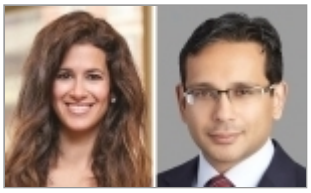
THE LAWYER'S DAILY

The Lawyer's Daily | 111 Gordon Baker Road, Suite 900 | Toronto, ON M2H 3R1 | www.thelawyersdaily.ca
Phone: (800) 668-6481 | Fax: (905) 479-3758 | John.Carson@lexisnexis.ca

In-House Counsel

Cryptocurrency and cybersecurity: A primer

By **Sharon Bauer and Imran Ahmad**



Sharon Bauer and Imran Ahmad

(November 22, 2017, 8:43 AM EST) -- As the value of bitcoins continues to soar, there has been increased interest in whether cryptocurrencies may one day replace traditional currencies. However, regulators and the broader public remain skeptical and concerned about whether digital currencies are vulnerable to manipulations and therefore, present a risk to our financial system.

What is cryptocurrency

Both individuals and organizations use fiat currencies as a medium of exchange when engaging in transactions. Banks, accountants, lawyers, financial service companies and even online payment processors such as PayPal, are necessary third party intermediaries when it comes to basic commercial transactions. Among other things, third parties validate all transactions, making it a "centralized" system.

Individuals and organizations not only pay third parties for their services, but they are also bound to their terms of service. These terms include revealing personal information such as the identity of the sender, the identity of the recipient and the amount of money being exchanged. Third parties also place limits on transactions, such as how fast a transaction can be processed, how much money can be exchanged and who can engage in such transactions.

Cryptocurrency transactions are unique in that they do not require a centralized system. Instead of using a third party intermediary, cryptocurrency transactions are peer-to-peer exchanges. There is no longer the need for individuals or organizations to comply with terms of service. Cryptocurrency transactions are faster, cheaper and more direct. They also have fewer transactional limitations.

This begs the question, if a decentralized system does not have a central third party to provide security, how safe are cryptocurrencies and what are the risks?

Security of cryptocurrency

In many ways, the decentralized system is more secure than the centralized system. Cryptocurrencies and its transactions are secured by cryptography making it virtually impossible for hackers to manipulate the system.

Under the traditional centralized model, bankers and other third parties validate traditional transactions and record them on a ledger. Human error or intentional deception can manipulate transactions, which may go unnoticed. This is highly unlikely in a decentralized system which relies on mathematical algorithms to verify each transaction. If the equation is not properly solved, the transaction will not be processed.

In a decentralized cryptocurrency system, rather than bankers, transactions are verified by "miners." Miners are individuals or pools of people who continuously verify decentralized transactions by solving complex mathematical equations. Once a number of transactions are verified, they are consolidated into a "block." Blocks are then merged to create a "blockchain."

In order to create a blockchain, miners must solve an additional complex mathematical problem. These problems are extremely time-consuming to solve and can only be calculated by machines using significant amounts of processing power. Due to the amount of power required, miners will

often pool together to solve mathematical equations. Once a miner solves an equation, the miner is rewarded with a newly created cryptocurrency coin as well as a transaction fee.

All transactions, whether a sale, purchase, or exchange of cryptocurrency, are stored in a blockchain, which is a public ledger. Similar to a bank ledger, the public ledger keeps track of all transactions, which have been validated.

While cryptocurrency transactions themselves are secure, malicious parties have identified and exploited vulnerabilities in the overall ecosystem. Cryptocurrency users, whether organizations or individuals, need to familiarize themselves with these vulnerabilities so that they can protect themselves against potential threats.

This is part one of a two-part series. Part two will appear next week.

Sharon Bauer is a partner at Wolfe Lawyers *and can be reached at* sbauer@wolfelawyers.com. *Imran Ahmad is a partner and national leader of the cybersecurity law practice at* Miller Thomson LLP *and can be reached at* iahmad@millerthomson.com.
