Private/Permissioned Blockchains Next Up for Distributed Ledgers

"The big difference between the original blockchain for bitcoin and the blockchain now widely talked about by banks is that instead of preferring transactions to be unknown, blockchain prefers transactions to be known."

WatersTechnology spoke with DataArt senior vice president Peter Vaihansky about blockchain technology.

The distributed-ledger technology blockchain has been widely talked about by banks. Last week, JP Morgan announced a trial project to test the use of blockchain technology for its loan trading operations, while Bank of America had filed for 15 blockchain-related patents. WatersTechnology's editors have predicted that 2016 will be the make-or-break year for blockchain.

For the capital markets to accept a new technology, it has to have attractive features and be an improvement upon and existing platform of process. For the capital markets, blockchain has obvious appeal with post-trade settlement and clearing, says Peter Vaihansky, senior vice president at DataArt.

"What it does very well is it brings everybody in a multilateral situation on to the same page...and it's achieved mathematically, cryptographically, by virtue of how the ledger is designed," he says.

The Appeal

The benefits of blockchain are wide and plenty. "It's a distributed database where every node, every participating machine in the network stores the exact same thing. There isn't one central repository where the data resides, the data resides everywhere and it's the same data by definition," Vaihansky says.

Another characteristic of blockchain is that it's irreversible. The distributed ledger technology is essentially a chain of blocks of transactions. It's designed so that those transactions can be ordered in an immutable way, so that it will always be clear which transactions came first and which came next, Vaihansky says. "So you can recreate the state of the ledger or who owns what, you can recreate it at infinitum. That's the appeal, and the appeal is obvious," he says.

No Longer Anonymous

Blockchain has come a ways since its original association with the cryptocurrency bitcoin. The lack of understanding comes in when people start confusing, instead of equivocating between different meanings of the word blockchain, Vaihansky says. The blockchain, originally used for bitcoin, has been divorced from the digital currency.

The big difference between the original blockchain for bitcoin and the blockchain now widely talked about by banks is that instead of preferring transactions to be unknown, blockchain prefers transactions to be known. In an environment where we're dealing with capital markets transactions and post-trade settlement, some of the design features of the original blockchain become either needed or downright harmful, Vaihansky says.

For bitcoin, the parties to the transactions are pseudonymous or anonymous. The technology was designed to enable trust where nobody knows anybody, algorithmically building certitude into how the chains of blocks are constructed, Vaihansky says.

"The need for that goes away once you realize that you actually do want to know who you're trading with, and there are also the regulations and the regulators that need to be watching the transactions," he says

Administrator Approval

In this case, for blockchain, only approved administrators have the power to verify transactions. The validators on such a network are not pseudonymous; they're very well-known and they are trusted, Vaihansky adds.

"The key design feature of the original blockchain – namely the proof-of-work algorithm [the algorithm users in the network use to verify transactions] – needs to go away, because this is a very costly feature, and people have figured it out," Vaihansky says. "Therefore, we're talking about private blockchains or permissioned blockchains where not just anybody can anonymously jump on the network and become a node; rather, you have administrators who allow you to enter the club, kind of like registering with an exchange to trade."

Link to full article: (requires subscription)
http://www.waterstechnology.com/sell-side-technology/analysis/2444684/private-permissioned-blockchains-next-up-for-distributed-ledgers