frontiers in Blockchain

PERSPECTIVE
published: 03 February 2021
doi: 10.3389/fbloc.2020.553671

What Do We Mean by Smart Contracts? Open Challenges in Smart Contracts

*Maria G. Vigliotti**

Sandblocks Consulting Ltd., London, United Kingdom

Contracts regulate most of our professional and personal life: they enable modern society to operate. The term "Smart Contract," coined in 1994 by Nick Szabo, means different things to different people. This editorial perspective explores the meanings of the term "smart contract" and the challenges about the legality of "smart contracts." We are familiar with contracts written in natural language, yet our relationships with smart contracts is yet to be defined. The advent of blockchain technology seems to have accelerated the development and the opportunities for the adoption of smart contracts. The purpose of this editorial is to create an interdisciplinary section where computer scientists and members of the legal profession participate in a constructive debate around smart contracts to positively influence future development.

Keywords: smart contracts, blockchain, legal contracts, security of code, formal methods

OPEN ACCESS

Edited by:
Olinga Taeed,
Centre for Citizenship, Enterprise and Governance, United Kingdom

Reviewed by:
Nadia C. Fabrizio,
CEFRIEL, Italy
Reshma Kamath,
Blockchain Research Institute, Canada

***Correspondence:**
Maria G. Vigliotti
maria@sandblocksconsulting.co.uk

Specialty section:
This article was submitted to Smart Contracts, a section of the journal Frontiers in Blockchain

Received: *19 April 2020*
Accepted: *16 September 2020*
Published: *03 February 2021*

Citation:
Vigliotti MG (2021) What Do We Mean by Smart Contracts? Open Challenges in Smart Contracts. Front. Blockchain 3:553671. doi: 10.3389/fbloc.2020.553671

1. INTRODUCTION

In recent years, the term "smart" has become very popular: we live in "smart cities," we use "smart fridges" or "smart ovens," and of course, we could not function without our "smart phones."

The adjective "smart" means the object's functionality has been vastly improved by means of software applications i.e., part of the functionality has been automatized. The "smart oven" will cook food as his obsolete counterpart, but is can be switched on and off remotely and monitored from distance. A smart phone is a phone that enables us to call people without having to touch the pad, and it will perform other valuable (yet repetitive) tasks for us.

When it comes to a "smart contract," is it correct to conclude that it is a:

contract where some of its functionality has been improved by means of software applications?

To answer the question, we will investigate the history of smart contracts and answer the following questions

- Are smart contract really contracts?
- Who is using smart contracts?
- Can smart contracts be deployed only on the blockchain?
- What are the current open challenges?

2. ARE SMART CONTRACTS REALLY CONTRACTS?

To address the question whether (Vigliotti and Jones, 2020) a *smart contract* is really a *contract* requires the understanding of the term "contract." According to the law of England and Wales, a "contract is a legally binding agreement, which can be enforced in a court of law." Furthermore, a contract requires four elements:

1. Offer
2. Acceptance
3. Consideration, and
4. Intent to create a legal relation

An agreement stipulates clauses and sets out obligations among parties, however clauses' enforcement would happen outside a court of law. To summarize, all contracts are agreements, but not all agreements are contracts.

Most contracts are presented in written form as a customary way to keep evidence of the agreed clauses. In some cases, however, the law prescribes the form of the contracts: for example, selling a property requires a written contract i.e., an oral contract could not be recognized in the court of law. As the law of England and Wales doesn't always specify the form a contract, it would be possible for a piece of code satisfying the four conditions to be considered, at least in principle, legally binding. This hypothesis will need to be tested in the courts of England and Wales (The LawTech Delivery Panel, 2020). In other jurisdictions around the world, contracts have different status so whether a contract written in code is legally binding depends on the country's legal system. In some extreme cases, like in Italy, a need for new legislation could arise as opposed to judges' interpretation as in the law of England and Wales.

For the purpose of this article, we define a smart contract

as an agreement among multiple parties written at least in part in computer code

meaning that there exist a piece of software that executes, and in some cases enforces, some of the terms of the agreement. The terms of the agreement may or may not be *understood* by the participants.

3. WHO IS USING SMART CONTRACTS?

Many of us already use smart contracts, without realizing it! Contactless bank card's payments for tube, bus journeys, or bike hiring are examples of deployment of smart contracts. Traditionally, bike hire would involve physically signing a document explaining the price and conditions associated to the rental; a deposit could be taken to cover potential damages. The document constitute the physical evidence of the contract and the payment would be taken when the bike is returned. By contrast, when we use bank cards to directly hire "smart bikes" from docking stations located in a "smart city" like London, Paris or Berlin, the bike is released and the correct amount of money is debited from the bank account when the bike has been returned. The clauses of the contracts are automatically managed without the need of human intervention. There is a strong argument to be made for this type of transaction, not least because cutting out human involvement speeds up the process and reduces costs. The Internet has accelerated the deployment of "smart agreements": the Article 9 of the European Union's Electronic Commerce Directive (Directive on electronic commerce, 2000) requires all member states to ensure that their legal systems facilitates the deployment of electronic contracts. The EU Commerce Directive (Directive on electronic commerce, 2000) uses the term "electronic contract," which essentially covers definition of smart contracts deployed in the this article.

3.1. A Brief History of Smart Contracts

Nick Szabo, an American computer scientist, is thought to have first used the term smart contract in an article in 1994. He wrote (Szabo, 1994):

> A smart contract is a computerized transaction protocol that executes the terms of a contract. The general objectives of smart-contract design are to satisfy common contractual conditions (such as payment terms, liens, confidentiality, and even enforcement), minimise exceptions both malicious and accidental, and minimise the need for trusted intermediaries. Related economic goals include lowering fraud loss, arbitration and enforcement costs, and other transaction costs.

Szabo's main thesis is that contracts are essential for trust in functioning societies. Two years later Szabo observed (Szabo, 1996):

> Whether enforced by a government, or otherwise, the contract is the basic building block of a free market economy.

Since the 1990s, computer scientists and mathematicians have created the technical tools to automate contracts. More to the point some technology to enable early and rudimentary form of smart contracts already existed at the time when Szabo was sharing his thoughts with the world. Example of such technology is the DigitCash by Chaum et al. (1988), a payment system that protected users' privacy.

Furthermore, Szabo believed that to make smart contracts more valuable to society they need to be: verifiable, observable, and enforceable. In this way, smart contracts would be part of the fabric of society which would in turn lower legal barriers, slash transaction costs, cut the time to execute the contract, and provide an opportunity to create new types of businesses. Szabo was spot on in his predictions: today, as smart contracts develop and replace some traditional contracts, they are reducing costs and speed up execution, as the example of the bike has shown.

4. DEPLOYMENT ON THE BLOCKCHAIN?

If smart contracts are already in use, why there is so much discussion about smart contracts on the blockchain?

The association between "smart contract" and "blockchain" was popularized by the development of Ethereum blockchain[1]. Solidity, the programming language for the Ethereum blockchain, deploys the term "contract" instead of the programming term "class," to define small pieces of code that identify specific operations. Another reason for the increased popularity of the term "smart contract" is associated to the trust created amongst participants by the blockchain: smart contracts enable trust by allowing all participants to verify clauses of a contract [2]. To clarify this point further, let's return to our example

[1] See https://ethereum.org/ (accessed April 4, 2020).
[2] The assumption is that participants can read code.

of the smart bicycle rental. Someone renting a bicycle doesn't need to audit or even see the software that releases the bike and collects the payment. If something does wrong, for example a cyclist is overcharged, the rental company has a clear obligation: to repay what is owed. Legally, this is because the software forms part of an unwritten contract: consumers have rights under English or EU law that protects them; such protection exists regardless the ways in which the contract is implemented. In the case of the smart bicycle rental, the electronic payment software is simply there to speed up an otherwise laborious process. This highlights how smart contracts can be part of a bigger legal contract framework, where some clauses are automated. This is sometimes called smart contract code (Clack et al., 2016).

By contrast, a smart contract on the blockchain is taken at face value: it is piece of code that represents the terms of an agreement among parties. The obligations are enforced via the consensus process when the parties deploy the contract. A smart contract on the blockchain enables participants to:

1. Inspect the code to ensure it meets the agreed clauses
2. Be reassured that an agreed contract, once registered on the blockchain is tamper-proof
3. Be reassured (to a certain degree) the contract executes in the same way for all participants

It is a well-known fact that code contains bugs, and smart contracts are not an exception. There are several examples where small bugs in smart contracts have had detrimental impacts (Atzei et al., 2017; Magazzeni et al., 2017; Dingman et al., 2019; Tai, 2019). Computer scientists have developed several techniques to mitigate against bugs in software. As it is not possible to provide full assurance that bugs cannot be eliminated, the question is what is the impact of bugs in business? Who bears the responsibility in case an execution goes astray? These are some of the challenges, if, moving forward, we envisage a society where smart contracts are part of contractual relationships. Financial services are already moving in this direction (2017; 2018), and it is likely that over the next twenty years, other sector will deploy smart contracts too.

5. OPEN CHALLENGES

Smart contracts come in different shapes and forms, and they have evolved significantly since Nick Szabo described them for the first time in 1994. There are fundamental scientific questions and challenges already addressed by both solicitors and computer scientists alike (Clack et al., 2016; De Filippi and Hassan, 2016; Bod et al., 2018; De Filippi and Wright, 2018; Fenwick et al., 2019; Tai, 2019): if they are really new it is important that the computing and legal community come together and identify the unique features of smart contracts. The literature on the topics is rather vast, and Law Societies around the world are also taking positions (The LawTech Delivery Panel, 2020), and collectively, the literature presents the following challenges:

Legality Key questions:

- Is it possible to make smart contracts, where all the clauses are written in code, legal in their own rights in any legal jurisdiction?
- Is it possible that to speed up execution, some contracts will be partially written in code, and remain legally binding?
- What needs to change in the national or international jurisdictions for any of these scenarios to become a reality?
- Would this new technology require changes in the international law?

Possible Research Topics The section would welcome investigations on the legal barriers in jurisdictions worldwide, that would prevent "smart contracts" to become legally binding. Thorough surveys to discuss where such barriers do not exists, and why, would also be of interest not only to solicitors but technologists as well. Research articles on how to modify international laws to make them more amenable to the deployment of smart contracts will be of great interest to the community.

Usability Key questions:

What would enable the wide usability of smart contracts, meaning:

- Would the coding part be written by solicitors rather than programmers or software engineers?
- How it is possible to ensure that these kinds of contracts, even in their simple form are understood by the general public rather than experts?
- Will judges or other members in the legal profession need to learn some computing to be able to evaluate cases?

Possible Research Topics The section would welcome investigations, surveys or case studies on how the legal profession needs to change to ensure the smart contracts are considered in a "fair way" in the legal sectors This research topics would connect with the recent discussion on Legal Tech (Fenwick et al., 2019; The LawTech Delivery Panel, 2020).

Impact Key questions:

- How would the deployment of smart contracts impact society?
- Would smart contracts ensure better contractual obligations or will they become a hindrance to some parts of societies?
- What is the role of Governments in ensuring a fruitful development blockchain technology and smart contract?

Possible Research Topics The section would welcome investigations, surveys or case studies that discuss how the digitalization of the legal profession, in particular via the deployment of smart contracts, will not penalize part of societies- for example people who are digitally illiterate.

We would welcome comparative studies on the role of Governments in various jurisdictions to ensure fairness of the deployment of smart contracts and blockchain.

Security & Privacy Key questions:

- How can we ensure a unified framework for best practice to protect the public from cybersecurity risks?
- What are the practical risks for the privacy of citizens?

Possible Research Topics The section would welcome investigations, surveys or case studies that investigate practical security measure to protect parties from hackers, and ensure that the widespread deployment of smart contracts will not lead to a "Big Brother" society.

It is crucial that members of the legal profession, social and computer scientists come together to carry out practical research to ensure that smart contracts will deliver the benefits envisaged by Nick Szabo, and the development and adoption of smart contracts will enable an equitable and fair society.

DATA AVAILABILITY STATEMENT

The original contributions presented in the study are included in the article/supplementary material, further inquiries can be directed to the corresponding author/s.

AUTHOR CONTRIBUTIONS

The author confirms being the sole contributor of this work and has approved it for publication.

REFERENCES

(2017). *Smart Contracts and Distributed Ledger: A Legal Perspective*. Available online at: https://www.linklaters.com/en/about-us/news-and-deals/news/2017/smart-contracts-and-distributed-ledger--a-legal-perspective (accessed April 5, 2019).

(2018). *Smart Derivatives Contracts: From Concept to Construction*. Available online at: https://www.kwm.com/en/au/knowledge/insights/smart-derivatives-contracts-from-concept-to-construction (accessed April 5, 2019).

Atzei, N., Bartoletti, M., and Cimoli, T. (2017). "A survey of attacks on ethereum smart contracts (sok)," in *Proceedings of the 6th International Conference on Principles of Security and Trust* (Berlin; Heidelberg), 164–186.

Bod, B., Gervais, B., and Quintais, J. P. (2018). Blockchain and smart contracts: the missing link in copyright licensing? *Int. J. Law Inform. Technol.* 26, 311–336. doi: 10.1093/ijlit/eay014

Chaum, D., Fiat, A., and Moni, N. (1988). "Untraceable electronic cash," in *Proceedings of the 8th Annual International Cryptology Conference on Advances in Cryptology, CRYPTO" 88* (London: Springer-Verlag), 319–327.

Clack, C. D., Bakshi, V. A., and Braine, L. (2016). Smart contract templates: foundations, design landscape and research directions. *CoRR,* abs/1608.00771.

De Filippi, P., and Hassan, S. (2016). Blockchain technology as a regulatory technology: From code is law to law is code. *First Monday* 21. Available online at: https://firstmonday.org/ojs/index.php/fm/article/view/7113

De Filippi, P., and Wright, A. (2018). *Blockchain and the Law: The Rule of Code*. Harvard University Press.

Dingman, W., Cohen, A., Ferrara, N., Lynch, A., Jasinski, P., Black, E., et al. (2019). Defects and vulnerabilities in smart contracts, a classification using the nist bugs framework. *Int. J. Netw. Distribut. Comput.* 7, 121–132. doi: 10.2991/IJNDC.K.190710.003

Directive on electronic commerce (2000). Available online at: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:en:HTML (accessed March 20, 2019).

Fenwick, M., Corrales, M., and Haapio, H. (eds.) (2019). *Legal Tech, Smart Contracts and Blockchain*. Berlin; Heidelberg: Springer.

Magazzeni, D., McBurney, P., and Nash, W. (2017). Validation and verification of smart contracts: A research agenda. *Computer* 50, 50–57. doi: 10.1109/MC.2017.3571045

Szabo, N. (1994). *Smart Contracts*. Available online at: http://www.fon.hum.5uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html (accessed December 20, 2018).

Szabo, N. (1996). *Smart Contracts: Building Blocks for Digital Markets*. Available online at: http://www.alamut.com/subj/economics/nick_szabo/smartContracts.html (accessed December 20, 2018).

Tai, E. T.T. (2019). "Challenges of Smart Contracts: Implementing Excuses," in *The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms*, eds L. DiMatteo, M. Cannarsa, and C. Poncibò (Cambridge: Cambridge University Press), 80–101. doi: 10.1017/9781108592239.005

The LawTech Delivery Panel (2020). *Legal Statement on Cryptoassets and Smart Contracts*. UK Law Society. Available online at: https://35z8e83m1ih83drye280o9d1-wpengine.netdna-ssl.com/wp-content/uploads/2019/11/6 (accessed February 26, 2020).

Vigliotti, M.G., and Jones, H. P. (2020). *The Executive Guide to Blockchain, 1st Edn*. London: Palgrave Macmillan.

Conflict of Interest: MV was employed by the Sandblocks Consulting Ltd.