

# ODR and Blockchain

*Tina van der Linden\**

This presentation is about blockchain in the context of ODR. My job is threefold: explain to you what blockchain is, how it operates and why it is relevant for ODR.

In the programme it says: “A primer, and discussion, on what is the blockchain and consideration of its potential role in resolving, if not pre-empting, disputes and thus its relevance to ODR.” However, later this afternoon, there is a session on smart contracts. So for now: just the basics, very briefly.

Blockchain technology was invented in 2008 by someone using the pseudonym Satoshi Nakamoto, in the search for anonymous currency online, an ongoing quest since the early 1990s. Blockchain technology was a solution, providing anonymity, solving the double spending problem and creating trust without the need to a so-called trusted third party (TTP). The result was the first so-called cryptocurrency: Bitcoin. The technique underlying Bitcoin is the blockchain. So, Bitcoin is the first application of this technique.

Blockchain is, basically, a new way to store data, that enables a new way to do business. Data are stored in blocks that are linked together creating a chain. The links are created by hashes; a hash is a mathematical way to ‘seal’ data, one-way only. The hash of the previous block is included in the data covered by the new block. In this way, blocks are securely chained together.

Transactions themselves are secured by asymmetric cryptography. Transactions are validated, lumped together and added to the blockchain by a successful mining operation. Mining consists of finding the nonce that gives, together with the transactions and the hash of the previous block, the hash that meets a certain predefined criterion. Finding the nonce is a bit like a Sudoku: solving it is really difficult, checking that the answer is correct is easy. This ‘proof of work’ method is a rather energy-consuming process: alternatives are available.

The resulting blockchain is often compared to a distributed ledger: because of the interlocking hashing, it is practically speaking immutable, and because it is stored by all the computers in a network, there is no central authority.

Thus, this is a revolutionary new and different way of creating trust between parties that don’t know each other and have no reason to trust each other. Importantly, for this trust, no TTP is needed, no reputation is needed and no enforcement is needed. We might even say that for blockchain transactions, no law is needed! This is, of course, a rather radical statement to make in a room full of lawyers.

In addition to cryptocurrencies, blockchain technology also enables so-called smart contracts, conditional transfer of values between parties. Smart contracts will be introduced and discussed in this afternoon’s session.

\* Professor Tina van der Linden is Lecturer in Law, Ethics, and Technology for the Vrije Universiteit Amsterdam.

Tina van der Linden

As far as I can see, there are at least three ways in which blockchain technology (in the form of smart contracts) is relevant for ODR.

First, disputes may be pre-empted by the use of smart contracts. Breaking promises is impossible, evidence of everything is available. Moreover, ODR may be included in the smart contract itself (possibly by use of so-called “Oracles” – human intervention in the automatic execution of the smart contract).

Then, ODR itself may be implemented as a smart contract. Thus, enforcement is ensured. An example is Kleros: crowdsourced ODR by jurors incentivized by game theory.

Finally, smart contracts may very well generate disputes. Parties to the contract may not understand the code implementing their agreement. The code may not reflect correctly the parties’ intentions or may contain mistakes – there is no software without bugs! And finally, unforeseen circumstances may arise.