# Blockchain Brings New Capabilities, but Proceed with Caution

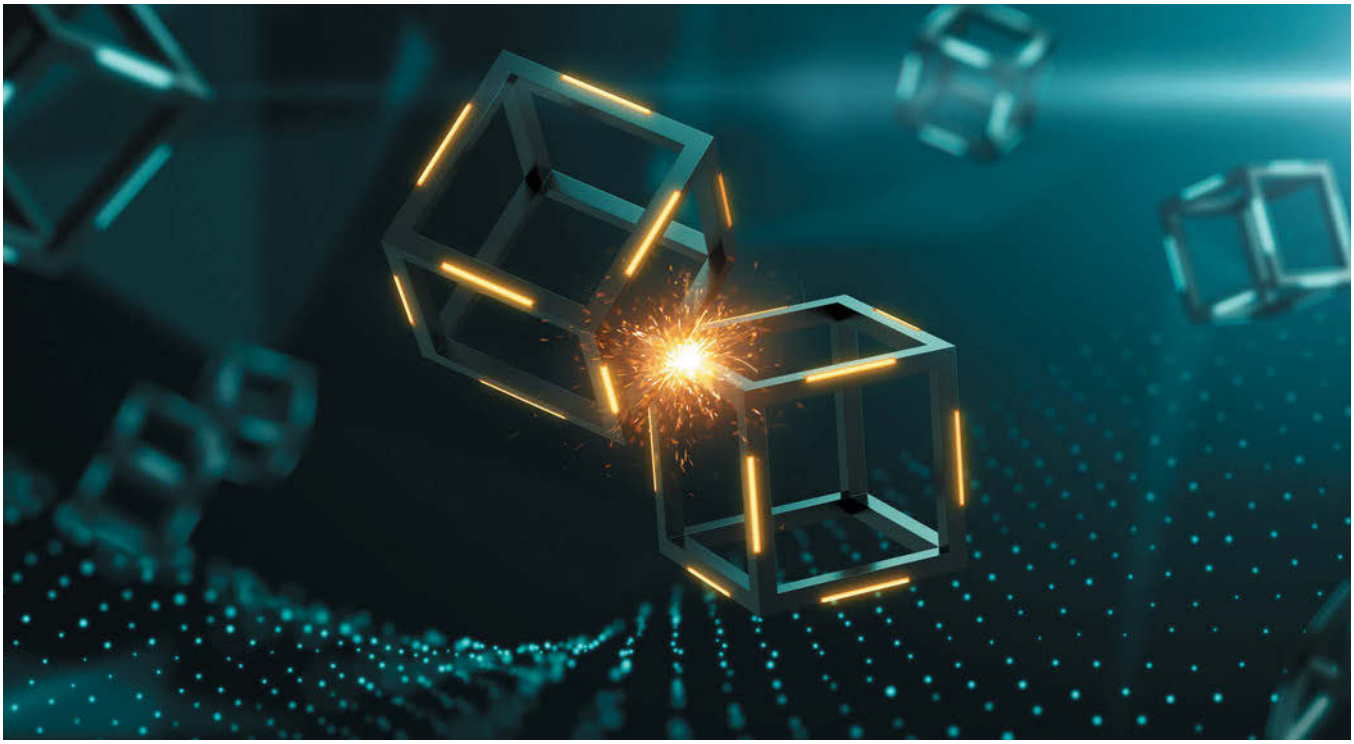
*Chuck Cook* | RENOVODATA

**THE TECHNOLOGY KNOWN as blockchain is generating a lot of buzz, but it is not very well understood. Developed in 2008 to support the Bitcoin cryptocurrency, blockchain is an update of the old mutually distributed ledger (MDL) products that were too clumsy to ever find wide acceptance.**

Now vendors are offering blockchain-type products for many applications besides cryptocurrencies. Some 3PL and trucking companies are employing blockchains for a variety of tasks.

Some facts about the technology:

- A blockchain is a peer-to-peer (P2P) ledger system, distributed across numerous computers.
- Content is not stored in any one place, nor managed by any single entity.
- Nodes transmit data packets called blocks, which are linked and verified by cryptographic validation.
- Data is continually current and updatable, without intermediaries.
- Content is shared directly between users, who are connected only to other users.
- Information is always available to all users, so multiple parties can work on the same document simultaneously.
- All items are preserved permanently.



PHIVE (/G/PHIVE)/SHUTTERSTOCK.COM

- Information can be shared but not copied or captured by anyone outside the network.
- Blockchains are guarded by encrypted public and private keys. A public key is a user's address and a private key is the user's password.

Among the benefits blockchain offers, these should be of particular interest to 3PL and trucking companies:

- More-efficient contracts
- Faster and more-accurate supply-chain auditing
- More-secure file storage
- Improved trend prediction
- Better control of the Internet of Things (IoT)
- Improved IT auditing.

## Potential problems

Because blockchain networks are not designed to be connected to any other systems, they contribute a level of security, but they do not overcome the dangers of breaches and breakdowns.

Indeed, blockchain brings new risks in the form of additional hardware, software and activities, all of which need to be defended.

Here are some possible difficulties with blockchain networks:

- Risks are highest during the early stages of any technology.
- When a blockchain network connects several companies, each of them is obligated to provide strong security. If even one company does not, all participating organizations are endangered.
- As with any system, blockchain can be compromised by human error, internal sabotage, server breakdowns, physical disasters, and other causes.
- Blockchain enhances data security within its own boundaries, but any system can be hacked.
- Because they contain critical and confidential data, blockchain networks present rich opportunities for ransomware attacks.
- Hackers can break into a blockchain by stealing public and private keys stored on paper or devices, easy targets that need to be kept secure.
- Blockchains can introduce vulnerable endpoints that can be exploited by hackers.
- The insertion of blockchain technology into a system creates added complexity, which necessitates more-sophisticated protections.

## Protection and Recovery

As with all other system components, solid data protection and disaster recovery capabilities present the strongest safeguards for blockchain networks. Data protection blocks or reduces the damage the above-mentioned events can cause. Disaster recovery ensures that when such mishaps take place, downtime can be eliminated or substantially diminished.

It is worth noting that blockchain networks themselves must be backed up as scrupulously as any other parts of a system.

## Implementing data protection

For an overview of the data protection issues facing our industry, check out "Network Security for 3PL and Trucking Companies," an article from RenovoData in the November 2017 issue of TIA's The Logistics Journal. It can be viewed on the members-only section of the TIA website. Key subjects include:

- The language of security risk
- Business meets technology
- Solving people problems
- What to protect
- Your enemies
- Your weapons
- Testing

## Planning for Strong Disaster Recovery

The main elements of a sound disaster recovery plan include:

- Preparing for all kinds of disasters
- Understanding the company's data
- The need for transparency
- The need for off-site emergency facilities
- Consistent scheduled testing

## Employees' Roles

Two imperatives for robust data protection and disaster recovery programs are employee buy-in and training. These are especially crucial for 3PL and trucking-company environments where IT-related activities are numerous, diverse and fast-moving.

All users should understand relevant potential crises, relevant best practices and what to do in emergencies. This means effective, ongoing training, including regular sessions for new employees.

When examining your data protection and disaster recovery needs in the blockchain era, be sure to seek expert counsel. Rely on skilled professionals with the experience and current knowledge that these complex and extensive activities demand.

Once again, blockchain can be a useful tool, and may well usher in significant advances, but it is not invincible. Data protection and disaster recovery are as important as ever because no system is immune to security threats.

*The author, Chuck Cook, is President of RenovoData. Michele Vayle, Marketing Director, may be reached at mvayle@renovodata.com or (877) 834-3684.*