Marriott Student Review

Volume 2
Issue 2 *A Bright Future*

Article 16

August 2018

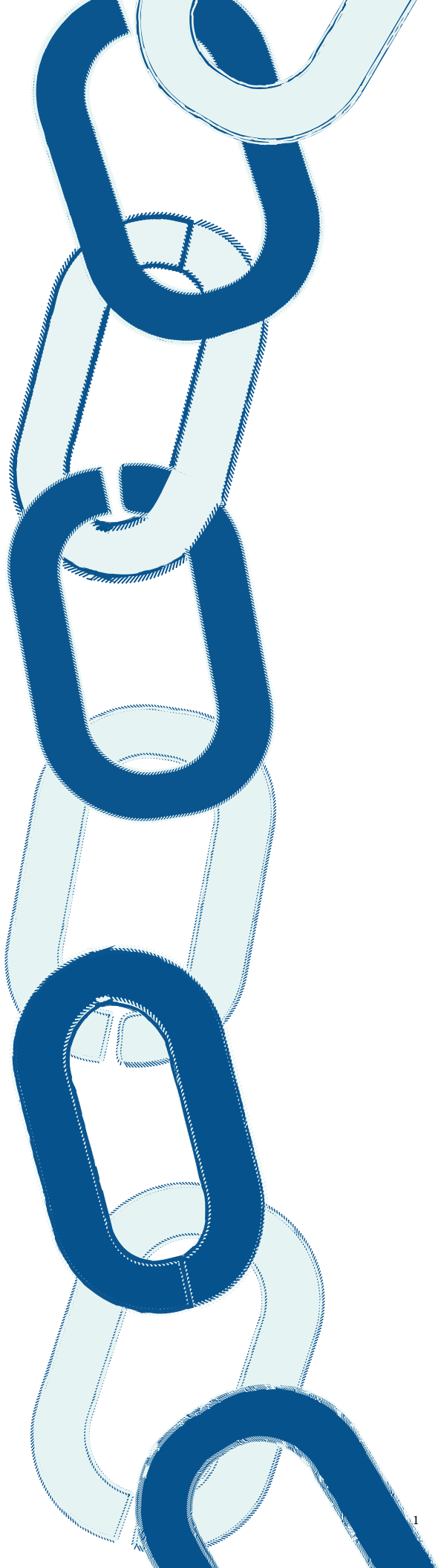
Synopsis: A Bit about Blockchain

Jonathan Chichoni
jchichoni@gmail.com

Synopsis: A Bit about Blockchain

Cover Page Footnote
This is a synopsis of the complete article found in this issue.

A BIT ABOUT BLOCKCHAIN



Note from the editor: The following article was adapted from an honors thesis entitled The Digital Global Supply Chain: The Growing Case for Blockchain Technology Expansion Within Global Supply Chain *written by the author. The full text is available on the ScholarsArchive website.*

What is Blockchain?

Blockchain is a decentralized and digitally distributed ledger or database of records and transactions that facilitates the process of recording transactions and tracking assets in a business network. Those assets can be hard assets like food goods, micro-chips or houses. They can also be digital assets like intellectual property, branding, copyrights and documentation. Blockchain's distributed ledger encompasses a list of connected blocks stored on a distributed network that is secured through cryptography. Blockchain derives its name from the manner in which it stores transaction data, in blocks that link together to form a chain. Each "block" contains encrypted information and hashed pointers to a previous block of information. The blocks record and confirm the time and sequence of transactions within a network that is governed by rules created by the network participants. As the number of transaction grows, so does the blockchain (Gupta 2017). Figure 1 is a diagram that shows the transaction process on a blockchain network.

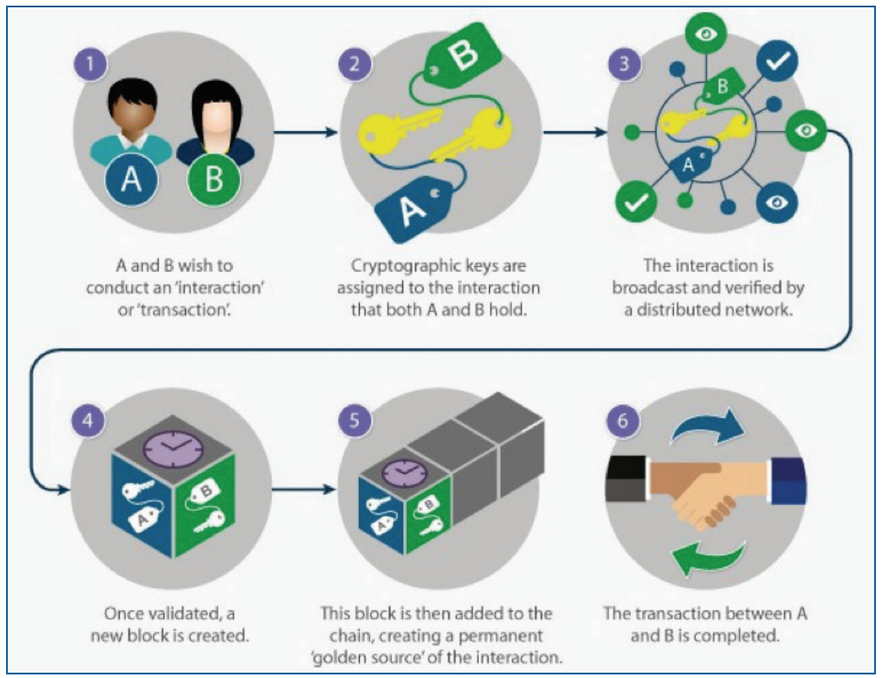


Figure 1-1 How Blockchain Works

(Standard Chartered 2018).

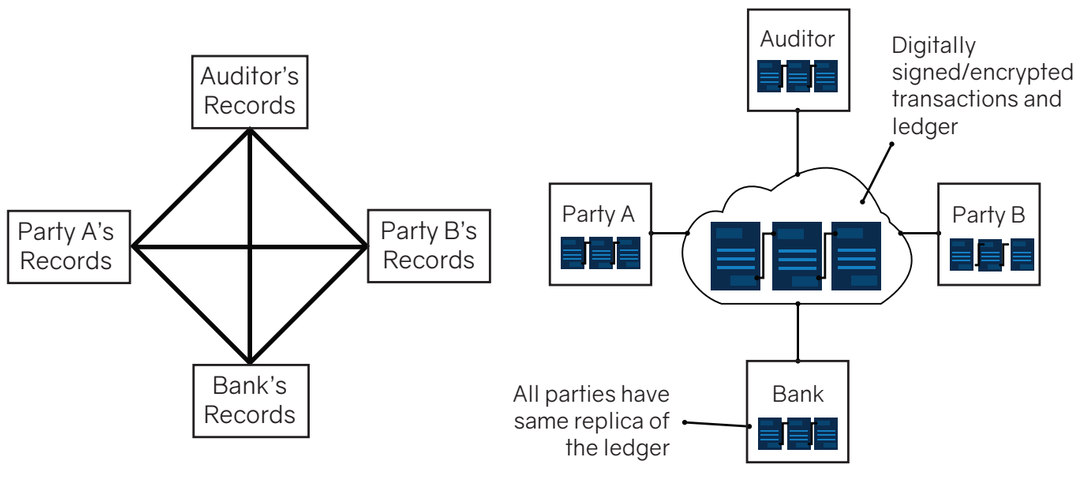


Figure 1.2 Business Networks with Blockchain (Shown Right)

(Gupta2017)

Blockchain technology is often referred to as a "de-centralized" technology meaning that it does not depend on intermediaries such as banks, clearing houses or escrow institutions to send, record, and store information. Traditional business networks rely on using different and multiple ledgers for each participant in the network. Blockchain allows all participants to be on the same network with a high degree of transparency and trust. Below are diagrams explaining the differences between a blockchain network and the network that businesses currently use.

This figure is illustrative of a few of the advantages of blockchain. As seen in figure 1, the blockchain network makes the business network more efficient and economical because it reduces duplication efforts and the need for intermediaries. All parties are able to see and access the same ledger. In addition to this simplified network shown in figure 1.2, a blockchain network operates on four key characteristics:

CONSENSUS

All participants in the blockchain network must agree on the network's validity. A blockchain network does this through trusted and transparent transactions in four separate ways:

1. *Proof of stake:* In order to validate transactions along a blockchain network the "validators" or network participants in the chain must hold a certain percentage of the network's total value. It is generally supposed that this feature can protect from malicious attacks on the network by reducing the incentive for attacks and making it extremely expensive to execute attacks (Gupta 2017).

2. *Multi-signature:* Each transaction along the blockchain network requires a majority of the validators to agree that a transaction is valid (i.e. 6 out of 10 must agree that the transaction is valid). Multi-signature provides for enhanced consensus among participants and greater security across the supply chain (Gupta 2017).

3. *Practical Byzantine Fault Tolerance (PBFT):* This is an algorithm designed to settle disputes among the competing network participants when one participant generates a different transactional output than the other network participants in the blockchain. This specific feature provides security from hacking in a blockchain network (Gupta 2017).

4. *Smart Contracts:* These are agreements made by the network participants that govern the different transactions along the blockchain network. They can contain many contractual and binding clauses that can be self-executing and self-enforcing. They can provide better security to contract law and can reduce the lead times between transactions because they are verifiable and self-enforcing/self-executing. Smart contracts provide integrity, traceability and transparency across the supply chain (Gupta 2017).

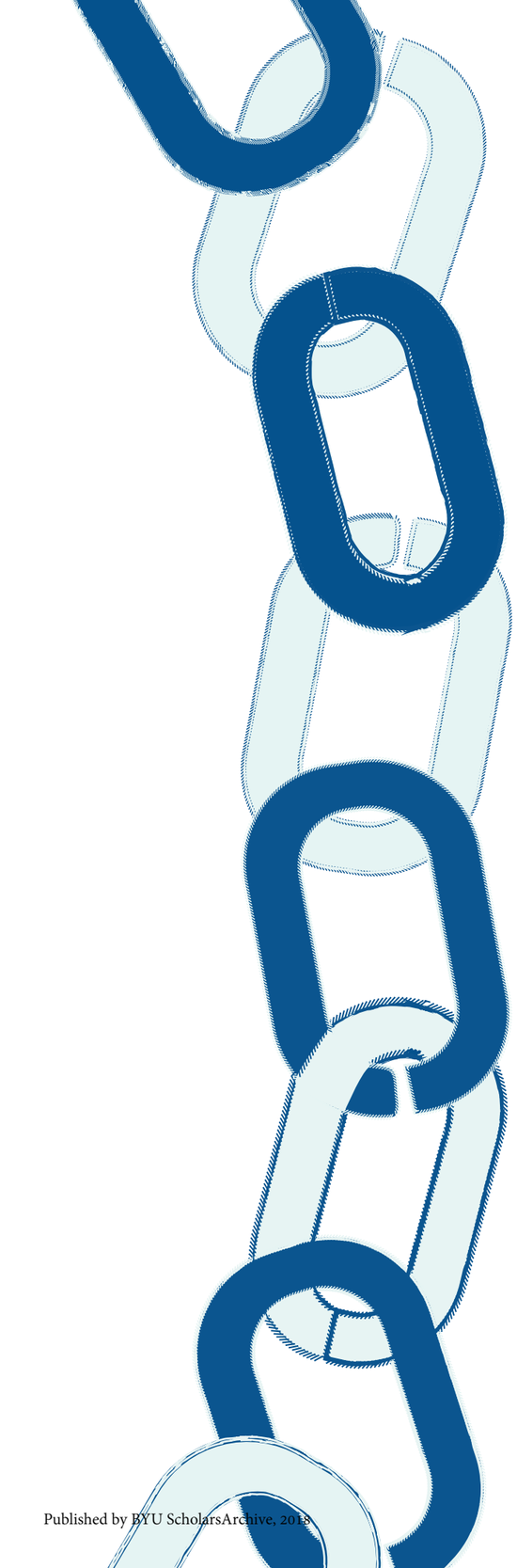
In a business application, a blockchain has pluggable consensus: network participants may determine which consensus measure is best to use for a specific blockchain or function.

PROVENANCE

Network participants are able to understand and confirm where the asset came from and how the ownership of the asset has changed over time. A blockchain network does this through its shared ledger technology. The shared ledger or distributed ledger application of blockchain possesses the following functions:

1. Records all transactions that occur in the business network – the shared ledger is the source of truth upon which all participants can independently verify transactions and asset/information transfers (Gupta 2017).

2. Is shared among all network participants and through replication, each network participant has a duplicate copy of the ledger. This allows for the seamless sharing of information amongst all permissioned ledger participants (Gupta 2017).



3. Is permissioned so network participants can only see the transactions that they are authorized to see. Each network participant has an identity that links to specific transactions, but participants can choose the transaction information that other network participants are authorized to view. This provides the necessary level of disclosure and network security to all network participants (Gupta 2017).

IMMUTABILITY

Network participants cannot tamper with transactions once they are recorded in the shared ledger. If the transaction is an error, then another transaction must occur to reverse the error with both transactions being visible to the network participants. A key feature of blockchain's immutability is its permissioned technology and cryptographic technology:

1. Permissioned technology allows each network participant to grant or restrict access to certain transactional details. Auditing parties in the blockchain network that are trusted by all other network participants can view that the transactions have taken place but can be restricted from viewing the specific details of that transaction. Regulators can be allowed to view all details of the transactions (Gupta 2017).

2. Cryptographic technology through the use of digital certificates provides identifying information and is forgery resistant. The identities can also be verifiable because they have been issued by a trusted and permissioned agency (Gupta 2017).

FINALITY

There is only one single ledger where each network participant can go to determine the ownership of an asset or the completion of a transaction. This ledger cannot be changed and can only be amended. Each amendment can be viewed and tracked, giving all participants knowledge of the amendment made (Gupta 2017).

A Brief History of Blockchain

The genesis of blockchain goes back several years before bitcoin, the famous cryptocurrency. The underlying theories and research that preceded the creation of blockchain is more defined than its founding. In 1991, Stuart Haber and W. Scott Stornetta published their research on cryptographically secured blocks in the Journal of Cryptography with the title "How to time-stamp a digital document." Their paper brought to light the first sequence of inalterable chains of digital documents whose time stamps and alterations could not be fraudulently changed (Haber 1991).

The discussion around cryptography and "blocks" evolved to generate the innovation of a de-centralized network file system that not only included cryptographic time stamping signatures on documents but also a network file system based on trust between two "block writers." These innovations were published in 2002 at The Symposium on Principles of Distributed Computing by David Mazieres and Dennis Shasha (Mazieres, Shasha 2002). Ultimately in 2008, blockchain technology as we know it today was released as a distributed ledger technology and in 2009 became the underlying technology behind the cryptocurrency bitcoin. Its creator or group of creators, whose identities are not known, are identified under the pseudonym Satoshi Nakamoto.

Near the time of blockchain's development, there was a growing global appetite for e-commerce, online banking, an increasing mobility of people and the rise of the Internet of Things (IoT). Each of these market dynamics presented unique challenges. First, in order to fuel global e-commerce growth, IoT expansion and online banking, payment networks needed to be faster than ever. Despite the creation of companies like PayPal and other merchant payment processing companies, many business transactions remained and to this day still remain inefficient. The time between the exchange of goods at the point of transaction and settlement can be long (especially in supplier transactions along a value chain). Many credit card companies created and have continued to sustain high prices of entry, leaving individuals and companies to pay the cost of onboarding and dealing with the time-consuming vetting and paperwork processes. Additionally, according to the World Bank, over half the population in the world did not have access to a bank account in 2009 and over two billion people today still remain without a bank account (World Bank 2017).

E-commerce could not actively engage those individuals due to lack of resources and consumer verification standards. Centralized systems such as banks placed all market participants at risk of fraud, cyber-attacks, network issues and systemic risk as seen in the 2008 market crash. The presence of these intermediaries created inefficiencies through the need for third-party validation and duplication of efforts across transactions. These only added to the challenges of e-commerce, online banking and IoT growth. The increasing mobility of people created an issue with dealing with local currencies and the slow and inefficient process of exchanging currencies. Hard currency was only useful in local transactions and in relatively small amounts. Against this backdrop, blockchain was created as a means of resolving these issues by providing benefits that would strengthen transparency, cost savings, time efficiency and trust among market participants.

Edited by Evan D. Poff

Curious how blockchain may affect manufacturing businesses? Want to see what logistics companies care about when it comes to this technology? For Jonathan Chichoni's analyses of the unique impacts on nearly 20 industries, as well as the complete thesis and bibliographical matter, visit https://scholarsarchive.byu.edu/marriottstudentreview/