UPDATE

Smart contracts

In 1994 computer scientist and cryptographer Nick Szabo introduced the concept of smart contracts, based on the translation of contractual clauses into code and the use of this code in software. The aim was to remove the need for trusted intermediaries and make it more difficult for malicious parties to undermine compliance with the terms of a contract.

Blockchain enables smart contracts to be implemented automatically and securely without external intervention.

Some of the benefits of smart contracts are that:
- they can automatically encode business logic (e.g. buy X number if price Y is reached);
- they are fixed: specific input will always result in the same output because the processing of the input is enshrined in the code;
- they are registered on the blockchain, so all parties can view their contents;
- all transactions that are executed on the blockchain using the contract can be monitored and/or verified by all parties.

Smart contracts versus traditional systems

Because smart contracts are implemented on a blockchain, they differ significantly from traditional systems. For instance, the code can manage aspects of the blockchain, such as cryptocurrency, and is implemented by and on the blockchain, making sure no-one can individually influence the output of the code. The major advantage lies in the fact that transactions are processed automatically and in a standardised way based on fixed agreements, no longer requiring the intervention of a trusted intermediary, and are visible to all blockchain members.

Various definitions

There are various definitions of the term ‘smart contract’. Some refer to a specific technology, i.e. the code that is included in a blockchain. On the other hand, sectors such as finance and law often consider them as contracts that can be used to draft, verify and enforce legal agreements between two or more parties. These smart contracts often combine encoded and ‘traditional’ clauses. Take the supply of goods to a buyer for example; the contract can automatically execute a payment when the goods are registered as received. However, they cannot automatically check goods for faults, so manual interventions are still required, with traditional clauses providing support if the delivery does not meet the specified requirements.

Since smart contracts are simply programmed code, agreements must be properly encoded and the code must do what it is intended to. The importance of the latter was reflected in the theft of more than 500 million dollars due to an error in a smart contract generated by a blockchain using the Ethereum network, which is comparable to the Bitcoin blockchain, but is far more flexible.

Although smart contracts implemented on the blockchain are difficult to manipulate, the accuracy of the encoding of the contract (i.e. the smart contract) is not guaranteed. This raises questions such as:

- How can a member be certain that (the code for) the smart contract does what it is supposed to do?
- What assurance is there that a transaction will only be processed if specific conditions are met?
- What assurance is there that the conditions laid down in the smart contract cannot be influenced?

Therefore, the IT auditor may need to provide insight into the reliability of implemented smart contracts.

This article is the second in a series on blockchain technology. Other articles in the series can be found at www.bdo.nl under IT Audit & Security.

More information?

If you would like more information or want to make a non-binding appointment, please contact one of our IT Audit & Security specialists, or visit www.bdo.nl.

Jeroen van Schajik
Partner IT Audit
T +31 (0)88 23 64 822
M +31 (0)614 230 797
E jeroen.van.schajik@bdo.nl

10/2017 – FA17210

Although this publication has been prepared and put together with due care, its wording is broad and the information contained in it is general in nature only. This publication does not offer recommendations for concrete situations. Readers are explicitly discouraged from acting, not acting or making decisions based on the information contained in this publication without having consulted an expert. For an advice geared to your specific situation, please contact BDO Accountants & Belastingadviseurs B.V. or one of its advisers.

BDO Accountants & Belastingadviseurs B.V., its affiliated parties and its advisers do not accept liability for any damages resulting from actions undertaken or not undertaken, or decisions made on the basis of the information contained in this publication.

BDO is a registered trademark owned by Stichting BDO, a foundation established under Dutch law, having its registered office in Amsterdam (the Netherlands).

In this publication '**BDO**' is used to indicate the organization which provides professional services in the field of accountancy, tax and advisory under the name 'BDO'.

BDO Accountants & Belastingadviseurs B.V. also acts under the trade names: BDO Accountants, BDO Belastingadviseurs, BDO Global Outsourcing, BDO International Tax Services, BDO IT Audit & Security, BDO Tax Consultants.

BDO Accountants & Belastingadviseurs B.V. is a member of BDO International Ltd, a UK company limited by guarantee, and forms part of the worldwide network of independent legal entities, each of which provides professional services under the name 'BDO'.

BDO is the brand name for the BDO network and for each of the BDO Member Firms.