Consensus, Cycle of Information and Blockchain Engine

Stéphane Caporali,

Caporali Conseil

April 19, 2023

Abstract

The creation of blockchain technology is generally dated to that of Bitcoin in 2008. However, the main question, perhaps the question of all the questions: “How to reconcile governance and decentralization? ?” is still open. The question is all the more critical in the case of permissionless public blockchain. An original approach, inspired by the concepts of thermodynamics, is presented in this article: the Blockchain Engine and its ideal information cycle. Some ideas are presented on the resilience of a blockchain, from the point of view of the information cycle. The object is to open new approaches in support of the industrial governance of the blockchain.

1. Introduction

Caporali (2020) [1] attempted to give a technical approach to the governance of a blockchain, based on the techniques used in the field of electronics and automation. The underlying idea was to be able to model the entire existing blockchain system in component blocks as for example in control theory where servo mechanisms are used to stabilize electric power against the action of parasitic signals and the resulting signal distortion. Caporali (2020) [1] proposed at the end of his article an abstract blockchain structure, which is called temporal structure of the blockchain consisting of these four functions : timestamp, ordering, alert, and control. However, this notion of information cycle must be refined and new broader ideas must be found in the behavior of the natural physical systems, to draw inspiration and provide a representation grid of what could be a decentralized system : the challenge is to provide unity of representation despite the multiplicity of actors involved. We begin in the next paragraph with some reminders from the field of thermodynamics.

2. The thermodynamic cycle (Carnot cycle : temperature-entropy diagram)

A Carnot cycle is the ideal thermodynamic cycle of any classical thermodynamic engine. The abscissa parameter is the entropy, the ordinate is the gas temperature. The idea here is not of course to deepen the operation of a thermodynamic engine but to ask ourselves question about what describes the important function of entropy.

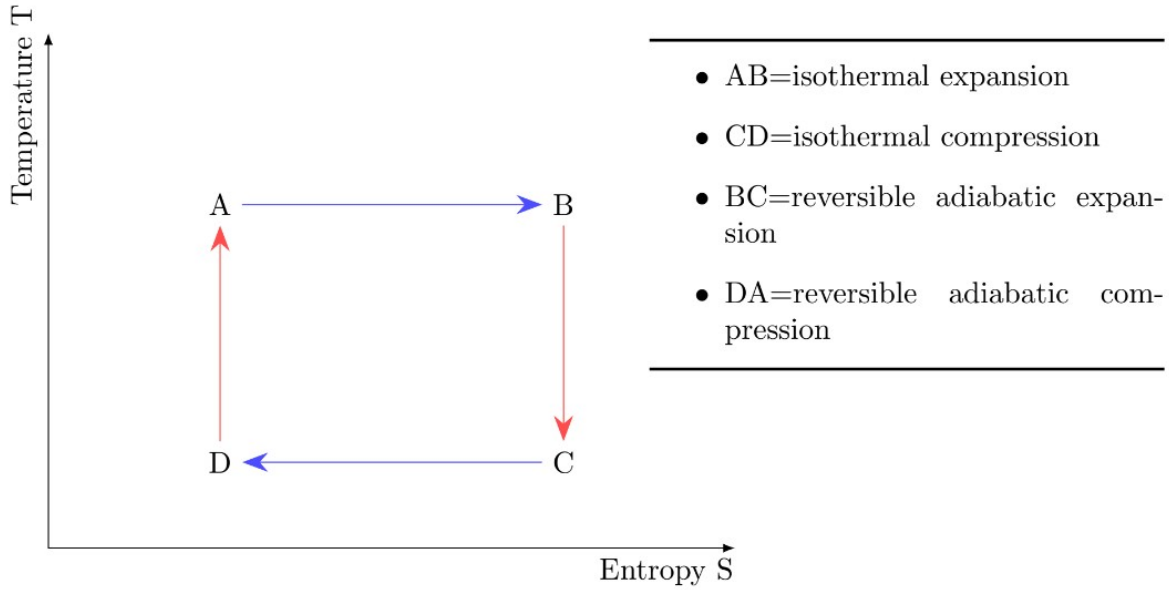

Figure 1: Ideal Carnot cycle.

- In a macroscopic point of view, the entropy S measures the tendency to spontaneous change.
- On the atomistic scale, entropy can be understood as the measure of the degree of disorder. The greater it is, the higher the entropy. For example, intuitively, for a given substance, entropy increases from the solid state to the gaseous stats : $S_{solid} < S_{fluid} < S_{gas}$.

These reminders of known notions being made, in the following paragraph, the choice is to present an approach combining consensus mechanism, thermodynamics, and concept of information.

3. Blockchain consensus processus

3.1 Definitions

What is the process of consensus for blockchain ? It is chosen to start from the definition of the consensus mechanism, according to ISO (2020) [2] standard.

Definition 1. Consensus : agreement among DLT nodes that 1) a transaction is validated and 2) that the distributed ledger contains a consistent set and ordering of validated transactions.

Definition 2. Validated : status of an entity when its required integrity conditions have been checked.

3.2 Diagram of the processus of consensus

It should be noted that in the definition of consensus there are two conditions in parallel. This is summarized in the following diagram, which is an illustration of the ISO definition.

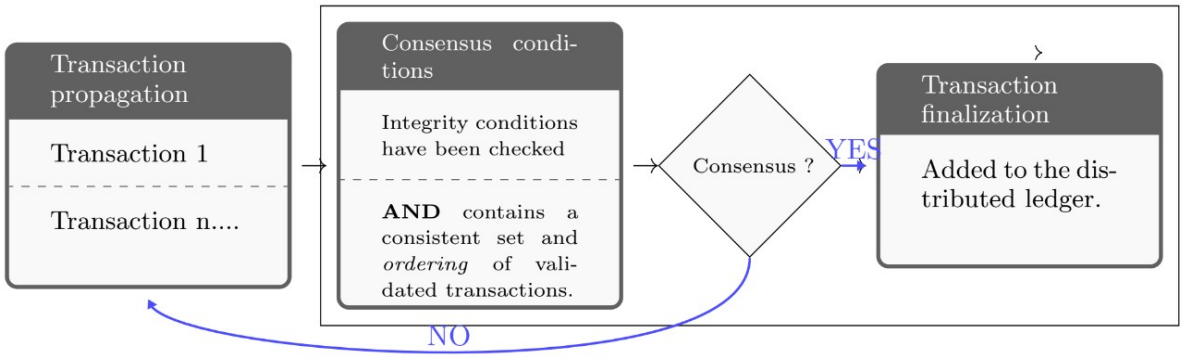

Figure 2: Blockchain consensus processus. The AND means that the verification of integrity can precede the determination of the ordering, or the contrary, depending on the cases

The fact that the consensus result can be : NO is different depending on whether you have a consensus algorithm that favors safety (like byzantine agreement) or liveness (like the PoW). Historically, these notions are first defined by Lamport (1977) [3] and roughly means that a safety property is one that says that something will not happen (exemple : the absence of consensus) and a liveness property is one that indicates that something must happen (example : that the program will terminate). With a consensus mechanism that favors safety, there is a little chance that the result of the consensus would be NO, even if it may take a long time to achieves this (if the calculation times depends on the number of node).

3.3 How to traduct the consensus process in the example of the Proof of Work (PoW) ?

It is chosen to take the example of the proof of work, because it is an educational consensus algorithm. The proof of work is used by Bitcoin. However, there are different possible implementations depending on the consensus mechanisms used. It is chosen to follow the original specifications given by Nakamoto (2008) [4]. Note that a block is created. However, in some cases, for example with the Byzantine agreement consensus mechanism, there is no block creation, and the process of ordering is quite different, consisting of an exchange of messages between nodes.The important is to understand the diversity of possible concrete situations depending on the choice of the consensus algorithm. However, two points must be taken into account :

- For some blockchains that use smart contracts, the process is more complex. There can be on-chain/off-chain interactions.
- The complexity comes from the fact that there is not one node but a multiplicity of nodes who act in a decentralized way.

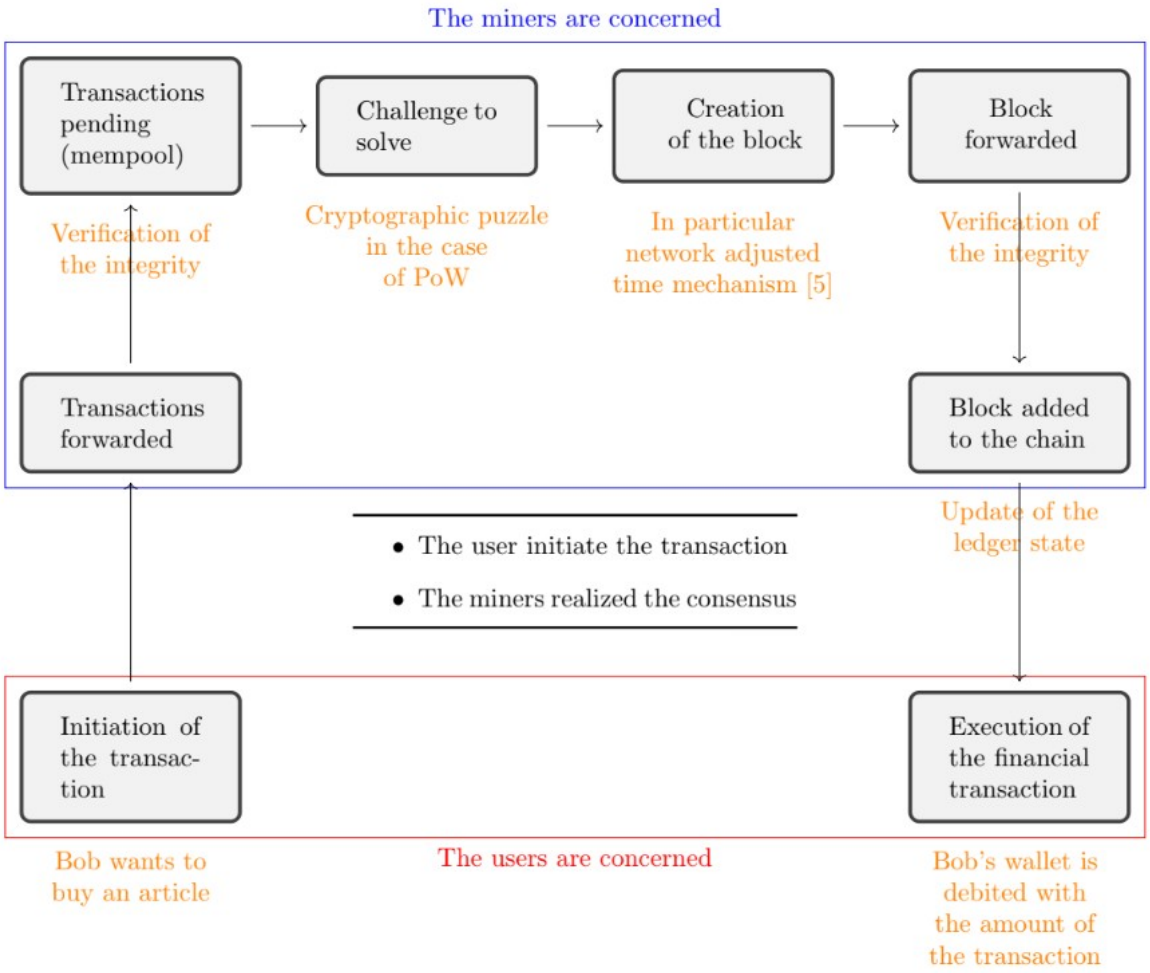

Figure 3: Blockchain consensus processus : case of PoW

The figure 3 is inspired by the description of the process of consensus made in the educational document written by Tran and Krishnamachari [6] in particular the differentiations between transaction forwarding and node forwarding.

4. Convergence between stability and resilience for blockchain

4.1 Sustainable and Development Goal

Is there an international goal for technical resilience ? The United Nations General Assembly (2015) [7] cites 17 Sustainable Development Goals or Global Goals, of which technical resilience constitutes the goal 9 (Build resilient infrastructure, promote inclusive and sustainable industrialization and foster innovation). This can be a strong point of convergence between industry, research and innovation on the subject.

4.2 Resilience vs stability

It is possible to bring together the notions of technical resilience and stability. Several meanings can be given to the word stability. For example, for Marsden and Ratiu (2013) [8] intuitively, stability means that small disturbances do not grow larger over time. What guarantees the stability of the process of consensus ? There is an economic approach which

shows that the economic and rational interest of the miners is the strategy which leads to a stable structure : for example the cooperation in pole of miners who share a common objective. This approach exists, but it is not the one favored in this document.

4.3 Approach of this document

In his previous work, Caporali (2020) [1] wrote that the industrial issue is the long-term maintenance and resilience capacity for long-term operations. The author used the term resilience in the sense of control system such as tolerance to fluctuations.In this article, a slightly different approach is presented. The goal is the same: to describe an information cycle, but it is inspired by the concepts of thermodynamics. There are many educational books on the subject of thermodynamic, for example Coopersmith (2010) [9] and Gicquel (2017) [10]. Indeed, everyone agrees that blockchain has a something to do with energy, especially work-based consensus mechanisms.

5. The cycle of information for blockchain

The delicate operation of translating thermodynamic terms into terms compatible with blockchain technology is now being attempted. We choose to adopt the point of view of the information cycle. Rather than an energetic entity, we prefer an informational entity. We start by defining five working hypotheses, in order to start from a framework: I make the following hypotheses:

Hypothesis 1. By way of illustration (in comparison with the Carnot heat-engine), the consensus process is compared to the energy cycle of an imaginary machine called: Blockchain Engine.

Hypothesis 2. Therefore, the resulting information cycle is not centered on the transaction process but on the consensus process.

Note: it is possible to compare with the TCP/IP protocol used for the Internet network. TCP validates IP through a mechanism of acknowledgment. For blockchain there is a couple consensus/transaction, but the big difference is that the validation for the blockchain is done in a decentralized environment.

Hypothesis 3. (Informational disorder). This parameter is related to the geographical configurations of the decentralized network of nodes.

Example :
• Regular position of nodes (weak disorder)
• Random position of nodes (strong disorder)

Hypothesis 4. (Informational quality). This parameter is related to the quality of meaning associated with the information.

Example :
• Case 1 : Two plus two is four (good quality)
• Case 2 : How much is two plus two ? (medium quality)

• Case 3 : Two plus two is five (poor quality)

At this point, it is necessary to keep in mind the approach of this document consisting in bringing together the information cycle of the blockchain and the concept of thermodynamics, in order to create an original model: the Blockchain Engine and its cycle. We can deduce the following table:

Thermodynamic cycle	Temperature T	Entropy S
Blockchain cycle of information	Informational quality	Informational disorder

Figure 4: Comparaison blockchain/thermodynamic cycle

We can now introduce the information cycle diagram of the Blockchain Engine, representing the informational quality as a function of the informational disorder.

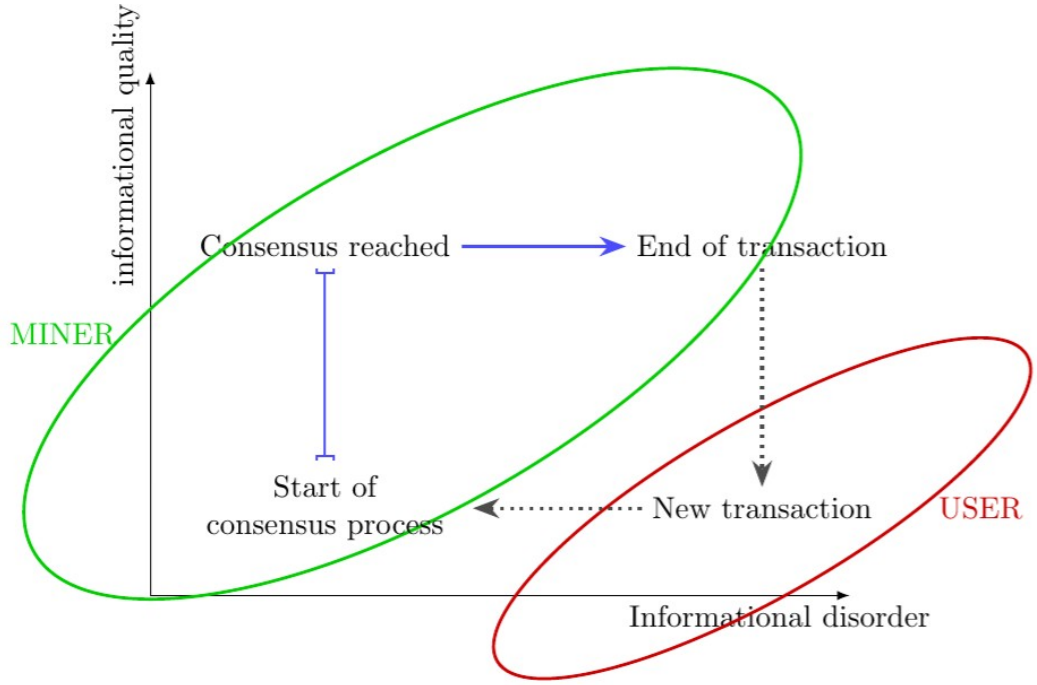

Figure 5: Ideal cycle of information for blockchain

How to interpret figure 5 ? we can see that there is an informational cycle : the information follows the different steps of the consensus process. However, there is a moment when the transaction ends and you have to wait for the start of a new transaction when a new user initiate a new transaction : this is the necessary condition for starting a new consensus process. However, this part of the cycle represented by the red lozenge-shaped is outside the cycle, because it is outside the consensus process. Thus the cycle of information is cut at a certain moment and it is for that reason that it is represented in dotted in figure 5. The cycle itself is the zone represented in the green lozenge-shaped. In fact, the off-cycle zone (in red) nevertheless constitutes a particular zone of the cycle.

6. The problem of the loss

6.1 Case of heat engine

The first law of thermodynamics states that the total energy of a system (sum of kinetic and potential energy) is constant. However, this is true only for frictionless systems. Frictions represents a loss preventing the system from returning to its initial energy state, that is to say to be reversible. For this reason, the Carnot cycle represents an ideal reversible machine. A macrostate of a system consists of of a very large number of microstates, which are characterized by the specific spatial and energetic arrangement of the particles. In the case of the blockchain, what could alter the information cycle? What is the equivalent of a microstate ?

6.2 Case of blockchain

What is the state of a blockchain ? There are divergente definitions, Tran and Krishnamachari [6] write that the blockchain state consists in the case of PoW of the set of current UTXO (Unspent Transaction Output) transactions. However, as part of the approach developed in this document, I favor that the state of the blockchain is the state of the ledger at a given moment. This implies that when a new block is created and is added to the chain, it creates a new state of the leger. However, note that a state refers to the ledger in its totality. It is a global parameter. We need a local parameter, local to a node, and for this reason I introduce above the definition of the micro state as a new hypothesis of work:

Hypothesis 5 (Informational microstate). A microstate is the ledger state, but locally to one particular node.

It is recalled that in the case of the PoW, the chain itself, ie the ledger, is hosted locally on all the machines constituting the nodes of the network. These nodes are geographically dispersed. The notion of the ledger's microstate is therefore linked to a geographical entity: a specific node. The following figure incorporates the issue of loss.

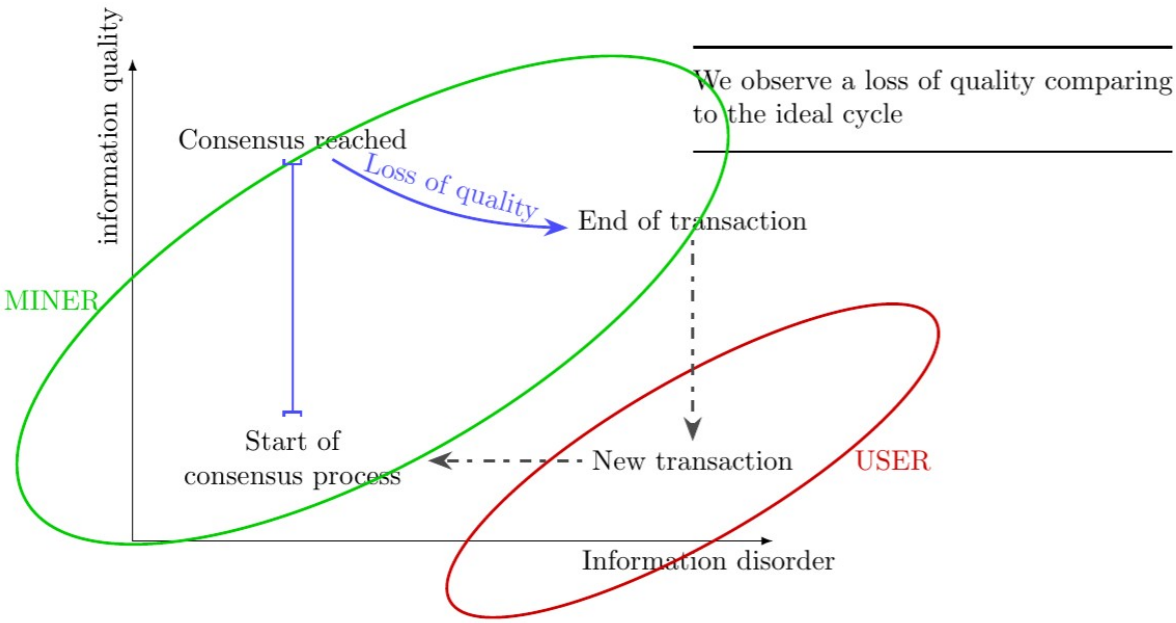

Figure 6: Practical cycle of information

How to interpret this figure ? We have seen that the difference between figure 5 and figure 6 is that in figure 6 there is a loss of informational quality. This loss of quality occurs when the level of disorder increases. In the ideal case, an increase in disorder does not necessarily mean a loss in quality. But in the practical case, it is an undesired event but which can occur. Indeed, the multiplications of minors involved multiplies the risks of non expected events. Here are some examples that apply to proof of work :

- There can be a natural fork : for some reason, two forks are built at the same time because there are two miners solving the puzzle in a short times : there are two parallel chains.
- There may be a fork due to a dishonest miner (51% attack).
- Different types of errors are possible during the construction of the block by the miner.
- In a general way, this phase of broadcast is a phase of vulnerability for the blockchain.

Concerning others consensus mechanisms, we know that we can classify consensus mechanisms in two categories :

- Those who favor safety.
- Those who favor liveness.

A typical example of consensus mechanism that favors safety is the Byzantine agreement, we know we will get a consensus, but we do not know how long it will take. A typical example of consensus algorithm that favors liveness is PoW, because it is sure to get a consensus in about 10 minutes, but the creation of a fork (accidental or consequences of a 51% attack) is possible. There are many consensus algorithms, but the verification of the existence of a cycle could be done by segmentation in two categories : safety and liveness. The ability of the practical cycle of the blockchain to move closer to the ideal cycle after drifting away from it is a mark of its resilience.

7. Conclusion: possible future research

Data governance involves informational resilience. This can be interpreted through an informational cycle as performed in this document. However, certain difficulties inherent in the concept of resilience exist, in particular the difficulty of finding tools to evaluate resilience. A fundamental point is the importance of the consensus mechanism in blockchain technology and the need to experiment across categories of use cases, as implementations of consensus algorithms are different across use cases Finally, here are some strong ideas :
• The notion of data flow can be developed to describe the information flows of a blockchain, as an innovative approach.
• Some concepts can be inspired by the physical sciences to imagine new models, considering the blockchain as an energy system, and this could constitute a research axis in its own right.
Note that there have been few major new developments in work-based consensus mechanisms since 2008, still dominated by bitcoin's historical PoW mechanism. However, avenues of research are being explored to limit energy consumption such as PoUW, Proof Of Useful Work, or the use of renewable energies. This, if successful, could revive the momentum of the family of work-based consensus algorithms.

References

[1] Stéphane Caporali. Time, Consensus and Governance by Design for Blockchain and DLT. 2020.
[2] ISO 22739:2020(en), Blockchain and distributed ledger technologies — Vocabulary. https://www.iso.org/obp/ui/fr/iso:std:iso:22739:ed-1:v1:en. (Accessed on 03/15/2023).
[3] L. Lamport. Proving the Correctness of Multiprocess Programs. IEEE Transactions on Software Engineering, SE-3(2):125–143, 1977.
[4] Satoshi Nakamoto. Bitcoin. A peer-to-peer electronic cash system. Bitcoin.–URL: https://bitcoin. org/bitcoin. pdf, 4(2):11, 2008.
[5] Stéphane Caporali. Governance with Consensus Mechanisms for Blockchain : Overview and Trends. 2022.
[6] Duc A. Tran and Bhaskar Krishnamachari. Blockchain in a Nutshell. arXiv e-prints, pages 7,12–13, April 2022. url=https://arxiv.org/pdf/2205.01091.pdf(visited 2023-04-18).
[7] General Assembly. Sustainable Development Goals. SDGs Transform Our World, 2030:6–28, 2015.
[8] Jerrold E Marsden and Tudor S Ratiu. Introduction to Mechanics and Symmetry: a Basic Exposition of Classical Mechanical Systems, volume 17, page 29. Springer Science & Business Media, 2013.
[9] Jennifer Coopersmith. Energy, the Subtle Concept : the Discovery of Feynman's Blocks from Leibniz to Einstein. Oxford University Press, New York, cop. 2010.
[10] Renaud Gicquel. Modéliser et simuler les technologies énergétiques : conversion thermodynamique de la chaleur. Les cours. Mines ParisTech, Paris, 2017.