TABB FORUM
WHERE CAPITAL MARKETS SPEAK

The Profitability Engine Behind Capital Markets
Sponsored by Broadridge

8 Key Features of Blockchain and Distributed Ledgers Explained

Robert Palatnick, DTCC
25 February 2016

Blockchain represents a generational opportunity to re-imagine the post-trade infrastructure. However, the key to realizing its promise is in fostering industry-wide collaboration and aligning the technology with the core principles of mitigating risk, enhancing efficiencies and driving cost efficiencies. Here are 8 key capabilities that have helped create this innovative platform.

The heated discussion – some might say “hype” – surrounding the potential for distributed ledger technology to alter the post-trade infrastructure has been unprecedented.

Is it a disruptive force on the verge of replacing legacy infrastructures, or will the technology produce only marginal impacts in the short-term? It is early in the blockchain debate right now and there are few definitive answers.

As an industry-owned and governed financial market utility, The Depository Trust & Clearing Corporation (DTCC) believes the technology represents a generational opportunity to re-imagine the post-trade infrastructure. However, the key to realizing its promise is in fostering industry-wide collaboration and aligning the technology with the core principles of mitigating risk, enhancing efficiencies and driving cost efficiencies.

[Related: “Is Blockchain the Holy Grail for Capital Markets?”]

But the first step in assessing opportunities where distributed ledgers may upgrade the current system for processing securities transactions is having a comprehensive understanding of the Bitcoin payment network and the individual components that form its underlying technology platform.

Here are 8 key capabilities that have helped create this innovative platform that has the potential to modernize the post-trade ecosystem:

1. The Asset Is Built-In: The asset called Bitcoin is produced and managed completely within the Bitcoin network. Therefore, the history and quantity of every movement of Bitcoins is mathematically verifiable by the recorded history in the distributed ledger of the Bitcoin network.

2. Party Identity Abstraction: Security by obscurity is built in to the platform, meaning individual parties are never identified. Instead, security keys (public and private key pairs) are required to gain access to transaction output. Only the holder of the private key can send Bitcoins or get access to received Bitcoins. Only the private key owners know their total aggregated amount of Bitcoins.

3. Transaction Linkage: Every transaction record (ledger entry) is linked to previous transactions and is standardized for every participating node. Every ledger entry is retraceable across its full history and can be reconstructed.

4. Transaction Scripts: These are the standardized rules and conditions applied to a transaction. Every node applies the same rules. In the simple Bitcoin model, a Bitcoin is moved from one party to another according to rules. Newer versions of the blockchain have expanded the scope and capabilities of those rules, which form the basis of what is called “smart contracts.”

5. Transaction Distribution: There is a standard network protocol that allows every participating node to receive every transaction and apply the same validation rules.

6. Blockchain: This is the single standard for how every node stores the transaction data (ledger data). Every node adheres to that standard and can have a full copy of the data. This is sometimes called the "distributed ledger." Records, or blocks of transactions, are added to the blockchain and include a link to the previously added block. This is the official point of immutable recording of a transaction.

7. Decentralized Consensus: This consists of the standards and rules for how every node exchanges the blockchain information, the mathematical rules for all nodes to agree on the integrity of that data (sometimes called "proof of work") and the payment incentive to support the consensus model. A key point of the model and this entire platform is a method to ensure all transactions are validated and all valid transactions are added once and only once. No valid transactions can be omitted (sometimes referred to as censorship) and, in the case of the Bitcoin network, a Bitcoin cannot be double spent.

8. Trust vs. No Trust, or Permissioned vs. Not Permissioned: The "No trust" model refers to the public and open access of the Internet on which the Bitcoin network was built. Anyone can download the open-source software and join. The Bitcoin network was constructed to distrust any node based on a model that works as long as a majority (>51%) of the nodes act as honest participants in the consensus activity described above. Trusted, or permissioned, implementations are significant modifications to that model, which requires permissioned servers to be approved and on-boarded in order to participate.

In short, the blockchain is a network and a database. It has rules and built-in security and it maintains internal integrity and its own history. These components create the value of the Bitcoin blockchain, but each of these concepts has the potential to be applied individually or in various combinations to improve existing processing of financial transactions.

To learn more about blockchain, download DTCC's new white paper, "Embracing Disruption – Tapping the Potential of Distributed Ledgers to Improve the Post-Trade Landscape." This article originally was published on the DTCC Connection blog.