Blockchain, smart contracts and DAO

WARDYŃSKI+ PARTNERS•

COALITION
FOR POLISH
INNOVATIONS

Partners:

COALITION FOR POLISH INNOVATIONS

IBM

userfeeds

imapp

Translation: Christopher Smith

The views expressed in this publication are based on the individual reasoning of the authors and do not constitute a legal opinion or other formal statement by Wardyński & Partners.

Contents

Introduction

Krzysztof Wojdyło, Jacek Czarnecki

When we were writing our report on virtual currencies two years ago, we had the impression that we had hit on a topic that would revolutionise the economy and the law. Time has shown that it was just the start.

Examining the growing interest in the blockchain technology which Bitcoin is based on, we were witnesses to a unique boom in innovation. The potential of this technology, initially perceived only by a small circle of cryptography enthusiasts, is now recognised by central banks, governments, and major financial institutions. It is already clear that it will extend far beyond the world of finance, and the real revolution is only beginning now, with the first practical implementations of the concept of smart contracts and decentralised anonymous organisations (DAO). This is a revolution also for the law, as we described back in 2014.

The funding campaign (initial coin offering—ICO) for one of the first DAOs, "The DAO," in May of this year was in many respects a breakthrough moment not only for the development of new economic models, but also for existing legal systems. The ICO succeeded in raising the equivalent of USD 150 million based exclusively on a contract existing in the form of an algorithm. Moreover, the funds went to an autonomous, decentralised organisation existing solely in cyberspace.

The traditional documentation of the ICO, drafted in natural language, was of secondary importance. The rights and obligations of the participants in the ICO were entered in the form of computer code. The events that played out after the ICO (theft of a large amount of the funds by an anonymous hacker) added a dramatic touch to the whole undertaking, underlining how pioneering and innovative these solutions are.

We don't believe the collapse of The DAO spells the end of smart contracts or DAO. To the contrary, all indications are that the events surrounding The DAO raised the interest in these solutions. They have huge potential for economic growth and for the public sector.

The first experiments with DAO and smart contracts clearly show that these solutions function in an arena that is practically entirely unregulated. It is already evident that for many interesting initiatives, this presents an increasingly serious barrier. Our report is an attempt to systematise the most important legal issues arising in connection with DAO and smart contracts. Unfortunately, the scale of the challenges is vast. The legal systems that are the first to rise to these challenges, even with interim solutions, have a chance to attract initiatives creating new economic models and to ride the growing wave of innovations which some say are comparable to the Internet itself. Some examples show that such initiatives can be effectively supported with surprisingly little effort.

We hope that the articles in this report provide inspiration for a broader debate on the measures that should be taken to encourage growth of blockchain-based technologies. It is a technology harnessing huge potential, but it cannot be unleashed without the support of regulations.

What are smart contracts and DAO?

Jacek Czarnecki

The idea of moving legal transactions to the digital sphere reaches back to the beginnings of the Internet. But the concept that a computer protocol could execute contractual terms far exceeded the technological capabilities at the time.

Originally the Web was made up of static content connected by links. Along with development of the Internet, an increasing role was played by generation of content by users and their mutual interactions, as demonstrated by social media. The web became a place where we create and obtain information and communicate with one another.

There are many indications that the next chapter in the evolution of the Internet was opened up by blockchain technology, which is sometimes identified with the broader notion of decentralised register technology. Perhaps this new phase will enable realisation of the vision of moving the legal system into cyberspace.

What is blockchain?

Blockchain is primarily a structure of databases containing a history of transactions. Much as traditional registers are ledgers containing chronological entries, the history of transactions recorded in a chain of blocks reflects the current state of affairs, such as the holdings of certain goods.

Blockchain comprises time-stamped blocks which constitute groups of transactions and are linked through secure encryption. Each block is linked in this manner with the preceding block and the following block, so that the ledger assumes the form of a chain of blocks. Modification of any of the blocks would break the chain.

The structure of a database in the form of a blockchain is only an original method for organising and arranging data—and not necessarily the most convenient or efficient method. The key aspect however is the protocol that ensures that the specific databases (chains of blocks), although stored in various places by various people, will be identical.

The first such protocol was Bitcoin. Its key element is the mechanism for achieving consensus among users of the Bitcoin network on the content of the databases maintained by them, which are a record of all historical Bitcoin transactions. An intriguing aspect of Bitcoin is that the mechanism of achieving consensus is built on economic incentives. This means that every participant in the chain confirming completed transactions has an economically measureable reason (a reward in the form of newly generated bitcoins) to confirm only transactions actually made and not to attempt to fraudulently add non-existent transactions (e.g. spending the same funds twice).

Blockchain in practice – Bitcoin

The blockchain technology was developed along with Bitcoin. In the case of Bitcoin, the blockchain is a ledger of all transactions ever performed in the Bitcoin network. Copies of these ledgers are stored all over the world.

Thanks to the innovative protocol and the mechanism for achieving consensus on the accuracy of the ledger entries, copies of all ledgers should be identical.

Consequently, Bitcoin constitutes a global network in which the ledger of transactions—the blockchain—is formed and maintained by thousands of nodes and thanks to numerous entities maintaining infrastructure confirming transactions.

In the case of Bitcoin, the mechanism for achieving consensus enables cooperation among participants in the network who do not know one another. Effective achievement of consensus means that these entities do not have to know each other or worry about mistrust between them. Bitcoin has shown that it is possible to eliminate the trusted third party as an intermediary in transactions (in this case the central bank and payment intermediaries).

Further blockchain applications

Following Bitcoin, plans for applying the blockchain technology are arising in other fields. One application is based on the assumption that non-cash carriers of value, e.g. securities, can be assigned to units in the given blockchain (bitcoins in the case of Bitcoin).

Blockchain in practice – register of diamonds

The blockchain technology may be used to create various types of registers. An example already implemented in practice is Everledger, a distributed register of diamonds. It consists of assignment of a unique number to each diamond, tied to its properties, and introduction of the number into a ledger based on a blockchain. Each diamond registered in this manner carries its own "passport" enabling verification of its origin and tracing of the history of transactions involving that diamond. This helps uncover illegal diamond trading and fraud.

As it turns out, the ability to attach additional conditions and features to a given transaction in the blockchain in the form of programming code presents huge potential. Then verification of the transaction by the consensus of the network also includes execution of the code.

What can be included in such programming code built into a given transaction? In the case of Bitcoin these possibilities are limited (although there are many projects seeking to change this). But new public blockchains, the most notable of which is Ethereum, carry much great possibilities. With them, the programming code can provide for anything that can be expressed in the programming language. Performing the transaction launches the execution of the code—independent of any third party or the parties to the transaction itself.

With this possibility, a transaction can become a way of executing the specific computer programme recorded in its content. The code may establish certain conditions, such as making execution of the transaction conditional on additional circumstances.

Blockchain in practice – voting

The blockchain technology may be applied in designing electronic voting systems. Currently, votes cast in various types of elections are recorded, counted and verified by centralised institutions. Blockchain could work for example in shareholder voting for corporate officers. Additionally, smart contracts (see below) could be used to immediately enter the results of voting in the appropriate register.

Smart contracts

At a conceptual level, a "smart contract" is a legal tie that can function independently in cyberspace, without the need to refer to the real world.

In practice, realisation of this concept should ensure the following:

- The legal relationship is **concluded** by electronic means, without the need to use paper documents or traditional signatures, and it may also be **modified** in this manner.
- **Performance** of the legal relationship or elements thereof does not have to be tied

to any action in the real world—it is automatic and subject only to the rules established in the smart contract.

An additional advantage of a smart contract is that its conclusion, modification and performance are not depend on the will of any third party (not a party to the smart contract), including a court. Smart contracts mean more than contracts. They can be used for any legal relationship (e.g. as elements of an organisation, voting system, public register, etc).

It turns out that these key features of a smart contract can be realised through transactions of the type referred to above in a public blockchain network like Ethereum, containing additional computer code.

These transactions are conducted solely in the digital sphere. Launching of the transaction is linked with execution of the attached programming code, which may freely shape the rules for performance of the transaction between the parties. Thanks to the features of the blockchain technology referred to above and achievement of consensus in a distributed network, performance occurs independently of the will of the parties or any third party. Thus blockchain technology enables actual exploitation use of the concept of smart contracts.

Smart contracts in practice – financial markets

The use of smart contracts on financial markets has generated a great deal of interest. The goal is to create possibilities for financial institutions to conclude financial contracts that are executed automatically, exclusively in the digital world.

The forms for contracts used in financial sector trading are typically standardised (with modifications only for identification of the parties and the subject of the transaction). This means that they can fairly easily be translated into computer code.

A smart contract is a programme that is executed due to a transaction in a given blockchain by making changes in the blockchain. It is recorded in the blockchain and executed by distributed nodes of the network, which eliminates the need for a trusted third party. Modification or influence on the operation of the smart contract requires a change in the consensus of the entire network.

Opportunities and limitations of smart contracts

The captivating notion of smart contracts—moving law to cyberspace—runs up against several major difficulties. First, smart contracts essentially function in one environment—within a given blockchain. If performance of a smart contract requires any information from the external world, it is necessary to gather and verify that data. A solution to this problem is offered by “oracles,” which we write about in the article “How to design smart contracts and DAO” (at p. 16). A similar problem also arises if the smart contract is supposed to exert effects in the external world (beyond the blockchain).

Second, smart contracts are deterministic. Typically there have no place for elements that are subject to value judgments or general clauses (like “reasonableness” or “fair dealing”). Using a smart contract, we obtain certainty that the code will be executed as written, but we often lose the ability to introduce intentional ambiguity. This results largely from the limitations on the language we can use to create a smart contract. This is an artificial computer language, unlike living, natural, human language. Perhaps the development of cognitive computers and artificial intelligence will slowly resolve this problem as well.

The creation of smart contracts has become possible thanks to blockchain technology, and thus the limitations on that technology are also limitations on implementation of smart contracts. It should nonetheless be assumed that subsequent generations of distributed, decentralised protocols will try to solve the apparent problems.

Notwithstanding the limitations, smart contracts are already working out well in situations involving schematic legal relations. An example is contracts on financial markets, where standard patterns are often used. Smart contracts enable digitisation of the process of concluding and performing such contracts, eliminating intermediaries and ensuring that contracts are executed.

But there are many more applications for smart contracts. They are often perceived as simply shifting civil agreements into the digital sphere. In reality, they can be used to build much more complicated structures. An example is DAO.

DAO

DAO (decentralised autonomous organisation) is a special form of smart contract. The idea behind it is an entirely autonomous entity existing only in cyberspace.

DAOs can perform various functions traditionally performed by institutions like companies, foundations, associations or cooperatives. DAOs may be created for different purposes. Certainly economic purposes will be the most frequent, and thus DAOs will really be analogous to companies.

DAO in practice – The DAO

The first example of a DAO was an organisation called The DAO. The DAO was supposed to function as a decentralised venture capital fund. The participants could pay funds into The DAO and obtain tokens in return. The tokens allowed the holders to vote on investments by the fund.

A DAO is a smart contract taking the form of organisation of an undertaking by a group of people (and may be open to new members). At the edges of the organisation there will always be people (at least until AI is sufficiently developed), but they will not always be easy to identify. Via the DAO they will seek to realise their joint undertaking. DAO participants do not have to have identical goals. As in the case of a regular company, the goals of the management and shareholders can sometimes be diametrically opposed. But this type of company is structured in such a way that management and shareholders can each pursue their interests while also furthering the joint undertaking.

While the simplest smart contract involves dealings between two entities, relations can be much more complex in a DAO. Various entities are involved in a DAO, have different ties to the DAO and are devoted to different goals. A DAO can also be open to new entities. This is presented schematically in the diagram on the next page.

Token holders

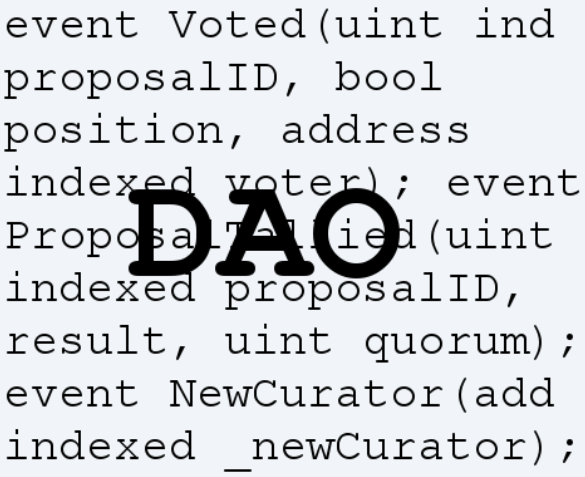
Holders of tokens (e.g. obtained via an ICO) can influence the actions of the DAO, draw profits from it, etc.

Coders

The authors of the DAO's code know its construction best but need not be involved in implementing the DAO.

Regulators

Public institutions, particularly in regulated industries, as well as tax authorities, may take an interest in the DAO's activity.



Contractors

Contractors are people cooperating with the DAO, e.g. providing certain services.

Oracles

Oracles provide various types of data and information from the outside world (beyond the blockchain).

Others

The platform (e.g. Ethereum) and its creators; curators (people who perform certain tasks for the DAO).

DAOs may be used as a vehicle for cooperation (joint venture) between entities in no real-life contact with one another. The "certainty of the code" means that these entities do not need to counter mutual mistrust (e.g. by using a trusted third party).

A DAO is bound by the same restrictions as smart contracts. The example of The DAO (as we write about on p. 25) clearly showed that attempts at total abstraction from the outside world—including the legal rules in force there—can end in disaster.

But these are still very early days for smart contracts and DAO. They offer a fascinating example of the attempt to extend digital reality to further areas of life, including law. We should observe closely how this unfolds. We may witness innovations occurring before our eyes that will change the world around us.

The adventure with smart contracts and DAO began with the blockchain technology, but without doubt we will soon experience further innovations.

The next stage in evolution of the Internet

An interview with Maciej Ołpiński, founder of the Userfeeds.io project, a platform for media applications based on open blockchain protocols, and also animator of the Ethereum community in Poland.

Jacek Czarnecki: What is DAO?

Maciej Ołpiński: DAO is a concept that was born in the community of blockchain enthusiasts, and it means a new form of organisation which can organise economic activity using computer code.

Broadly speaking, we can regard Bitcoin, for example, as a form of DAO. The creators of Bitcoin were the first to prove that economic incentives can be built into computer code, causing people to begin to contribute resources to the Bitcoin network in the real world. The Bitcoin protocol, which has no legal personality and exists only in the virtual sphere, is capable of motivating people in a very real way to supply it with real economic value.

The economic incentives written into the Bitcoin code make the "decentralised organisation" of Bitcoin capable of creating added value, delivering a product to the market which is a cryptocurrency with the economic properties of gold, and at the same time rewarding those who contribute to its success.

In other words, it does that which is the goal of any "classic" organisation. However, instead of hiring staff and renting offices, Bitcoin can gather these resources through incentives written in computer code. This sounds hard to believe, but the mechanism works in practice.

And it works not only for Bitcoin, but also for a range of other protocols attempting to apply the same mechanics to a range of other forms of organisation.

Is DAO a type of such a protocol?

DAO is a collective definition for various types of "economic networks" that operate along the same lines as Bitcoin, but their purpose is not necessarily to create a new cryptocurrency. They can be investment platforms, prediction markets, virtual worlds, social networks, and so on.

Some of these experiments end in disaster (such as The DAO), but I don't think this undermines the sense of the whole concept.

Personally I believe that the infrastructure of the Internet will gradually be replaced by open protocols similar to Bitcoin, and many services now provided by corporations will be provided by various DAOs.

In one of your articles you compared DAOs to the first stock companies in Renaissance Europe. What do they have in common?

Both are a form of coordinating resources (such as knowledge, capital and labour) on a large scale, and a method for dividing the profits flowing from efficient allocation of these resources. A stock company is a kind of abstraction that enables large groups of people to coordinate their economic activity and build value which they could not generate on a smaller scale.

This is obviously a metaphor, but in my view DAOs will be for the information age what global corporations were for the industrial age.

But these forms of organisation are based on a different infrastructure. For existing forms of economic activity, this is the letter of the law and judicial authority. For DAOs it is computer code and blockchain technology.

How does Ethereum enable creation, operation and management of DAOs?

Ethereum is a platform for an application based on blockchain, which enables anyone, via computer code, to record any economic relations and distribute them via the network. In practice, Ethereum allows for experimentation with various forms of DAOs without launching their own blockchain. This all operates on Ethereum's existing blockchain. This lowers entry barriers and makes the technology accessible for a broader number of developers.

At present this is very much a niche field, and at this stage is not understood by most people. Creating a DAO requires knowledge combining technology, economics and game theory. Potential gaps in the code can result in very real financial losses.

No one really knows what economic models will function in the future. It's a bit like the Internet in its first growth phase: complicated to use, unintelligible for most, but with huge potential for the future.

Now most interactions with DAOs occur via special client applications for the Ethereum network. Soon we will be able to connect to DAOs from the browser level. But how to protect the average user in interactions with DAOs is still an open question and will require lots of work.

Are Ethereum, DAOs and smart contracts more than just tech novelties?

Technologies that will change the world in the longer term initially look like novelties, gadgets or even toys for a small group. It will be the same in this case.

In my opinion, this is the next stage in evolution of the Internet. The first phase was the World Wide Web—documents and static web pages. Then we passed to social networks, which today are the standard for online communications for many people. DAO, Ethereum and blockchain are the beginning of global economic networks.

They have an entirely different nature from the previous types of networks. Their force of impact will be greater because they are based on transmission of real economic value, not just information.

It is hard to predict today which models of DAO will prove themselves, but certainly it is a phenomenon to watch.

Interview conducted by Jacek Czarnecki

●

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.

How to design smart contracts and DAO

Jacek Czarnecki

Smart contracts have various faces. They revolutionise the way agreements are concluded and performed, but their potential is much greater. Smart contracts can be used as building blocks for complex social and economic structures. DAO is one example.

The various applications of smart contracts share one thing in common: the potential for fundamental transformation of the legal system. Smart contracts offer the promise of completely shifting legal dealings to the digital world.

This revolution will not occur overnight. We currently have a well-developed legal culture grounded on traditional, analogue instruments. But further projects involving smart contracts continue to develop rapidly before our eyes. In the future these two streams will probably achieve convergence and mutual adaptation.

Before that occurs, we will no doubt face many situations governed on one hand by the coding of a smart contract and on the other hand by traditional legal rules. This is not just a theoretical issue. In practice, creation of smart contracts, including DAO, will require thoughtful and skilful use of traditional legal tools. I believe that these tools already allow us to tap into the potential of smart contracts. Below we describe how this can be done.

1. Combine smart contracts with the law

Traditional legal solutions and smart contracts need not be opponents. To the contrary, they can complement one another well. Skilful employment of the advantages of each can generate synergies, combining the certainty of smart contracts with the flexibility of traditional legal means.

In practice this may involve integration of two solutions that are both evolving. For example, a traditional agreement may serve as a framework providing for a series of further steps. These steps (transactions) may then be executed via smart contracts. In another example, an agreement may provide rules for use of “oracles” (see below), which may be essential for proper execution of the smart contract.

It is important that the smart contract and the traditional contract (or terms and conditions or other classic legal instrument) are not only created together and exist alongside each other, but are also linked. A traditional contract may enclose the terms of a smart contract as an attachment, and the smart contract may refer to the cryptographic hash of the contract digitally signed by the parties.

Certainly a large role will be played in practice by standardised patterns of smart contracts (e.g. for the purposes of certain financial transactions). In this model, the classic contract will serve as a kind of umbrella or packaging for smart contracts.

Sometimes it will be a good idea to embed the smart contract in the real world. An example is creation of a company which will be tied to a smart contract in the form of DAO and will be its link to the real world. Another idea is to tie the smart contract (e.g. in its content) to a specific jurisdiction. This can avoid doubts on which law (from which country) is applicable to the smart contract.

We must remember that a smart contract is not just a digital counterpart to a civil agreement. Numerous different legal relationships, and even complicated institutions like investment funds or public registers, may be reflected through a smart contract. In such cases, integration of classic legal solutions with smart contracts will also be useful.

2. Beware of regulations

Even if you don't follow the foregoing tips, that does not mean that your smart contract will not exert legal effects. It may turn out that conclusion and execution of the smart contract has certain consequences in the traditional legal sphere. For example, it may be deemed to be an element of a traditional contract. This also has to do with tax and regulatory issues, such as payment services, electronic money, securities trading, etc.

3. Ensure identification of the parties

Blockchain provides the possibility of effective cooperation and achievement of consensus among parties that do not know one another, as well as assurance that the parties can be certain that the rules of cooperation are complied with notwithstanding a lack of trust. Smart contracts can also serve this end. With a smart contract you can conduct a transaction with someone you don't know or trust, without the need to use the services of a trusted third party.

To ensure that your smart contract can also be enforced via the traditional legal route (for example if something goes wrong with the code), you must nonetheless ascertain the identity of the other party. This means adequately defining the parties so that there will be no difficulty e.g. in deciding whom to assert a claim against.

4. Take advantage of readymade tools (recognised by the law)

Appearances to the contrary notwithstanding, law and regulations are not entirely at cross-purposes with new technologies. Instruments in the digital world are growing quite rapidly which are recognised by the law and can thus be used to achieve various legal consequences.

A good example is the EU's eIDAS Regulation, which provides a foundation for creating means of electronic identification and tools for performing and using trust services (such as electronic signatures). It is partly thanks to this that soon we will be better-identified in the digital arena than we are using traditional proof of identity, and thanks to new trust services we will be able to sign documents digitally with the same effect as a handwritten signature.

Employing such tools can greatly simplify the use of smart contracts and also make it possible to define the legal consequences of any smart contract.

5. Use oracles skilfully

The limited ability to obtain, process and verify information from the real world (external to the blockchain) is regarded as a weakness of smart contracts. A smart contract whose execution is supposed to depend on performance of some act in the real world (such as concluding a marriage or acquiring a company) must, if it is to be effective, be in a position to verify whether the act has occurred.

In practice this is done using "oracles." Their main role is to confirm some state of affairs and forward the information in a form that can be accepted by the smart contract in the relevant blockchain. The oracle thus serves as a kind of messenger between the real world and the digital world and the blockchain in question.

Good construction of oracles in a smart contract is vital. If a person is to serve as the oracle, it must be ensured through traditional legal means that he will provide accurate information. An oracle could also take the form of an algorithm. In either case, the situation where something does not go right at the level of the smart contract must be provided for. Then traditional legal solutions may be the only rescue.

6. Consider how the smart contract will be executed and consider limitations

Just as a smart contract and the blockchain on which it functions may require external sources of information (oracles), so execution of a smart contract will often require a connection to the outside world. Essentially, a smart contract functions in the given blockchain, and the effect of the action is modification of the content of the database (i.e. the blockchain itself). So consider whether this consequence of execution of the smart contract will be sufficient for the parties. Perhaps it should be followed by actions within a traditional legal relationship.

7. Audit all existing solutions

The review should cover not only smart contracts and legal documentation. Their mutual compatibility is crucial. Perhaps it should be specified what will prevail if there is a conflict between the rules of the smart contract and the rules determined through classic legal arrangements.

8. Ensure the flexibility of the smart contract

A simple smart contract is a set of deterministic rules that will be executed automatically if the specified events occur. Once the smart contract has been created, the parties cannot change its rules. The smart contract is "blind" and will be executed exactly as it was programmed. On one hand this is an advantage, because the parties do not have to worry about enforcing the obligations of the other party. But experience shows that sometimes a contract must be amended or adapted to new circumstances. This can be furthered by traditional legal institutions such as *rebus sic stantibus* (an extraordinary change in circumstances), permitting modification of the parties' original arrangements.

It is worth considering adding some flexibility to the smart contract. This could consist of the possibility of amending it by both parties acting together or through a trusted third party.

9. Think about a safety valve

The example of The DAO vividly showed that a defective smart contract can lead to unforeseen consequences. Moreover, as mentioned, a smart contract is "blind." Consequently, even if it was constructed in accordance with the parties' intentions, a change in circumstances may incline the parties to seek to change the rules of play. It can be worthwhile to add a "safety value," a solution that allow you to escape unscathed from the smart contract even if something goes wrong.

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.

●

Blockchain is the foundation of a digital economy based on cooperation

An interview with Maciej Jędrzejczyk and Karolina Marzantowicz from IBM

Jacek Czarnecki: Blockchain is sometimes called the "Internet of value." How does IBM perceive the potential of this technology?

Maciej Jędrzejczyk: Blockchain is a distributed ledger technology, a new-generation technology we can apply in transactional systems. It provides cryptographically guaranteed trust and transparency while streamlining business processes with the use of a single decentralised register among users.

Thanks to this technology, we can reliably automate business interactions among numerous partners, and potentially also create new styles of digital interaction. Blockchain allows for great reduction in the operating costs of business processes and the complexity of processes between various organisations. The distributed ledger makes it possible to create business networks for a single market or group of partners where practically everything, every transaction, can be preserved without the need for a central control point.

Blockchain introduces new possibilities for exchange of values and resources in the digital economy. The distributed register encourages cooperation within a defined ecosystem, and cooperation is one of the foundations of the digital economy. Blockchain also makes it possible to build digital trust which does not have to be guaranteed by any third party. The technology excludes corruption, forgery or manipulation of facts (transactions).

Dispersion, decentralisation, irrefutability and finality are key features of the blockchain technology and the algorithms it uses. The applications for this technology are extremely broad and affect any sector where there are many different participants, where central registers are used, where values or funds are exchanged, or we need a guarantee of the status of the data.

But blockchain is not a panacea for all challenges of the digital revolution. It is a response to only certain of the challenges.

IBM is developing the Watson supercomputer, which can answer questions in natural language. Can blockchain be used in this project?

Karolina Marzantowicz: IBM Watson is a cognitive computing system. It understands natural language and formulates hypotheses and conclusions operating on large sets of unstructured data, including multimedia. It validates the data and also learns. Cognitive computing systems will change the way people interact with technology and expand out expert possibilities. IBM Watson is constructed to reflect the action of the human mind in the cognitive process, as far as the attainments of modern science allow.

Blockchain is assumed to provide confirmation of the origin of every block in the chain (and, it follows, the origin of what the transactions in the block involve), together with a full history of changes. Additionally, it provides a guarantee of the accuracy of the transactions, backed by advanced cryptography. In the future, blockchain will enable far-reaching automation of processing in the digital economy, particularly in the area of the Internet of Things, enabling business interactions between sensors and increasingly more intelligent devices. Firms can exchange with each other data processed in the Internet of Things via a blockchain network, because this solution will be less complicated and cheaper to install and maintain. Cognitive computing systems can be the source of knowledge, signals that will feed the blockchain network, or smart contracts. Blockchain is the foundation of a digital economy based on cooperation. The Internet of Things extends the boundaries of IT beyond traditional data centres and requires a new communication medium based on a distributed architecture. Traditional analytics are powerful when it comes to drawing conclusions from huge quantities of unstructured data. Cognitive computing systems are not only capable of helping find the answers a business needs, but are also changing the way we communicate with technology, which we will encounter more and more of in life.

What is the Hyperledger project?

Maciej Jędrzejczyk: Hyperledger is a consortium of over 80 firms from a range of sectors (IT, banks, startups, exchanges) jointly growing the forces of distributed ledger technology (DLT) based on blockchain. The project is administered by the Linux Foundation, which ensures complete objectivity and transparency in taking decisions on the direction of the measures taken. The goal of the Hyperledger project is to create an open standard for transformation of business relations and processes.

Hyperledger can be regarded as an umbrella under which three initiatives are currently being incubated:

- Fabric: implementation of blockchain technology tailored to business needs
- Sawtooth Lake: implementation of blockchain technology optimised for the Internet of Things
- Hyperledger Blockchain Explorer: a universal graphic panel for analysis of events and transactions in networks based on technologies using Fabric or Sawtooth Lake code.

The Hyperledger project also introduces an architectural framework that should be included in each incubated project. First, every initiative should base its solution on open standards, protocols and licensing models. Second, the solution should support communications between different networks based on blockchain, other distributed ledgers, or other traditional data systems (system of record or SOR).

As the target users of the solutions is business organisations, the incubated code should natively support transactions in every type of asset (monetary or non-monetary) that can occur in complete privacy between the parties. To meet the needs of business, another requirement is scalability, modularity, and expandability of the specific components (such as the consensus mechanism, role management, network access administration), and, following from this, total flexibility without the need to modify the basic source code.

Can Hyperledger be used to conclude and executive smart contracts?

Karolina Marzantowicz: Given the nature of the target user, it is obvious that the incubated solutions must support smart contracts. This follows from the interpretation of smart contracts as a method for moving existing business processes to code understood by the parties to the contract and the nodes functioning within the blockchain network. For example, in the Fabric incubator, smart contracts (called Chaincode here) are not only the carrier of the rules under which the parties will conduct transactions, but will literally become an intermediary in the interaction between the parties, which will later be entered in the blockchain. This is fundamental because it means that the basic source code of Fabric does not impose rules of interaction between the parties but leaves that to the logic of the smart contracts.

Here it should be mentioned that in the context of the requirement of full modularity, smart contracts on the Fabric platform may be recorded in various programming languages, and the interpretation of their contents is conducted automatically by the base code. This greatly reduces entry barriers for firms using this solution, because it is much easier to find a Java, Node.js or GOLANG programmer (Chaincode can be prepared "out-of-the-box" in all of these languages), than, for example, a Solidity programmer (the programming language for smart contracts for Ethereum).

As with all solutions designed for business, a key to success is security. In the case of Fabric, every smart contract is launched in a "sandbox," insulating the rest of the network and its participants from the effects of the executed code.

Are the law and regulations a barrier to development of blockchain technology?

Karolina Marzantowicz: Yes and no. On one hand, every day we witness the birth of new, often successful projects implementing solutions based on blockchain across numerous sectors of the economy. This takes place under the existing legal and regulatory order, including in sectors subject to strict oversight such as banking and public administration. The flip side of the coin is the countless initiatives launched in the cryptocurrency community and specific blockchain consortia aimed at raising lawmakers' awareness of the significance of these technologies and the need to open up to them. The very existence of such initiatives in many countries demonstrates the need for a discussion of the current legal system.

Analogous situations can be encountered locally in Poland. An example is the position concerning blockchain and cryptocurrencies, the fruits of a task force of lawyers from this "stream" formed at the initiative of the Ministry of Digital Affairs. The presentations and the speakers' conclusions presented during recent social consultations at the Polish Parliament show the need for ongoing dialogue with the government to create legal instruments enabling protection of ventures based on these new technologies.

How should the public authorities approach applications of blockchain technology such as smart contracts and DAO?

Maciej Jędrzejczyk: Technology usually outpaces the existing legal order, and this is a normal state of affairs. However, flexibility in the law allows existing standards to be adapted to new phenomena, such as smart contracts. Certainly there are parties out there conducting transactions in this form and dispensing with any official legal interpretation. But if it becomes necessary to resolve a conflict that was not provided for by the smart contract, they will turn to the law of their jurisdiction. The example of DAO is not so different in this respect, and should be treated the same way. The authorities should be prepared with the knowledge to deal with such situations. Fortunately, in this respect they can rely on the experts from the "stream" I mentioned.

Lawmakers should take a favourable approach to these new methods of arranging the rules for human interaction, also with an eye on the fruits of these interactions, i.e. digital assets and the register of ownership relations which have no equivalents in the physical world. Blockchain greatly facilitates the creation of such assets, and smart contracts expedite transactional processes of exchange.

Interview conducted by Jacek Czarnecki

What the history of The DAO says about the law

Agnieszka Kraińska

The rise and fall of The DAO tells a tale of how the reality of the virtual world outpaces existing legal regulations and generates new problems which have yet to find answers.

The DAO

"The DAO" was a type of decentralised autonomous organisation, a *sui generis* entity intended to generate income from investment activity using instruments similar to financial instruments. According to the founders' declaration on the website daohub.org, the purpose of The DAO was to use units of the Ethereum cryptocurrency (ethers, ETH) held by the organisation to support ventures generating favourable returns on investments for the organisation and its members. The structure thus shared certain features of a crowdfunding investment platform or a venture-capital fund.

The creation phase of The DAO ran from 30 April to 28 May 2016, when investors could pay in ETH and in exchange receive tokens of The DAO. The tokens entitled the holder to vote on how the funds gathered by the organisation would be invested. The launch phase proved a huge success, attracting funds worth about USD 150 million.

To understand later events, it is important to know that The DAO was a structure dependent on the actions of four types of entities: creators, investors, contractors, and curators. The creators were the authors of the open software through which the platform arose. The investors (DAO token holders) were those who obtained voting rights in exchange for contributing ETH. The contractors presented ventures which The DAO could invest in. The curators collected and verified proposals and put them up to a vote.

Attack

The DAO was hit by an attack on 17 June 2016 that drained about a third of the ETH from the organisation. The attack was made possible by exploiting a feature of the code of The DAO which the creators had missed. This resulted in the creation of a “child DAO,” called the “Dark DAO” which held the drained ETH.

The vulnerability of the system exploited by the hacker resulted from the characteristics of the “split” function enabling investors’ funds to be transferred from The DAO to a separate DAO. A consequence of the split was liquidation (burning) of The DAO tokens after transfer of the corresponding amount of ETH to the new child DAO. The characteristics of the split code (recursive call vulnerability) allowed the hacker to submit repeated demands to withdraw ETH, resulting in numerous transfers of ETH out of The DAO.

Response to attack

In terms of code, the Dark DAO was a clone of The DAO, so removal of the funds from the new organisation was possible only after completion of the process of creation of the Dark DAO and the time necessary to take the following steps. For this reason The DAO community had time to analyse the situation.

Considering the assumption that blockchain and smart contracts cannot be forged, are autonomous and not subject to institutional control, the question arose whether it could be said that the hacker had acted unlawfully at all. A letter from a person calling himself “the Attacker” appeared on the web. The Attacker explained that the removal of funds from The DAO resulted from specific features of the programme which he exploited, and thus his actions could not be regarded as theft.

But the discussions on The DAO and Ethereum forums showed that most participants in the Ethereum blockchain expected countermeasures to be taken against the attack by altering the current state of the blockchain so that the ETH invested in The DAO could be recovered. The DAO project proved to be debacle.

Meanwhile, a group of “white hats” exploiting the same split function as the creator of the Dark DAO withdrew the remaining 2/3 of the ETH from The DAO to the “White DAO” (a new child DAO) to prevent further attacks.

Hard fork

Finally it was agreed that on 20 July 2016 a “hard fork” would be introduced into the Ethereum blockchain. The scenario for the hard fork involved creation of a new blockchain containing a modification with respect to The DAO. For the change to be effective, it had to be approved by the users of the blockchain. The modification introduced with respect to The DAO was to consist of creation of a contract for refund of the ETH to all holders of The DAO tokens (as if the Dark DAO and the White DAO had never arisen). The hard fork scenario guaranteed the holders of The DAO tokens that they would recover their invested funds, but it carried the risk of splitting the Ethereum network into two separate networks; users who did not join the hard fork would remain in the original Ethereum blockchain.

The hard fork was introduced at the agreed time and over 90% of the users followed it. The contract for refund of ETH set the rate of 100 The DAO tokens per ETH. Within a few hours, 41% of the funds had been returned to the investors (and about 80% within a month). It might appear that the original blockchain would “die” because the cryptocurrency there would not be exchangeable, even though a fraction of the community had decided to maintain it.

However, contrary to earlier declarations, one of the cryptocurrency exchanges, followed by others, decided to admit ethers from the original blockchain into trading under the name ETC (the name ETH being transferred to the new blockchain). Consequently, the users of the new blockchain held not only the ETH, but also the corresponding ETC on the old blockchain, which, although worth less than ETH, are not worthless.

Legal issues

The rules for the project, disclaimers of liability and various caveats were presented on the website daohub.org. The main assumption was that the rules for operation of The DAO are based on the code of smart contracts in the Ethereum blockchain. It was also stressed that the code of The DAO's smart contracts and the generated tokens entail significant financial risk, including a risk connected with use of experimental software. It was stipulated that The DAO tokens do not represent shares or the equivalent in any company or other entity, in any jurisdiction, and that the documents presented do not constitute a prospectus or proposal to invest, nor an offer to acquire securities in any jurisdiction.

Acceptance of the presented rules for operation of The DAO results among other things in waiver of the right to file class actions or commence arbitration against any entity involved in creation of The DAO. This was deemed to mean acceptance of the experimental nature of The DAO and the risks connected with the trial platform Ethereum.

The attack against The DAO and the measures taken to prevent ultimate removal of the funds led to a re-examination of the view of the objective accuracy of blockchain, unfalsifiable and not subject to any institutional control. Contrary to the original assumptions of the creators of the project, the rules for operation of the project were not determined exclusively by the code (which contained an unforeseen property in the split function), but also by norms of contractual integrity generally recognised by the participants. In other words, most of the participants in the project were convinced of the inaccuracy of the objective truth captured in the blockchain and decided to change it by introducing and accepting the hard fork. Only in light of this common belief could there be said to be a difference in assessment of the actions of the hacker who created the Dark DAO and the hackers who created the White DAO. From the point of view of the code, their actions were of the same nature.

Contrary to the assumed autonomy of the blockchain in the history of The DAO, social oversight occurred and a situation unacceptable to the clear majority of the participants was corrected. The principle of the objective truth of the code was thus countered by a kind of generally recognised norm, and that norm prevailed.

The actions of the creators of the project, notwithstanding the exclusions of liability and the other caveats set forth in the assumptions for the project, clearly aimed at restoring the funds contributed to The DAO. Measures were taken to satisfy those investors who because of the change in the price of tokens in ETH at the time of creation of The DAO are injured by the rate of return (the "extra balance" problem). Measures were also taken in favour of those who made the split to the child DAO and burned their token in The DAO before the attack and creation of the Dark DAO and the White DAO.

The paradox is that despite all this, the original blockchain was still maintained, causing the existence of two alternative realities. This situation generates various controversies, including legal controversies connected with the manner of return to investors of the ETC maintained on that blockchain. Doubts are also generated by the behaviour of the cryptocurrency exchanges, which despite prior assurances decided to trade in ETC, keeping the original blockchain alive. The negotiability of ETC reduces the value of ETH, and thus investors could potentially assert claims against these exchanges.

But because The DAO was a *sui generis* entity and an exclusively digital existence, there was and is no law governing the behaviour with respect to these legal issues. Essentially we observed a process of self-regulation in accordance with general principles of equity and contractual integrity. Perhaps there is no possibility of regulating this phenomenon, and the events demonstrated that the community could cope by applying generally recognised metanorms.

●

We will complement existing structures

An interview with Julian Zawistowski, entrepreneur and leader of the Golem project

Jacek Czarnecki: What is the Golem project?

Julian Zawistowski: In this project we are creating software making it possible to perform dispersed calculations in a peer-to-peer network. The assumption is that every user linking to the network can transmit computational tasks to the network that are performed by other users. Of course, the user transmitting the task must pay the user performing the calculation for this service.

A characteristic feature of a P2P network is that it operates without central points. The relations between the specific users of the system are direct and no intermediary arises between them, for example regulating the market and buying or selling computing power. The fact that the system is entirely decentralised provides incredible technical possibilities but also presents serious challenges.

What role does Ethereum play in the project?

Ethereum is used as the transactional layer. A decentralised system for obvious reasons should use a decentralised payment system. Something can hardly be said to be decentralised, independent from a breakdown in the central node, if at the same time transactions are settled for example with credit cards or bank transfers. This naturally indicates that in Golem transactions should be performed using cryptocurrencies. Among those, Ethereum is the best choice due to a range of features enabling construction of a much more refined solution than in the case of other blockchain technologies.

For the project you use smart contracts based on Ethereum. What possibilities do such contracts provide you?

First, they enable construction of a fairly complex transactional system. A transaction need not consist of the simple transmission of funds from one account to another. Thanks to these contracts, the system can be significantly expanded, e.g. by grouping transactions and settling them in larger groups or even introducing more refined solutions, such as payment channels or probabilistic nanopayments. Without going into the details of these solutions, they enable significant reduction of transaction costs, to the level where it is possible to conduct many, many transactions of very low value.

Second, the contracts provide us great flexibility in selection of the payment model in the Golem network. This is particularly important for creators of software. When deciding to integrate with Golem, they will be able to define their own fee model for use of their software.

Third, we intend to use these contracts in reputation and identification solutions—which is key in a distributed system for proper functioning of a network which by definition lacks an overriding moderator who could for example remove harmful users from the network.

It should be stressed that we will not have to create all the components ourselves. The Ethereum community is very active, and a great many projects are being created based on this technology which we can use in the future.

Did you think of using DAO?

Yes, but the collapse of The DAO clearly showed that Ethereum is not yet ready for such complex solutions.

Before the collapse of The DAO you intended to use the funds gathered there. In your view, will the failure of this project impact the growth of other DAOs?

Certainly, but it should be borne in mind that there are two projects functioning based on assumptions similar to The DAO (Maker and Digix), which appear to be managing on the technology front. But The DAO made it clear to everyone that Ethereum, and in particular the Solidity programming language used in it, is much harder to use—particularly with complete security—than it might seem. I think that until this problem is solved, creation of such complex autonomous structures as The DAO is too risky.

You are thus creating a decentralised market for computing power together with a transactional layer, which thanks to Ethereum and smart contracts is also decentralised. Do you believe such solutions will replace existing structures and business models?

We will rather complement existing structures, altering to some degree their business model for gaining and retaining customers. I don't believe individual computers can replace professional computational centres on a mass scale. There are certain classes of applications for which an ordinary computer will be competitive with a computational centre, but in most instances professional solutions will have the advantage in quality and price. What we want to achieve is creation of an efficient market (approaching perfect competition) for computing power, integrated with the market for the programming using this capacity.

Interview conducted by Jacek Czarnecki

DAO and taxes – selected issues

Joanna Prokurat

"The subject of taxation is of the most essential importance in the economic conception of any tax. What the tax must be paid on is evidence of the imagination and knowledge of lawmakers and the degree of development of tax law" (W. Modzelewski, *Introduction to the Study of Tax Law*, Warsaw 2005). Not only in terms of the subject of taxation, but also other structural elements, DAO may prove an arch-difficult test for both the knowledge and the imagination of lawmakers drafting the tax law and the authorities enforcing it.

The tax system is principally characterised by universality of taxation, and only exceptionally can events or entities remain beyond its purview. As an abstract system, the subject of taxation is typically regarded as practically any event generating a certain value—for purposes of income tax generally an accretion of wealth, or for purposes of VAT, added value. And in turn, any entity, regardless of legal form, is generally regarded as a taxpayer, although a tax obligation may be assigned according to additional factors such as tax residency (for income-tax purposes) or the status of a trader and the nature of the transaction (for VAT purposes). As a DAO (decentralised autonomous organisation) can generate profits in the economic and financial sense, it may also be tied to a tax obligation. Certainly this result is the subject of interest of the treasury seeking to maximise public revenues.

But in the case of DAO—innovative entities shattering well-worn schemata—pursuing this task of the tax authorities may pose numerous difficulties. Even though virtual reality is not an entirely new phenomenon and has presented various challenges to the tax system for some time (as for example with the Internet), DAO appears to create an entirely new paradigm not only in terms of technology but also for economics and law, including with respect to tax obligations. The technical aspects of DAO are understood for now only by a small number of people, and for tax purposes DAO may not be grasped by anyone. Hence the difficulty in translating DAO into the language of the structural elements of the tax system created in Poland in the 1990s, when notions like blockchain, DAO, AI, or even universal Internet access were as far-fetched as intergalactic space travel.

First and foremost, DAO is not an entity recognised by the existing tax system. As this is not a logically closed system, it remains open to new forms of doing business, investing, or pursuing other activities generating revenue and profit. After all, DAO might be perceived in terms of a joint venture, a construction already recognised by the tax system, particularly for income-tax purposes.

A joint venture it not itself a taxpayer for purposes of income tax; rather, the participants in the joint venture are the taxpayers. They are required to declare their income (the personal income tax regulations distinguish 10 sources of business income subject to different settlement rules), expenses and other tax attributes arising out of the joint venture in proportion to their established share in the profits (or in equal proportions if this share has not been determined). So potentially DAO could be classified as a joint venture for purposes of tax law.

Such a classification should not conflict with the possible differentiation in the involvement by specific entities in the decision-making processes or property rights within the DAO. This tax conception of DAO is similar to that of a partnership without legal personality (other than a joint-stock limited partnership), which also is not a payer of income tax but the revenue, costs and other tax attributes generated by the partnership are allocated to the partners (assuming they themselves are not also transparent for income-tax purposes).

But this treatment of DAO may not be universal. For example, a DAO might not be an undertaking of a commercial or gainful character, and it appears that only such undertakings are currently treated as joint ventures under the tax regulations.

The concept of DAO as a joint venture may also not be consistent with the conception of the subject of taxation and not be suited to the potential transfers within the DAO. Such transfers may vary in nature, from those we could consider technical (e.g. linking to another DAO) or those that are truly financial and economic (e.g. sale of "rights" to the DAO). Viewed through the prism of the regulations now in force, unified treatment of DAO could lead to internal competition within the tax system, particularly for purposes of personal income tax, as the PIT Act breaks out 10 different sources of income. The notion of DAO as a joint venture for tax purposes implies that it should be taxed as a source of business income, but the given DAO may actually have a purely investment nature, or might constitute an online company comparable to the existing notion of a joint-stock company (although this does not mean a joint-stock company established on the Internet, but a new form of company based on DAO).

It should be pointed out by the way that treatment of DAO as a tax joint venture may not serve the interests of its participants (although their interests might not be considered relevant by the treasury pursuing its budgetary tasks). For example, participants in a non-profit DAO might wish to enjoy an exemption from income tax for organisations pursuing socially beneficial purposes defined in the tax law.

Moreover, classifying DAO as a joint venture (or for that matter as any other type of entity currently known to the tax law) doesn't answer the question of how to break through the anonymity of its participants which is inherent to DAO. Anonymity as such may be a temptation for tax evaders. But the tax system does have sanctions at its disposal, such as the possibility of imposing a 75% tax on income from undisclosed sources, which could include DAO (but this still leaves the question of identifying the taxpayers and collecting the tax).

At the early stages, the anonymity of DAO, combined with its cross-border reach, may at the very least hinder the allocation of potential revenue or profit to specific jurisdictions. For income-tax purposes, without answering the question of the tax residency of the holder, practically speaking DAO does not enable income to be assigned to a given country under the principle of taxation at the place where the income is generated. This could cause conflicts between countries managing to identify income from DAO and allocate it to their jurisdiction, leading to double or multiple taxation of the same income). Meanwhile, for VAT purposes, the anonymity of DAO means that the status of the participants as VAT payers, and their business location, cannot be identified, and thus it cannot be determined whether the operations are business-to-business or business-to-consumer—which is hugely important for determining the place of supply, and hence the place where VAT is charged, as well as determining who is required to pay the VAT.

Another challenge in identifying who is required to pay tax is presented by the nature of DAO and the fact that the identity of the participants could change many times in the course of a single day.

Documentation and recording of taxable events connected with DAO presents an equally difficult test for taxpayers and tax authorities alike.

Just a few general examples are presented above of the issues that may face taxpayers involved in DAO-type projects as well as the tax authorities. Legislative intervention appears premature at this stage, in part because of the shortage of relevant knowledge about the nature of DAO itself and its mechanisms, which could lead to adoption of inappropriate regulations. But legislative intervention cannot be ruled out in the future. Certain measures could also be taken by the authorities responsible for interpreting tax law, for example by issuing a general interpretation. This would not only make it easier for DAO participants regarded as taxpayers in Poland to settle their taxes, but if well constructed and clear could serve as an incentive for foreign players to choose Poland as their tax jurisdiction for DAO. Nor can it be ruled out that the treasury could make this mandatory for all DAO—or join DAO itself. This could give the authorities knowledge and even influence over the processes occurring within DAO. Automatic collection of tax could also come into play. This notion seems no more abstract than the notion of DAO itself.

DAO and criminal law

Krzysztof Wojdyło

The action of a DAO or smart contract may conflict with the laws in force in a given jurisdiction. How will criminal provisions apply in such situations? Who is exposed to a risk of criminal responsibility in that case?

Criminal law in the Internet era

The rapid growth of cybercrime, particularly in the last few years, has exposed weaknesses in contemporary criminal law. Offences in cyberspace are not only much harder to uncover, but they also are often international in scope. The international element can be the source of the biggest legal issues.

These offences are committed in cyberspace, an autonomous virtual arena which is difficult to assign to a specific jurisdiction. But the criminal law requires each offence to be identified with a certain jurisdiction (if for no other reason, to determine whether the act is indeed punishable, and if so, under what rules criminal responsibility can be imposed). Consequently, the rule in the case of cybercrime is to assess the offence simultaneously from the perspective of multiple jurisdictions, which generates great uncertainty among entities operating online.

In the face of this type of competition between legal systems, it becomes key to establish criteria enabling an ultimate selection of the jurisdiction. The laws of different countries define these criteria differently. One of the most common criteria is the place where the offence was committed. This criterion is also applied by the Polish Criminal Code, which provides that Polish criminal law will apply to a perpetrator who committed a prohibited act in the territory of the Republic of Poland, or on a Polish ship or aircraft. The code also provides that a prohibited act is deemed to be committed at the place where the perpetrator acted, or failed to take an action he was obliged to take, or where a consequence constituting an element of the offence occurred or was intended by the perpetrator to occur. The problem is that similar provisions are found in numerous legal systems, which given the nature of online offences does not eliminate a conflict between jurisdictions.

For example, a website providing illegal services may commit an offence in the state where the site's infrastructure is located, but also in the country where the user of the site is found. If one of the elements of the offence is the occurrence of consequences of the offence in the territory of a given country, the perpetrator's action or presence in the territory of that state is not necessary for the offence to be deemed to be committed in that state.

These rules may generate additional consequences seriously hindering online operations. A situation is readily imaginable where an activity is conducted legally in the country where the operator of a site is registered or has its technical infrastructure, but is illegal in countries where some users of the site are located. Thus the operator of the site might face criminal liability under the laws in force in the countries where the users are located, even though the activity is legal where the site is registered.

This instance also raises a factual difficulty in holding the perpetrator responsible, particularly if that person is in a country that does not recognise the given behaviour as a criminal offence. In such instances, potential extradition of the suspect to another country is governed by international agreements. The case is somewhat different when the perpetrator has assets in the state where his behaviour is punishable. Then the perpetrator faces the risk of sanctions being enforced against his assets in the other country.

DAO from the perspective of principles of criminal responsibility

These difficulties also apply to DAO (decentralised autonomous organisation) and smart contracts. Here there may also be competition between jurisdictions in terms of the legal classification of certain actions. Imagine a DAO that creates a model for a decentralised casino where individual users can enter into transactions that are a form of gambling. Depending on the jurisdiction, the activity organised using the DAO may be allowed or may be treated as an offence. From this perspective, the DAO is similar to other ventures organised in cyberspace.

But undoubtedly a distinguishing feature of DAO in the context of criminal responsibility is the difficulty in assigning potential responsibility to a specific person. In more traditional organisations, it is generally the members of the corporate authorities who may be held responsible for the organisation's conduct of illegal activity. But the construction of many DAOs does not provide for the existence of any authorities. DAO is an autonomous algorithm functioning in a dispersed network. It is the algorithm, not a specific person, that carries out the potential elements of the prohibited act. But fundamentally, criminal responsibility is imposed on persons and not on abstract beings in the form of an algorithm. This property of DAO undoubtedly hampers criminal enforcement. But appearances to the contrary notwithstanding, it does not make enforcement entirely impossible.

Who is responsible for DAO?

The lack of authorities of a DAO and the inability to ascribe to a DAO legal capacity or criminal capacity naturally gives rise to a need to seek out other entities who might potentially bear responsibility for unlawful actions carried out via DAO.

Returning for a moment to the gambling example, we assume that in the given jurisdiction a provision of criminal law states that organising games of chance is an offence. The action determining the offence in this case is "organising" games. Understood in this sense, this element of the offence is fulfilled primarily by the action of an impersonal algorithm. But it should be borne in mind that most criminal law systems recognise various forms of commission of offences. It is not only the immediate perpetrator fulfilling the elements of the prohibited act who can be held criminally responsible. The possibility of imposing criminal responsibility on an aider and abettor, or an accessory to an offence, seems particularly relevant in this context. Different legal systems will no doubt define these roles differently. For example, Polish law understands an accessory to an offence to mean one who, among other things, takes actions intended to create the conditions for taking the action immediately aimed at commission of the offence, while aiding and abetting might involve, for example, providing instruments facilitating commission of the offence.

Holding a specific person responsible as an accessory or for aiding and abetting will still require fulfilment of a number of prerequisites and will depend on the specifics of the DAO in question. But this possibility cannot be ruled out in advance. Given the nature of DAO, it may be assumed that the creators of the DAO algorithms and persons acting as oracles may be particularly exposed to potential responsibility. In certain situations, possible responsibility of holders of DAO tokens and users of the DAO also cannot be excluded.

Based on observations of early DAOs, it may be assumed that a particular legal risk may be connected with conducting an ICO (initial coin offering—see below). Collecting funds for growth of a DAO as well as issuing any tokens might make it necessary to comply with regulations governing public offering of financial instruments. Even if the persons organising the ICO are operating in a jurisdiction where the collection is permitted, it cannot be excluded that the ICO will be treated as an offence in other jurisdictions where the ICO is accessible. The restrictive regulations governing the US capital markets deserve particular attention in this respect.

Legal aspects of initial coin offerings and token crowdsales

Jacek Czarnecki

Many projects developed on the basis of public blockchains, such as Bitcoin or Ethereum, are fascinating technological solutions. One of the aspects of their development is the need to raise funds for this purpose. Recent months have shown dynamic growth in interest in new fundraising methods for blockchain projects: initial coin offerings (ICO), also known as "coin crowdsales" or "token crowdsales."

ICO

Often the easiest place for creators of blockchain projects to raise funds for development is in the community that best understands such projects and services and also includes future customers.

So it's no wonder that many such projects obtain financing through an ICO, i.e. issuing a specified (crypto)token on a public blockchain (most often Ethereum) and selling the tokens to anyone interested in investing in the project. The issued tokens are usually sold for cryptocurrencies with measurable economic value: bitcoins or ethers (the native unit of the Ethereum network).

An ICO may be conducted by a DAO (decentralised autonomous organisation) or a more traditional entity. These may operate classic business activity, even loosely connected with the blockchain technology. But the goal of the ICO is universal: obtaining funds for development of the project.

The ICO procedure can be much easier, cheaper and more efficient than traditional fundraising measures. The effectiveness of ICO was demonstrated by The DAO, where in exchange for issuance of its tokens The DAO raised ethers worth about USD 150 million.

Another advantage of ICOs is the flexibility in shaping the characteristics of each token sold. They can have various features.

1. **Decisional rights**. Sometimes a token acquired via an ICO carries certain entitlements for its holder which are not strictly financial in nature—for example the right to participate in voting (binding or non-binding) on matters material to the project, which makes it similar to the rights of shareholders in traditional companies. Sometimes the token plays major role in the decentralised application (dapp) developed in the project and can give the holder access to products and services offered via the dapp.

2. **Quasi-financial instruments**. The characteristics of some tokens means that they perform functions similar to traditional financial instruments. Some tokens have features similar to equity instruments, as their possession is tied for example to participation in future profits generated by the project. Other tokens,

drawing from the construction of debt instruments, offer the right to payment of a certain value upon fulfilment of specified conditions. Many tokens have a mixed character, combining some features of a financial instrument with access to services.

3. **Other**. Along with the growth of the blockchain technology and similar solutions, we may anticipate the appearance of new types of tokens. Sometimes we intuitively try to compare the rights arising out of a token with money, financial instruments or securities. The term "token" itself can be misleading as it suggests the existence of some medium. But tokens are generally entries in a database and can be used for various purposes. They can represent extremely varied types of values. In practice no exhaustive catalogue of types of tokens can be offered.

The investment potential of the acquired tokens is also vital from the point of view of the persons taking part in the ICO. Typically the tokens can be traded, e.g. on crypto-currency exchanges. Sometimes their trading prices are subject to huge fluctuations, encouraging speculation.

Moreover, successful projects offer a high rate of return on the virtual investment. For example, ethers were sold in the first phase of the Ether Sale at a rate of ETH 1 = BTC 0.0005 but by mid-March 2016 were trading at about BTC 0.0345/ETH 1. The flip side obviously is the extraordinary risk connected with investments in ICOs.

As noted, tokens sold in ICOs or similar campaigns can have various different characteristics. The possibility of shaping the rights tied to possession of a given token is essentially wide open and depends on skilful use of programming code. This makes it hard to capture in legal terms the successive phases in the life of a token: generation, sale, and possession.

Legal characteristics of tokens

An attempt to apply existing regulations on public trading in financial instruments to ICOs will largely depend on the answer to the question of whether the given token has the characteristics of a financial instrument under the existing legal definition.

In Poland, in each case this determination will require an analysis of a broad catalogue of financial instruments set forth in Art. 2 of the Act on Trading in Financial Instruments. The difficulty of this task can be illustrated by the attempt to determine whether the rights arising out of a token can be regarded as rights arising out of securities, and, as that implies, whether the token can be regarded as a type of security.

It should be pointed out by the way that a token will typically be regarded as a property right. The Civil Code uses a broad notion of property rights, deeming them in Art. 44 to cover various types of property interests (not only ownership). Sometimes tokens will hold a certain measurable value despite being bereft of any material substratum. They should thus be classified as a type of intangible, deemed to be property for purposes of the Civil Code and capable of being the subject of civil-law relationships.

A starting point for assessing the legal status of a token will be an analysis of the general provisions governing securities in the Civil Code. Pursuant to Civil Code Art. 921^{6}, a security has the following fundamental characteristics:

- It has the form of a document.
- An obligation of a given obligor arises out of the security.
- Possession of the security is necessary to effectively enforce the performance of the obligation by the obligor.

Leaving aside the special characteristics of securities that can take dematerialised form pursuant to special regulations, it appears that a barrier to classifying a token as a security in the foregoing sense is the requirement that the security be in the form of a document. But for some time a "document" has been legally defined in the Civil Code as "a carrier of information enabling knowledge of its content." This raises the doubt whether a token—typically an entry in a decentralised database—can be regarded as a carrier of information.

The issue of whether an obligation of a certain obligor arises out the token, and whether possession of the token is necessary to enforce the obligor's performance of the obligation, will generate a range of controversies. The construction of the legal institution of a security is based on contractual obligations among various entities. A token will not always have this character.

The regulations don't always enable a definitive determination of whether a given token is a financial instrument. Sometimes a basic analysis of the fundamental conditions from the definition of a given financial instrument will be necessary, but this does not guarantee that an unequivocal conclusion will be reached. So entities interested in conducting ICOs must be aware of these doubts and factor any related legal risks into their actions.

Legal issues related to ICO

From the legal point of view, the ICO triggers associations with known methods of fundraising by commercial entities—whether more traditional (a public offering of securities) or less traditional (crowdfunding). Because there are no special laws governing fundraising via ICOs, potential application of legal instruments from various fields of law should be considered.

The first question is whether ICOs and the sale of tokens in ICOs can be referred to in the context of regulations governing offering and trading of financial instruments. Not without reason, the term "ICO" alludes to the term "IPO" (initial public offering). In practice, the ICO displays many similarities to raising funds by a public offering of financial instruments.

In applying regulations on trading in financial instruments, the specific nature of the ICO must be borne in mind. One of the aims of these regulations is to ensure the efficiency of the market. This is furthered by the numerous reporting obligations imposed on entities operating in this field. Another aim of the regulations is to protect investors.

But an ICO, particularly when conducted via a DAO, often involves the openness of the code that it is based on. This means that the programming code defining the rules for conducting the ICO, as well as the functioning of the tokens being sold and the rights associated with the token, are accessible to anyone who is interested. So in practice the potential "investor" (acquirer of tokens) can verify in advance the rules for the venture he wants to take part in.

On the other hand, a barrier exists in the form of the technical knowledge needed to understand the code. This leads to a situation where the investor has access to all the essential information but may not be in a position to verify it. We may thus face a certain asymmetry of information. Similar problems confront investors in complicated structured financial instruments, but in that case they can seek protection in capital market regulations. But the specifics of ICOs require verification of the role played by the current regulations.

The second question is what an ICO has in common with raising of traditional forms of money through investment funds. Here again the example of The DAO is instructive. Its role, in simplified terms, was to gather a pool of funds and invest them in certain projects. This model is described as a "decentralised venture capital fund."

Although the example of The DAO automatically raises associations with investment funds, the question arises whether the regulations governing investment funds could also apply to situations of unconventional virtual collection of property values for further collective investment. The economic models of certain entities initiating ICOs will raise doubts of this type. Another issue is the practical application of the relevant regulations. How can they be applied for example to the decentralised structure of a DAO?

Obviously, ICOs and the tokens sold in them will also generate controversy under other regulations. Depending on their nature, tokens might be regarded as various types of legal instruments. For example, a finding that tokens qualified as electronic money would entail certain regulatory consequences for the entity (such as the initiator of the ICO) regarded as the issuer of the electronic money.

Other types of legal doubts will surround the purpose for which the entity is seeking funding. One example already mentioned is investment funds. If they have a character similar to deposits from which loans will then be granted, then the activity will have the character of deposit-taking and lending, which in a regulatory sense is generally restricted to banks.

Will lawmakers and regulators intervene?

Currently ICOs may be a niche product compared to other methods of raising funds on financial markets, but they are already on the way to raising tens of millions of dollars. It is hard to say whether public sale of tokens in this form will gain popularity at a rate that attracts the attention of regulators. But the current growth dynamic of such projects is striking.

Legislative or regulatory measures may be hindered by the supranational nature of ICOs. Organising such a venture and taking part in it requires nothing more than access to the Internet. The ICO itself occurs on the Web, making it extremely difficult to establish links with any single jurisdiction (particularly when the ICO is organised by a DAO).

It cannot be ruled out that the mainstream financial sector will take an interest in ICOs and similar methods of fundraising. In that event, the public authorities will have to respond. But even if ICOs and token crowdsales grow in a parallel reality outside of the regulated financial market, in time these phenomena are likely to attract the attention of lawmakers and regulators.

Conclusions

Huge potential of blockchain technology

Innovations arising thanks to application of the blockchain technology, as well as smart contracts and DAO, may influence the future of known business models and economic and social structures in a manner comparable to or even more far-reaching than the impact of the Internet. DAO and smart contracts may lead to the development of structures in which the exchange of goods, ideas and content can occur largely free of intermediaries, over a decentralised network. On one hand this opens up opportunities to create entirely new and more efficient models for operation of the economy. On the other hand, new technologies may have a catastrophic impact on traditional economic structures based on a model of intermediation. This applies in particular to such sectors as finance.

Blockchain is not just Bitcoin

An understanding of blockchain technology and the directions for its growth is vital. Blockchain must not be perceived, for example, only in terms of Bitcoin. This could lead to erroneous and harmful legislative decisions. It is already apparent that blockchain is being applied far beyond the narrow understanding of transactional and payment solutions.

Potential for the public sector

Public institutions must seek to understand technological changes and draw on good external examples in this area. Applications of the blockchain technology may be deployed successfully in the process of digitisation of the state. Most frequently mentioned in this context are public registers, voting systems, tax collection, oversight of public expenditures, and protection of critical infrastructure. We can already observe the potential of blockchain technology being reflected in government programmes. Such initiatives should be encouraged, but their success will require educational campaigns and support from scientific research on blockchain technologies.

Legal outlook on smart contracts and DAO

Some of the characteristics arising out of the phenomenon of new solutions developed within the blockchain technology include:

a. **Autonomous character.** In the case of smart contracts and DAO, certain actions of legal relevance (e.g. transfer of digital assets) occur automatically, as a result of execution of the code that is the basis for the contract. But traditional legal systems ascribe actions to entities, not abstract algorithms.

b. **Abstract nature.** Smart contracts and DAO exist in cyberspace as algorithms. No traditional legal structures are generally required for their correct operation, i.e. organising events in cyberspace. We can imagine that economic structures traditionally organised by legal entities (e.g. companies), such as exchanges and public registers, could function successfully exclusively in the form of an algorithm.

c. **Global character.** Smart contracts and DAO function in a distributed network which cannot be assigned to a discrete, traditionally understood spatial location. It may be said that DAO and smart contracts are "everywhere." But traditional legal systems always seek to assign legal phenomena to a specific jurisdiction.

d. **No central responsible entity.** In the case of DAO, it is very difficult to identify the entity or person responsible for its operation. There are no central authorities representing the DAO. Even the responsibility of the coders drafting the algorithm used by the DAO is limited, because after creating the code they largely lose control over its functioning.

Toughest legal issues

The following legal issues now seem to present the greatest barriers to further growth of smart contracts and DAO:

a. **Lack of legal personality of DAO.** DAO and smart contracts can implement complex legal and economic structures, analogous to the structures implemented by traditional legal entities. But unlike traditional entities, they do not have legal personality. They are legally transparent, meaning that from a legal perspective DAO basically means all of its participants. This is a highly impractical situation, particularly in instances when the DAO has to interact with external entities, e.g. when the DAO forms relations with external counterparties. The legal transparency of DAO is also a huge barrier for determining tax obligations connected with actions taken using DAO and smart contracts.

b. **No judicial capacity of DAO.** Although DAO may be used to organise highly complex economic exchanges, they cannot be parties to judicial proceedings. This causes a range of practical difficulties which may discourage others from entering into legal relations with a DAO, even though such relations may be necessary for its proper functioning (e.g. relations with "oracles" providing information essential to the activity of the DAO, or the programmers developing the code for the DAO). The prospect of suing all participants in a DAO is hardly feasible.

c. **Legal uncertainty.** Because of the decentralised nature of DAO and smart contracts, it is difficult to determine in advance the jurisdiction whose laws will govern the actions taken using a DAO or smart contract. This is vital in terms of criminal provisions and the legal risk faced by entities involved in creating the DAO (e.g. the writers of the algorithm). It cannot be unequivocally determined whether the actions of these people could violate provisions of criminal law in a given jurisdiction. This could be a major barrier to development of blockchain technology.

d. **Taxes.** As an entirely digital and decentralised entity, DAO has an unclear status for purposes of tax law. Possible classification of DAO as a joint venture does not reflect all of the challenges connected with DAO. Legislative intervention in the area of tax law appears premature at this stage, due in part to insufficient knowledge of DAO as such and its mechanisms, which could realistically expose a threat of an absence of appropriate regulations. But such intervention should not be ruled out in the future. But some measures could be taken by the authorities responsible for interpreting tax law, e.g. by issuing general tax interpretations. This would not only facilitate correct settlement of taxes by entities involved in DAO (and deemed to be taxpayers in Poland in this respect), but if a clear and appropriate construction is adopted could also provide an incentive for foreign players to opt for taxation of this activity in Poland.

e. **Unclear regulatory status of ICO.** Fundraising for projects based on blockchain technology via initial coin offerings is increasing in popularity. Given the numerous legal doubts in many countries (primarily connected with application of regulations on trading in financial instruments), there is a visible trend to seek a jurisdiction that offers a stable legal order and predictable rules for interested parties, as well as an open attitude toward innovations on the part of the public authorities.

Active measures are needed

The legal challenges discussed above could effectively paralyse further growth of blockchain technology. Adapting the legal system to meet the challenges posed by smart contracts is thus becoming a necessity if we care about further development of this technology. Lawyers are striving to understand the technology and facilitate its use. We project that in this respect there are possible short-term and long-term solutions.

a. **Short-term solutions.** Fairly straightforward short-term solutions are needed to ensure legal and tax security. This involves for example clearly defining the regulatory and tax consequences of participation in an ICO. Creation of makeshift traditional legal entities (such as foundations or companies) to serve as a link between the traditional legal system and blockchain could also be promoted. Such entities could at least partially handle the difficulties connected with the lack of legal personality of DAO and enable identification of the parties to commercial relations for tax purposes.

b. **Long-term solutions.** Further down the road, long-term solutions are required which would better reflect the nature of DAO. There is a wide range of possible scenarios. A change in the traditional paradigm of legal personality appears unavoidable. This institution could be made more flexible and for example applied on demand (upon fulfilment of certain criteria). Further growth in the blockchain technology will require backing from the state. Development of some blockchain technologies without clarification of their legal status would generate too much legal risk for their creators (e.g. under tax law and criminal law). It can be assumed with great likelihood that the price for a favourable attitude on the part of the state will be attempts to submit DAO and smart contracts to oversight by states and their legal systems. States will not want DAO and smart contracts to function in a regulatory vacuum, which would threaten chaos. Thus new ideas should be expected in terms of techniques enabling state intervention in DAO and smart contracts. For example, we can imagine that states will be prepared to recognise the legal personality of DAO, but only on condition that solutions are deployed in the given DAO enabling state intervention in the DAO's code (e.g. to enforce the legal order). Such solutions would be difficult to accept for many blockchain proponents who see in the technology a unique opportunity to create an economy completely free from state control and interference. But this may be the only direction enabling further development of blockchain technologies.

Blockchain technology—an opportunity for the Polish economy

Although technological progress is incredibly dynamic, we still find ourselves at the early stage of development of smart contracts and DAO. This creates an opportunity for countries like Poland to become leaders in developing innovations in this field. It is a unique situation, as in the case of many other types of new technologies Poland does not and in the shorter term will not have the resources to compete effectively with the most advanced economies. In the case of blockchain, Poland's great advantage is the excellent knowledge base it has in the form of some of the world's best IT personnel, who can offer natural backing for growth of these technologies. State support is also needed for research and for innovative enterprises.

Blockchain requires radical rethinking of how the law is applied

Smart contracts and DAO shift the law from the domain of natural language to the domain of algorithms. This makes it one of the most sweeping revolutions in legal history. With the growth of blockchain technologies, creation and application of the law will require entirely new skills, particularly the skill of smoothly and effectively passing back and forth between natural language and computer code. The growth of blockchain will to a large extent depend on acquisition of these new skill sets by the legal and IT communities as they must cooperate more closely in the process of creating and applying the law.

Authors

Jacek Czarnecki is an associate in the New Technologies practice at Wardyński & Partners. He handles regulations governing financial technologies (including blockchain and digital currencies), crowdfunding, trust services, telecommunications law, data protection, legal aspects of the Internet, civil law and corporate law.

E-mail: jacek.czarnecki@wardynski.com.pl

Maciej Jędrzejczyk has been affiliated with IBM in the area of Strategic Outsourcing since 2011. He is an IT architect responsible for IaaS and workplace engineering services for clients in Western Europe. He is a crypto enthusiast and moderate supporter of blockchain technology. Constantly active at the intersection of law, business, research and IT, he is a fan of history, cartography, travel and foreign languages.

E-mail: maciej_jedrzejczyk@pl.ibm.com

Agnieszka Kraińska is a legal adviser at Wardyński & Partners. She specialises in international law, EU law, and proceedings before the European Commission and the Court of Justice of the European Union.

E-mail: agnieszka.krainska@wardynski.com.pl

Karolina Marzantowicz works between the worlds of IT, business innovations, and psychology. She acts as a catalyst stimulating curiosity and helping enterprises adapt to rapidly evolving technologies. She represents IBM as a speaker and expert at public events in Poland and around the world. She is passionate about digital transformation. At IBM she serves as an IT architect and adviser to clients from the European banking sector. She has worked in the IT industry since 1994. She is a member of the IBM Academy of Technology, and also the mother of three children who loves spending time in the mountains.

E-mail: karolina.marzantowicz@pl.ibm.com

Joanna Prokurat is a tax adviser in the Tax practice at Wardyński & Partners. She is also responsible for the areas of crowdfunding, financing of new technologies, gaming, and research in the New Technologies practice. She advises in matters of Polish and international tax law, including corporate income tax, VT, international tax planning and tax optimisation, and taxation of transactions. She provides tax advisory services on personal income tax and social insurance, as well as gaming tax. Her services are aimed at both tax optimisation and management of tax risk. She conducts tax reviews, including due diligence projects, and prepares tax analyses for firms investing in Poland.

E-mail: joanna.prokurat@wardynski.com.pl

Krzysztof Wojdyło is an *adwokat* and partner at Wardyński & Partners, heading the New Technologies practice. He is also active in the Regulatory practice and the Payment Services practice. He handles regulations governing electronic payment instruments, crowdfunding, commercialisation of new technologies, telecommunications, robotics, claims trading and anti–money laundering. He participates in large, innovative projects across a range of new technologies. He regularly advises both startups and major tech companies. He is the author or co-author of publications on such issues as crowdfunding, robotics, virtual currencies, and new technologies in the financial services industry, in such titles as the banking journal *Monitor Prawa Bankowego*. He has appeared numerous times as a lecturer at conferences, including International Bar Association events. He also conducts training for entrepreneurs at startups. He is the coordinator of the regulatory working group in the Coalition for Polish Innovations.

E-mail: krzysztof.wojdylo@wardynski.com.pl

New Technologies Practice

For us, new technologies are all about new legal challenges. In many instances, we must tackle doubts surrounding the legal treatment of innovative products and services or an absence of relevant regulations. To assure clients legal security in such circumstances, lawyers must bring to the table experience, creativity, and an understanding of the business environment.

Therefore we created an interdisciplinary New Technologies practice within the law firm, bringing together highly skilled practitioners from selected fields of law. We are supported by technology experts cooperating with the firm and offering a wide range of technical knowledge.

Our firm has created a programme geared to tech startups. Ongoing support for these firms keeps our lawyers in touch with new technologies and the legal challenges they bring. Our firm coordinates the work of the regulatory group in the Coalition for Polish Innovations, where our lawyers help design solutions for improved regulations governing new technologies (e.g. for commercialisation of knowhow, dual-use technologies, and crowdfunding).

We strive to meet our clients' needs as they arise by creating highly specialised legal services addressed to specific segments of the new technologies market. We provide comprehensive regulatory, tax and transactional advice. Based on our existing experience, we have identified the following areas of our practice: biomedicine and modern foods, creative industries, crowdfunding, cybersecurity, e-commerce, financing of new technologies, gaming, information technology, new payment solutions, new technologies in searching for energy, public-private partnerships, protection of privacy, R&D, telecommunications, and trust services.

CONTACT

Anna Pompe
adwokat, partner

E-mail: anna.pompe@wardynski.com.pl
Tel.: +48 22 437 8200, 22 537 8200

Joanna Prokurat
tax adviser

E-mail: joanna.prokurat@wardynski.com.pl
Tel.: +48 22 437 8200, 22 537 8200

Krzysztof Wojdyło
adwokat, partner

E-mail: krzysztof.wojdylo@wardynski.com.pl
Tel.: +48 22 437 8200, 22 537 8200

Piotr Rutkowski
technology adviser

E-mail: piotr.rutkowski@wardynski.com.pl
Tel.: +48 22 437 8200, 22 537 8200

Wardyński & Partners

Wardyński & Partners was established in 1988. Drawing from the finest traditions of the legal profession in Poland, we focus on our clients' business needs, helping them find effective and practical solutions to their most difficult legal problems.

The firm is particularly noted among clients and competitors for its services in dispute resolution, M&A, intellectual property, real estate and reprivatisation (title restitution).

The firm now has over 100 lawyers, providing legal services in Polish, English, French, German, Spanish, Russian, Czech and Korean. We have offices in Warsaw, Kraków, Poznań and Wrocław.

We advise clients in the following areas of practice: agridesk, aviation law, banking & finance, bankruptcy, business crime, B2B contracts, capital markets, competition law, compliance, corporate law, difficult receivables recovery, dispute resolution & arbitration, employment law, energy law, environmental law, EU law, financial institutions, healthcare, infrastructure, insurance, intellectual property, life science, M&A, new technologies, outsourcing, payment services, personal data protection, private client, private equity, public procurement & PPP, real estate & construction, reprivatisation, restructuring, retail & distribution, sports law, state aid, tax, and transport.

We share our knowledge and experience through our web portal for legal professionals and businesspeople (www.inprinciple.pl), the firm *Yearbook*, and the "Law and Practice" publication series. We are also the publishers of the first Polish-language legal app for mobile devices (Wardyński+), available as a free download at the App Store and Google Play.

www.wardynski.com.pl

www.codozasady.pl

Wardyński+

Wardyński & Partners
Al. Ujazdowskie 10
00-478 Warsaw

Tel.: +48 22 437 8200, 22 537 8200
Fax: +48 22 437 8201, 22 537 8201

E-mail: warsaw@wardynski.com.pl