

## 1. Current limitations of smart contracts vs Hypersmart Contracts

The notion of 'smart contracts' became a generic term as a result of the notoriety gained by the Ethereum blockchain and the increased traction on distributed ledger technologies. However, the idea has been around for a long time. Nick Szabo, the cryptographer known for his research on digital currencies, wrote an article about smart contracts as early as 1996. Mr. Szabo defined the term smart contract as 'a set of promises, specified in digital form, including protocols within which the parties perform on these promises'.

In his 1996 article, Szabo predicted that the digital revolution would drastically change the way we currently construct contracts. Szabo saw early on that computers were making it possible to run algorithms that used to be too costly, and believed algorithms eventually would be developed for what he termed 'smart contracts'. The blockchain-based smart contracts, or self-executing contracts, were developed to automatically and securely execute obligations and release cryptocurrency payments on the basis of very simple and rigid set of conditions (like for example, an option agreement with a triggering event or an escrow agreement) and without the need for intermediaries. Although several business opportunities arise from the use of the smart contracts, **important limitations** ought to be carefully taken into consideration.

Firstly, the current implementation of smart contracts on the Ethereum platform is not fully secured. The consequences of unsafe and short-sighted design choices on the programming languages can be fatal for many businesses. We have witnessed this in the unfortunate epilogue of the DAO. Since then, many other vulnerabilities of smart contracts have been reported (N. Atzei, 2017).

Secondly, in contrast with contracts concluded in form of action, speech or writing, a smart contract is 'just' a computer program built on code: it is still unclear whether it can be considered a contract from the legal point of view, whether it has parties or it is merely a matter of decentralized computer programming (Lauslahti, Mattila, & Seppälä, 2017). In addition, smart contracts are very "rigid" because terms & conditions are coded immutably and not subject to real-life variability and construalability – demanding adjustments that only humans can decide upon.

Yet another major issue is that like any other piece of code, a smart contract can be prone to defects. However, unlike any other piece of code, a smart contract is not patchable: hence, once it is deployed, if it contains a serious defect, the smart contract could be very harmful to any dependent system .

Additional limitation is related to the impossibility, by design, of changing the behavior of a smart contract in response to some external event (every change of state on a blockchain must be completely deterministic): this is in contrast with the fact that modern value chains are highly complex (think of the iPhone suppliers network worldwide) and require more and more A.I., Machine Learning and Big Data Analytics algorithms (here defined as 'Hypersmart Algorithms' or simply A.I. Algorithms) for stochastic and dynamic automatic optimization and execution of trillions of process-related transactions.

Indeed, **'transactions' instead of 'contracts'** would be a more appropriate term for describing smart contracts. Smart contracts are supposed to automate not only decentralized organizations but also existing centralized or distributed business models. However, although value chains can already be optimally and automatically run by algorithms in terms of flow of goods ("which product should be delivered from where, to whom and by what route"), the **exchange of information** (including documents) and **money** (payments) within such value chains is still suboptimal due to the lack of trust among independent participants and due to procedural constraints. As a result, the flow of goods is slower than what would be possible with A.I. Algorithms, which are so to speak 'constrained' by the cumbersomeness of the administrative and payments cycles.

The solution to this issue, which is unnecessary costly is the connection of A.I. Algorithms with Blockchain technology, creating the new concept of **Hypersmart Contracts**. Hypersmart Contracts optimize and automate complex business transactions, including the decentralized management of information and documents, and the instant release of cryptocurrency payments by successful execution.

As matter of fact, on November, 06 2017 an unidentified person deleted a smart contract upon which Parity multi-signature wallets' functionality relied, causing more than \$300 million worth of ether being locked. See: <http://read.bi/2hHcDiK> (last visited 18 Dec 2017). Pertinent to mention, Parity fixed a previous bug in July, which allowed \$32 million in Ether to be stolen.