The block chain and the law

Jacek Czarnecki

WARDYŃSKI & PARTNERS
new technologies
new payment solutions
june 2015

Bitcoin opened up a spectrum of possibilities and a legal Pandora's Box. But block chain—the technology on which Bitcoin is based—generates even greater potential and further legal challenges.

The concept of the digital currency Bitcoin arose in 2008, and today it is one of the hottest topics in the debate about the future of the financial system. Bitcoin's innovative contribution is mainly based on the decentralisation of the currency. In the case of Bitcoin there is no central issuer, and, as in the case of cash and unlike cash-free money, the flow of payments does not require the intermediation of a trusted third party, such as a bank. Transactions are confirmed through a special type of consensus achieved through voting by users of the Bitcoin network known as "miners," where the value of the "vote" depends on the calculating power supplied by the given miner for the needs of confirming the transaction. Other characteristics of Bitcoin, such as the relative anonymity of transactions and the low (but not non-existent) transaction costs, are derivatives of the decentralisation of this digital currency.

It is the decentralisation of Bitcoin, combined with the digital nature of the currency, that causes the greatest legal and tax problems associated with the creation and trading of Bitcoin (as discussed in our Virtual Currency report). The absence of issuers and intermediaries, the anonymity of the participants in transactions, and the decentralised system for settlement of transactions make it difficult to apply traditional legal structures to Bitcoin.

Bitcoin 2.0

Bitcoin is primarily a communications protocol, i.e. a set of rules for exchange of information between devices. The Bitcoin protocol also uses advanced cryptography to ensure the security of the network. The computers communicating using the protocol generate a database which in the case of Bitcoin constitutes a ledger of all transactions performed.

This ledger is stored on various computers and servers throughout the world, known as "nodes" of the Bitcoin network. The database maintained by the nodes is referred to as the "block chain" because it takes the form of the longest possible chain of "blocks"—files containing a record of a group of transactions. The block chain is a decentralised base because it is not maintained by one central entity but simultaneously by thousands of nodes in the Bitcoin network. The architecture of the Bitcoin protocol ensures that most of the nodes in the network with huge probability will maintain an identical database. This consistency is assured through the consensus among the participants in the network mentioned above.

Along with spread of the Bitcoin protocol and the expanding block chain, concepts have arisen for applying this database to purposes other than storing records of transactions.

One such concept is the "proof of existence" function, which enables inclusion in the block chain of cryptographic information about a document selected by the user together with a timestamp. The document itself is not uploaded, but use of the achievements of cryptography makes it possible to verify with complete certainty that the document was not modified after inclusion in the block chain. Due to the decentralisation of the block chain, it is also impossible to tamper with the information about the document included in the block chain.

"Proof of existence" and the mathematical foundations for the operation of this function might be successfully used in the future by courts in order to admit a document into evidence. With respect to digital data, services of this type based on the block chain are comparable to notarial confirmation of the existence of a traditional document, except that they offer certainty backed by the laws of mathematics.

Decentralised exchange of value

Other ideas for using the block chain involve the assumption that records (balances) in the block chain's ledger of transactions might represent not a currency, but some other carrier of value. Since Bitcoin is a currency based on a block chain, other chains could be used for example as a ledger of shares in companies. Much as Bitcoin is a currency functioning without the need for the existence of a central bank, trading in units of shares based on the block chain technology could occur entirely without the intermediation of a stock exchange, without significant cost and other participants in traditional transactions, and practically in real time. Such solutions are already being introduced by NASDAQ in the US.

More far-reaching plans would give units in block chains the role of tokens representing intangibles or property rights. Potentially this could revolutionise our

thinking about ways of transferring value and about public registers. For example, tokens based on a block chain could incorporate rights to real estate or intellectual property.

These examples show one of the main strengths of the block chain technology—a method for decentralising the exchange of value. Using a frequently cited example, just as the internet enabled decentralisation of the exchange of information, so the block chain will do the same for the exchange of value. Bitcoin is just the first stage in the development of this technology, using the most popular means of exchange of value among people—money.

What does the law have to say?

Legal systems will soon have to rise to the challenges presented by block chain technology. It is quite likely that the first necessity will involve financial market regulations. Technologies similar to block chain are already being considered by banks and other financial institutions as an alternative to existing settlement systems. Meanwhile, central banks and national financial market regulators face challenges connected with issuance by the companies they oversee of digital currencies and digital share units based on block chain technologies.

Adoption of such technology by large financial institutions may go unnoticed by consumers, who will continue to settle their affairs using their current methods; only the possibility of using tools drawing on digital technologies will expand. However, the nature of the block chain technology means that even in such scenario, the mechanisms for protecting consumers would have to be significantly modified. This is because the decentralisation inherent in block chain technology makes it difficult to confirm which of the participants in a given transaction is responsible for any failure or error.

Many more examples could be given of fields of law that could potentially be affected by growth in block chain technology. But it may not be feasible to make individual changes in law without an overall reform of the legal system. Block chain applications impact the most fundamental legal concepts, such as contracts (we have already reported on "smart contracts") and legal persons (e.g. the notion of "Decentralised Autonomous Organisations"). Such solutions would be very difficult to introduce into the overall legal system in its current form.