Blockchain, smart contracts and DAO

WARDYŃSKI & PARTNERS

COALITION FOR POLISH INNOVATIONS

A few words about blockchain governance

Maciej Jędrzejczyk, Karolina Marzantowicz (IBM)

In school they used to tell us that mathematics was the queen of the sciences. The development of distributed ledger technologies (DLT) shows how true this is. One of the main advantages of this technology is the decentralised trust written into the source code of the IT programme. With this, in the age of the digital economy, we can move from a state where central persons, institutions and organisations serve as trusted third parties, to a state where their role is assumed by algorithms of decentralised consensus, i.e. mathematics.

One form of DLT is blockchain. The blockchain technology is leading the growth of information systems and digital communications in the direction of large-scale decentralisation. The human factor is minimised, and trust and accuracy of transactions are ensured through cryptography.

With the significance of this technology, it needs to be examined in terms of the governance under which new business models and sectors of the economy will arise. This will allow us to identify the fundamental characteristics and risks of solutions based on public and private blockchains.

Public blockchain, or creeping oligarchisation

A characteristic feature of a public blockchain is the lack of components for managing this solution. This influences the functioning and maintenance of the whole system. Decentralisation and distributed architecture counteract the concentration of power that could be gathered by a single person, role or organisation. This also increases the reliability of the system because of the lack of critical components (no single point of failure).

Unfortunately, this solution does not exclude grouping and accumulation of resources of the network (numbers of participants) within the main roles that will be involved in the implemented process served by the functioning network. This has to do particularly with "miners," who solve increasingly difficult mathematical tasks in order to take part in the process of verifying transactions and entering a block in the ledger. The person who solves the task first is rewarded by adding the appropriate value in bitcoins to his wallet.

The proof-of-work algorithm assumes that the accumulation of resources in the network will not exceed 51%. But as the degree of the tasks rises, miners group together into "mining pools" in which each miner solves only part of the problem and the reward is divided among all of them. Currently the four largest mining pools include over 65% of all miners involved in solving problems in the Bitcoin network. If one entity took control over the majority of the resources verifying transactions, it could exploit these resources to dictate conditions to the rest of the network.

The increasing number of mining pools is a serious threat to decentralisation and the fundamental principles of a public blockchain. A group (or organisation) possessing most of the resources performing proof-of-work calculations could manipulate the value of

verified blocks (insert false transactions or throw out true transactions). This is not just a hypothesis, as demonstrated by the recent unsuccessful attack on the Krypton network, where the attackers relied on computing power rented in the cloud to interfere with the integrity of the blockchain and the state of holdings of the cryptocurrency KR.

Moreover, public networks cannot choose who decides on consensus, or expose and monitor the identity of the nodes. For many business organisations subject to strict regulations this rules a public blockchain out of their consideration.

Anonymity and privacy – the fundamental difference between public and private blockchain governance

A public blockchain affords participants in the network anonymity secured by cryptography. The irreversible ledger may be a repository for documents, contracts, title deeds and other assets. Blockchain may be used to place information and instructions with a wide range of applications. The potential applications of this technology extend far beyond cryptocurrencies like Bitcoin. The fields of application of the DLT paradigm are potentially countless, because it enables decentralisation of verification and storage of transactions of all kinds between parties on a global scale.

But in many sectors of the economy where the blockchain technology could have applications, the participants cannot remain anonymous.

When conducting business or providing public services, we typically know (and want to know) our supplier and customer. Anonymity is neither necessary nor desired. In solutions that are divided and distributed among all participants in the network, appropriate management of privacy is required. A private or "permissioned" blockchain provides the possibility of extending DLT to include components such as management of participants and privacy. A private blockchain is most often created by a consortium or defined group of participants. They determine who can function in the network and under what rules. Moreover, a network in which the participants are not anonymous can use algorithms other than proof of work for distributed verification of transactions, such as Practical Byzantine Fault Tolerance.

An example is the open project Hyperledger, realised by the Linux Foundation. In the proposed Hyperledger Fabric architecture, there are functioning components responsible for management of the participants and their privacy and for issuance of certificates used for signing transactions and smart contracts so that the details are visible only to the parties to the given transaction. The functions of verifying node and passive node have also been separated, enabling greater oversight of actors participating in the consensus and holding a full copy of the register based on the blockchain. As transactions are recognised only after authorisation at numerous levels (signing of certificates, authentication of identity), "membership services" generally permit controlled access to the network, thus eliminating the anonymity of the nodes. At the same time, this type of service can guarantee the privacy of transactions by distribution of transaction certificates which encrypt a confidential transaction between two specific parties, rendering it illegible to others. It should be pointed out that all these features are integrated with the traditional advantages of the distributed ledger and consensus algorithms.

Business logic entered in blockchain, or smart contracts

One of the new features popularised with the Ethereum project is the concept of smart contracts, i.e. compiled programming code a copy of which is entered in the blockchain ledger and whose content represents the rules for executing transactions between the parties. Once distributed in the decentralised network, the smart contract is launched on all nodes as an executable programme, and the specific function provided for by the author is launched.

It can thus be said that a smart contract is a digital representation of the rules or processes functioning within a given business organisation that regulate the execution and course of transactions. The blockchain technology serves here as an irrefutable ledger of contracts governed by smart contracts. This context also raises the possibility of instant (and practically cost-free) execution of transactions between parties seeking to maintain anonymity, resolution of disputes without involving a trusted third party but relying on the transparency of the blockchain, and even automatic conclusion of contracts without involvement of the human factor.

New technology, new problems, new challenges

The irrefutability of contracts unfortunately does not eliminate potential legal problems. As in the case of any entity operating in commercial life, fundamental aspects of a comparative analysis of public and private blockchains in this context include:

- Clear identification of the entity responsible for a defectively prepared contract, and
- Identification of the process enabling quick remediation.

Other problems should also be mentioned, arising out of the ability of business organisations to comply with existing legal regulations, which often require that certain specific behaviours be included in the business process, such as disclosure of the parties to the contract, the privacy of transactions, or regulated access to data.

Smart contracts in public and private blockchains

In the case of networks based on a public blockchain, the correctness of the transaction between the parties is determined exclusively by the consensus of the network. The influence of organisations making up the membership of the given network is negligible, and without obtaining a supermajority of the capacity of the network (e.g. 51% of the hash rate in the case of networks based on proof-of-work consensus) there is no practical possibility of recognition of certain transactions or agreements executed by smart contracts as defective or invalid. This problem lay at the heart of the incident of The DAO in June/July 2016. The discovery of a smart contract susceptible to an attack by hackers (and exploitation of that susceptibility by an unknown perpetrator to drain over USD 60 million in cryptocurrency) caused a battle lasting several weeks for agreement on what remediation (if any) should be applied. A problem in and of itself was to achieve the agreement of the entire community, which displayed irreconcilable interests. Without a process in place for dealing with an incident of a defectively written smart contract, a decision was taken for direct intervention in the addresses registered in the Ethereum blockchain used to store the stolen funds. On one hand this allowed the funds to be restored to their owners and blocked them from being taken over by the hackers. On the other hand,

this was clearly a change in the rules in the middle of the game, and as such met with resistance from a large segment of the community faithful to the ideal of the integrity of the blockchain (more on this in the article "What the history of The DAO says about the law" at p. 25).

Solutions enabling implementation of blockchain technology in a closed, private environment are coming to the rescue. The greater level of trust *a priori* between the parties permits simplification of the consensus mechanism, a clear delineation of roles, and assignment of responsibility to specific units. The appearance of specialised auditors and administrators of identity with special entitlements allows for more effective control over transactions in the network based on the blockchain technology. In the event of defectively functioning transactions based on smart contracts, and with the small scale of the private network (typically some 10–20 nodes), there is a possibility for immediate intervention, and with simpler consensus a change can be accepted must faster by the entire network.

Law locked in code – the future of the legal professions in a world of blockchain and smart contracts

The neutrality of the principles of distributed consensus and verifiability of transactions may significantly contribute to a redefinition of current decisional processes, both in central organisations and in implementation of solutions covering all participants of a given market. Many new business models may rely on decentralised ledgers, distributed consensus and decentralised management. Depending on the needs and requirements, these could be networks for anonymous participants, where the details of transactions are publicly accessible to all, or private networks open to a defined group of participants, enabling management of privacy. In either case, mathematics and cryptography will enable the rules governing how the network executes and confirms transactions to be locked away in computer code.

This does not mean that the professions of advocates or notaries are condemned to extinction. To the contrary, the digitisation of assets, transactions, agreements and business logic between the parties within blockchain and smart contracts opens up new possibilities and perspectives. On one hand, the most basic, repetitive legal actions can easily be programmed and automated. This will allow lawyers to focus on more complex and labour-intensive matters. On the other hand, familiarity with the governing law will be the key to entirely new fields of activity, such as formulation of smart contracts describing an agreement or new type of business, or drafting legal opinions for businesses planning to base their activity on blockchain. Consequently, a knowledge of programming and algorithms may prove to be a key skill for the lawyers of the future.

What is DAO from the legal perspective?

Krzysztof Wojdyło

The question posed in the title would be moot if DAO functioned in complete isolation from the existing legal and economic context. But that is not the case, at least not at the current stage of development of DAO. Given the existing connections with the real world (forced at the very least by existing tax systems), there is a need to grasp the essence of DAO for purposes of current legal and commercial structures.

Exceptional nature of DAO

DAO (decentralised autonomous organisation) is undoubtedly an intangible creature. But that hardly makes DAO unique from a legal perspective. For centuries the law has recognised the existence of immaterial entities, and the significance of such entities continues to grow. In this context we could mention intellectual property rights or receivables, which do not have any material form but may carry great value.

DAO is a type of smart contract, but it should be distinguished from the smart contracts that may be concluded via DAO. DAO should be treated as a type of meta-contract that organises the scheme for conclusion of target contracts between participants in the given DAO. Thus a DAO can form legal relationships between its participants (that is, the participants in the given DAO hold certain rights and obligations). The legal relations in this case are created using non-standard methods, but thanks to DAO legal relations are effectively established between its participants.

The exceptional nature of DAO is also found in the far-reaching autonomy of its operation. DAOs function in an automated manner through execution of the code that is their foundation. DAO also lacks traditional representatives comparable for example to the directors and officers of a corporation.

Nonetheless, DAO and its participants enter into external relations with entities from outside the DAO. This occurs for example with respect to developers of the DAO programming or external providers of content to the DAO (e.g. "oracles"—trusted providers of data on the value of assets relevant to smart contracts concluded via DAO).

Many of the legal relations formed via DAO could no doubt be classified as relations recognised by traditional legal systems (e.g. a sale contract or lease agreement). But the legal treatment of the DAO itself presents much greater difficulties. It is hard to assign a DAO to a specific jurisdiction when current legal systems don't recognise the existence of DAO at all. In this sense DAO is an abstract being that eludes simple legal classifications and is difficult to ascribe to a specific legal order.

Legal capacity

This is also the approach to DAO presented by current Polish law. One of the fundamental concepts of civil law is legal capacity. Although it is not defined in the Civil Code, it is assumed to mean the capability of holding rights or

bearing obligations. Such capacity is possessed only by entities defined by law. These are natural persons, legal persons (the law provides for a fixed catalogue of types of legal persons), and organisational units that are not legal persons but are nonetheless vested with legal capacity by specific statutory provisions. DAO is none of these entities, and therefore under Polish law it does not have legal capacity and cannot be the subject of rights and obligations. Recognition of DAO as a legal entity by the Polish legal system would require legislative intervention expressly endowing DAO with legal capacity.

Essence of the issue

The lack of legal capacity of DAO makes it transparent from the point of view of current law. Thus any legal relations occurring in or with the DAO are theoretically relations occurring directly between the end users of the DAO. At first glance this might seem neutral. As long as the DAO functions properly, these considerations seem like moot, academic discussions.

But the problem is that DAO is not, and in the near term probably will not be, entirely abstracted from the reality conceived of in traditional, formal legal terms. This is primarily because the end users of DAO are natural and legal persons who are subject to specific legal systems. For example, for tax purposes it may be necessary to precisely identify the source of income from a DAO. Moreover, for its functioning and growth a DAO will often need to have dealings with external service providers (such as the creators of the programming).

In such instances, the legal transparency of DAO presents serious practical problems. The parties to legal relations formed within the DAO or the parties to legal relations with the DAO would have to be identified as being all of the DAO's participants. Identifying all these persons is not feasible. Moreover, this presents a major barrier to formation of any legal relations with DAO by external suppliers. Suppliers acting with due care seek to precisely identify their customers. They must know who they are actually entering into a transaction with, whom they might have to seek payment from and so on.

Short-term solution

To overcome these difficulties, creation of structures linking the legal relations arising in DAO with a traditional entity possessing legal capacity as recognised by traditional legal systems should be considered. The terms of the DAO might expressly indicate, for example, that a specific company or foundation is the party to relations with the DAO. This approach would certainly make it easier to form legal relations with the DAO. It would enable identification of the entity that is a party to the relations with the DAO and determine the legal system that will apply to relations with the DAO.

This solution would undoubtedly provide greater certainty in dealings with DAO. It is advantageous for the initiators of the DAO as it allows them to estimate with some precision the potential legal risks connected with launching the DAO in question. The DAO in this solution ceases to be suspended in a legal and regulatory vacuum. The first examples of DAO attempting to follow this scheme are appearing. It seems that in the short term, this is the only chance to ensure safe development of DAO and exploitation of its potential.

Long-term solution

But considering the nature of DAO, the solution indicated above should be regarded as makeshift. Ultimately, a special new construction of legal capacity should be

created for the purposes of DAO. This solution would much better reflect the true nature of DAO. By adopting the interim solution outlined above, we sanction a legal fiction. The traditional entity that is associated with the DAO for the purposes of the existing legal order will often not be in any position to control the activity of the DAO. The essence of DAO, after all, is largely found in its autonomous character. So the most natural solution would be to vest DAO with legal capacity.

DAO has a great many features in common with other immaterial entities which the legal system vests with legal capacity. The arguments in favour of ascribing legal capacity to entities such as legal persons do not differ that much from the case of DAO. Both legal persons and DAO are intangible creatures. Legal persons were invented to enable efficient dealings by ascribing subjectivity to an artificial entity between the end participants and stakeholders in economic exchange (such as shareholders, employees, consumers and suppliers). Thanks to this construction, each group of stakeholders in the exchange, such as suppliers, does not have to enter into direct relations with each other group, such as the owners of the means of production.

But it must also be acknowledged that giving legal capacity to DAO would present a huge challenge for the current legal system. As indicated above, one of the characteristics of DAO is that it cannot be identified with any specific jurisdiction, because DAO functions in a decentralised network. Meanwhile, the current legal system still functions on the basis of a paradigm assuming the need to associate every legal event with a concrete, traditionally understood jurisdiction. Looking at the examples of the challenges brought by the Internet (e.g. cybercrime, e-commerce and cloud computing), it is clear that this paradigm is not entirely suited to the realities of the global net. Many online events already raise thorny conflicts between legal systems (such as problems determining which law governs processing of data in cloud computing services). DAO accentuates the imperfections of the existing legal order even more.

It seems that the solution that would best suit the nature of DAO would be to ascribe a special type of legal personality to DAO while at the same time developing for the purposes of DAO a conception of a special "distributed" jurisdiction, different from jurisdictions as traditionally understood. But this approach is so far from the current order it can hardly be expected to be adopted within the foreseeable future.