The *TT20* Thought Leader Newsletter May 2022

ThinkTWENTY20
The Magazine for Financial Professionals

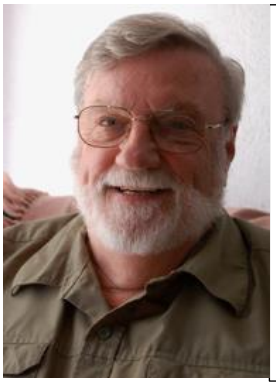
Dedicated to generating deep thought on the issues facing accountants and other financial professionals

Blockchain and the DLT Ecosystem

By Gerald Trites, FCPA, FCA

Origins

Blockchain first became well known as the underlying technological basis for Bitcoin, the successful crypto-currency introduced in a 2009 paper published by Satoshi Nakamoto, a person or persons so far not positively identified.



Jerry is Editor in Chief of ThinkTWENTY20 and a retired partner of KPMG. He also served as a Professor of Accounting and Information Systems and, for 12 years, as Director of XBRL Canada. He has published 14 books. His latest book 21st Century Corporate Reporting *is to be released in April by Business Experts Press of New York.*

Nakomoto never mentioned the term “blockchain” in that paper, although there was one reference to ”blocks are chained” in a discussion of the idea of grouping transactions into blocks and connecting them with the use of cryptography. The term blockchain, however, became popular only after the publication of the paper.

Blockchain is not a new technology but, rather, a unique combination of pre-existing technologies. It is a subset of Distributed Ledger Technology (DLT), which in turn is derived from distributed databases. “A distributed database is a database that consists of two or more files located in different sites either on the same network or on entirely different networks. Portions of the database are stored in multiple physical locations and processing is distributed among multiple database nodes.”[i] Distributed databases came into use during the 1970s.

Distributed Ledger Technology is a system for recording transactions in multiple places at the same time. Unlike traditional databases, distributed ledgers have no central data store or administration functionality, but instead are often managed by consensus of the participants, using protocols that vary and can be unique to particular systems. Transactions are timestamped to establish the date of their creation.

Blockchain took the idea of DLT a step further by grouping the transactions in a DLT into blocks and creating a cryptographic hash of the transactions. A hash is a unique string of letters and numbers created from text using a mathematical formula or algorithm. “Along with its own hash, each block

stores the hash of the block before it. Blocks are therefore "chained" together making the ledger (almost) immutable or unable to be changed."[ii]

There are different kinds of blockchains in use. One type is referred to as permissionless, which allows anybody to see the blockchain and requires no permissions to see it nor to participate in it. Permissioned blockchains do require permission, and are commonly used for business transactions, such as those in supply chains. Some permissioned blockchains are classified as private and are used for small groups of people involved in specific transactions, such as those handled by smart contracts.

The Bitcoin blockchain is a totally open, permissionless blockchain. Therefore, anyone can view the bitcoin blockchain; for example, you can see it here on the Blockchain.com website.[iii]

A number of myths or misconceptions have arisen,

some of which can lead to serious miscalculations in strategy.

Another well known, permissionless blockchain is Ethereum, which supports the currency ETH along with other applications. Ethereum is programmable and gained some publicity by introducing 'smart contracts.' "A smart contract is a self-executing contract with the terms of the agreement being directly written into lines of code. The code and the agreements contained therein exist across a distributed, decentralized blockchain network. The code controls the execution, and transactions are trackable and irreversible."[iv] Because they are based on blockchain, they permit agreements to be carried out among disparate, anonymous parties without the need for a central authority.

Myths About Blockchain

Blockchain has been called the most hyped technology of recent years and the least understood. Accordingly, a number of myths or misconceptions have arisen, some of which can lead to serious miscalculations in strategy.

First is the issue of trust. The myth is that there is no need for trust when using blockchain. The stated reason for this is that you can trust the technology., We know, however, that blockchain uses cryptography, which involves key management and requires trust in that process. Also, for permissioned blockchains, trust must be placed in the people giving the permissions. Even the initial whitepaper itself isn't about there being no need for trust. Rather it was about an electronic payment system based on cryptographic proof instead of trust in a central authority.

The second myth is that of immutability. The idea that transactions, once recorded in a blockchain are immutable (cannot be changed) comes out of the fact that the transactions are included in the block hash and that any change will change the hash in that block, which will then not match the hash in the subsequent block and therefor break the chain, which would be noticed by the participants and lead to the restoration of the original transaction or some remedial action. What this argument ignores is that transactions that alter or reverse the original transaction can be recorded in subsequent blocks, which would then be included in the hash for the subsequent block and, therefore, never break the chain. So, while it is true that the original transaction may be immutable, the ultimate effect of that transaction is not immutable.

The myth that blockchains are completely secure is just plain wrong. This myth itself is beginning to fade away, as people gain a greater understanding of blockchain. For example, professional organizations like CPA Canada have released some publications[v] that point to the audit and control issues around blockchain which make it clear that additional work is required to gain assurance that the system has integrity and is well controlled.

The myth that blockchains always produce accurate records is also wrong. It ignores one of the most basic attributes of computer systems that has existed since computers were first invented. That is the principle of GIGO or "Garbage in Garbage Out." If tainted information is input into a system, then the likelihood is that the output of the system will be tainted. In other words, a computer system just processes the information it is given. Blockchains are no different. In most computer systems, GIGO is dealt with by instituting input controls that help to guide the accuracy of the input information. Similar controls are needed for blockchain systems, despite the built-in systems in blockchain for authorization and acceptance of transactions. The Committee of Sponsoring Organizations of the Treadway Commission (COSO) has set out guidance on blockchain controls.[vi]

Despite these shortcomings, blockchain is very useful for various use-cases.

Known Use Cases

Bitcoins, as mentioned above, represent the best-known use-case of blockchain. Because the Bitcoin blockchain is permissionless, and blocks are added through a consensus mechanism known as mining, their level of immutability is very high. Bitcoins have proven to be very volatile, however, which limits their usefulness as an exchange currency. For example, the value of a bitcoin rose from around $4,000 to $60,000 during the past year and has experienced similar fluctuations for several years.

One answer to this volatility was the creation of stablecoin, a class of cryptocurrency that is usually pegged to a major currency, such as the US dollar. Tether (USDT) and TrueUSD are two examples.

On January 5, 2021, the Office of the Comptroller of the Currency in the U.S. published an interpretive letter explaining that national banks and federal savings associations are now allowed to use stablecoins and run blockchain nodes, adding that they need to meet reserve requirements. Such reserves are maintained by independent custodians and are regularly audited for adherence to the compliance rules. This regulatory acceptance was a major step forward for blockchain and cryptocurrencies.

Once a supply chain is traced with blockchain, the product can even be marked with a barcode that would reveal the history of the product.

Other Use Cases

According to a survey conducted in 2018 by PwC, blockchain applications in the financial industry constituted 46% of all use cases. Other industries with significant use cases included industrial products and manufacturing (12%), energy and utilities (12%), healthcare (11%) and government (8%).

Prominent among use cases in industry and manufacturing are those involving supply chain automation. Supply chains and healthcare are two areas that have been particularly affected during these pandemic times.

Supply Chain Use Cases

Supply chains represent the steps involved in getting a product or service from its original state to the customer, from raw materials to the end product. Modern supply chains have become very complicated, embracing a variety of suppliers, often from various parts of the globe. And there is often a concern among buyers as to where a product comes from and what materials and processes have gone into its production. For example, there is an interest in determining whether child labour, forced labour and/or human trafficking have been employed in the product. There also are concerns about the environmental impact of the product during its development.

At present, supply chains can be very opaque. Blockchain can provide a means of introducing transparency by capturing key data points, such as components, processes, certifications and claims, and then providing open access to all blockchain participants. This is possible because, when blockchain is introduced to map and visualize an enterprise's supply chain, all of the components can be traced for every stage of production.

Once a supply chain is traced with blockchain, the product can even be marked with a barcode that would reveal the history of the product to the consumer. It could be scanned with a smartphone app.

One study gave this example: "It is estimated that nearly 30,000 bottles of illegitimate wine are sold every hour in China, many mixed with a variety of dangerous additives. Origintrail, in conjunction with TagItSmart, developed a system using blockchain to track more than 15,000 unique wine bottles.

Eventually, they hope to stop the sale of illegitimate wine, because, by a simple scan of a barcode placed on each bottle, consumers will be able to know every detail regarding their purchase."[vii]

As another example: "Provenance, a supply chain transparency startup, recently started a project for tracking responsible sourcing of tuna in Indonesia via blockchain"[viii] There are numerous other examples in practice of blockchain usage for supply chains. Consortium blockchains, which use blockchain to bring together various members of the supply chain into a trustless relationship, previously could only be accomplished with a centralized intermediary.

Healthcare Use Cases

The field of healthcare involves the use of large amounts of very sensitive and private data. With the increased degree of automation in the industry – some spurred on by the pandemic – this trend is intensifying.

"Blockchain technology can be used to support drug prescriptions and supply chain management, pregnancy and any risk data management as well as to support access control, data sharing and managing of an audit trail of medical activities. Other healthcare areas that can benefit from blockchain technology are provider credentials, medical billing, contracting, medical record exchange, clinical trials, and anti-counterfeiting drugs."[ix] Blockchain also enables patients to take control over their own health records.

A study published in October 2020 for the government of British Columbia looked into the changes being faced in the healthcare system of that province and considered various alternatives for addressing them, including blockchain. Their conclusion was clear.

"Our analysis of British Columbia's health care data management revealed several challenges, including information silos, the potential for medical errors, the general unwillingness of parties within the health care system to trust and share data, and the potential for security breaches and operational issues in the current EMR infrastructure. A blockchain-based solution has the highest potential in solving most of the challenges in managing health care data in British Columbia and other Canadian provinces."[x]

Here to Stay

Although blockchain has been severely hyped, it is a sound technology and having a substantial impact. Its usage for cryptocurrencies is still spreading and is, perhaps, the most prominent use. Supply chain applications are growing in number, however, and have considerable potential for improving this important area. The profession is becoming more involved in audit and control issues, which is an important element of sound blockchain usage. It's clear that blockchain will be with us for a long time.

For more articles like this, you can subscribe to ThinkTWENTY20 at www.thinktwenty20.com and also you can purchase the **New Publication: Corporate Reporting, Quo Vadis, by Alan Willis, FCA, FCPA "Paradigm Shifts Shaping the Future of Corporate Reporting: Purpose, Accountability, Value and Sustainability"**

---

[i] https://searchoracle.techtarget.com/definition/distributed-database
[ii] OECD Blockchain Primer, http://www.oecd.org/finance/blockchain.
[iii] https://www.blockchain.com/explorer.
[iv] https://www.investopedia.com/terms/s/smart-contracts.asp.
[v] *Blockchain technology and its potential impact on the audit and assurance profession* (Toronto: CPA Canada, available at https://www.cpacanada.ca/en/business-and-accounting-resources/audit-and-assurance/canadian-auditing-standards-cas/publications/impact-of-blockchain-on-audit. Also, *Blockchain and crypto-assets resources for CPAs*, available at https://www.cpacanada.ca/en/business-and-accounting-resources/other-general-business-topics/information-management-and-technology/publications/cpa-perspectives-on-blockchain.
[vi] https://www.coso.org/Documents/Blockchain-and-Internal-Control-The-COSO-Perspective-Guidance.pdf.
[vii] https://openledger.info/insights/blockchain-in-the-supply-chain-use-cases-examples/#Logistics_Tool_for_Wine_Supplies.
[viii] https://www.provenance.org/tracking_tuna_on_the_blockchain.
[ix] Marko Hölbl, Marko Kompara, Aida Kamišalic and Lili Nemec Zlatolas (Maribor, Slovenia: University of Maribor, Faculty of Electrical Engineering and Computer Science, 2000, published in *Symmetry*, October 2018).
[x] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7647806/ (*Journal of Medical Internet Research*, October 2020).