European Journal of Privacy Law & Technologies



2019/1

G. Giappichelli Editore

European Journal of Privacy Law & Technologies

Directed by Lucilla Gatt

2019/1

G. Giappichelli Editore

European Journal of Privacy Law & Technologies
On line journal
Italian R.O.C. n. 25223

G. GIAPPICHELLI EDITORE - TORINO
VIA PO, 21 - TEL. 011-81.53.111 - FAX 011-81.25.100
http://www.giappichelli.it



The Journal is one of the results of the European project TAtoDPR (Training Activities to Implement the Data Protection Reform) that has received funding from the European Union's within the REC (Rights, Equality and Citizenship) Programme, under Grant Agreement No. 769191.

The contents of this Journal represent the views of the author only and are his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

Published Online by G. Giappichelli in June 2019
www.ejplt.tatodpr.eu

SMART CONTRACTS IN THE BLOCKCHAIN CONTEXT: WHAT HAPPENS?

Veronica Carriero

Abstract:

Thanks to the blockchain technology, the idea of an entire computer regulated contract has become a reality. However, only a careful study of the performance of this new contractual model will disclose all its advantage.

Key-words: Smart contracts

Summary: 1. Introduction. – 2. Smart contract and blockchain. – 3. Smart contract as a contractual model.

1. Introduction

The term "smart contracts" was created in the 1990s by Nick Szabo, a computer scientist, who defined it as a series of digitally fixed promises included in a protocol, with whose help the parties observe their commitments. The idea of Szabo was to enter into a contract that is completely monitored by a computer and without the assistance of agents [1]. It has been pointed out [2] that "the concept remained obscure for lack of the right technology" [3]. In recent years, especially by developing the blockchain technology, there has been a rebirth of the concept. The idea of smart contracts can be examined both in a broad sense and in a narrow sense. According to the first approach, a smart contract is deemed to be as a self-executing, computerized "if-then" relationship based on blockchain technology and with legal implications. According to the second one, any com-

[1] M. Fries, B.P. Paal (eds.), *Smart contracts*, Mohr Siebeck, Tübingen, 2019, 1.

[2] 'Not so clever contracts. For the time being at least, human judgement is still a better bet than cold-hearted code' [2016] The Economist (online).

[3] For further studies on the evolution of technological society and the informatic freedom see T.E. Frosini, *Liberté, egalité, internet*, Editoriale scientifica Naples, 2019.

puterized "if-then" relationship can be defined as smart contract, regardless of the deployment of blockchain technology [3].

2. Smart contract and blockchain

There are plenty of definitions for the blockchain, an efficient one is "a data storage system using linked sequential chunks of information. It is literally a chain of blocks designed to create an immutable ledger of transactions" [4]. This technology is capable of being used for many purposes including the creation and execution of smart contracts. The blockchain technology would implement the idea of an entire computer regulated contract, with no human intermediation. The fortune of the blockchain technology [5] lies in its special features. The mechanism is based on a process called "consensus" that regulates how information can be added to the shared storage in an orderly manner and by which "basic function of blockchains is to reliably share information among parties who may not trust one another. In other words, everyone can have his or her copy of a ledger and trust that all those copies remain the same, even without a central administrator or master version" [6]. Furthermore the system is distributed to the effect that every single node has a complete and accurate copy of the blockchain and there is no central control point [7]. Another trait is the autonomy: the blockchain technology relies on a peer-to-peer network and this fosters the execution of computer code in a manner that is independent of any one party [8]. The system is also immutable, resilient and tamper resistant: once information has been recorded to a blockchain it becomes immutable or at least exceptionally hard to change or delete because no single party has the power to modify or restore information saved on a blockchain or to shut down the execution of a smart contract once it has been implemented, unless allowed by the code [9]. Cryptocurrency based on the blockchain system ensures there is only one ledger with no contradictions by using a technique called "proof of work" that allows

[3] M. Fries, B.P. Paal (eds.), *Smart contracts*, n. 1.

[4] K. Werbach, *The Blockchain and the New Architecture of Trust*, MIT Press, 2018, 14.

[5] On the advantages of the blockchain technology in business *see* 'The promise of the blockchain technology. What blockchains may be able to do for your business, and what they can't' [2018] The Economist (online).

[6] K. Werbach, *The Blockchain*, n. 4, 7.

[7] K. Werbach, *The Blockchain*, n. 4, 96.

[8] P. De Filippi, A. Wright, *Blockchain and the Law. The Rule of Code*, Harvard University Press, 2018, 43.

[9] P. De Filippi, A. Wright, *Blockchain*, n. 8, 35.

the blockchain to be stored on every computer in the network at the same time and provides that each copy of the blockchain will be identical [10]. The information recorded is transparent and nonrepudiable in that anyone can download the entire blockchain and once a transaction occurs on a blockchain-based system, parties will find it difficult to refuse their involvement [11]. Furthermore, blockchain makes it possible for a person to store data or to carry out operations without revealing one's true identity because the system relies on digital signatures and key cryptography [12].

It has been pointed out [13] that in the life cycle of a blockchain-based smart contract there are different stages. The first one is the creation of the contract and in this phase it is defined and translated into a code. The second stage consists in "freezing" the software and adding it to the chain. The third step is the execution one: the software is read and implemented by the nodes. Finally, the smart contract is completed, information and transaction are recorded on the blockchain and the consensus protocol is validated.

3. Smart contract as a contractual model

Legal scholars have focused their attention on the legal nature, status and implications of the described mechanism. According to an authoritative doctrine [14], the position of a smart contract users is similar to the position of a receiver of "terms and conditions of a contract". Another approach [15] assumes that smart contract consists in a computer code with a contractual value.

It has been highlighted [16] that, unlike other contracts, a smart contract has a greater legal certainty and could ensure better that the outcome of the operation responds to the expectations of the parties. Furthermore, the smart contract can reduce the transaction costs, doubts of interpretation and increase the speed in the conclusion of the contract. Advantages would exist also in terms of trans-

[10] A. Rothstein, *The end of money. The story of bitcoin, cryptocurrencies, and the blockchain revolution*, Nicholas Brealey Publishing Boston, 2017, 43.

[11] P. De Filippi, A. Wright, *Blockchain*, n. 8, 37.

[12] P. De Filippi, A. Wright, *Blockchain*, n. 8, 38.

[13] M. Fries, B.P. Paal (eds.), *Smart contracts*, n. 1, 4.

[14] R. Pardolesi, A. Davola, '«Smart contract»: lusinghe ed equivoci dell'innovazione purchessia", 2019, 4, 195 ff.

[15] The Author reports a "technologic neutral" point of view: "*Aus technologieneutraler Sicht betrachtet versteht man hier den Smart Contract als Computercode mit vertragsrechtlicher Bedeutung*" in M. Fries, B.P. Paal (eds.), *Smart contracts*, p. 5.

[16] M. Fries, B.P. Paal (eds.), *Smart contracts*, *ivi*, p. 7 ff.

parency, traceability and monitorability of the transactions. The same Author points out that these smart contracts are neither "smart" nor "contracts". Smart contracts would not be smart because they are not capable to understand the language and they are not capable to assess in an independent manner external events that affect the execution of the contract: in this case is required a trusted third party source, commonly referred to as an "oracle", by which the blockchain system can interact with real world and react to external events. Moreover, smart contracts could not be defined as contracts in the technical sense: they consist in a sequence of orders incapable to take into account the environment and external facts which affect the process [17].

Regarding the weaknesses of a blockchain-based smart contract, one should consider that the described system ignores all the nuances of the language and this is all the more apparent in the open-ended contractual terms that outline performance obligation such as to act in "good faith" or to use "best efforts" to fulfil the obligations because it might be hard to define what is appropriate performance or because the most efficient manner of performance might not yet be predictable. "Act of God" as legal term cannot be translated into a code. It has been highlighted that open ended or ambiguous contractual provisions may result in more efficient contracts [18]. Furthermore, any undesirable transaction cannot be reversed nor is it possible to adapt the content of the agreement in case of external event modification, once the contract is effective [19]. It is possible that the best way to use this mechanism would be to create hybrid arrangements that combine natural language terms with smart contract translated in a code [20]. In conclusion, a smart contract is certainly a model of great interest and only a careful study of the performance practice of this model will reveal how to take full advantage of its capabilities.

[17] *Idem.*

[18] P. De Filippi, A. Wright, *Blockchain*, n. 8, p. 77 and note 24 for the source.

[19] M. Fries, B.P. Paal (eds.), *Smart contracts*, n. 1, 10.

[20] P. De Filippi, A. Wright, *Blockchain*, n. 8, 78.