(

Unknown date | Salvatore Babones

The Australian Securities Exchange endorses the distributed ledger

In a carefully-crafted 1,000 word press release, the Australian Securities Exchange (ASX) on Thursday announced its intention to become the first global stock exchange to adopt distributed ledger (DL) technology — aka the blockchain. News organizations around the world breathlessly reported that ASX is leading the way in adopting the blockchain, the database structure that underlies the Bitcoin virtual currency. With Bitcoin surging past the $10,000 mark last week, any story linking a reputable securities marketplace to the notorious cryptocurrency is bound to be big news.

They may have jumped the gun.

Tellingly, ASX never used the word "blockchain" in its press release. It said it was adopting "distributed ledger technology" (DLT) for clearing and settlement. The specific DL technology behind ASX's distributed ledger may or may not include blockchain applications. It certainly won't look anything like Bitcoin.

A blockchain is an "append only" database structure in which new records can only be added at the end. Each new record, for example a financial transaction, includes a unique ID code that is mathematically generated as a function of the collective information incorporated in all previous transactions in the database. As a result, if you know the ID code (called the hash) of the last transaction in the database, you can verify that all previous transactions are as advertised.

The blockchain approach makes it possible for multiple parties to work with identical copies of a single database because it ensures that everyone's copy of the database is the same. Just look at the final hash. If your hash matches my hash, we know we have the exact same data, even if the full database includes trillions of previous transactions.

The blockchain hash ensures the integrity of past data, but it doesn't determine who can add new data. For that, Bitcoin introduced the controversial practice of mining: every ten minutes or so Bitcoin holds an open competition to see who can solve a complicated mathematical puzzle. Whoever solves it first gets to record the next block of transactions in the Bitcoin ledger — and a small reward for their effort. That small reward is represented as the "mining" of new Bitcoins. The Bitcoin mining approach is controversial because it encourages miners to waste enormous quantities of electricity in the hope of earning a few bits of virtual currency.

ASX is not talking about opening the Australian securities market to freebooting miners who can win stock certificates for solving math problems. Unlike Bitcoin's open transaction ledger that anyone can view and add to, the ASX ledger will be run "on a secure private network where participants are known, 'permissioned' to have access, and must comply with ongoing and enforceable obligations." In other words, the banks and brokers will run the show.

That show will probably use blockchain technology for just one specific purpose: recording that a share transaction has occurred, without divulging the identities of the buyer and seller, the amounts sold, or even the price of the shares. All of these details are likely to be kept in a private contract store (PCS) maintained by each of the banks or brokers that is registered with the exchange.

At least, that's the approach detailed in working papers published by ASX's technology partner, Digital Asset (DA). In the DA approach to distributed ledgers, authorized market participants like banks and brokers maintain their own private PCS databases of share registrations and transactions. When they want to record a transaction, they report it to a global synchronization log (GSL) blockchain maintained by ASX. In theory, they don't have to report anything about who traded what to whom or for what price. The GSL is nothing more than a blockchain proof that a (private) transaction has been made.

Though DA calls their approach a distributed ledger, it's not so much a single distributed ledger as a collection of many private ledgers (the PCS databases) all linked together by shared blockchain (the GSL) that does little more than record that a transaction of some kind, any kind, has taken place. Not much transparency there. Market participants could even insert empty "phantom transactions" into the GSL blockchain to further obscure their activities.

Put it all together, and the blockchain technology that was supposed to usher in a new era of openness in financial technology (fintech) seems likely to be used to take even more transactions off the record and into the dark pools of privately-settled trading. Clearing and settlement, once conducted in the (relative) light of day by a regulated exchange, will increasingly be relegated to the secret PCS accounts of brokers and banks.

The brand of blockchain concocted by DA and ASX will probably require ordinary investors to put even more faith in banks and brokers to act in their clients' best interests. The PCS ledgers will almost certainly be off-limits to ordinary investors, and may even be secret from the exchange itself. That probably doesn't mean much to those of us who have already given up on holding brokers and bankers accountable. For everyone else, there's always Bitcoin.

Salvatore Babones

Return Home