Deutsche Bank
Research

Talking Point

# Understanding the blockchain revolution!

June 7, 2018

Author
Jochen Moebert
+49(69)910-31727
jochen.moebert@db.com

www.dbresearch.com

Deutsche Bank Research Management
Stefan Schneider

When reporting on bitcoin, blockchain and cryptocurrencies these days, the speaker is faced with the question: Shall he discuss the technology or move directly to the presentation of the social and economic implications? Conveying a complex technology in just a few minutes is risky. In Alice's rabbit burrow, the speaker and his audience quickly lose track of each other. But the audience may also be left clueless by the direct presentation of the potentially revolutionary implications. In the face of this dilemma and the complexity of cryptosystems, we will try to shed light on the issue by means of metaphors. We hope you will join us on our journey into the blockchain universe.

Blockchains are like dominoes! The tiles, not the Christmas pastries. Two variations of tiles are popular. In variant 1, the tiles are positioned in long narrow lines. Once a tile is knocked over, the others follow in a chain reaction. The world record is millions of tiles. In variant 2, a set of numbers or pictures are embossed on the tiles, which have to be added to the line pursuant to the rules of the game.

In a sense, a blockchain is a combination of the two variants. The domino tiles are positioned narrowly. This time, however, the tiles do not sport numbers or pictures, but "a tile belongs to a specific wallet". As you may have gathered from my remarks, the domino chain represents the blockchain. Every tile stands for a coin, and the wallets are the virtual purses of the cryptocurrency. When a wallet is opened, all coins currently linked to this wallet in the domino chain are displayed. When a coin changes hands, the so-called "miners" create a new tile with the new information. The former tile is no longer linked to a wallet; in this context, it has lost its value. But it remains part of the domino chain, which means that the complete history of the blockchain is maintained. Since the information is public, it can be accessed by all miners, as well as the average internet user.

Let's move on to the next parlour game: Sudoku!Alongside dominoes, the miners are also playing Sudoku. In exchange for setting up the tiles, they receive new coins. Therefore, they compete with each other. The reward is given to the miner who is the first to solve a super-complex Sudoku of sorts. Similar to the after-work Sudoku, some of the squares have numbers in them, thereby defining the solution to the puzzle. In the blockchain world, this preliminary information is provided by the ownership changes of coins. As the date of the transaction is also recorded, the preliminary information varies from tile to tile. Once the miner has solved the Sudoku, he writes the solution on the



tile. As with the after-work Sudoku, finding the solution is extremely difficult, whereas the correct solution can be easily identified by the miners.

Why is no-one cheating, manipulating or destroying the domino chain?

What is keeping the miners from cheating? Firstly, they control each other. Secondly, they invest massively in hardware and power to solve the super-complex Sudokus. As these investments would be lost should confidence in the cryptocurrrency fade, the miners comply with the rules. Thirdly, it is much more attractive to rake in new coins in exchange for solving the super-complex Sudokus. Whilst the miners might get more coins if they cheated, the coins and their total investment in hardware would be valueless, should the scam be exposed.

Why is no-one manipulating the domino chain? If someone removes a tile from the chain to write "this coin belongs to me" on it, the complete domino chain will collapse. In the blockchain world, at least, this is guaranteed, as all coins are interlinked - hence the term blockchain. Any retroactive changes to the coins' links would therefore falsify the entire blockchain. As a consequence, cryptosystems are said to be immutable.

Why is no-one destroying the domino chain? The self-healing powers are stronger.Blockchains are under constant attack. But there are thousands of copies of every domino chain resp. blockchain, and damage is quickly undone. These copies are stored on computers around the world, including those of the miners and other computers, e.g. those of the wallet providers. Forming a network, these computers are constantly sharing information on the current state of the domino chain. If the domino chain is manipulated on a computer, the originals are copied from one of the other network nodes. The system thus works like the healing of a small wound. The injury is repaired by the surrounding tissue in a timely fashion. This network structure is one reason why cryptosystems are regarded as decentralised.

Another decentralised element is the governance structure. The software and the code of many blockchains are open source. They are open to everyone, and many participate. But too many cooks may also spoil the broth. Not only are coders struggling for internal consensus on software updates, but they also have to convince the miners and the network nodes, who would otherwise ignore the updates. Whilst the governance structure is complexand the system inert, it is, at the same time, extremely stable and almost non-hierarchical.

The contents of the domino chain and ownership changes are secured by cryptography. First, cryptography is used to certify ownership changes by means of a digital signature. Second, the complete history of changes is encrypted that way. As a result, all ownership changes can be accessed via the internet, whilst the owners usually remain anonymous.

The crypto network works without the involvement of third parties. As described above, cryptocurrencies are immutable, decentralised and global. Given their transnational nature, which goes beyond the regular scope of national legal environments, they are hard to regulate. Moreover, neither fiduciaries nor "trusted third parties“ such as central banks or central clearing authorities are



needed. And persons sending coins neither need to know nor trust each other. Cryptosystems are therefore classified as "trustless“!

With such a system, information, e.g. on the ownership changes of a virtual coin, can in a sense be irrevocably stored. Since the bitcoin blockchain, for instance, features a small text field alongside the ownership changes of the coins, some crypto evangelists have registered their marriage on the blockchain, pinning their hopes on eternity. Can a blockchain be used to store other information, too? The answer to this question is electrifying crypto enthusiasts. Given the wide array of potential applications, some expect a blockchain revolution.