Deutsche Bank Research Talking point Blockchain - attack is probably the best form of defence

July 28, 2015

Debate over blockchain technology is raging in many online and offline media at present. In principle, the technology constitutes a decentralised ledger system that can be coordinated via peer-to-peer (P2P) networks. Any ownership or security issues arising in connection with the decentralised transactions conducted across the ledger system are handled by P2P mechanisms as well, i.e. also without a central node. Ownership status is established via the digital exchange of cryptographic keys (public vs private), while fraudulent transactions can largely be ruled out with the help of the cryptographic "proof of work" system. Using a proof of work, blockchain technology enables the rapid, inexpensive transfer of assets and financial products between individuals who neither know nor trust one another, without a compelling need for an intermediary to reduce existing information asymmetries.

Probably the best-known example of the P2P technology in application is Bitcoin, the cryptocurrency that is equally controversial. Incidentally, cryptocurrencies differ from conventional currencies in that the value of the currency is not guaranteed by law or an institution, but instead by trust in the underlying technology. However, the blockchain technology behind Bitcoin has much more to offer than a mere cryptocurrency. For example, discussions also involve standardised, fully automated and/or programmable agreements, referred to as smart contracts, that can be processed via the P2P network - bypassing intermediaries, national borders and, at present, even regulators. At least this was the idea originally espoused by the mysterious programmer Satoshi Nakamoto who initiated the first Bitcoin transaction in the P2P network in 2009. And thanks to the log of the entire string of transaction chains, it continues to be verifiable.

Blockchain technology is one of the first truly disruptive ideas from the fintech sector. After all, pure blockchain theory says that not only will individual business divisions of traditional banks become redundant in future, but there could also be a real paradigm shift in the prevailing financial system, because many intermediary services could be replaced by a P2P network.

Therefore, it comes as little surprise that traditional banks and other players from the financial sector are now taking increasing interest in this new technology. Several financial institutions have already established what are known as innovation labs that deal exclusively with all the technology involved in the blockchain. However, stock exchanges, credit card firms, clearing houses and insurers are also increasingly focusing on the technology and analysing the potential of the P2P movement for their own purposes. This may be because established intermediaries want to get an idea of whether the blockchain is actually a threat to

their existence or may ultimately even offer numerous opportunities - now in the digital age - to implement new proprietary technologies which will raise the digital profile of traditional transaction banking, boosting its efficiency and, above all, execution times. Financial services and products that can be offered virtually in real time around the globe in future while at the same time reducing costs could catapult the traditional banks back to top spot in the race to devise financial innovations.

Hence, traditional banks now need to focus in particular on timely analysis of these new technological challenges and on development of potential (collaboration) strategies in order to reclaim a more active role in the competitive race to innovate. One result of the planned potential analyses could be that financial institutions attempt to defend their business models by implementing certain parts of the blockchain technology for their own purposes and in their own IT environment, naturally without the peer-to-peer aspect.

Thus, it is entirely conceivable that banks could, for instance, set up a new digital booking and clearing system amongst themselves enabling them to offer client transactions featuring the benefits of the blockchain, such as speed, efficiency, internationality and cost savings. Since the banks most likely trust each other more so than the anonymous peers, a new, modern clearing system would probably in fact be even cheaper and more efficient than the blockchain, because the energy-hungry "proof of work" ("mining" at Bitcoin) would be made redundant.

Moreover, banks could configure their system in a user-friendlier fashion for less tech-sawy customers and enhance their offer with extra personalised financial services, which the blockchain cannot do as things stand today. With a new proprietary digital IT infrastructure banks could thus quite conceivably be able to position themselves relatively well in relation to the blockchain technology. Furthermore, in the blockchain age, it is also conceivable that banks could additionally assume new tasks - e.g. as custodians of cryptographic keys. While such activities would probably generate little revenue in comparison with today's business models, this extra service could help to ensure that customers stay on a bank's own financial platform longer in order to use other monetarisation options. To this end, traditional banks would have to play their wild card of trust - which they (still) hold - in a much better way than has been the case so far.

Currently, blockchain technology is still in its infancy. This means that the banks and other intermediaries still have time to analyse the new technological challenges. However, the resulting stimuli would subsequently soon have to be translated into the respective infrastructure environments. At the end of the day, the political component of course plays a key role, too. After all, an open P2P financial system, as provided for by the pure blockchain theory, will also confront regulators, legislators and last but not least the police or other investigation authorities (tax office, state prosecutor etc.) with new challenges. In other words there will continue to be a need for considerable discussion in future, and no doubt huge protests here and there. So far there has not been any regulatory restriction of P2P mechanisms in the

financial system. Introduction of the same could temporarily curb the technology's spread. Traditional banks should not rely on the regulator now, though, but instead actively experiment with the new technologies in their labs and collaborate without prejudice in order to create their own digital ecosystem in the medium run.

Authors: Thomas F. Dapp
Alexander Karollus

Deutsche Bank Research