it can preserve a certain degree of privacy when it is desired (still letting possible to explore the transaction related to the anonymous address).

E) *Traceability*: it is a direct consequence of the previous four functions. Blockchain allows for maintain tracking of anything across the network and it means that it is possible to know everything about the history of an item simply exploring the information contained in the distributed ledger.

3) Smart Contracts:

Smart Contract is a particular feature which is enabled by the preceding two features of Identity and Security that permit the execution of intelligent contracts on distributed network without the need of any intermediary that regulate or verify the terms. They can be used in many different scenarios and circumstances, letting the participant in the Blockchain to exploit these specific purposes:

A) *Agreements:* a smart contract permit to reach an agreement in the exact moment in which certain conditions are met inside the Blockchain. This means that it is possible to make legal agreement thanks to data that is not modifiable and it is well attributable to precise entities: in fact, Security and Identity assure that the contract is valid only under certain conditions that cannot be changed later by any parties and that cannot be repudiated by the authors who signed the contract due to the mechanism of the digital signature used by the Blockchain technology: of course, the terms of the contract can be renegotiated and modified when all parties come to a new agreement.

B) *Automation:* this feature consents to execute certain automatic actions when a series of programmed conditions occur, on the basis of several if-then-else statements. Smart contracts, hence, can automatically control over physical and digital objects though executable programs that are safe by design for relying on Blockchain systems: automation regards not only the performing of activities but also the gathering of data that take place through different types of oracles (*see paragraph 2.3.3*).

C) *Task Tokenization:* smart contracts act as agents that operate on behalf of the contractor and can offer the functionality of issue, manage and exchange tokens whether some or all the terms and conditions of the specified contract are verified. Hence, when a person, a machinery, a tool, a robot, a software, etc. accomplishes a specific task and write it on the Blockchain, it is possible to attribute to this task a monetary equivalent both whether the action is active or passive (i.e. an action is carried out by the machine, like a production of an item, or it is incurred by the machine, like a maintenance activity) creating a tokenization system that transform small tasks, large activities or entire operations in economic terms.

D) *Assets & Monetary Exchange:* with smart contract is possible to exploit an efficient exchanges function between numerous customer-supplier relationship

that can generate a model for opening, negotiating and concluding contracts without heavy documentation: faster, more reliable and cheaper exchanges could be accomplished between multiple parties involved in the agreement allowing a rationalized flows of money and assets inside the entire network.

4) Integration:

The integration between different entities and technologies in manufacturing is becoming more and more essential and Integration is an important function provided by distributed ledger technology. Blockchain permits 4 different types of integration:

A) *Vertical Integration*: this function let the Blockchain to support vertical integration by providing a trusted common point for exchanging data, information and money through a multitude of manufacturing actors, that participate in the value chain of the product, with which it interacts; moreover, when this connectivity becomes automatic, information can be collected and sent automatically by the multiple systems, inside the production plant, to one of the many players in the value chain (e.g. design team, manufacturing operators, etc.).

B) *Horizontal Integration*: distributed ledger technology allows manufacturers, suppliers and customers to cooperate together. This integration function permits the development of a flexible and fast (i.e. low latency) network, and when Blockchain is working with smart contracts, it become a suitable technology for horizontal integration mechanisms for all actors involved in modern industrial processes (by also to carrying out economic transactions). Furthermore, regarding the communication between manufacturers, it is achieved using IoT device (e.g. intelligent vehicles, smart machinery) whose security is essential and therefore the use of the Blockchain is again suggested.

C) *Dynamical Integration*: Blockchain is able to dynamically integrate different phases across the value chain (e.g. product design, engineering phases, supply chain management, etc.), making possible to obtain rapid reactions following the feedback received from the different actors (internal or external to the manufacturer) taking part in production process, accelerating certain bureaucratic activities that are used to allow such interactions.

D) *Integration of Multiple Technologies*: the ledger technology permits the integration of diverse technologies, changing the way workers interact with each other and with the working environment. This function lets the Blockchain to become an information exchange hub with which operators, devices, software (who are all technologically independent) just need to recall, through the usage of the Blockchain technology, the appropriate client functionality, without any worries about how other technologies will later interact with the ledger.

5) Control:

This is the last function that open to the possibility for Manufacturing to regulate and govern the real world by means of digital technologies. In particular it is possible:

A) *Real Time Monitoring*: distributed ledger technology suits the real time monitoring needs of manufacturer since information, once stored inside a block, is automatically propagated across the network to all the nodes. Thus, there is no need for asking for data since a Blockchain explorer is sufficient for retrieving necessary information creating an interconnected network that could operate live and monitor all the information real time.

B) *Micro Control & Dynamic Adjustment*: the distributed ledger technology can impact manufacturing systems by facilitating the dynamical control over processes thanks to the safe record of events and actions at the micro levels (e.g. a specific task operated by a machine, etc.) allowing for adjustments (e.g. a plants can increase/increase its production rate, etc.) that are based on information recorded on the distributed ledger by different participants.

C) *Metering*: all the activities and processes are recorded continuously inside the ledger with a fine detail, recreating a digital copy of everything happened in the physical systems; with this unalterable record, metering actions are possible with a distributed exploitation of KPIs all over the network. Different analysis can be done on the available information, letting a better understanding events, trends, incidents, problems, etc. that become source of knowledge for improving operations and create a more efficient and better safety processes.

D) *Auditing*: the presence of accurate records that are trusted and even guaranteed by the security level inside the Blockchain technology, can be used for auditing activities and as evaluation factor for the activities of manufacturer and thus it is useful for the evaluation of the market position and even financial standing of a company that is showing its activities through the Blockchain.

At this point, in order to clarify how different types of Blockchain can satisfy diverse industrial applications, it is essential to attribute to each Industry 4.0 requirement, that as already explained in *paragraph 3.6*, are *Interoperability, Service Orientation, Decentralization, Real Time Capability, Modularity* and *Virtualization*, the functionalities, that have just been individuated and described, offered by the distributed technology that allow these requirements to be fully satisfied.

The following *table 5* shows in a timely manner what are the key Blockchain functions that are suitable for the satisfaction of each possible requirement for industrial applications in the evolutionary scenario of Industry 4.0.

Figure 58: Focus on How Functions Satisfy Requirements in the Framework (Author's Own Finding)

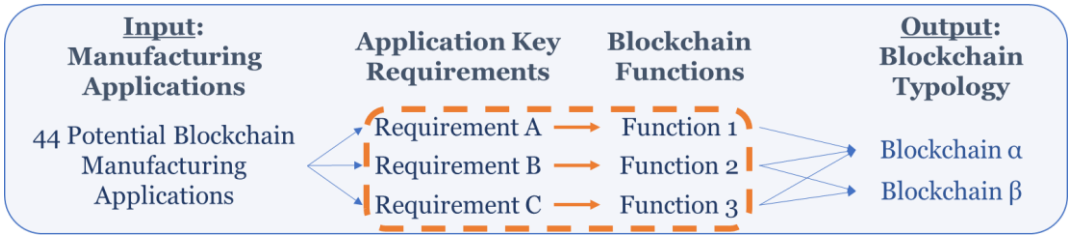


Table 5: Blockchain Functions Satisfy Manufacturing Requirements in Industry 4.0 (Author's Own Findings)

Blockchain Function / Industry 4.0 Requirement	Security					Identity					Smart Contract				Integration				Control			
	Data Security	Immutability	Decentralization	Privacy	Resilience	Authenticity & Trust	Accountability	Ownership	Transparency	Traceability	Agreements	Automation	Task Tokenization	Assets & Mon. Exchange	Vertical Integration	Horizontal Integration	Dynamical Integration	Int. of Multiple Technol.	Real Time Monitoring	Micro Control & Adjust.	Metering	Auditing
Interoperability	✓		✓	✓	✓	✓					✓	✓			✓	✓	✓	✓	✓			
Service Orientation						✓	✓	✓			✓	✓	✓	✓					✓		✓	✓
Decentralization	✓	✓	✓	✓	✓				✓	✓							✓	✓				
Real-time Capability												✓					✓		✓	✓	✓	✓
Modularity						✓	✓	✓	✓	✓	✓				✓	✓		✓				
Virtualization	✓	✓			✓	✓		✓	✓									✓				

4.2) Classification of Blockchain typologies based on their Characteristics

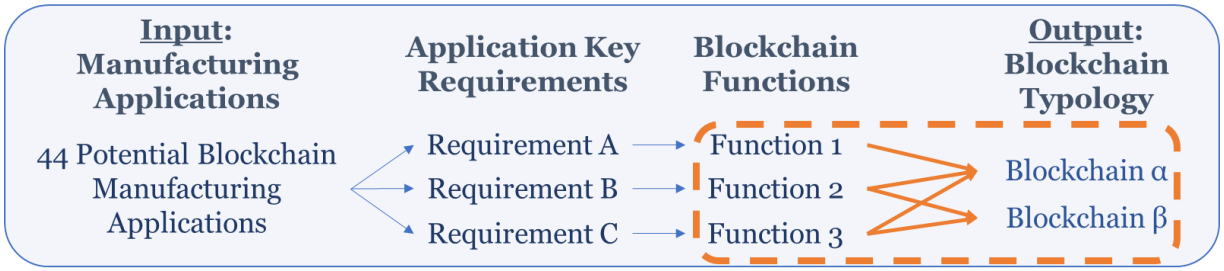


Figure 59: Focus of What Blockchain Types Enable Certain Functions in the Framework (Author's Own Finding)

In the *chapter 2* were explained the technical characteristics of the Blockchain technology: it is now essential to propose a classification based on technical characteristics for different Blockchain typologies in order to, later, establish which Blockchain is more suitable in each industrial application.

In particular, it is necessary to establish how the 5 individuated functionalities offered by the Blockchain vary according to its topological characteristics. In fact, each Blockchain is different from the other: as already explained in *chapter 2*, the differences between Blockchain typologies are mainly based on the users' interaction modality with the distributed ledger and on the way data is managed and accessed by the nodes.

So, from the literature of *chapter 2* were established 5 main characteristics that with their variations determine different Blockchain topological structure: these characteristics are *Access Regulation*, *Permission Control*, *Incentive Typology, Operational Modality* and *Consensus Algorithm*. Therefore, Blockchain can be distinguished by:

1. **Access Regulation**:
    a. ***Public Blockchain*:** in this kind of Blockchain there is no need for approval of someone for joining in the network, hence everyone is allowed to publish and validate transactions. When Blockchains are public, they are very useful in industrial situations where there is need for a very high degree of transparency or where huge consumer devices interactions is necessary. In these scenarios, the mining nodes receive some reward for their computing work (e.g. Bitcoin & Ethereum).
    b. ***Private Blockchain:*** here, the participation in the Blockchain activities is regulated by the network owner and for this reason there is a designated set of nodes that are responsible for the blocks' validation and some restrictive rules that consent the access to the Blockchain only to specified nodes. In private Blockchains there is not a centralization since they are still considered decentralized systems, but they operate like a closed and secured distributed

database that are very useful in industrial scenarios where participants are all recognised or where there is need for performing audits activities (e.g. Ripple).

c. ***Consortium Blockchain:*** these Blockchains could be considered an alternative of public Blockchains since in this configuration there is a group of owner, and not a single entity, that regulate the Blockchain by restricting the access of nodes to the ledger and by regulating the actions that are executed by permissioned users to the Blockchain (who can add transactions, who can mine blocks…). In these typologies of Blockchain the consensus algorithm is executed by a selected group of nodes that in this way are able to increase the privacy regarding the transactions even accelerating the validation process. The context in which are used consortium Blockchains is referred to groups of industrial firms that, since they are working in the identical field, need to share some information and transaction amongst them: it happens that each participant uses its personal validation node and whether a minimum number of different nodes approves the transaction, then it is put on the Blockchain.

d. ***Hybrid Blockchain:*** This typology is a mixture between private and public Blockchains. It combines the two types into one Blockchain that create an ecosystem which has the privacy benefits of a private and the transparency of a public. Hence it is possible to exploit both benefits of each approach creating a distributed ledger which is tailored to industrial cases where it is required to exploit both characteristics at different levels: for instance, in logistics and supply chains it could be ideal to manage the complexity by dealing with transactions of main parties in a private way, in order to have the key partners informed by the network in a secure way adding only trusted entities (e.g. large manufacturers in the supply chain); contemporary, maintaining a public Blockchain for a sub-list of smaller partners that are able to interact publicly to the network in a faster and dynamic way with an easier process of trust establishment (e.g. local transportation providers).

2. **<u>Permission Control</u>**:

a. ***Permissioned****:* in these Blockchains, an owner controls who can perform and deploy transactions on top of the distributed ledger. It is not possible for everyone to send transaction. The permissioned Blockchains can be applied on private and consortium Blockchains and for the private part of the hybrid Blockchains.

b. ***Permissionless****:* in these Blockchains, there is not a formal control on the Blockchain, hence everyone has the same faculties and can perform the same action onto the distributed ledger, placing transactions and mining blocks.

The permissionless Blockchains can be associated only to public Blockchain and for the public part of hybrid Blockchains.

3. **Incentive Typology**:
    a. ***Tozenized*:** Blockchains that use tokens which are exchanged amongst participants in order to incentivize the transactions and mining execution.
    b. ***Non-Tozenized***: Blockchains that do not depend on tokens for their executions: they run only for the interest in maintaining up the ledger and there is not a token system (i.e. a virtual currency) on top of it.
4. **Operational Modality**:
    a. ***Logic-Oriented***: they are able to run some certain logical applications: the most diffused applications are the Smart Contracts even if they could allow the executions of other different applications in a decentralized manner (i.e. dApps).
    b. ***Transaction-Oriented***: they are developed in order to only exchange transactions for tracking digitalized assets or virtual currencies without the possibility of executing other applications.
5. **Consensus Algorithm**:

    As already mentioned in the *paragraph 2.2.6.2*, each consensus algorithm provides peculiar characteristics to the Blockchain. In particular, in choosing between the different algorithms, it is necessary to consider the scalability trilemma and to choose the pair of characteristics that is more suitable on a case by case basis, evaluating the pros and cons of each algorithm in term of throughput, latency, size of the network, etc. In detail, the trilemma allows only three couple of characteristics:

    a. Security & Scalability
    b. Security & Decentralization
    c. Scalability & Decentralization

With them, it is possible to recognize the most suitable topology for each fundamental function. For doing so, the literature review permitted to integrate the results coming from the identification of the 5 functions of the Blockchain with the five main characteristic variables of each Blockchain technology, considering only the main functionalities without going into the details of the relative sub-functionalities (since sub-functionalities are always available when the main functionality is active): the *table 7* shows in detail the features that the different typologies of Blockchain should have to offer precisely certain functionalities. The *table 6* of acronyms is provided for supporting the reading.

Table 6: What Blockchain Characteristics Enable Certain Functions (Author's Own Findings)

Blockchain Function & Sub-Function / Characteristic of Blockchain		Access Regulation	Permission Control	Incentive Typology	Operational Modality	Consensus Algorithm
Security	- Data Security - Privacy	Pr	Ped	T	Tr	Se & De
	- Immutability - Decentralization - Resilience	C				
Identity	- Authenticity & Trust - Transparency - Traceability	Pu	Pess	T	Tr	Se & Sc
	- Accountability - Ownership	C	Ped			
Smart Contracts	- Agreements	C	Ped	NT	Lo	Se & De
	- Automation	Pr				
	- Task Tokenization	H	Ped & Pess	T	Tr	
	- Assets & Mon. Exchange	Pu	Pess			
Integration	- Vertical Integration - Horizontal Integration	C	Ped	T	Tr	Sc & De
	- Dynamical Integration	Pr				
	- Int. of Multiple Technol.	H	Ped & Pess	NT	Lo	
Control	- Real Time Monitoring - Micro Control & Adjust. - Metering	Pr	Ped	T	Tr	Se & Sc
	- Auditing	C		NT	Lo	

Table 7: Acronyms for Interpreting the Table 6 (Author's Own Findings)

Table of Acronyms	
Pu	Public
Pr	Private
C	Consortium
H	Hybrid
Ped	Permissioned
Pess	Permissionless
T	Tokenized
NT	Non-Tokenized
Tr	Transaction-Oriented
Lo	Logic-Oriented
Se & Sc	Security & Scalability
Se & De	Security & Decentralization
Sc & De	Scalability & Decentralization

4.3) Requirements for Potential Manufacturing Applications

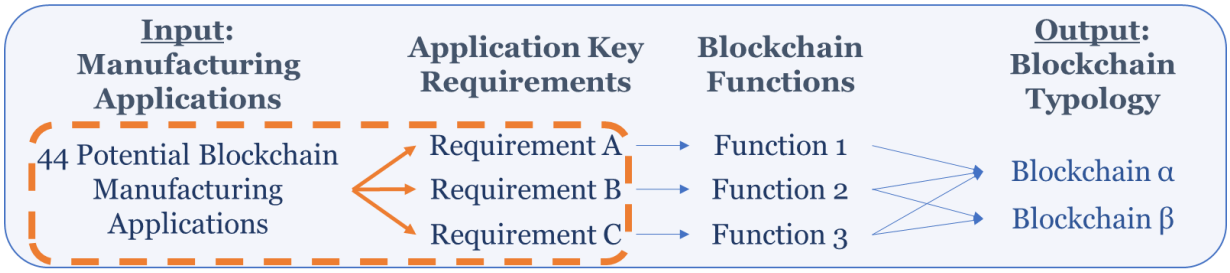


Figure 60: Focus of Which Requirements each Manufacturing Application Needs in the Framework (Author's Own Finding)

The analysis of the literature of *chapter 3* has resulted in the identification of 44 potential applications of the Blockchain in manufacturing that are illustrated in *the table 8*: these represent a sample that derives from the recognition of scenarios potentially suited to the Blockchain technology or from the identification of conceivable proof-of-concepts proposed by the literature or from the detailed analysis of the current Blockchain implementations that could have other usages in different scenarios so generating alternatives for the actual Blockchain applications or from different implementation field that have some analogies with the manufacturing context.

All these potential applications share several requirements that must be met before they can be used in a typical context of Industry 4.0: *table 9 & table 10* show which requirements these applications must have in order to be effectively implemented in a modern technological context.

Table 8: Potential Blockchain Manufacturing Application Obtained from the Literature Review (Author's Own Findings)

Potential Blockchain Manufacturing Application
- Industrial IoT Interaction in Smart Manufacturing Systems **(Teslya & Ryabchikov, 2017)**
- Decentralized & Trusted IoT System **(Li, et al., 2017)**
- IoT Identification, Nodes Identity Management **(Kravitz & Cooper, 2017)**
- High Security IoT Systems (**Suárez-Albela & Castedo, 2017**)
- Data Integrity Verification for IoT **(Liu, Yu, Chen, Xu, & Zhu, 2017)**
- Energy Efficient Decentralized Communication for Industrial Resource-Constrained IoT Devices **(Zhou, et al., 2014)**
- Fast and Scalable Decentralized IoT Network
- Safe horizontal cooperation between production systems **(Zhang, Liu, & Shen, 2017)**
- Collaborative manufacturing over customers and suppliers' factories **(Yan, Duan, Zhong, & Qu, 2017)**
- Tracking of raw materials/products over manufacturers' supply chain
- Provenance certification of raw materials/inputs/products amongst the entire value chain **(Lu & Xu, 2017)**
- Innovative Business Models: Maintenance-aaS, Virtual Network-aaS, Process-aaS, Robot/Machine-aaS

(Backman, Yrjola, Valtanen, & Mammela, 2017)

- Smart capacity management, Smart demand planning

- Historical shared ledger for product fabrication, material handling and machine/tools maintenance **(Lee & Pilkington, 2017)**

- Establishment of Safe Manufacturing Data Sharing Interface **(Abdullah, Hakansson, & Moradian, 2017)**

- Trusted Data Analytics Environment Creation **(Chen & Xue, 2017)**

- Transparent & Reliable Data Circulation amongst Industrial Partners without 3rd Parties **(Yue, Junqin, Shengzhi, & Ruijin, 2017)**

- Predictive & Prescriptive Manufacturing Analytics for Maintenance and Failure Prevention **(Menezes, Kelly, Leal, & Roux, 2019)**

- Distribution of Computational Power

- Assistance in Manual Assembly Systems for Increased Productivity **(Loch, Quint, & Brishtel, 2016)**

- VR/AR for Remote Live Support **(Schneider, Rambach, & Stricker, 2017)**

- Training and Skilling of Workers **(Boud, Haniff, Baber, & Steiner)**

- Industrial Design Processes: Product/System Development and Environment/Plant Layout Designing **(Cave, 2016)** & Distributed Prototyping **(Shin, Park, Jung, & Hong, 2014)**

- Data Security and Systems Availability

- Maintenance of Industrial Components, Virtual Disassembly, Analysis and Treatment of Equipment Failure **(Qing, 2010)**

- Improved Industrial Service Delivery **(Aleksy, Vartiainen, Domova, & Naedele, 2014)**

- Production Traceability of Robots & Cobots Operations **(Robla-Gomez, et al., 2017)**

- Warehouse and Autonomous Inventory Management **(Hasan, Datta, & Rahman, 2018)**

- Vehicle-to-Vehicle and Vehicle-to-Infrastructure Communication **(Singh & Kim, 2018) (Miller D. , 2018)**

- Objects Transportation in Industrial Areas **(Harik, Guerin, Guinand, Brethe, & Pelvillain, 2015)**

- Reputation System for Network of Autonomous AGVs & UAVs **(Yang, Zheng, Yang, & Leung, 2017)**

- Inspections of Industrial Facilities for Maintenance Purposes **(Nikolic, et al., 2013)**

- Autonomous Charging, Parking & Refuelling of Vehicles **(Huang, Xu, Wang, & Liu, 2018)**

- Data Storage in IoT Manufacturing Cloud **(Wu, et al., 2017)**

- Distributed Cloud Architecture for Secure and Reliable Storage Services for SMSs (**Li , Liu, Chen, Chen, & Wu, 2017**)

- Edge Computing for Industrial Resource-constrained Devices (**Rawat, Parwez, & Alshammari, 2017**)

- Data Collection and Verification from Multiple Resources

- Supply Chain Decentralization **(Winkler-Goldstein, Imbault, Uslander, & Gastine, 2018)**

- 3D Design Model Traceability; Intellectual Property Protection **(Holland, Stjepandic, & Nigischer, Intellectual Property Protection of 3D Print Supply Chain with Blockchain Technology, 2018)**

- Interconnected 3D Printers **(Trouton, Vitale, & Killmeyer, 2017)**

- License Management through Smart Contract **(Herbert & Litchfield, 2015)**

- Transparency to Third Parties for Auditing Purposes **(Holland, Nigischer, Stjepandić, & Chen, 2017)**

- Intra & Interconnection Industrial Cybersecurity **(Rawat, Njilla, Kwiat, & Kamhoua, 2018)**

- Enabling Simulation-as-a-Service **(Krammer, et al., 2018)**

Table 9: Which Requirements Each Manufacturing Application Need – First Part (Author's Own Findings)

Potential Manufacturing Application \ Industry 4.0 Requirement	Interoperability	Service Orientation	Decentralization	Real Time Capability	Modularity	Virtualization
Industrial IoT Interaction in Smart Manufacturing Systems	✓	✓				
Decentralized & Trusted IoT System	✓	✓	✓			
High Security IoT Systems	✓		✓		✓	
IoT Identification, Nodes Identity Management	✓		✓	✓	✓	
Data Integrity Verification for IoT		✓	✓		✓	
Energy Efficient Decentralized Communication for Industrial Resource-Constrained IoT Devices	✓	✓				
Fast and Scalable Decentralized IoT Network	✓		✓	✓		
Establishment of Safe Manufacturing Data Sharing Interface		✓	✓		✓	✓
Trusted Data Analytics Environment Creation	✓	✓			✓	✓
Transparent & Reliable Data Circulation amongst Industrial Partners without 3rd Parties	✓	✓				
Predictive & Prescriptive Manufacturing Analytics for Maintenance and Failure Prevention		✓			✓	✓
Assistance in Manual Assembly Systems for Increased Productivity	✓			✓		✓
VR/AR for Remote Live Support	✓	✓		✓		✓
Training and Skilling of Workers	✓	✓				✓
Industrial Design Processes: Product/System Development and Environment/Plant Layout Designing & Distributed Prototyping		✓	✓			✓
Maintenance of Industrial Components, Virtual Disassembly, Analysis and Treatment of Equipment Failure	✓	✓	✓			✓
Improved Industrial Service Delivery	✓	✓		✓		
Intra & Interconnection Industrial Cybersecurity			✓		✓	
Data Security and Systems Availability			✓	✓	✓	
Data Storage in IoT Manufacturing Cloud	✓		✓	✓		
Distributed Cloud Architecture for Secure and Reliable Storage Services for SMSs	✓	✓	✓			
Edge Computing for Industrial Resource-constrained Devices	✓	✓	✓	✓		

Table 10: Which Requirements Each Manufacturing Application Need – Second Part (Author's Own Findings)

Potential Manufacturing Application \ Industry 4.0 Requirement	Interoperability	Service Orientation	Decentralization	Real Time Capability	Modularity	Virtualization
Production Traceability of Robots & Cobots Operations		✓	✓	✓		
Warehouse and Autonomous Inventory Management	✓		✓	✓		
Vehicle-to-Vehicle and Vehicle-to-Infrastructure Communication	✓		✓	✓		✓
Objects Transportation in Industrial Areas	✓		✓	✓	✓	
Reputation System for Network of Autonomous AGVs & UAVs		✓			✓	✓
Inspections of Industrial Facilities for Maintenance Purposes	✓		✓			✓
Autonomous Charging, Parking & Refuelling of Vehicles	✓	✓		✓		
Supply Chain Decentralization	✓	✓	✓	✓		
3D Design Model Traceability; Intellectual Property Protection		✓	✓			
Interconnected 3D Printers	✓	✓				
License Management through Smart Contract		✓	✓			
Transparency to Third Parties for Auditing Purposes	✓	✓	✓			
Data Collection and Verification from Multiple Resources	✓		✓			
Distribution of Computational Power	✓	✓			✓	
Enabling Simulation-as-a-Service	✓	✓			✓	✓
Safe horizontal cooperation between production systems	✓		✓	✓		
Collaborative manufacturing over customers and suppliers' factories	✓	✓			✓	
Tracking of raw materials/products over manufacturers' supply chain		✓	✓	✓		
Provenance certification of raw materials/inputs/products amongst the entire value chain		✓	✓		✓	
Innovative Business Models: X-aaS	✓	✓	✓			✓
Smart capacity management, Smart demand planning	✓	✓	✓	✓		
Historical shared ledger for product fabrication, material handling and machine/tools maintenance	✓		✓	✓		

4.4) Blockchain Typologies for Effective Manufacturing Applications

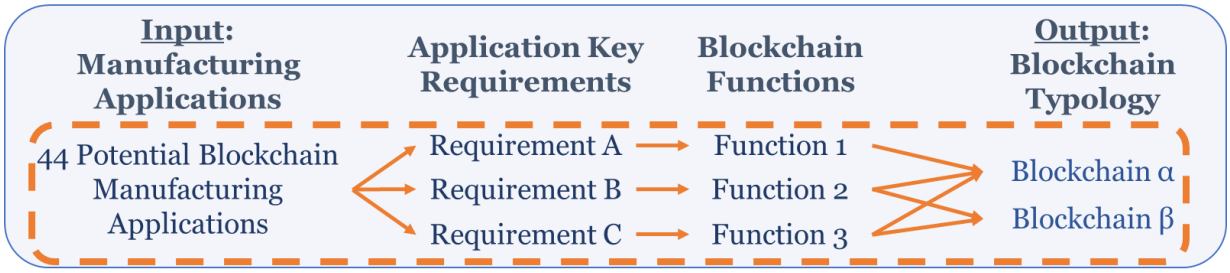


Figure 61: Application of the Results over the Whole Framework (Author's Own Findings)

Although it may be clear from the literature that different Blockchains can solve challenges or help to achieve the benefits of different manufacturing applications in the Industry 4.0 context, it is still necessary to establish how this can happen.

Therefore, after having established which characteristics the Blockchains must have to guarantee certain functionalities that satisfy the recognised requirements for the identified potential applications in manufacturing, with the help of the *tables 5, 7, 9 and 10*, all generated after the literature review of *chapters 2 and 3*, it is possible to map the different types of Blockchain for the different manufacturing applications taking into account the technological constraints that Blockchain technology must respect for a correct integration with the other technologies that are diffusing within the new smart manufacturing systems.

Hence, to clarify how the Blockchain should be applied in manufacturing, the identified potential applications have been analysed and mapped considering the different technologies with which the Blockchain must interface, by grouping them following the main technological pillars identified in the literature review (*paragraph 3.5*). In the following sub-paragraphs are explained the resulted different types and characteristics that the Blockchain must have in accordance to the identified Blockchain application in manufacturing.

Hence, the application of the defined framework permitted to attribute to each application the 5 main Blockchain variables that are specified in the following order:

1. Assess Regulation: Public, Hybrid, Consortium, Private
2. Permission Control: Permissionless (*Pess)*, Permissioned (*Ped*)
3. Incentive Typology: Tokenized (*T*), Non-Tokenized (*NT*)
4. Operational Modality: Transaction-Oriented (*Tr*), Logic-Oriented (*Lo*)
5. Consensus Algorithm characteristics: Security & Decentralization (*Se & De*), Security & Scalability (*Se & Sc*), Scalability & Decentralization (*Sc & De*).
   In addition, based on *table 1*, an example of consensus algorithm in suggested for the related manufacturing application and put into bracket.

4.4.1) Blockchains for Internet of Things in Manufacturing Applications

Table 11: Blockchain Typologies for IoT Manufacturing Application (Author's Own Findings)

Integration Technology: Internet of Things	
Blockchain Typologies	**Potential Manufacturing Application Examples**
- Private, Permissioned, NT, Lo, Se & De (pBFT) Blockchain	- Industrial IoT Interaction in Smart Manufacturing Systems (Teslya & Ryabchikov, 2017)
- Public, Permissionless, NT, Lo, De & Sc (PoS) Blockchain	- Decentralized & Trusted IoT System (Li, et al., 2017)
- Private, Permissioned, T, Tr, Se & De (PoId) Blockchain - Private, Permissioned, T, Tr, De & Sc (PoAh) Blockchain	- IoT Identification, Nodes Identity Management (Kravitz & Cooper, 2017)
- Public, Permissionless, T, Tr, Se & Sc (PoR) Blockchain - Private, Permissioned, T, Tr, Se & Sc (PoR) Blockchain	- High Security IoT Systems (Suárez-Albela & Castedo, 2017) - Data Integrity Verification for IoT (Liu, Yu, Chen, Xu, & Zhu, 2017)
- Public, Permissionless, T, Tr, Se & Sc (PoET, PoSp) Blockchain - Public, Permissionless, T, Tr, Se & De (PoW) Blockchain (with Scrypt / X11 Hash Function)	- Energy Efficient Decentralized Communication for Industrial Resource-Constrained IoT Devices (Zhou, et al., 2014)
- Public, Permissionless, T, Tr, De & Sc (DPoS) Blockchain (with Mini-Blockchain Solutions)	- Fast and Scalable Decentralized IoT Network

When traditional IoT technologies are used in industrial environments, in particular for Industry 4.0 applications, they are generally deployed through the massive use of sensors and actuator with machineries and devices that have connection capacities in smart interconnected environments. The Blockchain can be very useful for smart manufacturing systems that use IoT devices where, during the execution of different production phases, exchanges of information and decentralized decisions takes place within a trusted environment.

For the creation of an interconnected and secure environment, a Blockchain architecture based on *Smart Contracts* developed according to *Chaincode for Hyperledger Fabric* or *Smart Contracts* developed through *Solidity for Ethereum*, would allow the creation of a network with a shared data register where all transactions are signed and timestamped in real time, creating trust and reaching a consensus between a multitude of devices belonging to several different companies that do not necessary trust to each other. While Hyperledger Fabric is a *Private* and *Permissioned* Blockchain based on a *Practical Byzantine Fault Tolerance* consensus algorithm, suitable for smaller networks of selected manufacturing participants , the Ethereum Blockchain is based on a *Public* and *Permissionless* Network with a *Proof of Stake* consensus mechanism (i.e. *Ethash,* which allows programmability for Smart Contracts and it is faster for mining blocks), suitable therefore for open and large scalable Blockchain applications.

With these types of Blockchain it is possible to ensure different properties to the Industry 4.0 applications of IoT: first of all it is possible to guarantee *security* to the IoT network since the

applications based on Blockchain guarantee that the information generated by IoT devices are unalterable and cannot be deleted by anyone; then, of course, it is possible to guarantee *transparency* to the different participants within the Blockchain, whether they are members of the value chain, customers or other stakeholders, so creating *trust* in IoT devices owned by the company and therefore in the company itself; furthermore, these types of Blockchains allows distributed access to all information even if some nodes disconnect, thus creating a highly reliable network (compared to traditional centralized or cloud based systems) that remains available and fully-working even if more nodes go down; finally, thanks to the adoption of Smart Contracts it is possible to create a *standardized and automatic communication* where the interactions and transactions between the different IoT devices take place autonomously without the aid of people.

Furthermore, other Blockchain typologies can be used effectively for IoT applications, providing specific functionalities for different applications in manufacturing.

When, in a large industrial ecosystem, it is necessary to manage the identity of multiple devices, may be to guarantee their access to certain networks, may be to authorize their interoperability with other devices or when, vice versa, other members in the network must be authorized for using or controlling certain specific IoT devices, then it is essential to guarantee an advanced control of the identity of the nodes: this can be performed through the use of *Private* and *Permissioned* networks with *Proof of Identity* or *Proof of Authentication* consensus algorithms, which are by design adapt for assuring nodes identity and ideal for devices with few computational resources since they do not require high computational power but are lightweight and fast.

In other circumstances, it is possible to use the Blockchain in combination with IoT when it is required to guarantee data integrity in interconnected online environments, so when it becomes critical that the information exchanged by IoT devices in the network and stored on cloud infrastructure, are perfectly trusted, reliable and not damaged nor altered (this opens to the possibility of a safely generation of big data and permits reliable analytics on trusted distributed data without third party service providers). For this application, *Public and Permissionless Proof of Retrievability Blockchain* can be used, satisfying integrity and availability requirement: in addition, when the same Blockchain is made *Private* and *Permissioned*, it is possible to guarantee also confidentiality.

Usually, when the Blockchain is used for any type of IoT device with limited computational and energy resources, it is essential to adopt deeply modified versions of original Bitcoin Proof or Work: *Proof of Stake*, *Delegated Proof of Stake, Proof of Elapsed Time* and *Proof of Space* are the suitable consensus algorithms that allow a lower energy consumption

(fundamental for battery powered devices) and lighter CPU and memory requirements. In addition, other modifications may regard the hash algorithm: usually it is used the SHA-256 that is the most popular since is considered very secure, however alternative like *Scrypt* and *X11* for the hashing functions reduce the mining energy consumption while guaranteeing a faster computation. However, if it is necessary to maintain a high level of security without utilizing the power-hungry SHA-256 hash function, another asymmetric cryptographic scheme based on *lattice* problem is the best solution for IoT application: a typical example is a Blockchain based on *BlockLattice Directed Acyclic Graph*. Other DAGs that are promising for the creation of very high transaction rates IoT applications are *IOTA* and *Byteball* DAGs that enable all connected devices through verification of truth and transactional settlements.

Another variable that could be modified is the Block Size: *Increasing the Block Size* it is possible to increase the throughput of the Blockchain network that is generally low when using IoT devices. Another operation that can be performed for using the Blockchain with IoT is to change the Blockchain size: *compression techniques and mini-Blockchains* can make a working Blockchain network even with small devices with low computational power: they consists in the elimination of old blocks from the chain that can be forgotten by the network since nodes only require the newest portion of the Blockchain in order to synchronize with the network.

4.4.2) Blockchains for Horizontal & Vertical System Integration in Manufacturing Applications

Table 12: Blockchain Typologies for Hor. & Vert. Sys. Int. Manufacturing Application (Author's Own Findings)

Integration Technology: Horizontal & Vertical System Integrations	
Blockchain Typologies	**Potential Manufacturing Application Examples**
- Private, Permissioned, T, Tr, Se **& De (PoW) Blockchain (with** Open Multichain Platform)	- Safe horizontal cooperation between production systems (Zhang, Liu, & Shen, 2017)
- Private, Permissioned, NT, Lo, Se **& Sc (dBFT) Blockchain**	- Collaborative manufacturing over customers and suppliers' factories (Yan, Duan, Zhong, & Qu, 2017)
- Private, Permissioned, NT, Lo, De **& Sc (PoS) Blockchain (with Sidechain**)	- Tracking of raw materials/products over manufacturers' supply chain - Provenance certification of raw materials/inputs/products amongst the entire value chain (Lu & Xu, 2017)
- Consortium, Permissioned, T, Tr, De & Sc (PoS) Blockchain (with Off-Chain Module)	- Innovative Business Models: Maintenance-aaS, Virtual Network-aaS, Process-aaS, Robot/Machine-aaS (Backman, Yrjola, Valtanen, & Mammela, 2017) - Smart capacity management, Smart demand planning
- Consortium, Permissioned, NT, Lo, Se & De **(PoW) Blockchain (with Sidechain)**	- Historical shared ledger for product fabrication, material handling and machine/tools maintenance (Lee & Pilkington, 2017)

In the fourth industrial revolution, the horizontal and vertical integration of systems assumes an essential role more than ever, and communication between customers and suppliers but also data exchange amongst smart factories is something that has to be managed on a daily basis. Although there are already numerous examples of integrations between manufacturing systems (ERP Software, MES Platforms, etc.), the Blockchain can be fundamental to guarantee that greater level of security that would otherwise not be possible even with expensive systemic integrations: in fact, the level of integration required by these platforms needs the additional requirement of not sharing sensitive information between different industrial partners or with customers. Blockchain can certainly helpful for this requirement.

Multichain Blockchains are required for guaranteeing an effective form of collaboration between manufacturers that are sharing information needed to reach a horizontal system integration. It becomes easy, for instance, for a producer to publish specific required quantities of a wanted item, together with all the necessary parameters and specifics to be satisfied, within a select group of suppliers that can easily integrate their production systems on the basis of what their customers is asking for and collaborate together for the production process of that item. Therefore, this application employs different *Private and Permissioned PoW Blockchains* that are connected via a *Multichain Platform* that permits different Blockchains to communicate together establishing a connection between organizations: the visibility over others' Blockchains is kept private to avoid the proliferation of sensitive information but shareable information are available to all the participants in the network and the systems security remains very high since each Blockchain works independently from the mining point of view.

Similarly, when it is necessary to exploit the potential of smart contracts, then it is possible to provide this functionality with *Private & Permissioned Delegated Byzantine Fault Tolerant Blockchains*: they allow the *Smart Contract* deployment maintaining a private access control. Therefore, for integrating horizontally system in this case are necessary *Sidechains* that allow interoperability between independent Blockchains of different manufacturers. Hence, with Smart Contracts it is possible to automate production processes and operations between diverse authors within producers' production systems at the same level of the supply chain (thus horizontal integration) and at different level (vertical integration), maintaining private all the other confidential information inside the single Blockchains (which contain data related to the company production system) but transferring information though Sidechain mechanisms.

Another alternative for avoiding the usage of different separated Blockchains is the *Consortium & Permissioned Proof of Stake Blockchain* that still give the possibility to generate legal agreements between companies through Smart Contracts but restrict the

access to the Blockchain only to selected participants; then, for keeping sensitive the information amongst the selected participants, *off-chain modules* should be deployed in order to store content outside the main Blockchain while keeping *on-chain* only the needed transactions' information for reaching agreement between participants.

Furthermore, for a Blockchain-based vertical integration it could be used another type of Blockchain: *Consortium & Permissionless Proof of Stake Blockchain with Sidechain and Smart Contract* offer the possibility to enable as-a-Service models between manufacturers (for Machines-as-a-Service, Processes-as-a-Service) or amongst customer-supplier relationship (for the providing Maintenance-as-a-Service, Virtual Network-as-a-Service) and also make possible to enhance the entire value chain making a complete system integration for a smart capacity management for manufacturing resources and a smart demand planning for production systems.

4.4.3) Blockchains for Big Data & Analytics in Manufacturing Applications

Table 13: Blockchain Typologies for Big Data & Analytics Manufacturing Application (Author's Own Findings)

Integration Technology: Big Data and Analytics	
Blockchain Typologies	**Potential Manufacturing Application Examples**
- Public, Permissionless, T, Tr, Se & De (Po**W) Blockchain**	- Establishment of Safe Manufacturing Data Sharing Interface (Abdullah, Hakansson, & Moradian, 2017)
- Consortium, Permissioned, T, Tr, Se & De (P**oW) Blockchain** **- Private, Permissioned, T, Tr, Se & De (PoW) Blockchain**	- Trusted Data Analytics Environment Creation (Chen & Xue, 2017)
- Private, Permissioned, NT, Lo, Se & Sc **(dBFT) Blockchain**	- Transparent & Reliable Data Circulation amongst Industrial Partners without 3rd Parties (Yue, Junqin, Shengzhi, & Ruijin, 2017)
- Public, Permissionless, NT, Lo, De & Sc (fBFT) Blockchain	- Predictive & Prescriptive Manufacturing Analytics for Maintenance and Failure Prevention (Menezes, Kelly, Leal, & Roux, 2019)

Smart manufacturing production systems are, by definition, able to collect and process huge volumes of data from numerous sources throughout the entire value chain: manufacturing plants, customers and suppliers, logistics providers of the whole supply chain, external services providers and so on. All together this information is really valuable as their analysis generates a real knowledge that allows to obtain considerable competitive advantages: data is becoming a very valuable asset for manufacturing, however it is necessary to develop advanced data analytics techniques that require different characteristics that the Blockchain, in particular, can satisfy.

Blockchain technology can enhance the data collection since nowadays information that constitutes the industrial big data are dispersed and disseminated in different sources, so

with *Public & Permissionless or Consortium/Private Permissioned PoW Blockchain* it is possible to create a joint data sharing interface through which all the involved parties cooperate in a safe manner. Furthermore, distributed ledger technology can give to Big Data Analytics a very high reliability owed to the establishment of a trusted network of participant, the safeguarding of shared data and the provision of timestamped information. Finally, in an industrial environment in which information circulates continuously and where the data requires the consent of the owner to be exchanged, *Public & Permissionless fBFT Blockchain with Smart Contracts* or *Private & Permissioned Delegated BFT Blockchains with Smart Contracts* would make this procedure standardized and automatic, making them transparent to those who must receive data, allowing a high scalability thanks to the Byzantine Fault Tolerance consensus algorithm which suits when network needs to grows exponentially. It this case two different consensus algorithms may be chosen: *Federated BFT* when in the big data manufacturing application prevails the need for a low latency & high throughput network fully decentralized, or *Delegated BFT* when it is more important to have a very fast scalable Blockchain even with a certain degree of centralization tolerance. Hence, with a Smart Contract Blockchain storage model it is possible to offer to smart manufacturing systems privacy and credibility of data, establishing a reliable big data distribution system.

4.4.4) Blockchains for Augmented & Virtual Reality in Manufacturing Applications

Table 14: Blockchain Typologies for AR & VR Manufacturing Application (Author's Own Findings)

Integration Technology: Industrial Virtual & Augmented Reality	
Blockchain Typologies	**Potential Manufacturing Application Examples**
- Private, Permissioned, T, Tr, De & Sc (DPoS) Blockchain	- Assistance in Manual Assembly Systems for Increased Productivity (Loch, Quint, & Brishtel, 2016) - VR/AR for Remote Live Support (Schneider, Rambach, & Stricker, 2017) - Training and Skilling of Workers (Boud, Haniff, Baber, & Steiner)
- Public, Permissionless, NT, Lo, De & Sc (PoS) Blockchain	- Industrial Design Processes: Product/System Development and Environment/Plant Layout Designing (Cave, 2016) & Distributed Prototyping (Shin, Park, Jung, & Hong, 2014)
- Hybrid, Ped & Pess, T, Tr, De & Sc (PoS) Blockchain (with Off-Chain Solution)	- Maintenance of Industrial Components, Virtual Disassembly, Analysis and Treatment of Equipment Failure (Qing, 2010) - Improved Industrial Service Delivery (Aleksy, Vartiainen, Domova, & Naedele, 2014)

The use of Augmented and Virtual Reality Technologies is not very widely exploited in manufacturing and even if not much research has yet been carried out in this sector, it is conceivable that the Blockchain can provide significant advantages.

Since many AR and VR applications use wearable devices that, similarly to IoT, have not much computing power and memory, they usually rely on cloud or remote server for storage or computing functions: when this happens, certain information, like location, sensors' parameters, etc. that is used for delivering specific functions or just for traceability purposes, is exchanged by centralized services to a multitude of devices. Hence, Blockchain is very effective when those manufacturing applications need to share in a safe manner data between different nodes: a multitude of devices may communicate through a *Private and Permissioned DPoS Blockchain* which permits a low latency, that is essential for bandwidth restrictions of AR/VR application which need a nearly live communication, and allows also the parallel execution of AR/VR DApps (Decentralized Applications): processing parallelly it is possible to distribute the workload and save up time.

Hence Blockchain technology may become a mainstream for next-generation industrial AR/VR since allows distributed graphical networking that may perform better than a centralized one improving the data availability: with *Public & Permissionless PoS Blockchain with Smart Contract* it is possible to offer an enhanced data sharing and collaboration. These Blockchains let companies to use solutions that allow the storing and sharing of digital assets in a collaborative way (for example for the design of prototypes or 3D models) or by creating a smart space where it is possible to deliver AR/VR experiences and as well as virtual objects amongst different physical locations: even sensitive industrial information can be shared within a perimeter of authorized companies when the Blockchain is switched to *Private*. However, in these circumstances it is advisable to use *Hybrid Blockchains with off-chain solution* where the sensitive part (data relating to the digital asset, AR/VR flows of information, manufacturing technical specifications, etc.) is kept visible only inside the private part and with off-chain storage the data no longer needs to be hosted by all nodes but only by the nodes that are performing the computation, while other related information is validated and publicly shared with everyone in the public part (property rights, timestamps, etc.).

Hence, the Blockchain can be functional for different industrial applications that use AR/VR devices, solving problems similar to those of IoT hardware (i.e. battery powered, limited computational and memory resources) that needs similar Blockchain typologies.

4.4.5) Blockchains for Autonomous Robots & Vehicles in Manufacturing Applications

Table 15: Blockchain Typologies for Robots & Vehicles Manufacturing Application (Author's Own Findings)

Integration Technology: Autonomous Robots & Vehicles	
Blockchain Typologies	**Potential Manufacturing Application Examples**
- Private, Permissioned, T, Tr, De & Sc (PoS) Blockchain (with Off-Chain Solution) - Consortium, Permissioned, T, Tr, De & Sc (PoSp) Blockchain (with Off-Chain Solution)	- Production Traceability of Robots & Cobots Operations (Robla-Gomez, et al., 2017) - Objects Transportation in Industrial Areas (Harik, Guerin, Guinand, Brethe, & Pelvillain, 2015) - Autonomous Charging, Parking & Refuelling of Vehicles (Huang, Xu, Wang, & Liu, 2018)
- Public, Permissionless, T, Tr, Se & Sc (PoSp) Blockchain (with Off-Chain Solution)	- Inspections of Industrial Facilities for Maintenance Purposes (Nikolic, et al., 2013)
- Public, Permissioneless, NT, Lo, De & Sc (PoS) Blockchain	- Warehouse and Autonomous Inventory Management (Hasan, Datta, & Rahman, 2018) - Vehicle-to-Vehicle and Vehicle-to-Infrastructure Communication (Singh & Kim, 2018) (Miller D. , 2018)
- Public, Permissionless, T, Tr, Se & De (PoW) Blockchain (with Scrypt / X11 Hash Function)	- Reputation System for Network of Autonomous AGVs & UAVs (Yang, Zheng, Yang, & Leung, 2017)

The use of autonomous robots, collaborative robots and intelligent vehicles is increasingly widespread in modern SMAs but is still suffering from a lot of security vulnerabilities: indeed, one of the keywords for the fourth industrial revolution is certainly automation, which allows a notable increase in productivity within production systems and logistics but traditional security methods are incapable of providing secure communication between smart robots and vehicles. The Blockchain can be of considerable help for the industrial applications of robots and autonomous vehicles mainly thanks to the use of smart contracts, allowing Blockchain-based systems to collaborate and do business independently and with third parties.

In manufacturing, the simplest example that could be provided for justifying the usage of Blockchain is the inventory management: AGVs systems may automate the inventory of industrial items, with active RFID, thanks to vehicles that become able to receive the inventories and validate related data for making available to interested third parties. Similarly, with *Public & Permissionless PoS Blockchain* it is possible to deploy *Smart Contract* and organize a communication system between agents in a peer-to-peer network where numerous Autonomous Grounded Vehicles and Unmanned Aerial Vehicles become able to interact with each other and coordinate themselves. These Blockchains allow a variety of different agents, in this case represented by smart vehicles of any type, to be connected to a public network in which each agent is able to demand and offer different services (data transfer from agents' sensors, moving to a desired point, freight transport, etc.) that autonomous AGVs and UAVs can usually perform: of course, once the Blockchain-based

system is implemented, it allows either vehicles to interact with each other independently (i.e. Vehicle-to-Vehicle), or to coordinate with enterprise software like ERP systems (i.e. Vehicle-to-Infrastructure), or to respond to specific commands provided by human. However, as already mentioned in the previous paragraphs, even if these Blockchains suits different needs in many other applications, in these specific applications it is fundamental to clarify that they should be used only to deploy smart contracts: indeed, for the storage of data it is advisable to avoid the usage of blocks structure, since it is necessary for vehicles to access to information that are more complex and that usually dynamically change over time (e.g. maps and routes for transportation, cargo-related information like weight, items quantity, volumes, etc.), and it is advisable to rely on DAGs (e.g. IOTA and Byteball DAGs that provide a time and bandwidth efficient consensus approach that is also fair, immutable, and secure).

Other useful Blockchains, that permits the same separation between the data layer and the contracts layer, are scalable second layer Blockchain which are built on top on another Blockchain (that could be common *Public & Permissionless, or when necessary, Private/Consortium Permissioned PoW, PoS and PoSp*) by means of *off-chain solution*: in this way, on off-chain transactions can be stored information that are related to more operational data which is needed to be exchanged in a rapid way to a broad network of devices for allowing their real time interoperability while on the bottom of it there is another Blockchain that assure the execution of smart contract and the achieving of a consensus between node. These Blockchains permit different application in the industrial sector, like the creation of platforms for charging of autonomous devices, the development of distributed archives for tracking robots & cobots manufacturing operations as well as registry for object transportation in industrial areas.

4.4.6) Blockchains for Cloud Storage & Computing in Manufacturing Applications

Table 16: Blockchain Typologies for Cloud Manufacturing Application (Author's Own Findings)

Integration Technology: Cloud Storage & Cloud Computing	
Blockchain Typologies	**Potential Manufacturing Application Examples**
- Hybrid, Ped & Pess, T, Tr, Se & Sc (PoSp) Blockchain	- Data Storage in IoT Manufacturing Cloud (Wu, et al., 2017)
- Hybrid, Ped & Pess, T, Tr, Se & De (PoW) Blockchain	- Distributed Cloud Architecture for Secure and Reliable Storage Services for SMSs (Li , Liu, Chen, Chen, & Wu, 2017)
- Consortium, Permissioned, NT, Lo, Se & S**c (dBFT) Blockchain**	- Edge Computing for Industrial Resource-constrained Devices (Rawat, Parwez, & Alshammari, 2017)

In the contemporary industrial enterprises, software or application extensions already run through remote cloud services that allow the simultaneous collaboration of different manufacturing participants avoiding the local execution of programs. Of course, all these cloud systems suffer from common problems, such as information overload, malicious cyber-attacks, which can block the entire network. Therefore, real peer-to-peer cloud decentralized

Blockchain systems are very useful for industrial applications where it is convenient to avoid depending on intermediaries.

With a distributed ledger system solution, manufacturing data are divided into different blocks that are encrypted and signed before uploading to the Blockchain and distributed all over the network amongst the participants: blocks could be traded and exchanged like coins between industrial nodes which request or offer cloud storage space. A *Hybrid Proof of Work & Proof of Space Blockchain* is necessary for these purposes: it is composed of private Blockchain and public Blockchain. The first one, is designed for verifying hashes related to files that are stored in the blocks inside the public Blockchain (it must be reliable hence uses PoW), while the public Blockchain assists for the integrity of data since they are distributed across the network's nodes (it must rely on lower computational effort, hence PoS is used).

Other possibility regards the use of *Consortium & Permissioned dBFT Blockchain with Smart Contract* for deploying cloud computing system that are able to offer edge computing application for industrial resource-constrained devices in order to improve response times and save bandwidth: since, for instance, industrial IoT is expected to generate massive amount of data, Blockchain-enabled edge computing may elaborate data when singular devices have limited computing and storage capabilities; the consortium parameter regulates the access only to permitted industrial IoT and the dBFT consensus allows high throughput and scalability for a network of devices which may communicate with smart contract. In addition, such Blockchain assure high resiliency to tackle fault tolerance and attacks of IoT devices inside cyber-physical manufacturing systems.

4.4.7) Blockchains for Additive Manufacturing in Manufacturing Applications

Table 17: Blockchain Typologies for Additive Manufacturing Application (Author's Own Findings)

Integration Technology: Additive Manufacturing (3D Printing)	
Blockchain Typologies	**Potential Manufacturing Application Examples**
- Public, Permissionless, NT, Lo, De & Sc (PoS) Blockchain	- Interconnected 3D Printers (Trouton, Vitale, & Killmeyer, 2017)
- Public, Permissionless, NT, Lo, Se & Sc (Po**ET)** **- Public, Permissionless, NT, Lo, De & Sc (PoS, fBFT) Blockchain**	- 3D Design Model Traceability; Intellectual Property Protection (Holland, Stjepandic, & Nigischer, Intellectual Property Protection of 3D Print Supply Chain with Blockchain Technology, 2018) - Transparency to Third Parties for Auditing Purposes (Holland, Nigischer, Stjepandić, & Chen, 2017)
- Private, Permissioned, NT, Lo, Se & De (pBFT) Blockchain	- Supply Chain Decentralization (Winkler-Goldstein, Imbault, Uslander, & Gastine, 2018)
- Consortium, Permissioned, NT, Lo, Se & Sc (dBFT)	- License Management through Smart Contract (Herbert & Litchfield, 2015)

3D printing is one of the most important technological innovations in the Industry 4.0 context since the additive manufacturing is able to increase the level of flexibility of the production systems and customization of the products without requiring large investments that would be otherwise necessary without this technology. The combined use of the Blockchain is very promising in the production scenario and can be considered key mainly for the innovation brought by smart contracts.

In fact, with *Private & Permissioned pBFT Blockchain with Smart Contract* it is possible to create a real decentralized supply chain where the workload is divided and balanced within a specific network of producers, drastically reducing the production lead times, the stocks necessary for the proper functioning of the production systems, the variability of the loads of production, achieving a noticeably improved level of resource optimization and allowing to work in lean logic: all this is made possible mainly by the smart contracts that are employed within the Blockchain network from the producers until the customers and automate the negotiation and the communication processes, sending automatic transactions and orders amongst a decentralized factories network realising a proposal model for a just-in-time manufacturing system.

Furthermore, with *Public & Permissionless PoS/fBFT/PoET Blockchain with Smart Contract* it is possible to recreate a distributed ledger containing all the hashes related to 3D model files that are made by industrial companies or by independent designers: in this way it is possible to guarantee the uniqueness of the models avoiding their versioning or generating errors or duplicates thanks to a database synchronized with the whole network. Moreover, the transparency regarding the produced items is increased, helping manufacturer to demonstrate the origin of the product and also opening to the possibility to third parties to check the production for auditing purposed. Naturally, then, this lays the groundwork to guarantee the protection of the intellectual property of the models: thanks to the timestamp of the models and to the information contained in the blocks about the author of the model, it is possible to guarantee the authenticity of what is produced also recognizing the rights to the author.

Moreover, thanks to *Consortium & Permissioned dBFT Blockchain with Smart Contract*, it would be possible to automatically negotiate the production of objects starting from the models shared by designers within the Blockchain. On the other side, for companies it becomes much easier to manage the licenses acquired regarding the production of certain models: once the production is over, the interruption of payments would become automatic, respecting precisely that only the units actually produced were paid, reducing the risk of error and the associated costs.

4.4.8) Blockchains for Cybersecurity in Manufacturing Applications

Table 18: Blockchain Typologies for Cybersecurity Manufacturing Application (Author's Own Findings)

Integration Technology: Cybersecurity	
Blockchain Typologies	**Potential Manufacturing Application Examples**
- Public, Permissionless, T, Tr, Se & De (PoW) Blockchain	- Intra & Interconnection Industrial Cybersecurity (Rawat, Njilla, Kwiat, & Kamhoua, 2018)
- Private, Permissioned, NT, Lo, Se & De (pBFT) Blockchain - Consortium, Permissioned, NT, Lo, Se & De (pBFT) Blockchain	- Data Security and Systems Availability

The systemic evolution foreseen by the fourth industrial revolution requires necessarily and additional attention to the protection of all the systems involved in smart factories. It is in fact necessary to protect the most critical and vulnerable part of manufacturing systems to avoid cyberattacks that can cause ITC damages, such as the loss of information or the theft of sensitive and/or secret industrial data or the interruption or alteration of communication between systems, or the tampering of plants and machineries that can slow down or block entire production lines.

Hence, some kind of Blockchain can be really useful for protecting connections, communication and data since they are by definition able to offer high security mechanism thanks to cryptographic and hash functions: for instance, *Public & Permissionless PoW Blockchain* can create an open and trusted public network with high reliability and security since the consensus algorithm, that is by default very safe, could be modified ad-hoc for increasing the complexity and thus the security of the network, for example, by increasing the block time or the complexity of the puzzle to be solved for mining a block. Also, *Private/Consortium & Permissioned pBFT Blockchain with Smart Contract* guarantees high systems and data availability, since the restricted access to the network and even if one node is under attack, these Blockchains avoid the single point of failure typical of centralized systems.

4.4.9) Blockchains for Simulation in Manufacturing Applications

Table 19: Blockchain Typologies for Simulation Manufacturing Application (Author's Own Findings)

Integration Technology: Simulation	
Blockchain Typologies	**Potential Manufacturing Application Examples**
- Public, Permissionless, NT, Lo, De & Sc (PoS)	- Data Collection and Verification from Multiple Resources
- Consortium, Permissioned, NT, Lo, De & Sc (PoS) Blockchain (with Sidechain)	- Distribution of Computational Power - Enabling Simulation-as-a-Service (Krammer, et al., 2018)

By using simulation techniques, it is possible to model the behaviour of all the elements that impacts smart manufacturing system such as machinery, operators, flows of material and products, etc. recreating an exact copy of the physical world in a virtual one: simulation

software can test thousands of production parameters and variable, forecasting the outcomes for individuating issues or discovering potential improvements.

Even if there is not much literature, Blockchain can assists manufacturing simulation software: with *Public & Permissionless PoS Blockchain with Smart Contract* it is possible to gather information from an extensive number of sources whose interoperability can be provided by the instauration of a distributed data warehouse whose availability is guarantee by a multitude of nodes that store data in the blocks: furthermore, distributed ledger may reduce the uncertainty concerning data thanks to the verification of data authenticity with an enhanced image of future states of production plants at a specific moment.

Furthermore, a Blockchain like *Consortium & Permissionless Proof of Stake Blockchain with Sidechain and Smart Contract* can distribute computational effort thanks to the use of multiple side-chains related to the main one that are combined with smart contracts in order to improve the simulation capabilities providing innovative Simulation-as-a-Service models.

4.6) Final Results for Potentials of Blockchain Technologies in Manufacturing

The framework defined for the evaluation of potential applications in the manufacturing field of Blockchain technology has allowed to generate an exhaustive and schematic mapping of the different typologies of Blockchain suitable for these manufacturing purposes.

These results are summarized in the *table 20*, where it is possible to represent in a three-dimensional representation the five Blockchain variables grouped on three axes:

- on the *x-axis* the "Access Regulation" and the "Permission Control" are grouped together allowing 4 different exploitable combinations, thus excluding even technically possible combinations which have not have logical sense or practical uses. In detail:
    - ✓ Public (Access Regulation) & Permissionless (Permission Control)
    - ✓ Private (Access Regulation) & Permissioned (Permission Control)
    - ✓ Consortium (Access Regulation) & Permissioned (Permission Control)
    - ✓ Hybrid (Access Regulation) &, by definition, partly Permissioned partly Permissionless (Permission Control)
    - NO: Public (Access Regulation) & Permissioned (Permission Control)
    - NO: Private (Access Regulation) & Permissionless (Permission Control)
    - NO: Consortium (Access Regulation) & Permissionless (Permission Control)
    - NO: Hybrid (Access Regulation) & not partly Permissioned partly Permissionless (Permission Control).

- on the *y-axis* the “Operational Modality” and “Incentive Typology” are grouped together allowing 2 different combinations, thus excluding even technically possible combinations which have not have logical sense or practical uses. In details:
    - ✓ Transaction-Oriented (Operational Modality) & Tokenized (Incentive Typology)
    - ✓ Logic-Oriented (Operational Modality) & Non-Tokenized (Incentive Typology)
    - NO: Transaction-Oriented (Operational Modality) & Non-Tokenized (Incentive Typology)
    - NO: Logic-Oriented (Operational Modality) & Tokenized (Incentive Typology)
- on the *z-axis the “Consensus Algorithm”* which allows 3 different typologies in accordance with the scalability trilemma:
    - ✓ Security & Decentralization properties
    - ✓ Scalability & Decentralization properties
    - ✓ Scalability & Security properties

These variables permit to generate 24 possible combinations that represent the Blockchain typologies that sustain effectively the different manufacturing application.

Furthermore, additional considerations have been made analysing the results in order to obtain valid insights from the resulting thesis. Consistently with what is established in the literature review of *chapter 3*, after having divided the 44 potential applications of the Blockchain based on the main technology with which Blockchain will mainly interface, it is possible to deduce a "Level of Integrability" of the Blockchain with the 9 main technologies of the fourth industrial revolution as shown in the *figure 63*. This level was established empirically by observing the number of types of Blockchain for every technology with which the Blockchain must be integrated. It is therefore possible to establish a small scale from “High” to “Low”, where level “High” indicates that the Blockchain has a good integrability with this technology since there are many different types of Blockchain to meet the needs of the technology with which it integrates; “Low” indicates instead that the Blockchain turns out to have much less integrability since few Blockchains are suitable to work with these technologies for different technological constraints; “Medium” defines an intermediate level between the two extremes. The obtained result shows how the Blockchain could be applied in the Manufacturing field, illustrating what are the different typologies of Blockchain that are needed for different technological scenario in order to respond to a specific need in manufacturing. Moreover, it is possible to identify a "Potentiality of Application" of the Blockchain with the various manufacturing technologies (*figure 64*): in this way, it is possible to identify, on the basis of the number of related potential Blockchain application, which technologies have higher Blockchain adoption hurdles and may be a technological constraint.

Table 20: Results for Potential Blockchain Application in Manufacturing (Author's Own Findings)

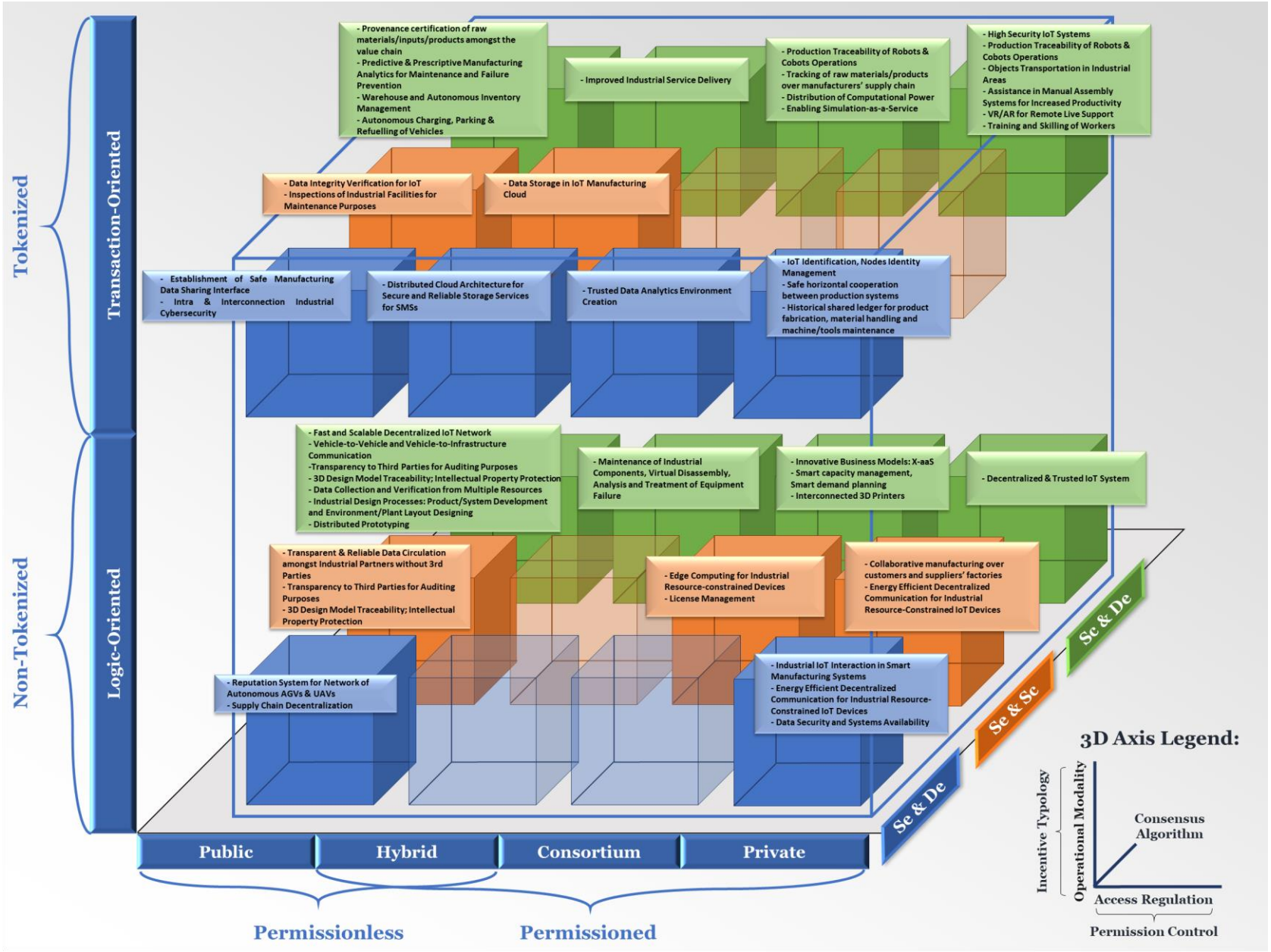


Figure 63: Level of Integrability of Blockchain with Main Technologies of Industry 4.0 (Author's Own Findings)

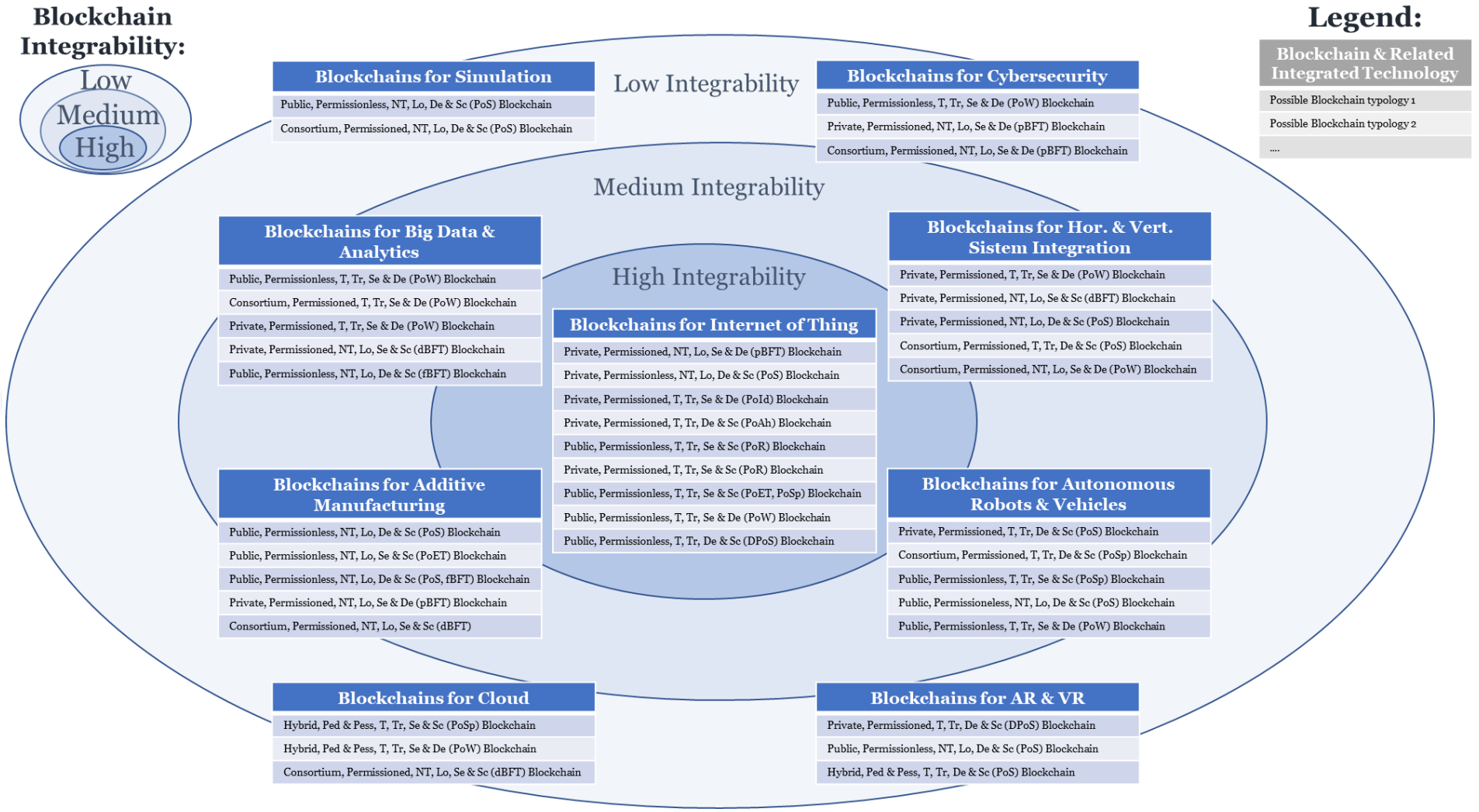
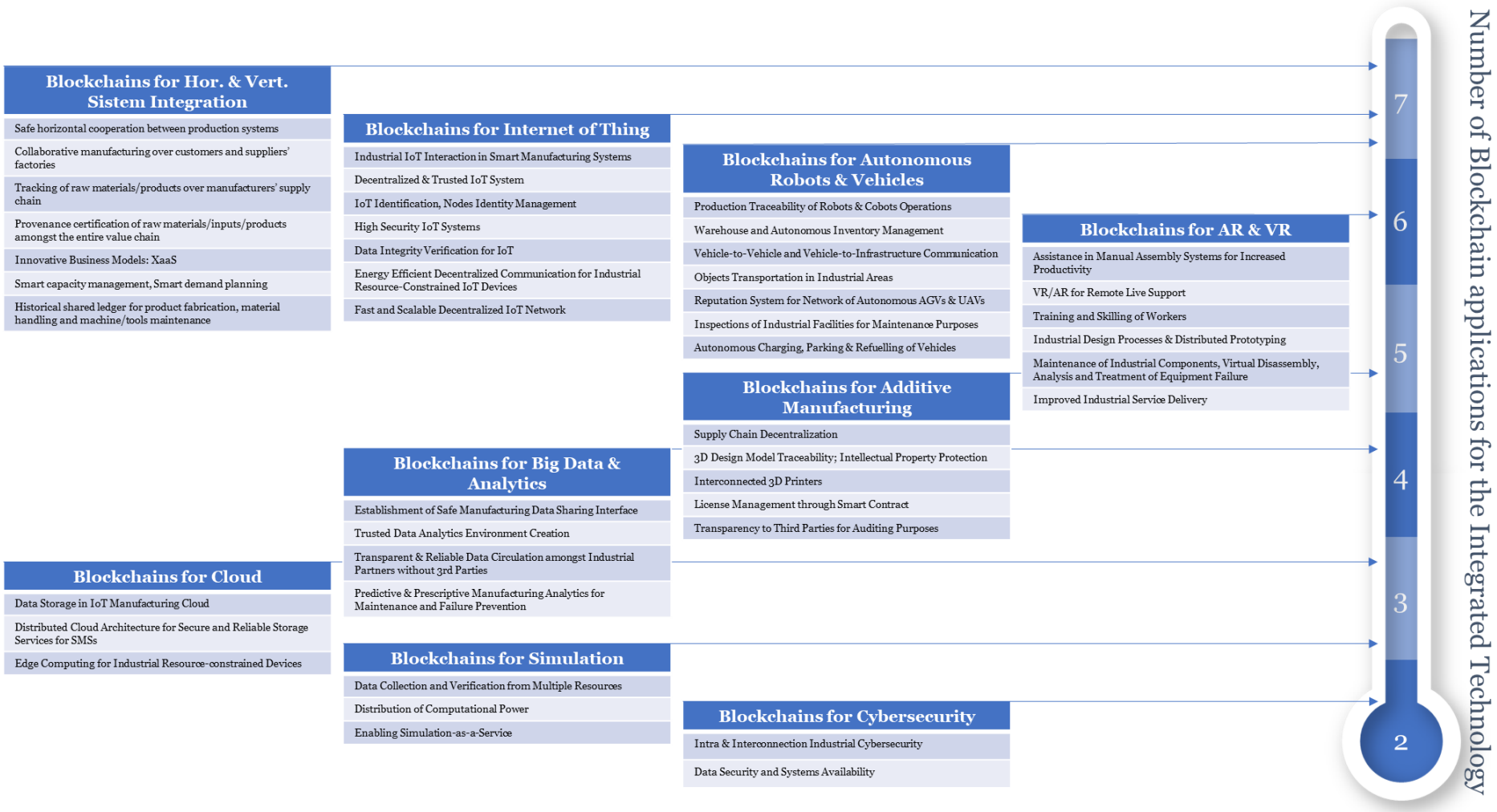


Figure 64: Potentiality of Application of Blockchain in Manufacturing with Each Technology in Industry 4.0 (Author's Own Findings)



4.5) Further Conclusive Considerations

Further conclusive considerations can be made by jointly considering the results of the thesis with the literature review of the previous chapters.

In particular, it is possible to summarize qualitatively what are the benefits of Industry 4.0 that the Blockchain helps to obtain and what are the challenges of the fourth industrial revolution that the Blockchain helps to overcome.

Finally, some future considerations regarding the actual implementation difficulties for real manufacturing Blockchain applications are illustrated in the last paragraph.

4.5.1) Blockchain Achieved Benefits for Manufacturing Application

Starting from the above analysed functions procured by the Blockchain technology for Manufacturing (*paragraph 4.1*), it is worth focusing on some of the Industry 4.0 Benefits (*paragraph 3.4*) that distributed ledger technology will help to convey to the industry, understanding how it is assisting manufacturing to turn out to be smarter and more efficient, achieving properties analogous to ones accomplished by the digital transformation in the last decades.

With Industry 4.0 the way manufacturers work will be changed deeply and irreversibly: the manufacturing industry, together with all the other related businesses (e.g. logistics, marketing, etc.) will become more efficient, faster and more customer oriented, opening to the possibility of new business models exploiting the optimization and automation provided by the usage of the most recent digital technologies (*paragraph 3.5*). Hence, it is possible to interpret the functions promised by the Blockchain with the benefits that may be achieved by smart manufacturing systems during the fourth industrial revolution.

A list of the identified Blockchain achieved benefits for manufacturing is the following:

- **Increased Productivity:**
  This is a key benefit for manufacturers and the first that they can realize with Blockchain. In fact, the optimization of processes and thus of productivity, is fundamental for many Industry 4.0 projects in which the main achievements are saving costs while increasing profits through a reduction in wastes, the automation of procedures and activities for avoiding mistakes or interruptions.
  Speed is decisive and speeding up the production, with the digitalization of paper works, working in real time along the supply chain, adopting preventive maintenance and intervening quicker in case of issues and so on… is very important. Blockchain

solutions range from improved asset utilization and smoother production processes to healthier logistics and inventory management.

- **Real Time Processes and Activities:**
  Speed is very important but not only for increasing productivity, it is a benefit in many other ways as well: in fact, speed fits in the viewpoint of enhanced customer-centricity. In Industry 4.0, the entire life cycle of products is considered strictly to the manufacturing process. The whole value chain and network within manufacturing operations reside, must be considered because inside it everybody are all customers that desire enhanced productivity.

  If the final client requests products fast and has high expectations regarding customer experience, quality, service and products that are delivered on time, this impacts the entire supply chain. Rapidity is not just a competitive advantage in a more and more real-time economy, it is a matter of alignment, costs and value creation: customers basically expect it. Hence, the role of data become crucial and Smart Factories must receive and deliver information in an instantaneous way and the role of the Blockchain technology is crucial in this context.

- **Enhanced Operational Efficiency:**
  The costs in time, money and resources employed for fixing assets and equipment during a system down caused by a broken part, could be very high because the entire production is affected, and it may cost a lot even after the reparation for the subsequent risk of dissatisfying customers. Hence, reputation can be affected seriously, and this can impact actual and future orders. Therefore, there are great benefits when the status of assets can be monitored through the IoT network because they become maintained in a proactive way, not reactive, and problem can be faced live or even predicted also for assets that are not close to the controller. Both maintenance and asset management are critical for manufacturers and in Industry 4.0 will become possible to discover insights and patterns for optimizing maintenances services and opening to new scenarios: the Blockchain technology find several applications in all these cases.
- **Quality Improvements:**
  When in the production system almost everything starts becoming connected and controlled (i.e. spread of sensors, diffusion of IoT…) in an automatic way, quality starts enhancing and the Blockchain is very useful thanks to the deployment of Smart Contracts: in fact, with automation is possible to monitor in real time lots of quality aspects and in combination with robots and cobots, not only quality is improved but also errors are reduced. In addition to this, it worth mentioning that the higher usage

of cobots is followed by a higher number of hired people: collaborative robots need cooperation between man and machine so Blockchain could help also in creating more jobs.

- **Better Working Conditions**

  The improvement of working condition regards primarily the possibility of controlling in real time many parameters of plants and warehoused where, together with the analysis of temperature and humidity, there is the quick detection of gasses, radiation, pollutants etc. with a heightened protection of workers: the distributed ledger technology acts as a secure register for all this information and help to guarantee that all these parameter are controlled and never altered. Moreover, it is possible to focus on ergonomics thanks to the focus on the design and development of tools and machinery that suits human needs and Blockchain has different application also in this design phases.

- **Mass Personalization and Higher Customer Satisfaction**

  In the recent era, the customer is evolved, he is more demanding and even needs very quick responses to changing in tastes and in the rising of new needs: customer prefers to have a high degree of customization and is dissatisfied with few alternatives. This is disrupting supply chains because customer with digital tools becomes able to interact directly to the supplier demanding for its desired version. Blockchain technology permits to connect with other digital technologies allowing automation, processes optimization that are required for reaching a high degree of mass customization which is a key benefit and a competitive advantage for manufacturers to survive in a global context.

- **Improved Flexibility**

  The Blockchain has different functionalities that allow the modularity and integrability of different technologies permitting to have in smart manufacturing a level of scalability and agility very similar to the one that come from information technologies (e.g. Cloud Computing allows an easy scaling up/down of services). In the Smart Factories, this is associated to the usage of innovative technologies, like Big Data, Artificial Intelligence, that applied in CPS permits to forecast and level the seasonality, regulating the production by up/downscaling the systems and all these technologies are integrated together by means of distributed ledgers.

- **New Business Models**

  With the fourth industrial revolution, the digitalization process assumes a key role and become a fundamental element for shaping an enterprise strategy in which processes and functions are completely transformed: Blockchain satisfy the requirement for new knowledges and new set of skills for following the strategy and

for enabling new revenue streams by using innovative capabilities such as, for example, the deployment of X-as-a-Service business model, innovative maintenance services, etc.

4.5.2) Blockchain Solved Challenges for Manufacturing Application

Similarly to the previous analysis of benefits, it is useful focusing on several Industry 4.0 Challenges (paragraph 3.7) that distributed ledger technology will help to deal with. This proposed list does not claim to be a thorough list since a full list of all the possible challenges which the Blockchain is addressing in the manufacturing development is not realizable: many different situations may generate different conditions very specific for each case study. However, it is feasible to recognize the most common and relevant challenges currently faced by typical industrial scenarios. The proposed list of the Blockchain addressed challenges for manufacturing is the following:

- **Application decentralization:**
  Blockchain attempts to realize decentralized application which are necessary especially for Industry 4.0 systems with huge users and lots of computational resources employed: they usually depend on expensive centralized servers that are also costly to deploy and maintain [in addition, many industrial firms rely on and pay third-parties for outsourcing centralized solutions (Koomey, Turner, Stanley, & Taylor, 2007)], therefore Blockchain becomes very important and desirable for achieving a successful decentralization of applications.
- **Authenticity of data, Protection and Anonymization**:
  It is necessary in most businesses trust in the genuineness of gathered data and in the authenticity of transaction completed between partners, manufacturers, suppliers, service providers, customers and even governments. Therefore, Blockchain permits to offers mechanism for enabling transparency, for verifying accountability and, in general, for adding trust. In addition to this, due to the fact that these requirements could be able to offset trusted third parties (Locher, Obermeier, & Pignolet, 2018), some supplementary security mechanisms would be implemented, not only at software level but also at the hardware one (Jin, 2015). Hence, data is key for many businesses and with distributed ledger technology could be protected and anonymized especially when it is exchanged with third parties. Similarly, IoT devices, which collect lots of data, with Blockchain could be protected and kept private to non-authorized companies, avoiding the abusive read or usage by external entities.
- **Open Source Approach**

Blockchain can address the problem of lack of trusts that arose by the non-transparency approach regarding how the inner source codes work in many manufacturing software, since lots of industrial companies prefer to work on closed source code. It is for this reason that is fundamental to switch to an open source approach based on Blockchain in order to provide not only trust but also security.

- **Operational efficiency and improved competitiveness to ensure long-term sustainability**

  Blockchain can reduce different costs ensuring a long-term sustainability: verification costs that are related to the ability of verify in a cheap way the attributes of a transaction and transition costs which are related to the capability of operate in without the need of any intermediary.

- **System Updates**

  Due to security issues or to upload and install new software or firmware, it is very frequent the activity of updating the manufacturing systems and devices (e.g. IoTs). Nevertheless, this updating process is not an easy task because in some circumstances it requires to perform manual activities in numerous devices that are disseminated all over the factories. Hence, Blockchain technology is a way for distributing software/firmware updates automatically and simultaneously to many smart devices, without complex, long and inefficient manual activities: this activity could be compliant to security policies and integrity requirements for avoiding malicious or faulty updates.

4.5.3) Main Blockchain Future Implementation Challenges for Manufacturing

Together with the consideration about the benefits provided by the application of Blockchain to the Industry 4.0 and the addressed challenges that are solved by the distributed ledger technology, there are some constraints that need to be considered during the development, deployment and delivery of Blockchain solutions to the manufacturing because these limitations create real challenges that require further attention.

1) **Scalability:** whatever architecture is chosen for sustaining the Blockchain in the industrial context, it would have to face up to the massive amount of transactions' traffic that these applications usually produce. This problem is not a novelty as demonstrated by (Preden, et al., 2015) regarding fog computing architectures: indeed, it is common also in the actual traditional cloud-based centralized services in which the architecture is slowly moving towards a situation where the services are furnished physically close to the systems in which are needed. Therefore, also Blockchain systems must take into consideration their necessary evolutions over the time

allowing scalability since they will grow and become more complex and more populated by different nodes.

2) **Cryptosystem for resource-constraint devices:** another important issue regards the devices which are involved in the manufacturing firms. (Li, et al., 2017) elucidated that the majority of these devices, such as tools, actuators, sensors, machinery, etc. have not high computational resources in terms of processing power and memory, hence they have difficulties with the recent secure public-key cryptography algorithms: as already stated in the *paragraph 2.1.2.7*, even if many Blockchains use the Elliptic Curve Cryptography (i.e. the Digital Signature Algorithm) which is, in comparison to the same security level, commonly lighter than the more common RSA Public-Key Cryptosystem, the cryptography still require relatively high power (Suárez-Albela, Fraga-Lamas, Castedo, & Fernández-Caramés, 2018). In addition to this, every company, which has the priority of keeping data secure, must take into consideration the future threat of quantum computing era by looking for efficient but enough safe algorithms (e.g. in the *paragraph 2.2.6.2.1.1* is explained the problem in case of 51% attack with high power computers).
3) **Consensus algorithm selection**: it is essential to choose the correct consensus algorithm for having a Blockchain that works properly. Indeed, every Blockchain application requires different characteristics that could not be satisfied with every consensus algorithm. Considering that, theoretically, there is not an algorithm that can really solve the trilemma (i.e. scalability, decentralization, security) but there are many algorithms that have different performances with different characteristics, the best approach may be to distinguish amongst the four classes individuated in the *paragraph 2.2.6.2.1* taking into consideration that: the algorithm with "*high degree of centralization*", fits to distributed ledgers which are used for private and permissioned Blockchains whilst algorithm with "*low degree of centralization*" suits to public Blockchains; then, the "*degree of externality*" regulate the external resources required for maintaining up the Blockchain, generating more or less incentive for contributing to the generation of blocks, and for creating or not a tokenized system. After these preliminary consideration on the consensus algorithm, which must take into consideration and agree to the four key characteristics of the Blockchain architecture (i.e. access to the Blockchain, participation to the consensus, tokenized/non-tokenized incentives and logic/transaction oriented operation mode) that generate different types of Blockchain, it is fundamental to evaluated the common performance of the Blockchain that generally are the throughput and latency (i.e. validation speed), security level, costs, power requirements, incentive system, scalability, etc. for assessing which consensus algorithm is the best for a certain

application identifying also all the advantages or limits that it produces. E.g. a massive CPU-usage algorithm, like the PoW, although it is very helpful in public Blockchain, it is useless in other scenarios where the computational effort (and energy & time consumed) can be reduced because not required by the system environment: in a more secure private Blockchain, faster and less expensive algorithms are much more attractive.

4) **Privacy and security**: there are still issue concerning the privacy and integrity of data and also regarding the identity certification for the devices inside Blockchain. In a manufacturing context, must be considered all the challenges which derives from the implementation of Blockchain system beside the IoT devices as already explained in the *paragraph 4.5.1*.
5) **Energy efficiency, throughput and latency**: these problems, which mainly affect the Industrial IoT and the Cyber Physical Systems, can be attributed to other Blockchain implementations. In particular, regarding the energy consumption, the combined usage of mining and cryptographic algorithms, together with not very efficient peer-to-peer protocols, results in a computationally complex activity that have a critical impact on the energy consumption, not only for small battery-operated devices but also for common devices in many scenarios. Moreover, the way the consensus algorithm works and, more in deep, the mechanism of block creation and propagation, influence both the throughput and latency of the Blockchain: traditional database systems are generally faster and able to provide real time responses while Blockchain difficulty can furnish such functionalities (see *paragraph 2.2.4* for technical solution attempts).
6) **Required infrastructure**: it is fundamental to arrange a specific hardware infrastructure for using certain Blockchain application software, such as additional storage and mining computational hardware. Then, the expected high amount of data traffic generated by the nodes' interactions require communications infrastructure and interfaces able to sustain the predictable load.
7) **Management of multi-chains**: the large diffusion of Blockchains may require manufacturers to hold up at the same time many of them (e.g. a firm manage simultaneously its financial transactions using Bitcoin instead its smart contracts are executed on applications based on Ethereum). Consequently, delivered solutions should be designed and implemented considering using different Blockchains at the same time.
8) **Interoperability and standardization**: actually it is very common to notice that every company develop its own Blockchain solution even if it is necessary to have a certain degree of interoperability between different employed Blockchains in order to

accomplish a high level of integration and a seamless solution. It is necessary to deploy specific standards which regulate and aim at guarantee interoperability of Blockchain technologies in different fields: for example, IEEE Standards Association is currently working on different project with the objective of creating a globally recognized standard setting for Blockchain technology into various industry sectors.

9) **Regulatory and legal aspects**: technological challenges are not the only aspect to take into consideration, because also regulation and laws play an important role for the development of Blockchain, in particular in international contexts. In fact, governments and regulatory agencies may create restrictions and limits the Blockchain usage outside a certain territory or limit the exchange of data amongst different country, creating huge limitations regarding the applicability of Blockchain in international context.

5) Conclusions

This thesis was articulated into two main phases: the first two chapters (*chapter 2* and *chapter 3*) consisted in the review of the review of the scientific literature needed to study deeply the Blockchain technology and the Industry 4.0 respectively. Subsequently, the second phases consisted in the development of a framework for the identification of the potential Blockchain application in the Manufacturing field.

The *main research question* of this work was:

Considering different manufacturing scenarios, application benefits and technology constraints, how the Blockchain technology could be applied in the Manufacturing field?

From the review of the scientific literature it was possible to deduct that the Blockchain technology could have valuable applications in the Manufacturing sector.

Initially, the study conducted on the functioning of Blockchain technology led to an understanding of the functioning of the Blockchain. In this phase, the key elements of this technology were analysed, including the structure of the blocks, the mining mechanism, hash functions, the encryption system and the digital signature.

The most advanced features of its underlying working mechanism were then explored, obtaining a very technical mapping of all the variables that regulate and govern the functioning of the Blockchain: here, more than 23 consensus algorithms have been identified and classified with which the fundamental trilemma was clarified, the block propagation mechanism in the network has been studied, the effect that the block sizes have on latency and throughput and the different types of attacks to the Blockchain with their impacts have been examined.

Later, several more advanced types of Blockchain have also been studied: some of them make possible to have available the use of Smart Contracts, other can be based not on blocks but on different structures such as the Directed Acyclic Graph (of which 6 different structures were investigated) and two additional mechanisms of Sidechain and Off-Chain that modify the functioning of the Blockchain itself were considered.

The research then placed attention on the current uses of the Blockchain in sectors other than manufacturing: 8 industries that can currently benefit from the technology were investigated; subsequently the contemporary state of the art for the use of the Blockchain in the

manufacturing industry was investigated where some potential applications have been mapped through the Porter Value Chain model.

Therefore, the literature review has also investigated Industry 4.0 phaenomenon in order to identify any gaps between the current use of the Blockchain in manufacturing and the potential applications of this technology. Consequently, this trend has been studied in detail and starting from the research for a possible definition have been examined the 4 Design Principles, the 9 nine key enabling technologies of this revolution, the objectives of Industry 4.0 together with the benefits it can bring, the challenges it faces and the 6 main requirements that the modern applications must have to follow the Industry 4.0 trend.

All this led to the second phase of this thesis. The collection of 44 potential cases of application in manufacturing required the definition of a reference framework for the analysis of the effective implementation of a Blockchain-based solution for these applications. To do this, the 5 main functionalities and the 22 sub-functionalities allowed by the Blockchain were conceived and it was clarified how they could satisfy the requirements of the Industry 4.0 applications. Subsequently, for each of the 44 potential applications the set of necessary requirements was identified. Consequently, by defining 5 key variables which, based on their combination, allow different functions to be deployed, it was possible to assign the necessary Blockchain typology for each potential application.

The results were then analysed on the basis of the 9 main Industry 4.0 technologies with which the Blockchain must deal before it can actually be implemented and the "Level of Integrability" and the "Application Potential" of this innovative technology have been defined.

Hence, this master thesis can demonstrate three different key insights generated from the extensive research activity that are considered the foremost answers to the *main research question* of this work. These three key insights could be considered as three sub-research questions that helped to answer the "*if*", the "*how"* and the "*in which scenarios"* the Blockchain technology could be applied in Manufacturing and thus replying entirely to the main research question.

1) **"*If the Blockchain has reason to be applied in Manufacturing*"**

First of all, the in-depth analysis of obtained results of the thesis researching activity, makes it possible to demonstrate firmly that the Blockchain can be a technology with a key role in manufacturing: the identified 44 potential applications identified should be considered as endorsers for the Blockchain, since they are able to create considerable value for the manufacturing industries.

In fact, by using the strategic Porter Value Chain Model, it is possible to affirm that the potential applications affect both the primary and support activities of a manufacturing companies which decide to adopt Blockchain solution, so creating a real strategic value for manufacturing firm: *Inbound & Outbound Logistics*, *Procurement*, *Product Development*, *Process & Technology Development*, *Operations*, *Sales & Marketing*, *Human Resource Management and Firm Infrastructure*. With this extensive coverage of activities, a manufacturer may exploit the creation of competitive differentials by the adoption of the Blockchain innovative technology, allowing firms to achieve an advantage over competitors that turns into higher margins and so higher profits. This encouraging preliminary result permit to affirm that there are promising reasons to use the Blockchain technology in Manufacturing, thus allowing to go further in the researching activity.

2) "*How the Blockchain could be successfully applied*"

Secondly, since the application of Blockchain in Manufacturing is revealed encouraging, the researching activity moves toward the demonstration of the effective applicability of this technology in the Industry 4.0 scenario.

The Blockchain ledgers, in fact, with their functionalities are able to satisfy the different requirements coming from the fourth industrial revolution: their applicability does not depend only on the technical feasibility of the integration of Blockchain technology with the potential applications but it is pushed by the requirement that those application are demanding. If businesses do not ask for Blockchain functionalities, then no reason to put effort in its development.

However, by analysing requirements of the identified potential application, it is evident that *Interoperability*, *Service Orientation* and *Decentralization* are the most demanding requirements of identified potential applications (*table 22*).

Table 22: Requirements distribution in potential Blockchain manufacturing applications

Requirement	Number of occurrences in potential applications
Interoperability	*32*
Service Orientation	*30*
Decentralization	*29*
Real-time Capability	*18*
Modularity	*14*
Virtualization	*13*

These three top demanded requirements are largely satisfied by the *Security*, *Smart Contract* and *Integration* functionalities of Blockchain: this result is very significant since it permits to translate the most demanded industry requirement into the most desired Blockchain characteristics and, thus, Blockchain typology.

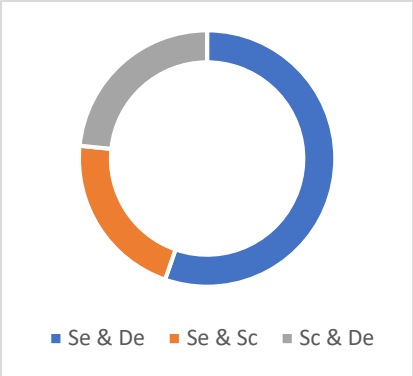
Indeed, it is valuable to extract information from the most needed Blockchain because it permits to answer to research question with a set of most useful Blockchain typologies that can satisfy Manufacturing requirements (*table 23*).

Table 23: Most useful Blockchain architecture for Manufacturing applications

Blockchain architecture: Access Regulation, Operational Modality, Consensus Algorithm	Number of potential manufacturing applications
Public, Logic Oriented, Sc & De	*7*
Private, Transaction Oriented, Sc & De	*6*
Public, Transaction Oriented, Sc & De	*4*
Consortium, Transaction Oriented, Sc & De	*4*
Private, Logic Oriented, Se & De	*3*
Public, Logic Oriented, Se & Sc	*3*
Consortium, Logic Oriented, Sc & De	*3*
Private, Transaction Oriented, Se & De	*3*
Private, Logic Oriented, Se & Sc	*2*
Public, Logic Oriented, Se & De	*2*
Consortium, Logic Oriented, Se & Sc	*2*
Public, Transaction Oriented, Se & De	*2*
Public, Transaction Oriented, Se & Sc	*2*
Hybrid, Transaction Oriented, Sc & De	*1*
Hybrid, Transaction Oriented, Sc & Se	*1*
Hybrid, Transaction Oriented, Se & De	*1*
Consortium, Transaction Oriented, Se & De	*1*
Private, Logic Oriented, Sc & De	*1*
Hybrid, Logic Oriented, Sc & De	*1*

The obtained results permit to affirm that the most useful type of Blockchain for the Manufacturing application is the Public & Permissionless Blockchain with Non-Tokenized Logic Oriented Operational Modality and Consensus Algorithm with Scalability and Decentralization characteristics. This Blockchain type is followed by another one that is useful in Manufacturing: Private and Permissioned Blockchain with Tokenized and Transaction Oriented Operational Modality and Consensus Algorithm with Scalability and Decentralization characteristics. Both these two Blockchain use Consensus Algorithm which is the most used in Manufacturing application: Scalability and Decentralization are the best couple of characteristics (*table 24*) that satisfy the Manufacturing application requirements and are widely represented by Algorithm like PoS, DPoS and fBFT.

Table 24: Consensus Algorithm usage in potential Manufacturing application



3) "*In which scenario the Blockchain has the most relevant impact*"

Concerning different Manufacturing applications, it is important to learn where the Blockchain technology makes the most of its potential. Analysing the resulting thesis outcomes, it is clear that the Blockchain is very needed where there is need for Horizontal and Vertical System Integration and for Industrial IoT.

In fact, Horizontal and Vertical System Integration, and similarly Industrial IoT, need a technology that is able to satisfy the requirements of Decentralization and Interoperability contemporary delivered by a very scalable & reliable system and the Blockchain effectively satisfy these requirements promising even a high security level not available with conventional technologies. This is demonstrated by the high number of Blockchain applications for System Integration and IoTs (14 potential applications, 7 for each one) and the wide Blockchain typologies that could be efficiently exploited by those application (9 for IoT and 5 for System Integration).

These three main results permit to answer positively to the main research question of this thesis, showing that exists numerous potential application in manufacturing and that the Blockchain technology is a great technology useful for being applied in different manufacturing scenarios with different technologies, generating consistent benefits for the manufacturer.

Finally, some concluding remarks have closed some outstanding questions opened during the literature review activity, answering how the Blockchain can help to achieve the benefits promised by Industry 4.0, how it is able to solve the challenges of the Industry 4.0 and what future problems need to be addressed for an effective implementation of the Blockchain in Manufacturing.

Annex: Literature Review Research Methodology

A systematic literature review was conducted with the aim of obtaining a valid and consistent current state-of-the-art concerning the subject of the present thesis.

The methodology began with the definition of a specific set of keywords needed to search for a set of documents large enough to contain a significant amount of information but enough narrow to avoid the spread of an excessive amounts of redundant or unmanageable data.

Therefore, to obtain an exhaustive and complete literature as the foundations of this work, two exploration areas have been researched: the Blockchain technology and the Industry 4.0 trend. In particular, the aim was to firstly identify the different characteristics of the Blockchain technology, then to analyse in detail the phenomenon of the fourth industrial revolution and finally to find correlation areas to detect potential Blockchain applications in manufacturing.

The research was performed by searching the following terms and expressions:

- "*Blockchain*"

  The term *Blockchain* is researched in combination with the following terms forming short expressions:
  - "*Blockchain Technology*", "*Blockchain Characteristics*" or "**Characteristic*"
  - "*Blockchain Consensus*", "*Blockchain Access*" and "*Blockchain Control*"
  - "*Blockchain Smart Contracts*" or "**Smart Contract*"
  - "*Blockchain Directed Acyclic Graphs*" or "**Graph*" or "**DAG*" or "**DAGs*"
- "*Industry 4.0*"

  The term *Industry 4.0* is researched in combination with the following terms forming short expressions:
  - "*Industry 4.0 Technologies*" or "**Technology*"
  - "*Industry 4.0 Benefits*" or "**Benefit*"
  - "*Industry 4.0 Challenges*" or "**Challenge*"
  - "*Industry 4.0 Requirements*" or "**Requirement*"

  Then, combined researches are performed for discovering further information and enrich the literature using a last set of keywords:
- "*Blockchain Industry 4.0*"
- "*Blockchain Manufacturing*"
- "*Blockchain Applications*" or "**Application*"

The search was executed on three online electronic databases that are “Web of Science”, “Scopus” and “ACM”. In order to refine the research, some Inclusion and Exclusion Criteria were considered for the documents related to the selected keyword:

- *Inclusion Criteria*:
  - Articles’ titles, abstracts and keywords contains the researched terms and expressions
  - English language
  - Publication Data: for Blockchain [2009; 2019], for Industry 4.0 [2011; 2019].
- *Exclusion Criteria:*
  - Full text not available
  - Do not contain researched terms and expressions in titles, abstracts or keywords.

In accordance with the master thesis objective, this research helped in analysing the potential applications of the Blockchain technology in the manufacturing field. Hence, the study started analysing the Blockchain characteristic from a technological point of view for developing a certain knowledge about the technology: after a preliminary that generates consciousness, it was possible to enrich the research for focusing of some fundamental and more technical information about the Blockchain. Similarly, in a subsequent phase, it was explored the Industry 4.0 trend by firstly investigating the phaenomenon as a whole and by secondly looking at specific characteristics of this topic. Finally, these two phases were combined together by jointly examining topics that had a certain affinity, refining the researching activity with the last set of keywords.

The preliminary step of the researching activity by keywords on the three selected databases, generated an immense quantity of documents that were not manageable: therefore, the application of inclusion and exclusion criteria were fundamental for the literature review. After these steps, a filtering activity was performed to further refine the search: only the categories related to management, computer science, business, industrial engineering and manufacturing were taken into consideration, whereas excluding irrelevant subject areas such as agricultural and biological sciences, arts, dentistry, humanities, social sciences, etc.

At this point of the literature research process, an important step was the revision of titles and abstracts for selecting the most suitable papers for the thesis: after this step, a subsequent skimming phase examined the whole papers to find out the possible documents relevant for discovering potential Blockchain applications. The resulting papers were subjected to an intensive reading that permitted to generate the framework used for developing and arguing the master thesis result in the *chapter 4*.

The literature review research process is illustrated in the following image:

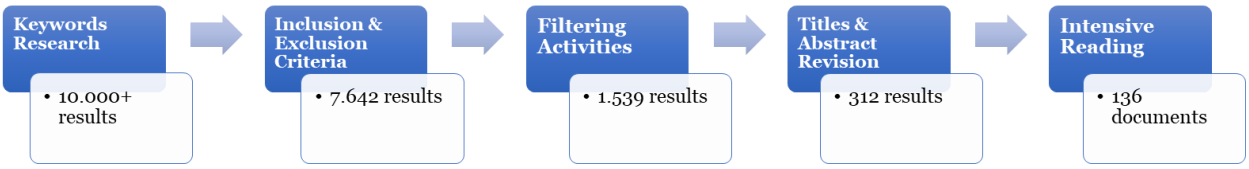


Figure 65: Literature Review Research Process

The process already shown generates a set of 136 documents. This set was analysed for generating a chronological distribution of the documents, in order to verify the consistency of the set and eventually verify if existed insights.

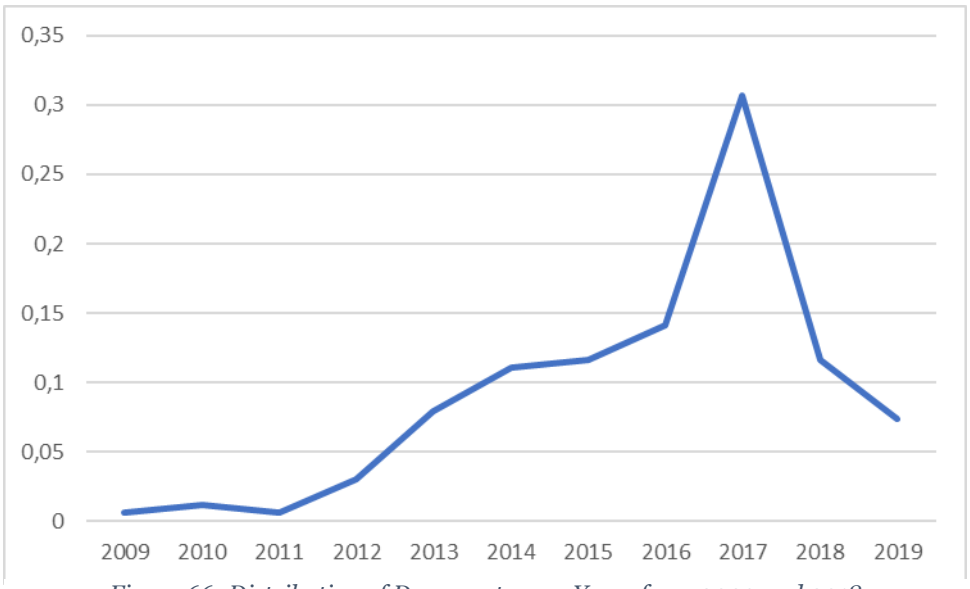


Figure 66: Distribution of Documents over Years from 2009 and 2018

It is interesting to note that the increasing number of documents was particularly constant until the 2016, since both the Industry 4.0 and Blockchain terms started spreading in two very close years (2011 and 2009 respectively) and they reached a peak in 2017. This is due an increased interest in the Blockchain that generated great rumours in the year 2017. As demonstrated by the results of the search on Google Trends, while the keyword "Industry 4.0" continued to growth constantly, concerning the term "Blockchain" this keyword has a peak in the 2017, simultaneously with the overcoming of the threshold of 5000 dollars by the

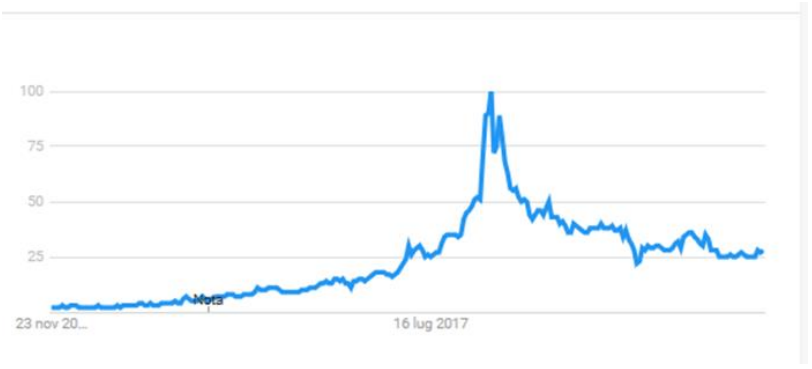


Figure 67: Google Trends Results regarding the Blockchain Keyword

Bitcoins that generated the first peak of enthusiasm. This phaenomenon generated a high attention and pushed to an increase in the release of academic paper on the distributed ledger topic.

Finally, the set of documents was classified based on three main different categories: "*Computer Science*", "*Engineering*" and "*Business, Management & Accounting*".

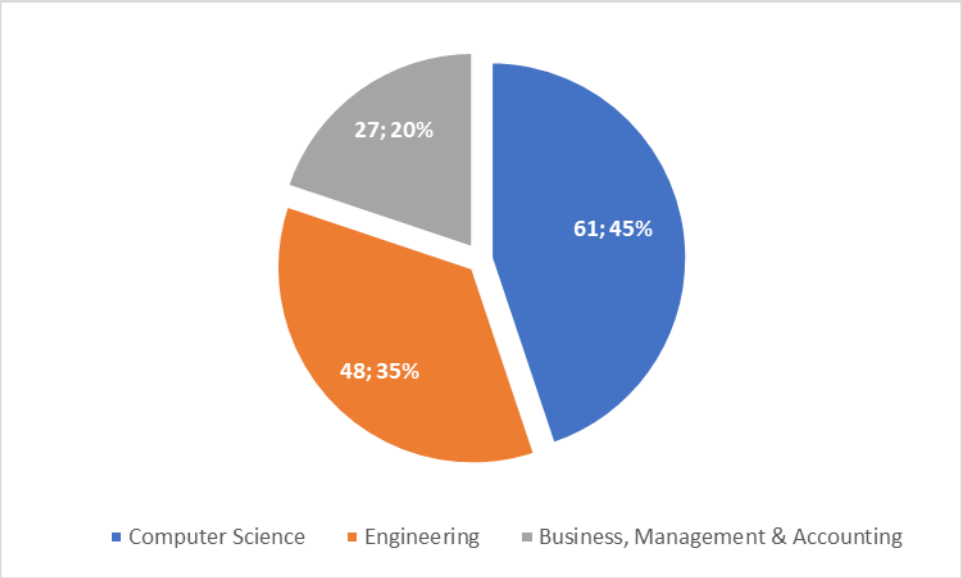


Figure 68: Documents Classification based on Three Main Categories

The distribution of documents is fairly homogeneous. Almost one half of the papers (45%) belongs to the category "*Computer Science"* and this is due to the informatics nature of the Blockchain while the remaining second half (55%) belongs to the categories of "*Engineering*" and "*Business, Management & Accounting"* and this was expected since when talking about Industry 4.0 are considered topics related not only to industrial production but also to the economic and managerial implications of this phenomenon.

Bibliography

Abdullah, N., Hakansson, A., & Moradian, E. (2017, 7). Blockchain based approach to enhance big data authentication in distributed environment. *2017 Ninth International Conference on Ubiquitous and Future Networks (ICUFN)*. IEEE. doi:10.1109/icufn.2017.7993927

Akhtar, P., Khan, Z., Tarba, S., & Jayawickrama, U. (2018, 11). The Internet of Things, dynamic data and information processing capabilities, and operational agility. *Technological Forecasting and Social Change, 136*, 307-316. doi:10.1016/j.techfore.2017.04.023

Akkoyunlu, E. A., Ekanadham, K., & Huber, R. V. (1975). Some Constraints and Tradeoffs in the Design of Network Communications. *Proceedings of the Fifth ACM Symposium on Operating Systems Principles* (pp. 67-74). New York, NY, USA: ACM. doi:10.1145/800213.806523

Aleksy, M., Vartiainen, E., Domova, V., & Naedele, M. (2014, 5). Augmented Reality for Improved Service Delivery. *2014 IEEE 28th International Conference on Advanced Information Networking and Applications*. IEEE. doi:10.1109/aina.2014.146

Aste, T. (2016, 6). The Fair Cost of Bitcoin Proof of Work. *SSRN Electronic Journal*. doi:10.2139/ssrn.2801048

Ateniese, G., Bonacina, I., Faonio, A., & Galesi, N. (2014). Proofs of Space: When Space Is of the Essence. In M. Abdalla, & R. De Prisco (Ed.), *Security and Cryptography for Networks* (pp. 538-557). Cham: Springer International Publishing.

Awais, M., & Henrich, D. (2013, 12). Human-Robot Interaction in an Unknown Human Intention Scenario. *2013 11th International Conference on Frontiers of Information Technology*. IEEE. doi:10.1109/fit.2013.24

Ba, M. (2019, 1). The effect of propagation delay on the dynamic evolution of the Bitcoins blockchain. *Digital Communications and Networks*. doi:10.1016/j.dcan.2019.01.006

Backman, J., Yrjola, S., Valtanen, K., & Mammela, O. (2017, 11). Blockchain network slice broker in 5G: Slice leasing in factory of the future use case. *2017 Internet of Things Business Models, Users, and Networks*. IEEE. doi:10.1109/ctte.2017.8260929

Bahrin, M. A., Othman, M. F., Azli, N. H., & Talib, M. F. (2016, 6). INDUSTRY 4.0: A REVIEW ON INDUSTRIAL AUTOMATION AND ROBOTIC. *Jurnal Teknologi, 78*. doi:10.11113/jt.v78.9285

Baird, L. (2016, May 31). *The Swirld Hashgraph Consensus Algorithm: Fair, Fast, Byzantine Fault Tolerance*. Retrieved from swirlds.com: https://www.swirlds.com/downloads/SWIRLDS-TR-2016-01.pdf

Barhamgi, M., Perera, C., Ghedira, C., & Benslimane, D. (2018, 9). User-centric Privacy Engineering for the Internet of Things. *IEEE Cloud Computing, 5*, 47-57. doi:10.1109/mcc.2018.053711666

Bauernhansl, T., Hompel, M., & Vogel-Heuser, B. (Eds.). (2014). *Industrie 4.0 in Produktion, Automatisierung und Logistik*. Springer Fachmedien Wiesbaden. doi:10.1007/978-3-658-04682-8

Bentov, I., Lee, C., Mizrahi, A., & Rosenfeld, M. (2014). Proof of Activity: Extending Bitcoin's Proof of Work via Proof of Stake [Extended Abstract]y. *IACR Cryptology ePrint Archive, 2014*, 452.

Bernstein Technologies. (2019). *Blockchain solutions for securing intellectual property assets and innovation processes*. Retrieved from Bernstein: https://www.bernstein.io/

Bititci, U. S., Suwignjo, P., & Carrie, A. S. (2001, 1). Strategy management through quantitative modelling of performance measurement systems. *International Journal of Production Economics, 69*, 15-22. doi:10.1016/s0925-5273(99)00113-9

BitShares Foundation. (2015). *The BitShares Blockchain*.

Bondi, A. B. (2000). Characteristics of Scalability and Their Impact on Performance. *Proceedings of the 2Nd International Workshop on Software and Performance* (pp. 195-203). New York, NY, USA: ACM. doi:10.1145/350391.350432

Bonomi, F., Milito, R., Zhu, J., & Addepalli, S. (2012). Fog computing and its role in the internet of things. *Proceedings of the first edition of the MCC workshop on Mobile cloud computing - MCC 12*. ACM Press. doi:10.1145/2342509.2342513

Boud, A. C., Haniff, D. J., Baber, C., & Steiner, S. J. (n.d.). Virtual reality and augmented reality as a training tool for assembly tasks. *1999 IEEE International Conference on Information Visualization (Cat. No. PR00210)*. IEEE Comput. Soc. doi:10.1109/iv.1999.781532

Brewer, A., Sloan, N., & Landers, T. L. (2019). Intelligent tracking in manufacturing. *Journal of Intelligent Manufacturing, 10*, 245-250. doi:10.1023/a:1008995707211

Brown, A., Amundson, J., & Badurdeen, F. (2014, 12). Sustainable value stream mapping (Sus-VSM) in different manufacturing system configurations: application case studies. *Journal of Cleaner Production, 85*, 164-179. doi:10.1016/j.jclepro.2014.05.101

Buxmann, P., Hess, T., & Ruggaber, R. (2009). Internet of Services. *Business & Information Systems Engineering: The International Journal of WIRTSCHAFTSINFORMATIK, 1*, 341-342. Retrieved from https://EconPapers.repec.org/RePEc:spr:binfse:v:1:y:2009:i:5:p:341-342

Cai, H., Xu, B., Jiang, L., & Vasilakos, A. V. (2016). IoT-based Big Data Storage Systems in Cloud Computing: Perspectives and Challenges. *IEEE Internet of Things Journal*, 1-1. doi:10.1109/jiot.2016.2619369

Cai, T. (2014). Robust Optimization for Smart Manufacturing Planning and Supply Chain Design in Chemical Industry. In *Smart Manufacturing Innovation and Transformation* (pp. 21-37). IGI Global. doi:10.4018/978-1-4666-5836-3.ch002

Cao, Q., Wang, W., Zhu, X., Leng, C., & Adachi, M. (2016, 7). Study on ubiquitous robotic systems for smart manufacturing program. *2016 IEEE Workshop on Advanced Robotics and its Social Impacts (ARSO)*. IEEE. doi:10.1109/arso.2016.7736275

Castro, M., & Liskov, B. (1999). Practical Byzantine Fault Tolerance. *Proceedings of the Third Symposium on Operating Systems Design and Implementation* (pp. 173-186). Berkeley: USENIX Association. Retrieved from http://dl.acm.org/citation.cfm?id=296806.296824

Cave, H. (2016, 4). VR in... the factory of the future. *Engineering & Technology, 11*, 44-47. doi:10.1049/et.2016.0321

Chen, J., & Xue, Y. (2017, 6). Bootstrapping a Blockchain Based Ecosystem for Big Data Exchange. *2017 IEEE International Congress on Big Data (BigData Congress)*. IEEE. doi:10.1109/bigdatacongress.2017.67

Choi, S., Jun, C., Zhao, W. B., & Noh, S. D. (2015). Digital Manufacturing in Smart Manufacturing Systems: Contribution, Barriers, and Future Directions. In *Advances in Production Management Systems: Innovative Production Management Towards Sustainable Growth* (pp. 21-29). Springer International Publishing. doi:10.1007/978-3-319-22759-7_3

ChronoLogic. (2018, October 11). *Temporal Innovation on the Blockchain*. Retrieved from chronologic.network: https://chronologic.network/paper

Churyumov, A. (2016, October 1). *Byteball: A Decentralized System for Storage and Transfer of Value.* Retrieved from obyte.org: https://obyte.org/Byteball.pdf

Conner, B. P., Manogharan, G. P., Martof, A. N., Rodomsky, L. M., Rodomsky, C. M., Jordan, D. C., & Limperos, J. W. (2014, 10). Making sense of 3-D printing: Creating a map of additive manufacturing products and services. *Additive Manufacturing, 1-4*, 64-76. doi:10.1016/j.addma.2014.08.005

Davis, J., & Edgar, T. (2019). Smart Process Manufacturing – A Vision of the Future. *Design for Energy and the Environment (Proc. 7th Int. Conf. FOCAPD 2009)*, pp. 149-165.

Decker, C., & Wattenhofer, R. (2013, 9). Information propagation in the Bitcoin network. *IEEE P2P 2013 Proceedings*. IEEE. doi:10.1109/p2p.2013.6688704

Deloitte. (2018). Industry 4.0 Challenges and solutions for the digital transformation and use of exponential technologies.

Deschamps, F., Saturno, M., & Pertel, V. (2017, 7). Proposal of an automation solutions architecture for Industry 4.0.

Dieterich, V., Ivanovic, M., Meier, T., Zäpfel, S., Utz, M., & Sandner, P. (2017). Application of blockchain technology in the manufacturing industry. *Frankfurt School Blockchain Center, Germany*, 1-23.

Diffie, W., & Hellman, M. (2006, 9). New Directions in Cryptography. *IEEE Trans. Inf. Theor., 22*, 644-654. doi:10.1109/TIT.1976.1055638

Dods, C., Smart, N. P., & Stam, M. (2005). Hash Based Digital Signature Schemes. In N. P. Smart (Ed.), *Cryptography and Coding* (pp. 96-115). Berlin: Springer Berlin Heidelberg.

Douceur, J. R. (2002). The Sybil Attack. In P. Druschel, F. Kaashoek, & A. Rowstron (Ed.), *Peer-to-Peer Systems* (pp. 251-260). Berlin: Springer Berlin Heidelberg.

Dziembowski, S., Faust, S., Kolmogorov, V., & Pietrzak, K. (2015, August). Proofs of Space.

Feeney, A. B., Frechette, S. P., & Srinivasan, V. (2015, 6). A Portrait of an ISO STEP Tolerancing Standard as an Enabler of Smart Manufacturing Systems. *Journal of Computing and Information Science in Engineering, 15*. doi:10.1115/1.4029050

Fernandez-Carames, T. M., & Fraga-Lamas, P. (2018). A Review on the Use of Blockchain for the Internet of Things. *IEEE Access, 6*, 32979-33001. doi:10.1109/access.2018.2842685

Fotiou, N., & Polyzos, G. C. (2018, 6). Smart Contracts for the Internet of Things: Opportunities and Challenges. *2018 European Conference on Networks and Communications (EuCNC)*. IEEE. doi:10.1109/eucnc.2018.8443212

Fraga-Lamas, P. (2017). Enabling Technologies and Cyber-Physical Systems for Mission-Critical Scenarios. doi:10.13140/RG.2.2.22769.79202

Frazier, W. E. (2014, 4). Metal Additive Manufacturing: A Review. *Journal of Materials Engineering and Performance, 23*, 1917-1928. doi:10.1007/s11665-014-0958-z

Froiz-Miguez, I., & al., e. (2018, 8). Design, Implementation and Practical Evaluation of an IoT Home Automation System for Fog Computing Applications Based on MQTT and ZigBee-WiFi Sensor Nodes. *Sensors, 18*, 2660. doi:10.3390/s18082660

Gaetani, E., Aniello, L., Lombardi, F., Margheri, A., & Sassone, V. (2017, 1). Blockchain-based database to ensure data integrity in cloud computing environments.

Gervais, A., Karame, G. O., Wüst, K., Glykantzis, V., Ritzdorf, H., & Capkun, S. (2016). On the Security and Performance of Proof of Work Blockchains. *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security* (pp. 3-16). New York, NY, USA: ACM. doi:10.1145/2976749.2978341

Gilad, Y., Hemo, R., Micali, S., Vlachos, G., & Zeldovich, N. (2017). Algorand: Scaling Byzantine Agreements for Cryptocurrencies. *Proceedings of the 26th Symposium on Operating Systems Principles* (pp. 51-68). New York, NY, USA: ACM. doi:10.1145/3132747.3132757

Giusto, D., Iera, A., Morabito, G., & Atzori, L. (2010, 9 1). *The Internet of Things*. (D. Giusto, A. Iera, G. Morabito, & L. Atzori, Eds.) Springer-Verlag GmbH. Retrieved from https://www.ebook.de/de/product/9151135/the_internet_of_things.html

Gmytrasiewicz, P. J., & Durfee, E. H. (1992). Decision-theoretic Recursive Modeling and the Coordinated Attack Problem. *Proceedings of the First International Conference on Artificial Intelligence Planning Systems* (pp. 88-95). San Francisco, CA, USA: Morgan Kaufmann Publishers Inc. Retrieved from http://dl.acm.org/citation.cfm?id=139492.139503

GoChain Foundation. (2018). *GoChain Whitepaper*. Retrieved from gochain.io: https://gochain.io/gochain-whitepaper-v2.1.2.pdf

Gorecky, D., Schmitt, M., Loskyll, M., & Zuhlke, D. (2014, 7). Human-machine-interaction in the industry 4.0 era. *2014 12th IEEE International Conference on Industrial Informatics (INDIN)*. IEEE. doi:10.1109/indin.2014.6945523

Gray, J. (1978). Notes on Data Base Operating Systems. *Operating Systems, An Advanced Course* (pp. 393-481). London: Springer-Verlag. Retrieved from http://dl.acm.org/citation.cfm?id=647433.723863

Haber, S., & Stornetta, W. S. (1991). How to Time-Stamp a Digital Document. *J. Cryptology, 3*, 99-111. doi:10.1007/BF00196791

Hankel, M., & Rexroth, B. (2015). The reference architectural model industrie 4.0 (rami 4.0).

Hardiess, G., Mallot, H. A., & Meilinger, T. (2015). Virtual Reality and Spatial Cognition. In *International Encyclopedia of the Social & Behavioral Sciences* (pp. 133-137). Elsevier. doi:10.1016/b978-0-08-097086-8.43098-9

Harik, E. H., Guerin, F., Guinand, F., Brethe, J.-F., & Pelvillain, H. (2015, 3). UAV-UGV cooperation for objects transportation in an industrial area. *2015 IEEE International Conference on Industrial Technology (ICIT)*. IEEE. doi:10.1109/icit.2015.7125156

Harris-Braun, E., Luck, N., & Brock, A. (2018, February 15). *Holochain: scalable agent-centric distributed computing*. Retrieved from holo.host: https://github.com/holochain/holochain-proto/blob/whitepaper/holochain.pdf

Hasan, M. G., Datta, A., & Rahman, M. A. (2018, 4). Poster Abstract: Chained of Things: A Secure and Dependable Design of Autonomous Vehicle Services. *2018 IEEE/ACM Third International Conference on Internet-of-Things Design and Implementation (IoTDI)*. IEEE. doi:10.1109/iotdi.2018.00048

Haug, K. C., Kretschmer, T., & Strobel, T. (2016, 4). Cloud adaptiveness within industry sectors – Measurement and observations. *Telecommunications Policy, 40*, 291-306. doi:10.1016/j.telpol.2015.08.003

Haug, K. C., Kretschmer, T., & Strobel, T. (2016, 4). Cloud adaptiveness within industry sectors – Measurement and observations. *Telecommunications Policy, 40*, 291-306. doi:10.1016/j.telpol.2015.08.003

Hays, D. K. (2018, June). *Crypto Research Report, Edition III, Chapter 3, Consensus Mechanisms*. Schaan/Liechtenstein: Incrementum AG. Retrieved from Cryptoresearch: https://cryptoresearch.report/crypto-research/consensus-mechanisms/

Hedelind, M., & Jackson, M. (2011, 9). How to improve the use of industrial robots in lean manufacturing systems. *Journal of Manufacturing Technology Management, 22*, 891-905. doi:10.1108/17410381111160951

Heilman, E. (2014). One Weird Trick to Stop Selfish Miners: Fresh Bitcoins, A Solution for the Honest Miner (Poster Abstract). In R. Böhme, M. Brenner, T. Moore, & M. Smith (Ed.), *Financial Cryptography and Data Security* (pp. 161-162). Berlin: Springer Berlin Heidelberg.

Hellman, M. E. (November 1978). An overview of public key cryptography. *IEEE Communications Society Magazine, vol. 16, no. 6*, pp. 24–32.

Helu, M., Libes, D., Lubell, J., Lyons, K., & Morris, K. C. (2016, 8). Enabling Smart Manufacturing Technologies for Decision-Making Support. *Volume 1B: 36th Computers and Information in Engineering Conference*. American Society of Mechanical Engineers. doi:10.1115/detc2016-59721

Herbert, J., & Litchfield, A. (2015). A novel method for decentralised peer-to-peer software license validation using cryptocurrency blockchain technology. *Proceedings of the 38th Australasian Computer Science Conference (ACSC 2015)*, *27*, p. 30.

Hermann, M., Pentek, T., & Otto, B. (2015). Design Principles for Industrie 4.0 Scenarios: A Literature Review. Unpublished. doi:10.13140/rg.2.2.29269.22248

Hermann, M., Pentek, T., & Otto, B. (2016, 1). Design Principles for Industrie 4.0 Scenarios. *2016 49th Hawaii International Conference on System Sciences (HICSS)*, (pp. 3928-3937). doi:10.1109/HICSS.2016.488

Holden, W. (2018). *The Future of Blockchain: Key Vertical Opportunities & Deployment Strategies 2018-2030*. Basingstoke, Hampshire: Juniper.

Holland, M., Nigischer, C., Stjepandić, J., & Chen, C. H. (2017). Copyright protection in additive manufacturing with blockchain approach. *Transdisciplinary Engineering: A Paradigm Shift, 5*, 914-921.

Holland, M., Stjepandic, J., & Nigischer, C. (2018, 6). Intellectual Property Protection of 3D Print Supply Chain with Blockchain Technology. *2018 IEEE International Conference on Engineering, Technology and Innovation (ICE/ITMC)*. IEEE. doi:10.1109/ice.2018.8436315

Hong-Seok, P. A., & Ngoc-Hien, T. R. (2015). Development of a cloud based smart manufacturing system. *Journal of Advanced Mechanical Design, Systems, and Manufacturing, 9*, JAMDSM0030--JAMDSM0030. doi:10.1299/jamdsm.2015jamdsm0030

Huang, X., Xu, C., Wang, P., & Liu, H. (2018). LNSC: A Security Model for Electric Vehicle and Charging Pile Management Based on Blockchain Ecosystem. *IEEE Access, 6*, 13565-13574. doi:10.1109/access.2018.2812176

IBM, & Maersk. (2019). *Digitizing the Global Supply Chain*. Retrieved from TradeLens: https://www.tradelens.com/

Imaging & Machine Vision. (2018, October 11). *Pirelli to improve quality control with automated tyre inspection*. Retrieved from IMVEurope: https://www.imveurope.com/news/pirelli-improve-quality-control-automated-tyre-inspection

Internet4Things. (2017, October 2). *Logistica: Goglio usa l'IoT per rendere più efficiente la produzione*. Retrieved from internet4things: https://www.internet4things.it/industry-4-0/logistica-goglio-usa-liot-per-rendere-piu-efficiente-la-produzione/

Ji, W., & Wang, L. (2017, 4). Big data analytics based fault prediction for shop floor scheduling. *Journal of Manufacturing Systems, 43*, 187-194. doi:10.1016/j.jmsy.2017.03.008

Jin, Y. (2015, 10). Introduction to Hardware Security. *Electronics, 4*, 763-784. doi:10.3390/electronics4040763

John H. Wenslfy, L. L.-S. (1979). SIFT: design and analysis of a fault-tolerant computer for aircraft control. *Microelectronics Reliability (Proceeding IEEE66, (10) 1240), 19*, 190. doi:https://doi.org/10.1016/0026-2714(79)90211-7

Kaestle, C., Fleischmann, H., Scholz, M., Haerter, S., & Franke, J. (2016, 10). Cyber-Physical Electronics Production. In *Industrial Internet of Things* (pp. 47-78). Springer International Publishing. doi:10.1007/978-3-319-42559-7_3

Kagermann, H. (2014, 12). Change Through Digitization - Value Creation in the Age of Industry 4.0. In *Management of Permanent Change* (pp. 23-45). Springer Fachmedien Wiesbaden. doi:10.1007/978-3-658-05014-6_2

Kagermann, H., Anderl, R., Gausemeier, J., & Schuh, G. (2014). Industrie 4.0 in a Global Context.

Kagermann, H., Helbig, J., Hellinger, A., & Wahlster, W. (2013). *Recommendations for Implementing the Strategic Initiative INDUSTRIE 4.0: Securing the Future of German Manufacturing Industry ; Final Report of the Industrie 4.0 Working Group*. Forschungsunion. Retrieved from https://books.google.it/books?id=AsfOoAEACAAJ

Kahn, A. B. (1962, 11). Topological Sorting of Large Networks. *Commun. ACM, 5*, 558-562. doi:10.1145/368996.369025

Kannan, S. M., Suri, K., Cadavid, J., Barosan, I., Brand, M., Alferez, M., & Gerard, S. (2017, 4). Towards Industry 4.0: Gap Analysis between Current Automotive MES and Industry Standards Using Model-Based Requirement Engineering. *2017 IEEE International Conference on Software Architecture Workshops (ICSAW)*. IEEE. doi:10.1109/icsaw.2017.53

Kapitonov, A., Lonshakov, S., Krupenkin, A., & Berman, I. (2017, 10). Blockchain-based protocol of autonomous business activity for multi-agent systems consisting of UAVs. *2017 Workshop on Research, Education and Development of Unmanned Aerial Systems (RED-UAS)*. IEEE. doi:10.1109/red-uas.2017.8101648

Karame, G. O. (2012). Two bitcoins at the price of one? double-spending attacks on fast payments in bitcoin. *In Proc. of Conference on Computer and Communication Security*.

Kiayias, A., Russell, A., David, B., & Oliynykov, R. (2017). Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol. In J. Katz, & H. Shacham (Ed.), *Advances in Cryptology -- CRYPTO 2017* (pp. 357-388). Cham: Springer International Publishing.

Kiel, D., Muller, J. M., & Arnold, C. (2017, 12). Sustainable industrial value creation: benefits and challenges of industry 4.0. *International Journal of Innovation Management, 21*, 1740015. doi:10.1142/s1363919617400151

Kipper, G. (2013). What Is Augmented Reality? In *Augmented Reality* (pp. 1-27). Elsevier. doi:10.1016/b978-1-59-749733-6.00001-2

Komodo Platform. (2018). *Komodo: advanced blockchain technology, focused on freedom*.

Koomey, J., Turner, P., Stanley, J., & Taylor, B. (2007, 1). A Simple Model for Determining True Total Cost of Ownership for Data Centers.

Krammer, M., Benedikt, M., Blochwitz, T., Alekeish, K., Amringer, N., Kater, C., . . . Andert, J. (2018). The Distributed Co-Simulation Protocol for the Integration of Real-Time Systems and Simulation Environments. *Proceedings of the 50th Computer Simulation Conference*. Society for Modeling and Simulation International (SCS). doi:10.22360/summersim.2018.scsc.001

Kravitz, D. W., & Cooper, J. (2017, 6). Securing user identity and transactions symbiotically: IoT meets blockchain. *2017 Global Internet of Things Summit (GIoTS)*. IEEE. doi:10.1109/giots.2017.8016280

Kwon, J. (2014). Tendermint : Consensus without Mining.

Lamport, L. (1998, 5). The Part-time Parliament. *ACM Trans. Comput. Syst., 16*, 133-169. doi:10.1145/279227.279229

Lamport, L., Shostak, R., & Pease, M. (1982, 7). The Byzantine Generals Problem. *ACM Trans. Program. Lang. Syst., 4*, 382-401. doi:10.1145/357172.357176

Landau, S. (2013, 7). Making Sense from Snowden: Whats Significant in the NSA Surveillance Revelations. *IEEE Security & Privacy, 11*, 54-63. doi:10.1109/msp.2013.90

Lee, E. A. (2008, 5). Cyber Physical Systems: Design Challenges. *2008 11th IEEE International Symposium on Object and Component-Oriented Real-Time Distributed Computing (ISORC)*. IEEE. doi:10.1109/isorc.2008.25

Lee, H.-W., & Liu, C.-H. (2016, 7). High Precision Optical Sensors for Real-Time On-line Measurement of Straightness and Angular Errors for Smart Manufacturing. *Smart Science, 4*, 134-141. doi:10.1080/23080477.2016.1207407

Lee, J.-H., & Pilkington, M. (2017, 7). How the Blockchain Revolution Will Reshape the Consumer Electronics Industry [Future Directions]. *IEEE Consumer Electronics Magazine, 6*, 19-23. doi:10.1109/mce.2017.2684916

Lee, Y. T., Kumaraguru, S., Jain, S., Robinson, S., Helu, M., Hatim, Q. Y., . . . Kumara, S. (2017, 2). A Classification Scheme for Smart Manufacturing Systems' Performance Metrics. *Smart and Sustainable Manufacturing Systems, 1*, 20160012. doi:10.1520/ssms20160012

LeMahieu, C. (2015). *Nano: A Feeless Distributed Cryptocurrency Network*. Retrieved from nano.org: https://nano.org/en/whitepaper

Li, J., Liu, Z., Chen, L., Chen, P., & Wu, J. (2017, 12). Blockchain-Based Security Architecture for Distributed Cloud Storage. *2017 IEEE International Symposium on Parallel and Distributed Processing with Applications and 2017 IEEE International Conference on Ubiquitous Computing and Communications (ISPA/IUCC)*. IEEE. doi:10.1109/ispa/iucc.2017.00065

Li, J., Liu, Z., Chen, L., Chen, P., & Wu, J. (2017, 12). Blockchain-Based Security Architecture for Distributed Cloud Storage. *2017 IEEE International Symposium on Parallel and Distributed Processing with Applications and 2017 IEEE International Conference on Ubiquitous Computing and Communications (ISPA/IUCC)*. IEEE. doi:10.1109/ispa/iucc.2017.00065

Li, N., Liu, D., & Nepal, S. (2017, 10). Lightweight Mutual Authentication for IoT and Its Applications. *IEEE Transactions on Sustainable Computing, 2*, 359-370. doi:10.1109/tsusc.2017.2716953

Li, Z., Kang, J., Yu, R., Ye, D., Deng, Q., & Zhang, Y. (2017). Consortium Blockchain for Secure Energy Trading in Industrial Internet of Things. *IEEE Transactions on Industrial Informatics*, 1-1. doi:10.1109/tii.2017.2786307

Liao, Y., Deschamps, F., Freitas Rocha Loures, E., & Ramos, L. F. (2017, 3). Past, present and future of Industry 4.0 - a systematic literature review and research agenda proposal. *International Journal of Production Research, 55*, 3609-3629. doi:10.1080/00207543.2017.1308576

Lin, S.-W., Miller, B., Durand, J., Joshi, R., Didier, P., Chigani, A., . . . others. (2015). Industrial internet reference architecture. *Industrial Internet Consortium (IIC), Tech. Rep.*

Lin, Y.-C., Hung, M.-H., Huang, H.-C., Chen, C.-C., Yang, H.-C., Hsieh, Y.-S., & Cheng, F.-T. (2017, 7). Development of Advanced Manufacturing Cloud of Things (AMCoT)—A Smart Manufacturing Platform. *IEEE Robotics and Automation Letters, 2*, 1809-1816. doi:10.1109/lra.2017.2706859

Link3D. (2019). *Additive Manufacturing Execution System*. Retrieved from https://solution.link3d.co

Liu, B., Yu, X. L., Chen, S., Xu, X., & Zhu, L. (2017, 6). Blockchain Based Data Integrity Service Framework for IoT Data. *2017 IEEE International Conference on Web Services (ICWS)*. IEEE. doi:10.1109/icws.2017.54

Liu, Y., Wang, L., Wang, X. V., Xu, X., & Jiang, P. (2019, 7). Cloud manufacturing: key issues and future perspectives. *International Journal of Computer Integrated Manufacturing, 32*, 858-874. doi:10.1080/0951192x.2019.1639217

Lo, S. K., Xu, X., Chiam, Y. K., & Lu, Q. (2017, 11). Evaluating Suitability of Applying Blockchain. *2017 22nd International Conference on Engineering of Complex Computer Systems (ICECCS)*. IEEE. doi:10.1109/iceccs.2017.26

Loch, F., Quint, F., & Brishtel, I. (2016, 9). Comparing Video and Augmented Reality Assistance in Manual Assembly. *2016 12th International Conference on Intelligent Environments (IE)*. IEEE. doi:10.1109/ie.2016.31

Locher, T., Obermeier, S., & Pignolet, Y. A. (2018). When can a distributed ledger replace a trusted third party? *2018 IEEE International Conference on Internet of Things*

(iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), (pp. 1069-1077).

Lu, Q., & Xu, X. (2017, 11). Adaptable Blockchain-Based Systems: A Case Study for Product Traceability. *IEEE Software, 34*, 21-27. doi:10.1109/ms.2017.4121227

Lu, X., Qu, Z., Li, Q., & Hui, P. (2015, 1). Privacy Information Security Classification for Internet of Things Based on Internet Data. *International Journal of Distributed Sensor Networks, 11*, 932941. doi:10.1155/2015/932941

MacDougall, W. (2014, July). *Industrie 4.0: Smart Manufacturing for the Future.* Brochure, Germany Trade and Invest, Gesellschaft f\"{u}r Au{\ss}enwirtschaft und Standortmarketing mbH, Berlin. Retrieved from http://www.gtai.de/GTAI/Navigation/EN/Invest/Service/publications,did=917080.html

Mannabase Incorporated. (2018). *Mannabase Technology*. Retrieved from Mannabase: https://www.mannabase.com/technology

Mazières, D. (2016, February 25). *The Stellar Consensus Protocol: A Federated Model for Internet-level Consensus*. Retrieved from www.stellar.org: https://www.stellar.org/papers/stellar-consensus-protocol.pdf

Menezes, B. C., Kelly, J. D., Leal, A. G., & Roux, G. C. (2019). Predictive, Prescriptive and Detective Analytics for Smart Manufacturing in the Information Age. *IFAC-PapersOnLine, 52*, 568-573. doi:10.1016/j.ifacol.2019.06.123

Merkle, R. C. (1990). A Certified Digital Signature. In G. Brassard (Ed.), *Advances in Cryptology --- CRYPTO' 89 Proceedings* (pp. 218-238). New: Springer New York.

Miller, A., Juels, A., Shi, E., Parno, B., & Katz, J. (2014, 5). Permacoin: Repurposing Bitcoin Work for Data Preservation. *2014 IEEE Symposium on Security and Privacy*, (pp. 475-490). doi:10.1109/SP.2014.37

Miller, D. (2018, 5). Blockchain and the Internet of Things in the Industrial Sector. *IT Professional, 20*, 15-18. doi:10.1109/mitp.2018.032501742

Milutinovic, M., He, W., Wu, H., & Kanwal, M. (2016, 12). Proof of Luck: an Efficient Blockchain Consensus Protocol., (pp. 1-6). doi:10.1145/3007788.3007790

Miranda, J., Makitalo, N., Garcia-Alonso, J., Berrocal, J., Mikkonen, T., Canal, C., & Murillo, J. M. (2015, 3). From the Internet of Things to the Internet of People. *IEEE Internet Computing, 19*, 40-47. doi:10.1109/mic.2015.24

Mohamed, N., & Al-Jaroodi, J. (2019, 1). Applying Blockchain in Industry 4.0 Applications. *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)*. IEEE. doi:10.1109/ccwc.2019.8666558

Moyne, J., & Iskandar, J. (2017, 7). Big Data Analytics for Smart Manufacturing: Case Studies in Semiconductor Manufacturing. *Processes, 5*, 39. doi:10.3390/pr5030039

Nakamoto, S. (2009). Bitcoin: A peer-to-peer electronic cash system. Retrieved from http://www.bitcoin.org/bitcoin.pdf

Nebulas Team. (2018, April). *Nebulas Technical White Paper: The value-based blockchain operating system and search engine*. Retrieved from nebulas.io: https://nebulas.io/docs/NebulasTechnicalWhitepaper.pdf

NEM Foundation. (2018, February 23). *NEM Technical Reference*. Retrieved from nem.io: https://www.nem.io/wp-content/themes/nem/files/NEM_techRef.pdf#section.7

Nikolic, J., Burri, M., Rehder, J., Leutenegger, S., Huerzeler, C., & Siegwart, R. (2013, 3). A UAV system for inspection of industrial facilities. *2013 IEEE Aerospace Conference*. IEEE. doi:10.1109/aero.2013.6496959

Noran, O., Romero, D., & Zdravkovic, M. (2014). The Sensing Enterprise: Towards the Next Generation Dynamic Virtual Organisations. In *Progress in Pattern Recognition, Image Analysis, Computer Vision, and Applications* (pp. 209-216). Springer International Publishing. doi:10.1007/978-3-662-44745-1_20

Nunes, M. L., Pereira, A. C., & Alves, A. C. (2017). Smart products development approaches for Industry 4.0. *Procedia Manufacturing, 13*, 1215-1222. doi:10.1016/j.promfg.2017.09.035

Oceana. (2013). *Oceana Study Reveals Seafood Frauds Nationwide*. Retrieved from Ocean Organization: https://oceana.org/reports/oceana-study-reveals-seafood-fraud-nationwide

Oertwig, N., Jochem, R., & Knothe, T. (2017). Sustainability in Model-based Planning and Control of Global Value Creation Networks. *Procedia Manufacturing, 8*, 183-190. doi:10.1016/j.promfg.2017.02.023

Oks, S. J., Fritzsche, A., & Möslein, K. M. (2016, 10). An Application Map for Industrial Cyber-Physical Systems. In *Industrial Internet of Things* (pp. 21-46). Springer International Publishing. doi:10.1007/978-3-319-42559-7_2

Ong, S. K., & Nee, A. Y. (2013). *Virtual and augmented reality applications in manufacturing*. Springer Science & Business Media.

Ongaro, D., & Ousterhout, J. (2014). In Search of an Understandable Consensus Algorithm. *Proceedings of the 2014 USENIX Conference on USENIX Annual Technical Conference* (pp. 305-320). Berkeley: USENIX Association. Retrieved from http://dl.acm.org/citation.cfm?id=2643634.2643666

Panetto, H., & Molina, A. (2018, 9). Enterprise Integration and Interoperability in Manufacturing Systems: Trends and Issues. *Computers in Industry, 59*.

Park, H.-S., & Tran, N.-H. (2014, 4). Autonomy for Smart Manufacturing. *Journal of the Korean Society for Precision Engineering, 31*, 287-295. doi:10.7736/kspe.2014.31.4.287

Paul, W. J., Tarjan, R. E., & Celoni, J. R. (1976, 12 01). Space bounds for a game on graphs. *Mathematical systems theory, 10*, 239-251. doi:10.1007/BF01683275

Pease, M., Shostak, R., & Lamport, L. (1979, 4). Reaching Agreement in the Presence of Faults. *J. ACM, 27*, 228-234. doi:10.1145/322186.322188

Pereira, A. C., & Romero, F. (2017). A review of the meanings and the implications of the Industry 4.0 concept. *Procedia Manufacturing, 13*, 1206-1214. doi:10.1016/j.promfg.2017.09.032

Poon, J., & Dryja, T. (2015). *The bitcoin lightning network: Scalable off-chain instant payments*. Tech. rep., Technical Report (draft). https://lightning. network.

Popov, S. (2018, April 30). *Academic Papers: The Tangle*. Retrieved from iota.org: https://www.iota.org/research/academic-papers

Porter, M. E. (1985). *Competitive Advantage: Creating and sustaining superior performance*. (Vol. 167). The Free Press.

Porter, M. E., & Heppelmann, J. E. (2014). How smart, connected products are transforming competition. *Harvard business review, 92*, 64-88.

Preden, J. S., Tammemae, K., Jantsch, A., Leier, M., Riid, A., & Calis, E. (2015, 7). The Benefits of Self-Awareness and Attention in Fog and Mist Computing. *Computer, 48*, 37-45. doi:10.1109/mc.2015.207

Project Provenance Ltd. (2019). *Provenance - Case Studies*. Retrieved from Provenance: https://www.provenance.org/case-studies

Provenance Organization. (2019). *Every Product has a Story*. Retrieved from Project Provenance: https://www.provenance.org/

PwC, & Stanford Woods Institute. (2018). *Building Block(chain)s for a Better Planet*. Geneva: World Economic Forum.

Qing, H. (2010). Research and application of virtual reality technology in mechanical maintenance. *International Conference on Advanced Technology of Design and Manufacture (ATDM 2010)*. IET. doi:10.1049/cp.2010.1301

Rathinasabapathy, R., Elsass, M. J., Josephson, J. R., & Davis, J. F. (2016, 7). A smart manufacturing methodology for real time chemical process diagnosis using causal link assessment. *AIChE Journal, 62*, 3420-3431. doi:10.1002/aic.15403

Rawat, D. B., Njilla, L., Kwiat, K., & Kamhoua, C. (2018, 3). iShare: Blockchain-Based Privacy-Aware Multi-Agent Information Sharing Games for Cybersecurity. *2018 International Conference on Computing, Networking and Communications (ICNC)*. IEEE. doi:10.1109/iccnc.2018.8390264

Rawat, D. B., Parwez, M. S., & Alshammari, A. (2017, 10). Edge Computing Enabled Resilient Wireless Network Virtualization for Internet of Things. *2017 IEEE 3rd International Conference on Collaboration and Internet Computing (CIC)*. IEEE. doi:10.1109/cic.2017.00030

Ren, L. (2014, April). *Proof of Stake Velocity: Building the Social Currency of the Digital Age*. Retrieved from Reddcoin.com: https://www.reddcoin.com/papers/PoSV.pdf

Robla-Gomez, S., Becerra, V. M., Llata, J. R., Gonzalez-Sarabia, E., Torre-Ferrero, C., & Perez-Oria, J. (2017). Working Together: A Review on Safe Human-Robot Collaboration in Industrial Environments. *IEEE Access, 5*, 26754-26773. doi:10.1109/access.2017.2773127

Rosenfeld, M. (2014). Analysis of Hashrate-Based Double Spending. *CoRR, abs/1402.2009*. Retrieved from http://arxiv.org/abs/1402.2009

Rüßmann, M., Lorenz, M., Gerbert, P., Waldner, M., Justus, J., Engel, P., & Harnisch, M. (2017). Industry 4.0: The future of productivity and growth in manufacturing industries. *Boston Consulting Group, 9*.

Santos, F. J., & Villalonga, S. G. (2015, 3). Exploiting Local Clouds in the Internet of Everything Environment. *2015 23rd Euromicro International Conference on Parallel, Distributed, and Network-Based Processing*. IEEE. doi:10.1109/pdp.2015.117

Schipper, I., & Cowan, R. (2018). *Global mica mining and the impact on children's rights*. Retrieved from Somo: https://www.somo.nl/global-mica-mining/

Schneider, M., Rambach, J., & Stricker, D. (2017, 3). Augmented reality based on edge computing using the example of remote live support. *2017 IEEE International Conference on Industrial Technology (ICIT)*. IEEE. doi:10.1109/icit.2017.7915547

Schuh, G., Potente, T., Wesch-Potente, C., & Hauptvogel, A. (2013, 9 23). Sustainable increase of overhead productivity due to cyber-physical-systems. In *Proceedings / 11th Global Conference on Sustainable Manufacturing : innovative solutions ; Berlin, Germany, 23rd - 25th September, 2013 ; proceedings / sponsored by the International Academy for Production Engineering (CIRP). Technische Universität Berlin, Institute of Machine Tools and Factory Management. Günther Seliger, ed.* (pp. 332-335). Berlin: Univ.-Verl. der TU. Retrieved from https://publications.rwth-aachen.de/record/477526

Seele, P. (2017, 6). Predictive Sustainability Control: A review assessing the potential to transfer big data driven `predictive policing' to corporate sustainability management. *Journal of Cleaner Production, 153*, 673-686. doi:10.1016/j.jclepro.2016.10.175

Shin, C., Park, B.-H., Jung, G.-M., & Hong, S.-H. (2014, 12). Mobile Augmented Reality Mashup for Furture IoT Environment. *2014 IEEE 11th Intl Conf on Ubiquitous Intelligence and Computing and 2014 IEEE 11th Intl Conf on Autonomic and Trusted Computing and 2014 IEEE 14th Intl Conf on Scalable Computing and Communications and Its Associated Workshops*. IEEE. doi:10.1109/uic-atc-scalcom.2014.131

Simovici, D. A., & Djeraba, C. (2008). Partially Ordered Sets. In *Mathematical Tools for Data Mining: Set Theory, Partial Orders, Combinatorics* (pp. 129-172). London: Springer London. doi:10.1007/978-1-84800-201-2_4

Singh, M., & Kim, S. (2018, 2). Trust Bit: Reward-based intelligent vehicle commination using blockchain paper. *2018 IEEE 4th World Forum on Internet of Things (WF-IoT)*. IEEE. doi:10.1109/wf-iot.2018.8355227

Slimcoin. (2014, May 17). *Slimcoin: A Peer-to-Peer Crypto-Currency with Proof-of-Burn*. Retrieved from slimco.in: https://github.com/slimcoin-project/slimcoin-project.github.io/raw/master/whitepaperSLM.pdf

Sluijs, C. (2017, June 28). *Antwerp start-up T-Mining develops Blockchain solution for safe, efficient container release*. Retrieved from portofantwerp: https://www.portofantwerp.com/en/news/antwerp-start-t-mining-develops-blockchain-solution-safe-efficient-container-release

Sompolinsky, Y., Lewenberg, Y., & Zohar, A. (2017). SPECTRE : Serialization of Proof-of-work Events : Confirming Transactions via Recursive Elections.

Steamchain. (2019). *Accelerating and Transforming Manufacturing*. Retrieved from Steamchain: https://www.steamchain.io/

Stevens, M., Bursztein, E., Karpman, P., Albertini, A., & Markov, Y. (2017). The First Collision for Full SHA-1. In J. Katz, & H. Shacham (Ed.), *Advances in Cryptology -- CRYPTO 2017* (pp. 570-596). Cham: Springer International Publishing.

Suárez-Albela, M., & Castedo, L. (2017, 8). *A Practical Evaluation of a High-Security Energy-Efficient Gateway for IoT Fog Computing Applications* (Vol. 17). doi:10.3390/s17091978

Suárez-Albela, M., Fraga-Lamas, P., Castedo, L., & Fernández-Caramés, T. (2018, 12). Clock Frequency Impact on the Performance of High-Security Cryptographic Cipher Suites for Energy-Efficient Resource-Constrained IoT Devices. *Sensors, 19*, 15. doi:10.3390/s19010015

Suri, K., Cadavid, J., Alferez, M., Dhouib, S., & Tucci-Piergiovanni, S. (2017, 9). Modeling business motivation and underlying processes for RAMI 4.0-aligned cyber-physical production systems. *2017 22nd IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*. IEEE. doi:10.1109/etfa.2017.8247702

Teslya, N., & Ryabchikov, I. (2017, 11). Blockchain-based platform architecture for industrial IoT. *2017 21st Conference of Open Innovations Association (FRUCT)*. IEEE. doi:10.23919/fruct.2017.8250199

Thames, L., & Schaefer, D. (2017). *Cybersecurity for industry 4.0*. Springer.

The Internet of Services Foundation. (2017, December 31). *IOST: THE NEXT-GENERATION, SECURE, HIGHLY SCALABLE ECOSYSTEM FOR ONLINE SERVICES*. Retrieved from iost.io: https://iost.io/iost-whitepaper/

The Linux Foundation. (2018, Gennaio 30). *PoET Specification*. Retrieved from Sawtooth Hyperledger: https://sawtooth.hyperledger.org/docs/core/releases/latest/architecture/poet.html

Thulasiraman, K., & Swamy, M. N. (1992). *Graphs: Theory and Algorithms*. New York, NY, USA: John Wiley & Sons, Inc.

Trouton, S., Vitale, M., & Killmeyer, J. (2017, November). *3D opportunity for blockchain: Additive manufacturing links the digital thread.* Retrieved from Deloitte Insights: https://www2.deloitte.com/us/en/insights/focus/3d-opportunity/3d-printing-blockchain-in-manufacturing.html

Trusted IoT Alliance. (2019). *Securing IoT Products With Blockchain*. Retrieved from https://www.trusted-iot.org/

Uhlemann, T. H.-J., Lehmann, C., & Steinhilper, R. (2017). The Digital Twin: Realizing the Cyber-Physical Production System for Industry 4.0. *Procedia CIRP, 61*, 335-340. doi:10.1016/j.procir.2016.11.152

Unger, H., Börner, F., & Müller, E. (2017). Context Related Information Provision in Industry 4.0 Environments. *Procedia Manufacturing, 11*, 796-805. doi:10.1016/j.promfg.2017.07.181

Vargas, A., Cuenca, L., Boza, A., Sacala, I., & Moisescu, M. (2014, 3). Towards the development of the framework for inter sensing enterprise architecture. *Journal of Intelligent Manufacturing, 27*, 55-72. doi:10.1007/s10845-014-0901-z

Vila, C., Ugarte, D., Rı´os, J., & Abellán, J. V. (2017). Project-based collaborative engineering learning to develop Industry 4.0 skills within a PLM framework. *Procedia Manufacturing, 13*, 1269-1276. doi:10.1016/j.promfg.2017.09.050

Vilarinho, T., Farshchian, B. A., Floch, J., & Mathisen, B. M. (2013, 7). A Communication Framework for the Internet of People and Things Based on the Concept of Activity Feeds in Social Computing. *2013 9th International Conference on Intelligent Environments*. IEEE. doi:10.1109/ie.2013.24

Vukolić, M. (2016). The Quest for Scalable Blockchain Fabric: Proof-of-Work vs. BFT Replication. In J. Camenisch, & D. Kesdoğan (Ed.), *Open Problems in Network Security* (pp. 112-125). Cham: Springer International Publishing.

Wang, S., Wan, J., Zhang, D., Li, D., & Zhang, C. (2016, 6). Towards smart factory for industry 4.0: a self-organized multi-agent system with big data based feedback and coordination. *Computer Networks, 101*, 158-168. doi:10.1016/j.comnet.2015.12.017

Waves Platform. (2016, Aprile 1). *Waves Whitepaper*. Retrieved from wavesplatform.com: https://blog.wavesplatform.com/waves-whitepaper-164dd6ca6a23

Weyer, S., Meyer, T., Ohmer, M., Gorecky, D., & Zühlke, D. (2016). Future Modeling and Simulation of CPS-based Factories: an Example from the Automotive Industry. *IFAC-PapersOnLine, 49*, 97-102. doi:10.1016/j.ifacol.2016.12.168

Williamson, J., Liu, Q., Lu, F., Mohrman, W., Li, K., Dick, R., & Shang, L. (2015, 1). Data sensing and analysis: Challenges for wearables. *The 20th Asia and South Pacific Design Automation Conference*. IEEE. doi:10.1109/aspdac.2015.7058994

Winkler-Goldstein, R., Imbault, F., Uslander, T., & Gastine, H. (2018, 6). Fractal Production Reprogramming Industrie 4.0 Around Resource and Energy Efficiency? *2018 IEEE International Conference on Environment and Electrical Engineering and 2018 IEEE Industrial and Commercial Power Systems Europe (EEEIC / I&CPS Europe)*. IEEE. doi:10.1109/eeeic.2018.8494395

Wu, L., Meng, K., Xu, S., Li, S., Ding, M., & Suo, Y. (2017, 4). Democratic Centralism: A Hybrid Blockchain Architecture and Its Applications in Energy Internet. *2017 IEEE International Conference on Energy Internet (ICEI)*. IEEE. doi:10.1109/icei.2017.38

Xage. (2019). *Xage*. Retrieved from Universal industrial security: https://xage.com/

Yakovenko, A. (2017, November). *Solana: A new architecture for a high performance blockchain*. Retrieved from Solana.com: https://solana.com/solana-whitepaper.pdf

Yan, Y., Duan, B., Zhong, Y., & Qu, X. (2017, 10). Blockchain technology in the internet plus: The collaborative development of power electronic devices. *IECON 2017 - 43rd Annual Conference of the IEEE Industrial Electronics Society*. IEEE. doi:10.1109/iecon.2017.8216159

Yang, Z., Zheng, K., Yang, K., & Leung, V. C. (2017, 10). A blockchain-based reputation system for data credibility assessment in vehicular networks. *2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*. IEEE. doi:10.1109/pimrc.2017.8292724

Yin, S., & Kaynak, O. (2015, 2). Big Data for Modern Industry: Challenges and Trends [Point of View]. *Proceedings of the IEEE, 103*, 143-146. doi:10.1109/jproc.2015.2388958

Yue, L., Junqin, H., Shengzhi, Q., & Ruijin, W. (2017, 8). Big Data Model of Security Sharing Based on Blockchain. *2017 3rd International Conference on Big Data Computing and Communications (BIGCOM)*. IEEE. doi:10.1109/bigcom.2017.31

Zhang, E. (2014). *A Byzantine Fault Tolerance Algorithm for Blockchain.* Retrieved from neo.org: https://docs.neo.org/en-us/basic/consensus/whitepaper.html

Zhang, F., Liu, M., & Shen, W. (2017, 10). Operation modes of smart factory for high-end equipment manufacturing in the Internet and Big Data era. *2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC).* IEEE. doi:10.1109/smc.2017.8122594

Zhang, J., Ding, G., Zou, Y., Qin, S., & Fu, J. (2017, 8). Review of job shop scheduling research and its new perspectives under Industry 4.0. *Journal of Intelligent Manufacturing, 30*, 1809-1830. doi:10.1007/s10845-017-1350-2

Zhou, K., Liu, T., & Zhou, L. (2015, 8). Industry 4.0: Towards future industrial opportunities and challenges. *2015 12th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD).* IEEE. doi:10.1109/fskd.2015.7382284

Zhou, Z., Xie, M., Zhu, T., Xu, W., Yi, P., Huang, Z., . . . Xiao, S. (2014, 11). EEP2P: An energy-efficient and economy-efficient P2P network protocol. *International Green Computing Conference.* IEEE. doi:10.1109/igcc.2014.7039171

Zīle, K., & Strazdiņa, R. (2018, 5). Blockchain Use Cases and Their Feasibility. *Applied Computer Systems, 23*, 12-20. doi:10.2478/acss-2018-0002

Zuehlke, D. (2010, 4). SmartFactory—Towards a factory-of-things. *Annual Reviews in Control, 34*, 129-138. doi:10.1016/j.arcontrol.2010.02.008