Blockchain

by Alexander Westphal

What is a blockchain?

Blockchain, or distributed ledger technology, emerged as the technology underlying bitcoin, the first significant virtual or crypto-currency created in 2009. The blockchain is the operating model that allows bitcoin transactions to be processed and recorded. While public attention was previously focused on the economic role and monetary aspects of bitcoin and other crypto-currencies, over past months the focus has clearly shifted to the underlying distributed ledger technology and its possible applications which are considered to extend far beyond virtual currencies or payments more generally.

Distributed ledger technology introduces a form of collective bookkeeping via the internet. More specifically, the blockchain is a fully decentralised record of ownership which is shared across a network of computers linked through specific software. This shared public ledger contains records of all transactions in the crypto-currency (or indeed potentially any other asset) that have ever been processed by the blockchain. This in turn implicitly allows verification at any moment in time of who owns how much of it. Each of the computers connected to the network hosts a complete copy of these records. The so-called mining process described further below thereby allows new transactions to be verified and added to the ledger in a consensual, fully decentralised way. Unlike in conventional payment systems, in the blockchain there is no need for a trusted central authority to do this job. Distributed ledger technology is said to "decentralise" trust, probably its main innovative feature.

How does it work in practice?

As the name indicates, all transactions contained in the blockchain are packaged into blocks. These blocks in turn are embedded in the chain in a chronological sequence. In the case of bitcoin, the addition of new blocks happens through a technically elaborate and competitive process called "mining". This process is at the core of the blockchain as it ensures its integrity and security. Every computer connected to the blockchain can in principle participate in the mining process, ie become a "miner". Miners pick a set of transactions of their choice from a pool of all recently concluded transactions and package them into blocks. However, before miners can add their block to the public ledger they need to go through two steps. They first need to solve a specific mathematical puzzle, which requires a significant (computational) effort. Only once a miner has solved this iterative puzzle, he will publish the block to all other computers in the network who then validate it. Only blocks which contain transactions that have all been unanimously agreed are added to the

chain. While this confirmation process ensures the validity of each single transaction, the effort put in by miners secures the blockchain as it ensures that there is only one trusted blockchain at any moment in time.

The effort required by miners however also makes it necessary to incentivise them to do the heavy lifting of collecting and verifying transactions. In the bitcoin system miners are remunerated through a combination of newly issued currency and transaction fees. In other distributed ledger systems it would in principle be possible to rely solely on transaction fees or other incentives.

The mining process is configured in a way that, on average, every 10 minutes a new block gets added to the blockchain. In order to maintain this timeframe, the system automatically adjusts the difficulty of the mathematical puzzles that miners need to solve before adding a new block to the chain. With each new block added to the chain all other blocks in the chain are confirmed one more time. The longer a transaction is part of the chain, the more difficult it becomes to reverse it and the more certain is its validity.

Why is this relevant for financial markets?

Although developed specifically for bitcoin, the concept of distributed ledgers is by no means limited to crypto-currencies or indeed payments more generally. Every system that currently relies on trusted central authorities for the transfer and recording of asset ownership could theoretically be replaced by decentralised systems such as distributed ledgers, although the extent to which this will actually happen will depend on many factors.

Given that already today most securities exist solely as digital records in the books of banks and infrastructures, the extension of distributed ledger technology to financial markets seems a logical next step. As the current processing and settlement of financial transactions relies heavily on intermediaries and central infrastructures to oversee and control the transfer and recording of ownership in securities the decentralised nature of the blockchain potentially promises important efficiency gains in the post-trade processing of transactions. Distributed ledger technology could substantially reduce the time needed for a transaction to settle, in particular in markets that still involve a high degree of manual processing such as syndicated loan markets for instance, and is expected to lead to significantly lower transaction and collateralisation costs. Overall, potential yearly cost reductions achievable via distributed ledger technology over the next few years have been estimated at up to $20 billion in a recent report prepared by Santander and others.

Efficiency gains are only one part of the potential advantages of the blockchain. Firms might also benefit from lower risk exposure as a result of the disintermediation through distributed ledgers which would allow them to interact directly with their counterparty. Finally, the decentralised and inherently global nature of the blockchain might also improve access to capital markets, particularly in economies with a less developed financial market infrastructure. While the potential benefits of the technology are thus without a doubt substantial and expectations are enormous, as evidenced by the various industry initiatives that have recently been announced in this field, it is also important to note that the blockchain story is still very much at the beginning. There are significant risks and a number of fundamental questions that would need to be addressed before the technology can seriously be considered an alternative to the way securities markets currently operate.

Such questions include for instance concerns about the confidentiality and misuse of information in an open source blockchain, or the obviously critical issue of cyber-security. Other questions concern inevitable capacity and resource constraints of a continuously growing blockchain amid the sheer number of financial transactions processed on global markets today. There are also fundamental questions on how to ascertain the legal ownership of securities. And finally, there is the crucial issue of regulation of distributed ledger technology. Given the substantial efforts made over the past years to make the existing financial system safer and the complex regulatory environment that has evolved from these efforts, it is far from obvious how a technology without central authority and liability can fit into the picture. It is not difficult to predict that regulators around the globe will face important challenges in this regard as they are starting to assess potential implications of disruptive financial innovations (see main text).

It will be interesting to see if and how these and other obstacles can be overcome by further innovation. ICMA will be following closely the evolution of this interesting development.

Contact: Alexander Westphal
alexander.westphal@icmagroup.org