BLOCKCHAIN AND SMART CONTRACT: LEX CRYPTOGRAPHIA ?

Denis PHILIPPE
Attorney at Law, barred in Brussels and Luxembourg
Professor at the Catholic University of Louvain
Visiting Professor at the University of Paris Ouest.

Table of Contents

I.   BLOCKCHAIN

A. *Definition and main characteristics*

A blockchain is a digitized, decentralized, public ledger of all transactions. Constantly growing as 'completed' blocks (the most recent transactions) are recorded and added to it in chronological order, it allows market participants to keep track of digital currency transactions without central recordkeeping. Each node (a computer connected to the network) gets a copy of the blockchain, which is then automatically[1] downloaded.

The most important actors are Bitcoin and Ethereum. But this article will focus on the relation between contract, clauses, and smart contracts, and not the legal regime.

B. *The advantages of blockchain are:*

- It is immutable: you cannot falsify the blockchain; it is an important element of trust.
- It is time stamped.
- It is decentralized: it is a peer to peer mechanism (*see table 1*), but it is possible to limit the access to a certain number of persons, owners of a public key (the peers). To have access, you also need to have a private key; the user is the sole person knowing the access code of the private key and this key must be kept carefully; if you lose your private key, you also lose the assets you put in the system, such as, your bitcoins.
  - In some important operations, there are multiple keys. The public key can be anonymous, and you can use a pseudo.
- It is abundant: there is no limit in the creation of blockchains.
- It is transparent: everybody can have access to the successive operations.
- There is no intermediation any more. Thus, the blockchain is libertarian: code is law.

---

[1] See O FLYNT, *Smartcontracts,* Investopedia ; P. DE FILIPPI & A.WRIGHT, *Blockchain and the role of code* Harvard University press 2018 p.13; Maciej HULICKI the legal framework and challenges of smart contract applications; TWDVXXVZ/SmartLaw2017_paper_3.pdf. TAPSCOTT, *Blockchain revolution How the technology behing bitcoin is changing money, business and the world,* PInguin, 2016; https://www.eublockchainforum.eu/sites/default/files/reports/20180727_report_innovation_in_europe_l ight.pdf (Eu Level) ; H. JACQUEMIN & Y. POULLET, Blockchain: une revolution pour le droit, *J.T.,* 2018, pp.801 à 819.
On the mechanism of the blockchain, see https://anders.com/blockchain/
https://www.youtube.com/watch?v=JskDZ8brPu8

[2] Joshua A.T. FAIRFIELD, 9-2014 Smart Contracts, Bitcoin Bots, and Consumer Protection, *Washington and Lee Law Review on line*, 71/2, p.35.We can also mention the *Distributed Automated Organizations* (DAO).: *a bundle of smart contracts, cumulating in a set of governance rules that are automatically enforced and executed through blockchains* The blockchain is thus regulated by ab autonomous system of rules. See H. JACQUEMIN & Y. POULLET, Blockchain: une revolution pour le droit, *op.cit.,* n°8.

Table 1

CENTRALIZED (A)   DECENTRALIZED (B)   DISTRIBUTED (C).
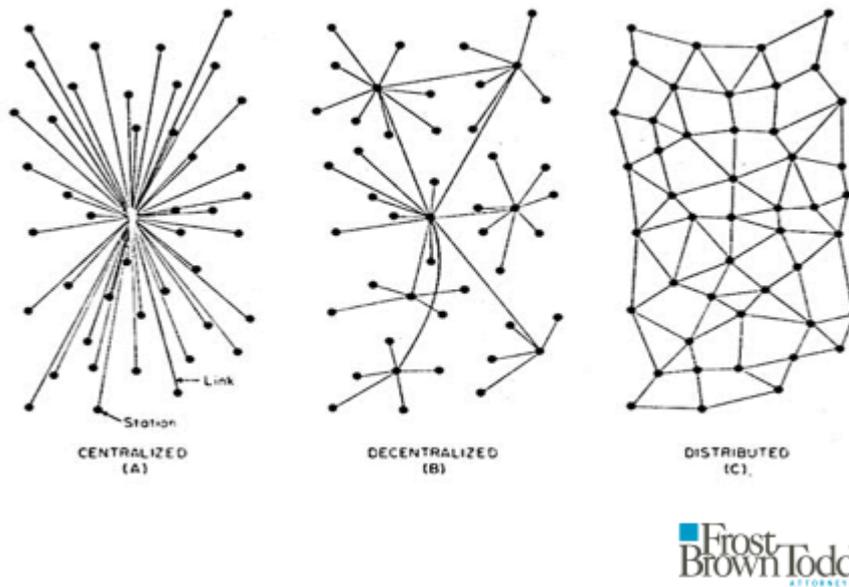
The blockchain is based on a working protocol.[2]

The trust function lies in the blockchain mechanism.[3]

C. Functions

Blockchain is used more specifically for cryptocurrencies (we will speak shortly on this because it has already been apprehended by many authors).[4] Let us already observe that in order to invest in cryptocurrencies, you need to have a wallet which you can use to make investments.

The blockchain can subsequently replace the trust party. Many persons play the role of trust persons in our society, such as, the bank, the notary, the auditor, the accountant. These persons will have to reassess their role.

For instance, the intervention of a notary could be replaced by a blockchain where all the acts are registered. The land registry can be replaced by a blockchain where all operations of sale

---

[2] Joshua A.T. FAIRFIELD, 9-2014 Smart Contracts, Bitcoin Bots, and Consumer Protection, *Washington and Lee Law Review on line*, 71/2, p.35.We can also mention the *Distributed Automated Organizations* (DAO).: *a bundle of smart contracts, cumulating in a set of governance rules that are automatically enforced and executed through blockchains* The blockchain is thus regulated by ab autonomous system of rules. See H. JACQUEMIN & Y. POULLET, Blockchain: une revolution pour le droit, *op.cit.,* n°8.

[3] Ibid.

[4] See P. DE FILIPPI *op.cit.*

and acquisition are registered on a chronological basis. In this configuration, the notary could be the certificatory of the well-functioning of the blockchain.

The blockchain will allow the development of e-government, land register, shares register, crow funding, keeping of digital assets, supply chain management, supply of electricity coming for instance from renewable energy.

It could also be used to auto-execute European standard forms, such as the European Certificate of Succession which gives authoritative information to banks and land registries, for example on heirs and their inheritance rights.

DLT (distributed ledger technology) is already used to replace some back-office functions of banks and insurance providers.[5]

D. Blockchain and mining.

The miners validate the transaction.

To add new blocks, require the respect of a specific procedure and all blocks require a valid hash. The hash begins with a specified number of leading zeros and the hash contains a lot of characters and the generation of a valid hash require repeated calculations.[6] These calculation (game of trial and error) are called mining. When the miner has found the valid hash, they communicate it to the network. The block is then added to the other blocks. There is a consensus; the more parties on the blockchain, the more difficult it is to compromise.
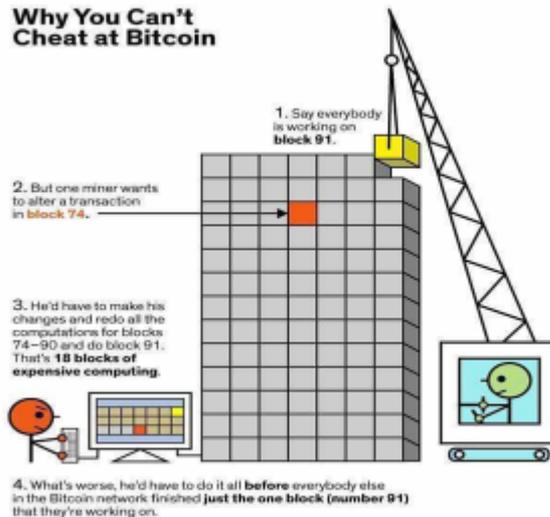
Table 2
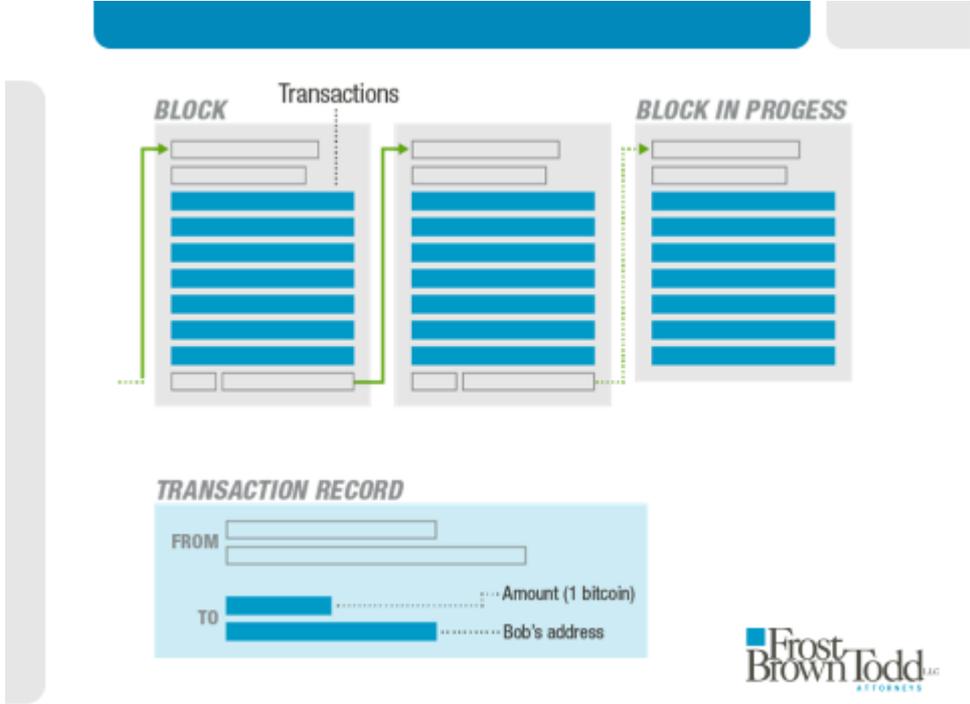
[5] TAPSCOTT, *Blockchain revolution How the technology behind bitcoin is changing money, business and the world,* Penguin, 2016.
[6] P. DE FILIPPI a.o. *op.cit.*, p.23

Table 3

Why You Can't Cheat at Bitcoin

1. Say everybody is working on **block 91**.

2. But one miner wants to alter a transaction in **block 74**.

3. He'd have to make his changes and redo all the computations for blocks 74–90 and do block 91. That's **18 blocks of expensive computing**.

4. What's worse, he'd have to do it all **before** everybody else in the Bitcoin network finished **just the one block (number 91)** that they're working on.

Frost Brown Todd ᴸᴸᶜ ATTORNEYS

A split into multiple copies occurs "when different portions of the network add a different block to the blockchain."[7] In the cryptocurrency world, the miner is remunerated with bitcoins.[8]

The next question arises: is the blockchain an independent legal entity,[9] but this goes beyond the scope of this article.

E. Disadvantages

a) The mining consumes electricity; millions of tries must be operated.
b) The cybersecurity; in the blockchain Ethereum, 50 million have been stolen due to a defect in the programming of a smart contract; it was not the blockchain Ethereum which was hacked, but a peripheral application; we know that millions of bitcoins have been stolen due to cyber fraud.[10] Due to this defect, the consensus necessary for the

---

[7] Ibid. p.24.
[8] J. HAIRFIELD, *op.cit.* p 37.
[9] See the planetoid, which received bitcoins and can pay on her own artists.
[10] See also in the consumer transaction, J. HAIRFIELD, *op.cit.*, p.45. However the blockchain presents more guarantees than the payment by creditcard. It is possible to make a sale trough an automated agent and the identify of the consumer will be kept secret. See J. HAIRFIELD, *op.cit.*, p.46.

good functioning of the blockchain disappeared; a fork was created and the blockchain has been divided in two blocks.

c) Privacy; due to the fact that all information is public (at least in public blockchains), even if you put a pseudo in your private key, privacy can be endangered.[11] We can give a simple example: the GDPR foresees in a right to be forgotten: how would it be possible to implement this right in case of an immutable mechanism.[12]

F. Legislation.

Blockchain has been recognized in different countries.[13] In Luxemburg, a draft law has been submitted by the Minister of finances on September 26, 2018,[14] and effects can be registered and transferred by the mechanism of blockchain.[15] Tokens are digital assets registered on the blockchain. Various countries organize or will organize rapidly the legal regime of tokens. The ICO (public offering of tokens) is or will be regulated in various countries.[16]

II.SMART CONTRACTS

A. Definition.

A smart contract is a set of promises, specified in digital form, including protocols within which the parties perform on these promises:[17]

"Smart contracts exerting the blockchain technology can allow for a system of digital and open transactions between network users within a decentralized database."[18]

The following slides explain the difference between a smart and a traditional contract:

---

[11] See www.eublockchainforum.eu/sites/default/files/reports/20180727_report_innovation_in_europe_light.pdf, p.16. H. JACQUEMIN & Y. POULLET, *op.cit.*, n°27 a.f.

[12] . H. JACQUEMIN & Y. POULLET, *op.cit.*, n°30 a.f.

[13] See for instance the new Maltese legislation dd. 1 August2018.

[13] See for instance the new Maltese legislation dd. 1 August2018.

[14] 7363.

[15] See In France, Article L 223-12 Cmon & fi (coming from the ordonnance dd. April 28, 2016; Loi Sapin 2, December 9, 2016, article 120; both provisions define blockchain as a "shared electronic recording device."

[16] It is accepted as a security in the US; regulated in Malta, will be regulated in France and Switzerland; banned for instance in China.

[17] Nick SZABO, Smart Contracts: Building Blocks for Digital Markets, 1996.

[18] Maciej HULICKI, *op.cit.* n°1 who quotes:R. BECK, C. MÜLLER-BLOCH, Blockchain as Radical Innovation: A Framework for Engaging with Distributed Ledgers as Incumbent Organization, Proceedings of the 50th Hawaii International Conference on System Sciences, 2017, pp. 3-4.

Smart contracts

- Parties reach an agreement,

- which is reduced to binary,

- then written into code,

- hashed

- and submitted to a blockchain.

- The code is executed on the blockchain,

- which triggers events according to the agreement.
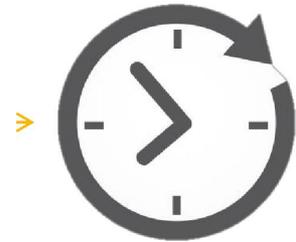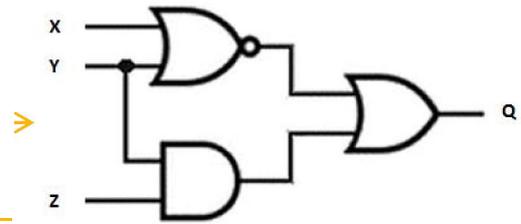
The following slides explain the difference between a smart and a traditional contract:
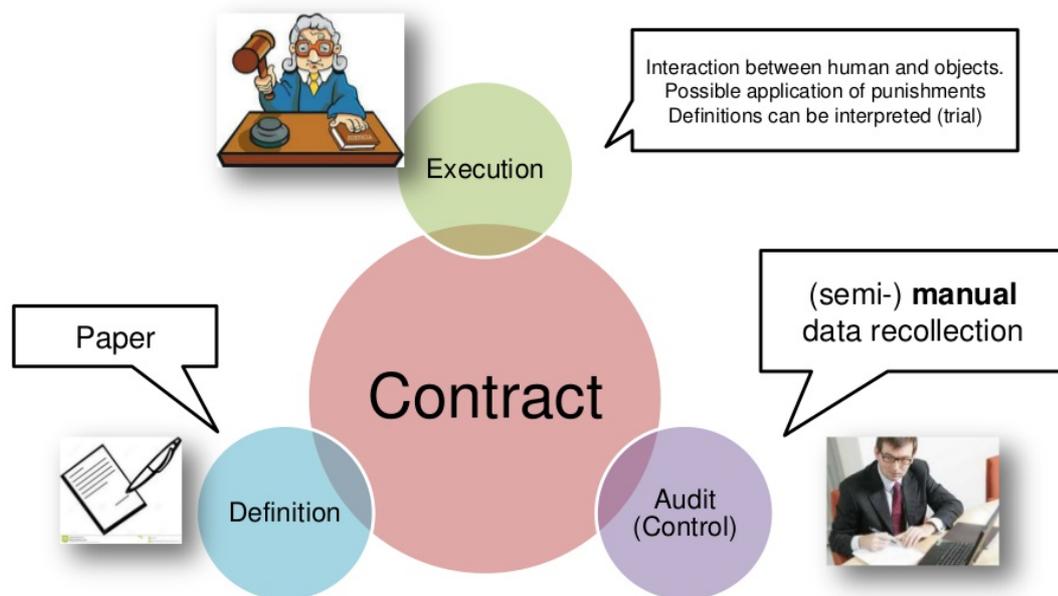
March 9, 2017, This is the Title 4:
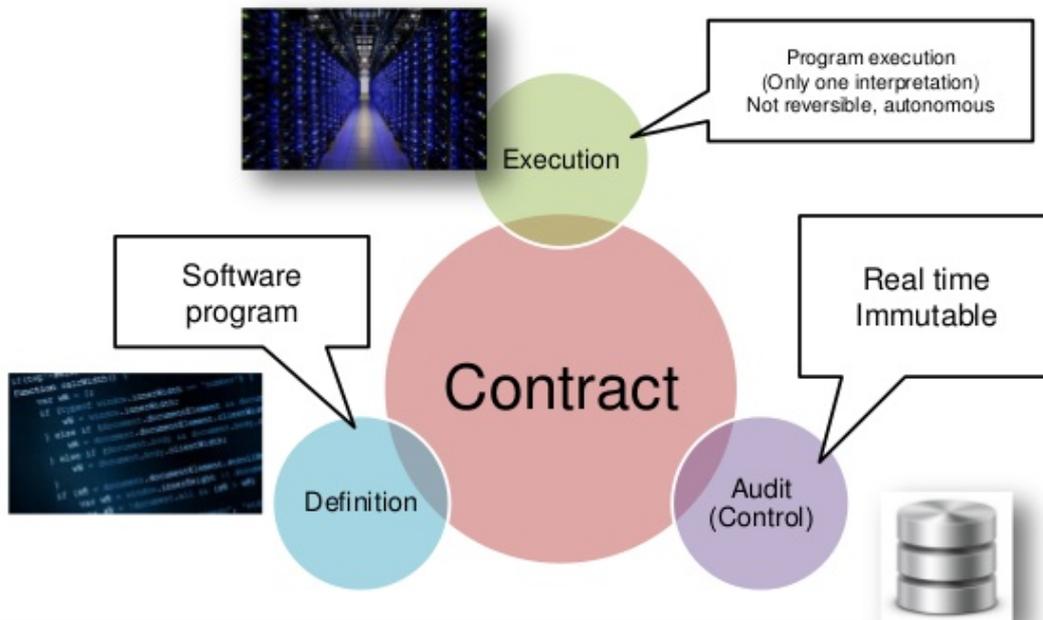
• Parties reach an agreement,
• which is reduced to binary,
• then written into code,
• hashed
• and submitted to a blockchain.
• The code is executed on the blockchain,
• which triggers events according to the agreement.[19]

---

[19] See J. TAN, Olswang, slide 4.

Thus, a smart contract is an event driven functionality. It is autonomous: software developer who created them need not actively maintain, monitor, or even be in contact with them while they operate[20]

In the performance of the smart contract, the obligation is inserted in a code using a strict and formal programing language. There is no reliance on the trust of the person to perform the contract. The contract is based on an algorithm. The performance can be fueled by data which is in the blockchain.

The implementation of the smart contract is preceded by a protocol which defines the main terms of the functioning of the smart contract.[21]

B. History.

The smart contract was conceived by Nick Szabo in a paper "formalizing and securing relationships on public networksHe explained that cryptographic protocols could make it possible to write computer software that resembled contractual clauses and would narrow

---

[20] See PERKINS COLE, Legal aspects of smart contracts application, 2017, J.DAX HANSEN & C.REYES, p.3.
[21] E. LEROUX & P. BRULEZ, Smart contracts and blockchain technology, uitdagingen in het contractenrecht, in *Le droit des affaires en évolution (Evolving Business Law),* coord. M. BEYENS,Larcier, 2018, p.189.

opportunities to terminate its performance obligations. In the following years, computer based contractual languages has been studied by scholars.

Computerized financial contracts were conceived in the late nineties. [22] More recently in 2012, Professor Harry Surden explored the creation of computable contract terms.[23]

With the growing of bitcoin, there was an increased interest in transforming legal agreements into code.[24] Technology was provided by blockchain based protocols and with the blockchain technology, parties can enter into a contract by using code and they use software to manage the contractual performance.

C. Advantages.

The smart contract presents the following advantages:

- Reduction in costs and time of the transaction;
- Smart contract offers predictability and auditability. Its trace is public and immutable. A smart contract can interact with other smart contracts.
- Transparency;
- Performance is automatic and thus safer;[25] parties know that they cannot change the terms of the contract, and they have to be sure that the contract can be implemented automatically without any discussion.[26]

D. External event: Oracle.

The performance is possible by using a trusted third-party source called Oracle. Oracle is an individual program that stores and transmits information from the outside world providing a means for blockchain based systems to interact with real world personnel or external events.[27] For example, they can be linked to an index of information like temperature. Oracle can also support dispute resolution. The Oracles permit to adapt the contract, to changing conditions in real time, for instance parties can modify payment flows or adapt contracts to receive new information.

E. Relations between the classical contract and the smart contract

---

[22] P. DE FILIPPI & A.WRIGHT, *Blockchain and the role of code* Harvard University press 2018 p.75.
[23] H. SURDEN, Computable contracts University of California – *Davis law review* 46 (2012: 629-700).
[24] P. DE FILIPPI & A.WRIGHT, *op.cit.* p.74
[25] E. LEROUX & P. BRULEZ, *op.cit.* p.192.
[26] See for a comparison between smart contracts and bank guarantee and documentary credit, . H. JACQUEMIN & Y. POULLET, *op.cit.*, n°48.[27] P. DE FILIPPI op.cit .p75.
[27] P. DE FILIPPI op.cit .p75.

a) Consent

First off, the parties must negotiate the terms of their agreement. When they agree, they can trust the performance of this contract to a smart contract.[28]

At a certain moment in time, even if the contract is performed automatically, the parties must have expressed their consent by a computer formality or by the consent to a protocol. Thus, there is then a valid legal contract. We know that the consent can validly be expressed electronically.[29]

We can compare this to framework contract. But a framework contract is a contract which establishes the general terms of specific contracts which will be entered into force in the future. In smart contracts, consent is expressed at the beginning in the protocol and the implementation occurs in an automatic way. But does the automatic succession of contracts reflect a valid agreement of parties for each contract? It has been disputed [30] but if parties have *agreed* that *successive* operations can take place after they agreed on the original contract (protocol) we do not see how one of the contracting parties can deny their consent to these successive operations. However, the danger is that people who express their consent on the computer, do not always realize the consequences of this self-executed program. But in principle, a contracting party must not sign a contract when she does not understand the scope and the terms of the contract. Furthermore, the performance of a contract can have different steps. We can take the following example: you lease a holiday home at the beach. You receive the entry code when the payment has been registered. Afterwards, the house was in a very bad state and it was not possible for you to live there. Of course, even if there was a smart contract related to the performance of the contract, you can still claim the annulment of the contract on the basis of mistake.[31]

Legal problems can arise when minors participate in the process. Because the contracting party, through the blockchain, does not know the identity of the co-contracting party, devices must be found to be sure that the contracting party has the legal capacity to enter into the contract. The blockchain protocol organizing the blockchain must take this aspect into consideration. In addition, the specific rules for consumer contracts must apply.[32] For instance, the possibility for a consumer to withdraw within fourteen days must be foreseen expressly in a distance contract.

b) Kind of contracts.

Examples where smart contracts are or could be used.

Use and lease.

For instance, you rent a bicycle in the city in a bike park; when you detach the bicycle, the payment is made simultaneously.

---

[28] E. LEROUX & P. BRULEZ, *op.cit.*, p.203.
[29] E. LEROUX & P. BRULEZ, *op.cit.*, p.202 ; article XII.15 of the economic code.
[30] E. LEROUX & P. BRULEZ, *op.cit.*, p.204 and the authors quoted by them.
[31] I will not enter into details but termination could also be claimed due to non conformity of the house.[32] Ibid. p.206.
[32] Ibid. p.206.

Sales and operation with tokens

Tokens are investment instruments to buy bitcoins; ICO (subscription of tokens) are known as an important development and the transactions of tokens are the most frequent smart contract.[33]

Sales contract of land.

The amount is paid at the transfer of property through the blockchain. A connection with the land registry will be organized so that the registration will occur at the same time as the payment of the price. Authorities hope to reduce fraud through smart contracts which are transparent.[34]

Transport.
In air transport, if the plane registers a delay of more than 20 minutes, an amount of 200€ is paid automatically on the account of the passenger.

Keeping of digital rights

The author automatically receives the royalties when a book is bought in a library.

Fintech

We can give more sophisticated examples and address the fintech.

You go to a leasing company; the car is open when you make the first payment and the leasing fee is paid automatically every month. If you do not pay the rent, the car stops automatically. The same applies for traditional loan agreements; the smart contract allows the conclusion and the control of the performance of the obligations of the borrower and in case of non-payment, the entirety of the amount can be claimed automatically (for instance direct payment to the bank of the amount of the guarantee).

In *investment,* smart contracts are used for the exchange of tokenized assets. Fundraising can occur through tokens.

And *share certificates* can be issued through smart contracts.[35]

The *supply chain* apprehends the creation, distribution of goods, to the finished product, to the consumer. Due to globalization, supply chains become more opaque.[36] The traceability cannot be guaranteed. Smart contracts can offer a suitable remedy.

In *international transport* by container; you can follow the container and all operations (customs, duties, payment of the carrier at arrival,…) are done automatically.

Insurance: the control of the payment of the premium is guaranteed.

---

[33] See PERKINS COLE, Legal aspects of smart contracts application, 2017, J.DAX HANSEN & C.REYES., p.6.
[34] Ibid. p.10.
[35] Ibid.
[36] Ibid. p.8.

Smart contracts can be also multisigniture[37]and underly more complex contracts.

c) Kind of clauses.

Which can be inserted in a smart contract? *Operational* clauses are readily capable of being expressed as Boolean logic. As a result, they are highly susceptible to being machine-automated.

We can mention the following clauses:

- A clause that requires an amount to be payable on a payment date equal to the product of a calculation amount, a floating rate (plus or minus a spread) and a day count fraction; it is transformed in algorithms.
- The smart contract can be accompanied with a *condition precedent* for; for instance, a guarantee of performance to be provided before the entering into force of the contract.

These clauses which can be checked on a computerized way can be easily inserted.

Operational clauses can be contrasted with clauses that *do not embed such conditional logic* but that, in some respect, relate to the wider legal relationship between the parties. We can give the following example:
• A clause that dictates that when making a decision or a determination, the person making the calculation shall do so in good faith and in a commercially reasonable manner;

Such clauses are patently of a different nature to operational clauses, although the boundary line is sometimes difficult to draw.

Non-operational clauses are less susceptible to being expressed in pure Boolean logic. However, this does not mean they could not be expressed in a more formally that would allow computer software to interact with them in a useful manner.[38]

We can further discuss some clauses often present in contracts.

a) *Force majeure clause.*

This clause exempts the debtor of his liability for nonperformance when this nonperformance is due to new unforeseeable circumstances which render the performance of the contract impossible. The effects are the termination of the contract when the performance becomes definitively impossible and suspension when the obstacle is temporary.

Can force majeure be organized in a smart contract? Some circumstances can be apprehended by an Oracle; for instance, we can foresee that when the temperature falls below -20° Celsius, the services must not be delivered; thus, through an Oracle, which gives the temperature, this provision can be executed automatically. But, in international contracts, renegotiation is often

---

[37] TAPSCOTT, *op.cit.*, p.103.
[38] Voy. ISDA Linklaters, White Paper, Smart contracts and Distributed Ledger, Legal Perspective, p.11.

the traditional effect of force majeure and renegotiation cannot, at this stage, easily be organized through smart contracts.

b) The *hardship clauses* allow the adaptation of the contract when new unforeseeable circumstances occur which render the performance of the contract excessively burdensome.

This clause can hardly be inserted in a program because it implies a renegotiation of the contract.[39] However the clause can in certain hypotheses be in a software program; for instance, if the price of raw materials increases by 20% what can be measured through an oracle, the program can foresee that the sales price will also increase by 20% automatically.

c) *Representations and warranties*

Representations and warranties give some assurances to the contracting party related to the underlying matters or facts that are being presented in terms of contract, like the existence of the contracting party, her capacity to enter into the contract, the substance of the object of the contract.[40]

Some of the representations and warranties can be implemented in a smart contract; for instance, the existence of a company, the articles, the name of directors can be indicated through a connection to the trade register. But it will be more difficult to assess through smart contract that there are no disputes pending before the court.

Ontologies are a formal way of defining the structure of knowledge of a domain and the relationships between concepts. By modelling the information and relationships that are contained in a contract in a formal manner, it raises a wider range of possibilities for a useful application of computer technology to such a contract.

Take the example of a standard representation from a party that it is duly organized and validly existing under the laws of the jurisdiction of its organization or incorporation. This is not a statement of conditional logic and would not be susceptible to pure Boolean logic. It is a representation of a legal state. But if there were a sufficiently developed ontology for legal contracts, it would be possible to conceive a world where a computer could understand what is meant by the terms 'party', 'duly organized', 'validly existing', 'jurisdiction' and 'organization and incorporation', and could check automatically with relevant company registries whether this representation is correct at the time it is given.

This example is illustrative, however, because it immediately highlights some of the issues that would have to be resolved to arrive at a common ontology. What precisely does 'duly organized' mean? Is it a synonym for 'validly existing'? What is the difference between 'organization' and 'incorporation' and do we need both terms? Who would develop such ontology, and would there be common standards across all contracts, no matter of what type or legal system?

---

[39] E. LEROUX & P. BRULEZ, *op.cit.* p.204.
[40] D.PHILIPPE, Warranties & Representations Material adverse change, Faux amis et innovation, *DAOR,* n°98, 2011, pp. 255 to 274.

d) Interpretation of the contract.

When parties do not agree on the meaning or working of a clause or an algorithm, the smart contract gives little room for interpretation.[41] Smart contracts cannot easily introduce contextualization in the interpretation of the contract.[42] But ontology can also contribute to a better insertion of contextualization (for instance, exchange of letters between parties before the signature of the protocol) to interpret the contract.

e) Non-performance of the contract. Abuse of rights

i. Liability

What happens in case of a defective code or a wrongdoing in the working of the smart contract? Who is liable? Hacking has been possible recently through a software defect,[43] or through bugs in the program.[44] They have enabled the diverting of money (in one case $50 million was diverted).[45]

In principle, if you have a lease agreement incorporated in a smart contract conceived by the lessor, the lessor could be liable. If the service provider of the software is a subcontractor of the lessor, the lessor will be liable for his subcontractor. An exemption clause can be inserted in the protocol between lessor and lessee.

If it is a peer to peer contract where a smart contract conceived was put at disposal by a third party, this third party can be held liable. But this third party can also, which happens frequently,[46] insert an exemption clause in his contract putting the software at the disposal of contracting parties. Between parties, the defect is a force majeure case, but the most suitable solution is to insert a clause allocating the risks in the contract.[47]

But, more broadly, the person liable will be more difficult to identify due to the important number of actors and the complexity of operations in a blockchain.[48]

ii. Abusive remedies in case of non-performance.

We can take the next example already mentioned earlier. You lease a car under a smart contract. You forget to pay your monthly fee. As a result of the automatic performance and control, your car is stopped automatically in the middle of a cross road. You caused a traffic accident due to this abrupt interruption. Who is liable for the accident?

---

[41] E. LEROUX & P. BRULEZ, *op.cit.* p.201.
[42] Ibid.
[43] E. LEROUX & P.BRULEZ, *op.cit.*, p.214.
[44] See PERKINS COLE, Legal aspects of smart contracts application, 2017, J.DAX HANSEN & C.REYES.
[45] Ibid. p.5. RASKIN, *op.cit.* p.340; H. JACQUEMIN & Y. POULLET,*op.cit.*, n°31 a.f..
[46] E. LEROUX & P.BRULEZ, *op.cit.*, p.220 with a clause in Ethereum. But the authors wonder whether these exemption clauses will not discredit the reliability of smart contracts.
[47] E. LEROUX & P.BRULEZ, *op.cit.*, p.216.
[48] . H. JACQUEMIN & Y. POULLET, *op.cit.*, n°31 a.f
[49] M. RASKIN , The law and legality of smart contracts, *Georgetown law technology review,*2017, p.329.

First it is technically avoidable. The starter interrupter can be manually overridden with a code in certain instances in cases where life and limb are at stake. The creditor can give a sheet of a number overwrite codes, each of which can only be used once to prevent abusing the leniency for exigent circumstances. These common-sense exceptions to the power of the starter interrupters are included in best practices guidelines for the industry.[49]

If these best practices are not included in the software, the designer of the software and the creditor could be held liable.

f) Law applicable

This matter must be regulated in the protocol. Otherwise, the applicable law will be uncertain; People participating in smart contracts can be located all over the world and are sometimes not identified.
We know that on the basis of Article 4 of the Rome I Regulation,[50] the law applicable is the law of the country where the party required to effect the characteristic performance of the contract has his habitual residence.[51]

g) Dispute.

Dispute regulations are normally dealt with in the protocol, as the law applicable.
The protocol can foresee that "*In a case of dispute, parties can renegotiate the underlying arrangement and, case of failure of the renegotiation, go to court or arbitration panel.*"

Even if the performance is automatic, the competent judge can order all the remedies like termination by fault, damages etc.

But of course, the contracting party must have a name, and address; thus, when one party uses a pseudo, the possibility to enter into a dispute with her becomes more difficult.

Because the performance of the contract is automatic, the intervention of a referee judge will be less efficient because the contract is already performed.

Mechanisms inherent to the block chain can also be implemented. We mentioned earlier the multisignature smart contract where parties can determine the number of keys generated and the keys required to complete a transaction. Parties can agree to employ a third-party arbitrator to assist them in finalizing the operation. The operation needs two keys to complete the transaction and each of them has one key. Let us take as example, a sale between A, seller, and B, buyer. B received the goods but is unhappy with the delivery and refuses to give his key to A. Then both parties call upon C, the arbitrator, who holds the third key in order to settle the dispute. C, as an arbitrator, has a limited mission and has no access to the funds.[52]

---

[49] M. RASKIN , The law and legality of smart contracts, *Georgetown law technology review,*2017, p.329.
[50] Regulation 593/2008
[51] The regulation gives more details for different contracts. For the law of sales, it will be the law of residence of the seller (Article 4.1 a)).
[52] TAPSCOTT, *op.cit.*, p.162.

F. *Regulationand law.*

Code is law: authors allege that the traditional law is replaced by a new legal order: the code what is, in my opinion, not true.

I think that these new mechanisms cannot be ignored by the law and by the regulator. Consumer must be protected.[53] For instance, the service or product provider must be identified. Fairfield writes paradoxically that the disappearance of intermediaries can play a positive effect on the consumer because the sometimes-illicit behaviors of intermediaries will become evanescent. On another side, consumer must accept a list of terms and conditions which he cannot negotiate. However, there are programs (E-Bay) where the consumer can modulate his offer. In case of last-minute sale, then the price can be lower.[54]

Furthermore, public policy must be respected. Regulation and law must avoid the signature of smart contract dealings, for instance with the sale of drugs.[55] Besides an intervention of the legislator, maybe a regulator can be called upon; the regulator can check by controlling the operations of the smart contracts, whether these operations are in conformity with the law. The regulator can also give recommendations or issue guidelines on the terms and conditions.

Conclusions.

Smart contracts can revolutionize the contractual life.

Smart contracts are convenient for the contract whose performance is more or less automatic but at this stage, not convenient for complex contracts as joint ventures[56] or building contracts.[57] Authors also advise against the use of smart contracts for long term agreements where change of circumstances can arise.[58]

We have seen that some clauses cannot be organized automatically. Then maybe a framework contract (protocol) that contains the terms which cannot work via the software.

The technology will know a huge evolution in the next years and decennia among others thanks to the development of artificial intelligence. Maybe this article will be rapidly obsolete. Any what will not disappear is the necessity for regulation in this sector.

---

[53] Joshua A.T. FAIRFIELD, 9-2014 Smart Contracts, Bitcoin Bots, and Consumer Protection, *Washington and Lee Law Review on line*, 71/2, p.36. The author writes that the disappearance of intermediaries can play a positive effect on the consumer because the sometimes illicit behaviors of intermediaries will vanish.
[54] Ibidem, p.45.
[55] What seems to happen, see E. LEROUX & P. BRULEZ,*op.cit.*, p.208. and the cases mentioned.
[56] E. LEROUX & P. BRULEZ, *op.cit.*, p.198.
[57] E. LEROUX & P. BRULEZ, *op.cit.*, p.200. The authors write that the output of the building contract cannot be transformed in a code.
[58] E. LEROUX & P. BRULEZ, *op.cit.*, p.198.

Currently, the contractual basis of smart contracts remains in the protocol agreed upon, before the implementation of the smart contract. As we have seen, some specific contractual clauses must be inserted in the protocol. We propose that the consumer associations and the federation of industries work together on the drafting of an equilibrated contract.

Some functions or professions in the society will become superfluous because the trust function of these professions will be replied by the blockchain. But as long as there can be some uncertainties in the trustworthiness of the blockchain, professions can become the certification bodies; for instance, the notaries can certify the reliability of the blockchain registering the sales transactions of land.[59] More than certificatory, the notaries can make their own blockchain, they can be mediator or arbitrator in case of dispute and of course, advisors because a real estate transaction can be very complex.[60]

Currently smart contracts do not use artificial intelligence as such.[61] But we can expect that in a near future, artificial intelligence will be introduced to smart contracts and that new legal problems will arise, what will constitute a very interesting challenge a.i. for lawyers.

Do we live in the new world of the *lex cryptographia*? Is the judge is replaced by a code.[62] Is the law replaced by self-regulation?[63] We think that lex cryptographia must live in harmony with regulation and law.

---

[59] See de website van de Koninklijke Notariële Beroepsorganisatie (www.knb.nl) Home/Actueel/Nieuwsberichten 30 november 2017
[60] E. LEROUX & P. BRULEZ, *op.cit.*, p.199.
[61] E.LEROUX & P. BRULEZ, *op.cit.*, p.193.
[62] Alyssa HERTIG Code of Law; How Bitcoin Could Decentralise the Courtroom, www.motherboard.vice.com, 3 July, 2014
[63] RASKIN, *op.cit.* p.335.