Blockchains and distributed ledgers: What are they and why are they important for trade security?

Everyone is talking about blockchain and the benefits that innovation brings, including, potentially improving supply chain security. Jenny Cieplak and Jeff Snyder examine the technology and ask: Is it right for you and if it is, are you prepared to take advantage of it?

Blockchain and distributed ledger technologies are receiving almost universal praise as a potential solution to outdated financial infrastructure, corruption in international business, supply chain security, health and safety tracking for pharmaceuticals, food, and high-value products, among others.[1] How much of it is real and what will blockchain mean for trade security? To answer these questions we need to explore just what blockchain is and how it works. After that we can look at why blockchain interests those who care about international trade, and look at some of the emerging applications for blockchain in trade.

Sooner or later you will be asked, as part of this shift to blockchain, whether your company is prepared to participate in a blockchain as part of sales to a particular customer or to participate in certain transactions with selected governments. What do you have to do to get permission to participate in a blockchain? What risks are associated with it? What if your trade records, maintained in blockchain form, have to be audited? Will you be prepared to explain how the blockchain works and why the technology is being used? If a third party gives you a blockchain record to demonstrate ownership or some other important right, will you be prepared to audit it? Will you know what it can be used for and what it cannot?

Blockchains and distributed ledgers: What are they and why should you care?

Blockchains and distributed ledger technology ('DLT') are becoming increasingly prevalent. The World Economic Forum ('WEF') estimates that over $1.4 billion has been invested in blockchain technology over the last three years. A recent Juniper Research survey found that 56% of companies with more than 20,000 employees, were either considering deploying, or were in the process of deploying, blockchain solutions. Over 200 companies have joined the Enterprise Ethereum Alliance, a consortium formed to explore use cases for the blockchain and smart-contract platform used by the cryptocurrency Ether.

> What do you have to do to get permission to participate in a blockchain? What risks are associated with it?

R3, a consortium formed to provide distributed ledger solutions to the financial industry, has raised $107 million in its Series A funding round. The WEF estimates that over 2,500 distributed ledger technology-related patents have been filed over the last three years. Goldman Sachs Investment Research projects that the implementation of blockchain technology could result in savings of $6 billion annually in capital markets. Bankers, regulators, and lawyers, among others, have all weighed in on how best to integrate this technology to improve business functions.

Among the use cases for blockchain are:

- Payments systems
- Securities trading
- Derivatives trading and 'smart' contracts

- Syndicated loans
- Receivables financing
- Tracking ownership of patents, fine art, aircraft, real property – any asset for which there is or could be a central registry
- Sharing records and information in a permissioned context (e.g., medical records, KYC information)

Initially, the largest interest in blockchain and distributed ledger technology was in the financial industry, where the new technologies could be used to track and transfer financial assets such as securities. However, users are finding that the legacy systems used by global financial intermediaries will take time to transition into distributed ledger systems. Thus, solutions in areas such as supply chain, where legacy technical infrastructure is sometimes non-existent, are a growing area of interest for many solution providers as these industries implement technology infrastructure for what may be the first time.

At its core, blockchain technology is essentially an engine for processing exchanges of information. It is not a static record. A blockchain is a type of distributed database that tracks transactions in assets and exchanges of information. It is a chronological sequence of verified transactions within a certain network. A 'transaction' can be the transfer of an asset, the creation of a new medical record, or the entry into a swap transaction.

Blockchain is definitely NOT Bitcoin: Bitcoin is just one of many virtual currencies that use blockchain technology for tracking and transferring purposes.

There is not just one blockchain, just like there is not one database. Different blockchains can be created for different needs, with different operating rules. Anything can be tracked and transferred via a blockchain. Blockchains can be used to track and transfer financial assets such as securities. But blockchains can also be used to store medical records, send secure messages, and track ownership of real estate or personal assets.

Multiple participants have access to the same 'golden record' – there is no single official copy. The ledger automatically updates when new transactions take place, and so there is prompt verification of completed transactions across the system. Blockchain is an example of a distributed ledger, but distributed ledgers don't have to be based on blockchain.

Different blockchains can be created for different needs, with different operating rules. Anything can be tracked and transferred via a blockchain.

Together, blockchain and distributed ledger technologies incorporate several key concepts:

- **Data security**: Transaction data is encrypted at all times.
- **Single 'Golden Record':** Each participant sees the same view of the same data; no single 'official' copy.
- **Append-only:** Transactions can be added to the chain, but cannot be deleted. Thus, blockchains are designed to preserve data quality, creating a complete and theoretically immutable record of transactions. Error transactions can be eliminated by entering into a 'reversing' transaction.
- **Prevents double-spend**: Each transaction changes the state of the entire ledger. A following transaction cannot spend assets from a previous state.
- **Real-time transactions**: Transactions complete in close to real-time, with prompt verification and updates across the system.

How does all this work?

Users access assets or information on the ledger using a public key, which is matched to a private key. Keys are computer-generated, and users can have multiple sets of keys. Public keys are visible to all users who have access to the ledger. Private keys are kept secret by the users. A transaction is effected when a user uses his or her private key to unlock assets that are assigned to his or her public key. The user can then transfer the assets to another user. A user can also add information to the ledger and associate that information with his or her public key. The user can choose to make that information public or available only to persons who possess certain public key/private key combinations.

Distributed ledgers can use non-blockchain technology. In a blockchain, each participant in the network has access to the full database (even if some data is encrypted). In other distributed ledger models, transactions are only broadcast to parties to the transaction. Regulators can receive specialised access to specific transaction data. Since each transaction does not propagate across the entire ledger, another method is needed to prevent double-spending. For example, you could use a notary service provided by a trusted third party to confirm no double-spending.

Distributed ledgers can be either 'permissioned' or 'permissionless'

Permissioned distributed ledger networks are in development to fit numerous business needs where knowledge of counterparties is important. Networks can vary by market type (e.g., global financial market, regional financial market, etc.), nature of the business relationships, or any other set of parameters the participants deem necessary. A registration authority issues identities and permissions to stakeholders participating in the network. While the identities of network participants are known among the participants, identities are not disclosed to unauthorised parties. Transactions are not available to persons who are not participants on the network. Content confidentiality is achieved within the network by encrypting transactions such that only stakeholders can decrypt and execute them, or not by sending all transactions to all participants.

Smart contracts make distributed transactions work

Smart contracts are computer protocols incorporated into a distributed ledger that implement the terms of a negotiated contract in a self-executing manner. They may either be written entirely in standalone computer code, coupled with traditional written agreements reflecting the same negotiated terms codified in the computer code, or partially governed by computer code and partially governed by a traditional written agreement that is incorporated by reference in the code.

Links and notes

[1] Blockchain has been identified as a solution for many supply chain and trade related functions, including export controls: https://thebulletin.org/blockchain-new-aid-nuclear-export-controls11204

2 https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=CPV03008USEN

3 http://www.opengovasia.com/articles/8129-singapore-exploring-use-of-blockchain-to-link-national-trade-platform-to-trade-platforms-in-other-countries

They can have broad applicability and may be used to govern or facilitate many types of transactions. Smart contracts can take information input into the contract (such as the arrival at a port of a container of goods) and use that information to automatically update title to the goods or cause payments under a letter of credit. Smart contracts can automatically compress derivatives portfolios, or can create a restriction on transfers of an asset (i.e., a lien) and automatically release that lien when the loan is repaid.

Smart contracts are enforceable just like other contracts

Smart contracts and traditional contracts are fundamentally and conceptually equivalent. Mechanics used in smart contract transactions are simply a logical progression of business practice. Over time, parties have transitioned from delivery of physically signed documents, to transmission of signed documents via fax and pdf, to use of digital signatures, including increased adoption of click-wrap agreements. Courts have readily enforced digital signatures and click-wrap agreements, and smart contracts are a natural extension.

Statutory enforcement mechanisms exist for smart contracts

Digital signatures using distributed ledger technology haven't been tested in court. But, under the Electronic Signatures in Global and National Commerce Act ('E-Sign Act') and the Uniform Electronic Transactions Act ('UETA'), a digital signature using public key encryption technology should qualify as an electronic signature, as would the mere inclusion of one's name as a part of an e-mail message – so long as in each case the signer executed or adopted the symbol with the intent to sign.

For example, the US Uniform Electronic Transactions Act provides for a broad variety of electronic methods of assenting to a contract, including 'an electronic sound, symbol, or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record'. This does not mean that electronically-executed documents, including smart contracts, are automatically valid. Whether a contract has actually been executed, and whether that contract is enforceable, are questions that fall outside of these statutes and are governed by common law.

Is blockchain a revolutionary new technology? Will it eliminate the use of ERP systems? Will it do away with the problems that continue to plague supply chain management today?

Oracles can make smart contracts practical

To automate performance, the smart contract must have access to any metric by which performance must be measured. Smart contracts, like other computer code, can be described as a series of 'if-then' statements. To activate the process, one must know whether the condition has occurred. For example: if loan payments will be automated, the smart contract will need access to an interest rate provider. 'Oracles' are third-party information services providers that will digitally 'sign' a transaction, attesting to the occurrence of specific conditions. This doesn't make the oracle party to the transaction – the oracle is just attesting that the condition has occurred. The oracle's digital signature can be retained on the distributed ledger so that parties can review the payment process and confirm that payments were made correctly.

Access to the means of performance is also needed to make smart contracts practical. In practice, this means access to funds or other assets. Early smart contract implementations for cryptocurrencies required parties to deposit all cryptocurrency necessary to perform the contract into a segregated account, which is impractical for commercial use. However, enterprise distributed ledger providers are working on integration with existing payment systems and mechanisms on the ledger for payments without requiring deposits of all funds necessary to perform the contract. Distributed ledgers can also integrate with asset registries to impose and lift liens and even transfer assets as payments are exchanged through the ledger.

Blockchain and the supply chain

Supply chain management has long sought an efficient, accurate, and paperless process. A system that records each event, is transparent when it needs to be, confidential at other times, designed to meet the regulatory obligations around government filings, commercial demands, insurance claims, and on and on. The evolution of ERP systems, such as SAP and Oracle, for example, have taken this ambition to new heights.

Is blockchain a revolutionary new technology? Will it eliminate the use of ERP systems? Will it do away with the problems that continue to plague supply chain management today? Or is it evolutionary, likely to operate as an adjunct or supplement to existing systems? Perhaps the latter, but it's important to be prepared.

One of the touted merits of a supply chain DLT is that it would solve challenges such as provenance (diamonds), sourcing (origin claims), important admissibility issues (forced labour), and even emerging issues such as conflict minerals. Indeed, many of the use cases thus far have focused on high-value goods, such as diamonds. But the Maersk-IBM initiative to put routine records on the blockchain,[2] the use by Singapore of DLT for import record processing,[3] and others illustrate that DLT is moving into the mainstream.

Are you ready? What risks exist for you?

Important questions about blockchain and the supply chain include:

1. **Do you have a blockchain strategy?** Many companies in the supply chain have yet to develop a strategy. As the applications grow, more companies are being asked to participate in or adopt blockchains. Do you know if it makes sense for you? Do you know what risks exist?

2. **Have you managed the risks of using blockchain?** One set of risks is participation without understanding. Adoption of a production blockchain solution can create obligations when the blockchain engine processes transactions and creates records, rights, and obligations. A similar risk is inherent in the decentralised nature of distributed ledgers – on a multi-party distributed ledger network, trust and authority is shared among all the network participants.

3. **Other risk centres on risk under the trade laws.** Blockchain will add some valuable tools for supply chain managers. The 'append-only' feature of blockchain makes it impossible (some say) to tamper with – if a transaction needs to be corrected, later additions to the blockchain are required. The original record remains in the blockchain to be reviewed if needed. But with this opportunity comes risk. If privileged or incorrect information is added to the blockchain, it cannot be removed.

4. **Information security is another significant risk.** Consider: Who has access to the ledger and how is access controlled? What information will be stored on your blockchain? Is that information subject to controls? Network participants will also need clarity of ownership of data that is stored on the blockchain. If oracles will be used, it is necessary to ensure those oracles continue to provide correct information through service level agreements or other mechanisms. Consider how future software updates will be implemented and whether they will raise fresh security concerns.

One of the touted merits of a supply chain DLT is that it would solve challenges such as provenance (diamonds), sourcing (origin claims), important admissibility issues (forced labour), and even emerging issues such as conflict minerals.

5. **One risk is that of over-reliance:** Will it accomplish what you expect? For instance, if you are buying ore from a particular mine in Myanmar, and the certificate from the mine is hashed and added to the blockchain, and you have permission to see it, that's great, you can verify that the ore is what you want. Or can you? Unfortunately, blockchain does not eliminate fraud. If the party issuing the certificate wants to provide a false statement, there is nothing about blockchain that will cure it. Blockchain may well make it easier to isolate and identify fraud, but it cannot eliminate it. This risk is the risk of compliance – will your transactions be more or less compliant in blockchain? This will depend on those who have access and on whose performance that you rely on, as is the case now.

6. **A secondary risk is commercial, and is a function of the process.** With a smart contract, payment for exported goods could occur automatically as part of the engine in the blockchain processing the transaction. If a mistake or fraud occurred in the real world before the records are added to the blockchain, you may not receive what you bargained for, but you will have paid for the goods nonetheless. Elimination of this risk, just like today, is to build in whatever measures – inspection, verification, or other steps – that ensure that the engine processes the correct transaction.

What's next?

Blockchain and distributed ledgers are entering the mainstream. In 2018, you can expect to see more implementations and so now is the time to develop a blockchain strategy and to develop a risk profile so that you will be ready to take advantage of the benefits of this new technology. Now is the time to:

- conduct a blockchain 'audit' to determine the opportunities and risks;
- explore how others are using blockchain, to avoid surprise;
- develop an approach to participation;
- develop standard risk-management clauses for contracts;
- monitor regulatory developments – agencies are studying blockchain and what it means for the industries they regulate. ■

Jenny E. Cieplak is a counsel in Crowell & Moring's Washington, DC office and is the head of the firm's blockchain and distributed ledger technology initiative. Jeff Snyder is a partner in the firm's International Trade Group.

jcieplak@crowell.com

jsnyder@crowell.com

This article is reprinted from the January 2018 issue of Trade Security Journal.
www.tradesecurityjournal.com