Smart contracts: How will blockchain-based applications influence financial services?

Magdalena DZIEDZIC[1]
Europejska Wyższa Szkoła Prawa i Administracji

Abstract. Smart contracts and blockchain technology have the potential to change tremendously the contractual practices. Together with the development of blockchain-based technology, many well-known companies and other private or public entities such as governments take advantage of smart contracts. On the one hand, there are costs connected with the programming and coding of smart contracts, or training those administering them, on the other hand, however, it seems to be true that smart contracts will bring greater certainty and extra cost saving for those who apply them in their business dealings. During recent years, rapid technological development has resulted in plenty of changes in the way how financial services are conducted. Blockchain technology is predicted to disrupt the current environment of business dealings by enabling the unprecedented ways to cooperate and communicate between the parties of the contract.

Keywords: smart contracts, blockchain technology, financial services, financial dealings, bitcoin, cryptography.
JEL Codes: G1, G2, K2, O3.

1. Introduction

In 1996, the computer scientist and lawyer Nick Szabo first published an article expressing his view that with the rapid advancement in technology, algorithms would finally be invented to manage all kinds of contractual dealings [Szabo 1996, pp.1-2]. Although Szabo's concepts were brilliant, they were definitely too advanced for the infrastructure existing at the time to bring them to life [Glatz 2014, p. 34]. The creation of blockchain in 2008 delivered the necessary background to perform smart contracts. Since then blockchain technology has gone forth, decentralized consensus architectures have been built, and both have found application in plenty of different contractual contexts. Key examples that adopted those technologies are the trade clearing and settlement of the cash equities market, supply chain and finance

---

[1] Contact with author: Magdalena Dziedzic (ORCID 0000-0003-0649-1763), Europejska Wyższa Szkoła Prawa i Administracji, Okopowa 59, 01-043 Warszawa, e-mail: mdziedzic@ewspa.edu.pl.

document handling. Recent advancements in blockchain platforms such as Ethereum, Fabric and Hyperledger as well as programming languages such as Solidarity have been of great use in terms of creating opportunities for smart contracts.

According to Szabo's idea smart contract mean machine-readable transaction protocols which establish a contract with pre-determined terms, in different words a computerized transaction protocol that executes the terms of contract [Szabo 1997, p. 3]. According to a newer definition, a smart contract is a machine-readable program, written in code which execution is automated when a set of pre-determined terms has been met.

Bearing in mind the interest, opportunities and application of smart contracts, it is essential to understand what they are, how they work, what technology they are based on so that it can be ascertained what use they can bring to the financial services market. This article proceeds in four parts, as follows. First, there is an explanation of blockchain technology, what it is and its importance for financial services dealings. Second, there is a brief review of virtual currencies and the origins of Bitcoin. Third, the article explores the idea of smart contracts, and their significance for the market. Finally, the article discusses some possible applications for this new technology. The purpose of this contribution is to do brief research into the challenges confronted by financial services providers as a result of these rapid developments in technology.

2. The creation of blockchain

The meeting of financial industry leaders at the 2016 World Economic Forum presented a number of baffling predictions as to the near future of financial services. An obvious lesson is that global financial, economic, legal and political systems will have to adapt quickly to the challenges and opportunities standing ahead of us. Among the most interesting comments concerning these near term scenarios were that: "cash in ten years probably won't exist" and blockchain technology will be applied to collect taxes (also within ten years). Moreover, during early 2016 news reports revealed that "Andrey Sharov, a vice president at Russia's Sberbank, said banks would disappear by 2026 on account of the rising use of blockchain technology. 'In 10 years' time, there will be no banks, I'm afraid,' according to a translation of Sharov's remarks by the Coinfox bitcoin news website."

Many governments and companies have appreciated the application of smart contracts. Dubai has started a strategy to use blockchain technology to boost efficiency across all governmental transactions. Sweden is testing a blockchain-based land registry, implying it would bring savings exceeding USD 100 million each year. Goldman Sachs expects that the application of smart contracts for cash equities transactions will improve efficiency, saving more than USD 6 billion globally. Banks and financial institutions are checking the ways how they can benefit from blockchain technology. Many American states have passed legislation, or are seeking to do it in order to officially acknowledge and take advantage of smart contracts and blockchain technology.

Although, as a matter of fact, the idea of smart contracts was created before blockchain, the latter put some new light in that area since the development of smart contracts happens due to the use of blockchain. The first evidence of blockchain was noted as early as 2009 with the evolution of the cryptocurrency Bitcoin, and still blockchains are basically associated with cryptocurrencies, e.g. Bitcoin, but it is important to distinguish between the two. Blockchains are commonly applied as a generic technology that can be used for many different purposes, such as payment networks, a platform for asset and supply chain management or a technology facilitating recordkeeping [Kiviat 2015, pp. 570-571]. To make it short and simple the blockchain is a decentralized, peer-validated crypto-ledger that guarantees a visible for all, chronological and permanent record of all prior transactions. It can be described as a spreadsheet that anybody can add a row to, but cannot otherwise update or delete anything that has previously been put on the block [Kiviat 2015, p. 574]. The main idea behind the creation of blockchain was to prevent double spending of cryptocurrencies in a system without a centralized body monitoring the issuance or transfer of such currencies [Nakamoto 2008, pp. 4-5].

As has already been mentioned, the execution of smart contracts takes place through the use of blockchain. Recently, there have been established a number of new platforms that exploit the power of blockchain to build smart contracts. Blockchain is 'digital technologies that combine cryptographic, data management, networking and incentive mechanisms to support the checking, execution and recording of transactions between parties.' [Staples et al. 2017, pp. 16-18, 23-24, 43-44]. To keep it short, a blockchain is a transaction (a block) that is added to a list (a chain). Having been added to the list, the transaction becomes part of the blockchain 'ledger' that is an incorruptible and irreversible electronic record of all transactions conducted on the blockchain [Cai, Zhu 2016, pp. 3-4].

To understand how the blockchain functions it is important to explore its key features, that is, the decentralized nature, its anonymity and resilience. First, as for the decentralized nature of the blockchain, it must be mentioned that it is the most original part of blockchain, the decentralized nature refers to authorizing and recognizing blockchain transactions [Wright, De Filippi 2015, p. 23]. We distinguish three categories of blockchain: public, consortium, and private [Pilkington 2016, pp. 33-34]. Only the public blockchains, however, thanks to their fully decentralized nature find application in cryptocurrency trading because of the security of the platforms. Consortium blockchain finds great application in organizational cooperation mainly between banks. Private blockchains, however, are suitable for traditional commerce and governance, where the owners would like to take advantage of the blockchain without losing control over the management of the platform for the sake of unknown people [Catchlove 2017, pp. 19-20].

Transactions which are put on blockchain can be anonymous, though that is not most important. Public blockchains, e.g. Bitcoin, as a rule, are anonymous and generally based on encryption to be trusted. There is no special authority whose role is to grant admission to the blockchain or verify identity. Private blockchain,

on the other hand, require a user to be permitted to add a block to the chain, and the permission is usually granted by an entity which created it, and, hence, the user is obliged to disclose and verify its identity.

The cryptography that is applied in blockchain transactions is aimed to prevent interference and ensures their permanent nature. When a transaction takes place on blockchain, an encrypted record of that transaction is forwarded to every other node being part of the same blockchain [Savelyev 2016, pp. 10-11, 19-20]. In this way it is ensured that every time a new block is added to the chain, its legitimacy has been verified and it is neither possible to modify nor to remove the blockchain. Hence, the transaction data held in the individual blocks is highly resilient.

3. The origins of Bitcoin

The origins of Bitcoin date back to virtual online currencies that developed during the mid-1990s with massive multiplayer online games, e.g. World of Warcraft, DiabloIII, Everquest. The creation of Bitcoin in 2009 is associated with Satoshi Nakamoto, considered by many to be a pseudonymous hacker [Trautman 2016, pp. 234-235]. One of the definitions describes Bitcoin as "a cryptographic object represented as a chain of digital signatures over the transaction in which the coin was used" [Trautman 2014, pp. 20-21, 26-27]. Therefore, "Bitcoin aims to be completely distributed, free of central authorities or points of control, and at least somewhat anonymous." [Trautman 2014, pp. 44-45].

Participants start to use Bitcoin by first buying a program called a Bitcoin wallet and one or more Bitcoin addresses [Bohme et al. 2015, pp. 223-225]. Then it is stored on a computer's hard drive as electronic files, and then Bitcoins can be accumulated or sent like an e-mail. Software algorithms inserted in the online Bitcoin network keep secure against fraud and guarantee that the files have not been counterfeited. Every Bitcoin transaction is registered that everybody can see it thanks to using a master transparent public ledger called blockchain. The blockchain ensures that the identical Bitcoins have not been used in the previous transaction, in that way making it impossible to double spend the same Bitcoins.

Bitcoin is an example of a successful application of DLT (decentralized ledger technology) that combines a group of cryptographic tools and protocols used to exchange, verify and secure data without the need for centralized intermediaries [Sklaroff 2017, pp. 265-267]. Bitcoin can be used as payment in thousands of companies and service providers. Bitcoins protocols give reward to participants who cooperate and punishment to those that present opportunistic behaviours, so that the transaction in the system can be traced and recorded with confidence. Bitcoin made it possible to transfer value, without the need for banks or other institutions.

The Bitcoin project is the reference point applied in creating the majority of virtual coins capitalized on the market: some of them, e.g. Ripple, is based on the no asset backed redesign of a pre-existing protocol; others, like Litecoin have introduced

some characteristic features of Bitcoin. There are other protocols, such as Namecoin, which are target-oriented and consist in creating a domain naming system alternative to ICANN, or the Ethereum Platform assigned to smart contracts.

4. The concept of smart contracts

Smart contracts are agreements which execution is automated. They are represented in code and signed by computers. They are concluded online and their performance is enabled and secured by a network of centralized, co-operating computer nodes, known as blockchains [Mik 2017, pp. 289-291]. In the beginning, smart contracts were formed mainly within transactions concerning financial instruments, that is financial derivatives or prediction markets. Gradually, more and more contracts can become smart and many obligations arising thereof may be enforced by code, this is taking place particularly in broadly understood commerce. Smart contracts can make the contracting process more effective, reduce transaction costs by eliminating intermediaries and make contract enforcement more efficient and simple by eliminating the need to ask for protection from courts.

Formation of a smart contract using blockchain gives an opportunity for the code to govern the terms of the contract and to execute some, or in some cases all, of the terms of the contract [Werbach, Cornell 2017, pp. 334-335, 348-349]. Smart contracts are able to do it by registering the title of either digital assets, or digital representations of offline assets, in blockchain [Savelyev, *Contract Law…*, pp. 13-14]. The electronic form of a smart contract is equipped with the functionality that makes it possible for the parties to start performance based on special electronic triggers added to the blockchain. What is more, since smart contracts are based on cryptography, each interaction with the smart contract calls for the use of a digital signature or a key.

One of the problems with traditional contracts is that performance is not guaranteed. A smart contract provides for a higher degree of implementation. When the terms of a contract have been programmed into code and executed onto a blockchain, there is no longer a reliance on the willingness of the parties to want to perform the contract [Savelyev, *Contract law…*, p. 18]. Apart from specific conditions programmed into the code, it is possible to directly codify asset transfer and other requirements of performance into a smart contract. In this respect, the frame for opportunistic breaches is importantly reduced or even eliminated. Therefore, a smart contract provides for a higher likelihood of performance than traditional agreements.

Any serious discussion about smart contracts must be based on the fact what is legally and technologically possible for now. In the area of commercial transactions, in case of rather simple dealings, there are, as a matter of fact, quite few legal barriers to the use of smart contracts, e.g. regarding simple payment instructions. More complex transactions call for more advanced blockchains or protocols. In case smart contracts are connected with the performance of some obligations in the real world, their efficiency involves plenty of dependencies on external and quite possibly rather insecure bodies. From a practical point of view, it must be stated that only certain

types of contractual obligations can be expressed in code and only some obligations may be perceived as computationally ascertainable [Savelyev, *Contract law…,* p. 20]. There are legal concepts, such as reasonableness, fair dealings, due diligence or best efforts that may be difficult, or even impossible, to be put into code, since they require general evaluation of contractual performance.

The most simple example of smart contract use may be the process of apartment buying. At present it is a rather complex process involving a lot of parties as e.g. real estate agents, mortgage bank, public notary while signing the contract or a lawyer who prepares such a contract. In the future real estates with all their characteristics will be saved on the blockchain together with electronic property title, from which results if the property has some burdens or not. After paying the prepayment the future-to-be owner will have access to blockchain with all the record of the real estate – there is no need for relying on a real estate agent or a lawyer.

There are many other possible applications of smart contracts, e.g. programmable money with saved conditions as to its payment, which was used i.e. in ICO – most projects operating in this mode are based on smart contracts. Investors send financial resources in the form of ether for the address of a particular smart contract, which automatically pays them out a suitable number of tokens. Another use of smart contracts are escrow functions in auction services; the buyer sends financial means for a special escrow account and the means are released at the moment of the buyer receiving the goods. Smart contracts are used for digital ID – personal data is saved on a blockchain and the person who they belong to decides how to make use of it. Smart contracts make it possible to limit the number of identity thefts. Furthermore, smart contracts may be used in any kind of elections – they minimalize the number of forgeries since the votes are saved on the blockchain, they also make the process of votes counting quicker and voting itself may take place online. Smart contracts are used for management since they make the process of workflow more efficient. It is possible to build smart contracts in physical objects such as car or real estate to give a better control to its owners or in case of credits to banks or other financial institutions, also as a basic element in the internet of things. Smart contracts are very useful also for insurance, e.g. automatic settlement of damage and paying out damages, calculating the amount of contributions, or reporting insurance incidents (e.g. flight delays).

5. Conclusions

The incredible growth in data processing ability and a reduction in transaction costs connected with that make it possible to provide innovative technological products and services that would have otherwise been beyond the bounds of possibility just a few years ago. The technological advances of the recent years have resulted in great cost efficiencies for both consumers and businesses, e.g. cost savings in loan servicing, or the ability to leverage unused assets in the sharing economy (powered by fintech companies) [Peters, Panayi 2014, pp. 4-5].

The development of new technologies has led to significant changes in the way how financial services are offered to consumers, or more generally clients. Broad application of internet and increasing digitalization generated acceleration of the processes with regard to financial services, limitation of the procedures, increase of efficiency for clients, which is becoming a competition game for the financial services providers. There are, additionally, many threats connected with them, such as ensuring the safety of the transactions.

It must, however, be stated that as for now we do not have a contract technology that would be suitable for all transactions. Smart contracts seem a good solution for contracting parties under certain conditions, such as when there is high certainty or where performance monitoring would be rather very costly as well as for quite simple transactions.

References

Böhme R., Christin N., G. Edelman B., Moore T., 2015, *Bitcoin: Economics, Technology, and Governance*, "Journal of Economic Perspectives", vol. 29(2).

Cai Y., Zhu D., 2006, *Fraud detection for online businesses: a perspective from blockchain technology*, Financial Innovation 2(1), 20.

Catchlove P., 2017, *Smart Contracts: A New Era of Contract Use*.

Mik E., 2017, *Smart Contracts: Terminology, Technical Limitations and Real World Complexity,* "Law, Innovation and Technology", 9(2), Research Collection School of Law.

Peters G.W., Panayi E., 2014, *Understanding Modern Banking Ledgers through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet of Money*, arXiv.

Pilkington M., 2016, *Blockchain Technology: Principle and Application,* Elgar.

Satoshi N., 2008, Bitcoin: A Peer-to-Peer Electronic Cash System, http://bitcoin.org/bitcoin.pdf.

Savelyev A., 2017, *Contract law 2.0: Smart contracts as the beginning of the end of classic contract law*, "Information and Communication Technology Law", vol. 26, 2.

Sklaroff J.M., 2017, *Smart Contracts and the Cost of Inflexibility*, University of Pennsylvania Law Review, vol. 166, 263.

Staples M. et al., 2017, *Risks and opportunities for systems using blockchain and smart contracts*, Data61, vol. 2.

Szabo N., 1996, *Smart contracts: building block for digital* markets, Phonetic Sciences Amsterdam, http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/ Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html.

Szabo N., 1997, *Formalizing and Securing Relationships on Public Networks*, First Monday http://firstmonday.org/ojs/index.php/fm/article/view/548/469.

Trautman L.J., 2014, *Virtual Currencies: Bitcoin & What Now After Liberty Reserve, Silk Road, and Mt. Gox*?, "Richmond Journal of Law & Technology", vol. 20(4).

Werbach K., Cornell N., 2017, *Contracts Ex Machina*, "Duke Law Journal", vol. 67, 313.

Wright A., De Filippi P., 2015, *Decentralized Blockchain Technology and the Rise of Lex Cryptographia*.

Inteligentne umowy: Jak technologia blockchain wpłynie na usługi finansowe?

Streszczenie: Rozwój tzw. inteligentnych kontraktów przypadł w dużej mierze na okres ostatnich kilku lat, a stało się to możliwe dzięki dużym postępom w technologii blockchain. Inteligentne umowy postrzegać należy jako kolejny krok w rozwoju umów w Internecie. Jest to związane z wprowadzeniem kryptografii, a dodatkowo także automatyzmu procesów oraz umożliwienia automatycznego wykonywania umów, po tym jak spełnią się przesłanki zaprogramowane w kodzie programistycznym. Technologia blockchain, w tym inteligentne umowy, mają istotne znaczenie dla całego sektora finansowego, gdyż umożliwiają zwiększenie przejrzystości oraz ograniczeniu kosztów transakcji, w tym kosztów ukrytych. Ma to miejsce dzięki bardziej wydajnemu zarządzaniu danymi, ograniczeniu pośrednictwa finansowego i usprawnieniu procesów.

Słowa kluczowe: umowy inteligentne, smart contracts, technologia blockchain, usługi finansowe, transakcje finansowe, bitcoin, kryptografia.
Kody JEL: G1, G2, K2, O3.