Ensuring that global supply chains are managed in ethical, safe, and environmentally friendly ways is challenging, particularly from the perspectives of data quality and data management. Despite the value it would provide, creating an accessible and auditable trail of information that captures a product's journey through the supply chain has traditionally been cost prohibitive. Blockchain provides one potential mechanism for solving this problem. This article provides an in-depth examination of blockchain-based distributed ledger technologies in the context of global supply chain management (SCM). It contrasts trustless consensus environments, used by many cryptocurrencies including Bitcoin, and permissioned consensus environments, more often in business applications like SCM. Transactional use cases are presented to illustrate key concepts in applying permissioned blockchain to SCM.

KEY WORDS

blockchain, efficiency, Hyperledger, private blockchain, supply chain, traceability, transparency

Blockchain for Supply Chain: Improving Transparency and Efficiency Simultaneously

M. C. BENTON, N. M. RADZIWILL,
A. W. PURRITANO, AND C. J. GERHART

INTRODUCTION

In December 2003, Japan banned the import of all U.S. beef following a U.S. Department of Agriculture report of a single case of bovine spongiform encephalopathy (BSE), aka "mad cow disease") discovered in Washington state. The ban lasted more than two and a half years, with an estimated cost to the U.S. beef export industry of over $3 billion (ElAmin 2006). As a condition of reopening its markets to U.S. beef, Japan insisted that the United States create a program that would allow each animal's place of origin to be traced (O'Neill 2005). Meanwhile, by 2008, researchers like Weber and Matthews (2008) were investigating the environmental impacts of transporting food—so-called "food miles"—and making recommendations to consumers about how to minimize greenhouse gas (GHG) emissions by either "buying local" or changing their diet to include less GHG-intensive food (Weber and Matthews 2008). Similarly, people are also increasingly concerned about the presence of genetically modified organisms (GMOs) or "frankenfoods" in their diets (Schurman 2004). In short, for a variety of reasons, people are increasingly concerned about where their food comes from and what it is made of.

This concern is not restricted just to food. Around the turn of the century, society began to express broad concern for the proliferation of "conflict diamonds" or "blood diamonds" mined by children enslaved by warlords who used the profits to fund their armies (Baker 2015). More broadly, the necessity to identify conflict minerals such as gold, copper, cobalt, and "coltan"—critical to miniaturization in the manufacture of many modern electronic devices—has led geologists to devise scientific techniques that allow them to determine the geographic source of these minerals (Melcher et al. 2008). Less tangibly, consumers interested in using electricity generated only from renewable sources have been able to purchase tradable renewable energy credits (RECs) for almost two decades (Berry 2002). Concern for where things come from, what they contain, and how they were made extends to everything from textiles to TV shows. Given trustworthy information and a choice, a significant portion of consumers has demonstrated that they prefer "clean" or "green" sourced products and are frequently willing to pay more for them.

Until recently, creating an accessible and reliably auditable trail of information for every bushel of organic apples, every fair-trade can of coffee, and every non-sweatshop pair of sneakers has been cost prohibitive. Determining that all of the processes comprising the global supply chains are conducted in ethical, safe, and environmentally friendly ways is extraordinarily time and energy consuming (Zorzini et al. 2015). Given that most of the time consumers have neither the time, the energy, nor the means to determine the source of the products they consume, manufacturers and producers have been able to cut corners or turn a blind eye to injustices for the sake of increasing profit margins. In the relatively near future, however, blockchain technology promises to make a fully transparent and open supply chain not only economically feasible, but necessary. As this happens, the authors predict that consumers will come to demand products sourced and produced in a socially responsible way. Producers of supply chain management (SCM) software should begin building and adapting their systems to incorporate the capabilities afforded by blockchain now.

Social responsibility will not be the only—and likely not even the largest—driver of the push to incorporate blockchain into supply chain. There are enormous efficiencies to be reaped from this technological evolution. A key to making this happen will be understanding the mechanisms by which trust is first established, then *automated*, and then maintained. Never before has it been truly possible for a company to validate claims about the soundness of its supply chain without, periodically, *physically* sending a representative to the part of the globe where the process occurs to personally inspect it. It remains to be seen whether blockchain will be capable of automating trust. This article will begin to explore that possibility.

Earlier, the authors provided a general overview of blockchain technology and speculated on a number of potential applications that would be relevant to software quality professionals (Benton and Radziwill 2017). In this article, the authors dive deeper into one of those application areas—the use of blockchain for SCM—with particular focus on the potential social impacts of incorporating blockchain into SCM software. The authors explore the concept of traceability as it relates to social responsibility and building trust relationships with consumers. They also explore the automation of trust using Hyperledger, an emerging, open-source, blockchain-development platform, as one example of using trust automation to streamline logistical processes. They conclude with a discussion of what actions software quality professionals should be taking right now and in the near future to prepare for and incorporate blockchain into their supply chain management applications.

TRACEABILITY

People care deeply about how things are made and where they come from. Since prehistoric times, human societies have been organized around work and the production of the goods and services required to support life. Some even identify this trait as a defining characteristic of *homo sapiens* (Hannan and Kranzberg 2017). Beginning as early as ancient Rome, but flourishing in medieval Europe and Ming Dynasty China, craft guilds became responsible for the economic and political organization of labor, and for quality assurance of goods and services (Epstein 1995; Ying 2006). The dynamic between production (knowledge) and regulation (power) was one main subject of influential 20th century philosopher Michel Foucault's work (Eribon 1991). Even though the term "traceability" does not appear in an ISO standard until 1994 (ISO 8402:1994), after Foucault's death, Chamayou (2014) articulates that:

> "Traceability forms an apparatus in the Foucauldian sense, that is to say, a heterogeneous ensemble consisting of concepts, institutions, procedures, regulatory decisions, and scientific knowledge. It encompasses non-discursive elements (for example, the diverse techniques of identification: passwords, barcodes, RFID labels, electronic bracelets, DNA tests, retinal scanners,

> face recognition software, etc.), as well as discursive elements (for example, the imperative of security, along with the problematics met by the prevention of risk and the redefining of sanitary responsibility)."

In short, a deep concern for the origin of the goods and services that maintain life and well-being is embedded deep within the psyche of every person, and is arguably related to what it means to be human. The ability to trace these origins with ever-increasing precision is likely to have broad impacts that ripple subtly and overtly throughout society. It is important, therefore, to consider what is meant by the term "traceability."

GS1, the global standards organization that introduced the barcode in 1974, defines "traceability" as (2017, 6):

> "the ability to trace the history, application or location of an object [ISO 9001:2015]. When considering a product or a service, traceability can relate to: origin of materials and parts; processing history; distribution and location of the product or service after delivery."

While this is a generic, pragmatic definition, a great deal of the traceability literature deals specifically with the food industry. In this context, "traceability" has been defined by the European Union Commission (Tian 2016, 2) as:

> "The ability to trace and follow a food, feed, food-producing animal or substance intended to be, or expected to be incorporated into a food or feed, through all stages of production, processing and distribution."

Bosona and Gebresenbet (2013) report that in the EU food producers have been legally bound to implement food traceability systems (FTS) since 2005. They approach the definition of "traceability" more broadly and associate it with the similar terms "tracing" and "tracking." They report on at least 14 different definitions that range from heuristics such as "the probability of finding the source of a problem," to pragmatic, operational definitions like "the ability to trace the history, application, or location of an entity by means of recorded identifications," which was the original ISO definition in 1994.

While traceability is clearly an important, well-defined, and well-understood concept (the GS1 standard referenced previously describes parameters for the interoperability of traceability systems), just because a record (digital or otherwise) specifies the source and handling of all of the entities involved in a production system, that doesn't mean all of the stakeholders in the system automatically trust the veracity of that record. For example, in the United States, regulating bodies such as the Food and Drug Administration (FDA) and the Federal Trade Commission (FTC) determine the meaning and usage of terms like "organic" and "all natural." Despite these rules, savvy consumers know that there is significant latitude in these definitions, and that just because a product claims to be "organic" doesn't necessarily mean all components of the product live up to the spirit of what the term implies. They know the FDA and FTC have neither the time nor the resources to perfectly enforce all of their regulations. The principle of *caveat emptor* ("let the buyer beware") is still very much the norm. Ensuring the believability of claims about product quality is a key niche that blockchain technology proposes to fill.

Modern information technology makes it possible to collect voluminous amounts of data about the source, condition, and handling of all components of a production system, from the mine or farm where the raw materials were harvested, to the finished product in the hands of the end user. It also makes it possible to document the faithfulness with which all of the production processes were executed. Modern technology also makes it possible, and frequently easy, to falsify, fabricate, or fake this production data, to fool a consumer into believing they have received a product of high quality and integrity, when in fact, they have not. Blockchain promises to solve this problem, that is, to make it impossible to commit fraud in the context of the supply chain. Shortly, the authors will addresses the mechanisms by which trust can be achieved, or more accurately, obviated. First, however, they briefly explain the basics of blockchain.

BLOCKCHAIN BASICS

At its most basic, a blockchain is a database of transactions, frequently referred to as a "ledger." Transactions take place in the context of a network of stakeholders, each of which possesses and maintains a complete, independent copy of the ledger. A "transaction" is any event in which data are written to the ledger for which there are at least two stakeholders that care about the validity of that data. A "stakeholder" is any entity (person, group, organization) that stands to gain or lose something of value (money, property, status, reputation, time) that is somehow related to the transaction. By definition, the overlap between the interests of any pair of stakeholders must be less than 100 percent.

Typically, every transaction recorded in the ledger represents a potential transfer of value from one stakeholder to another. Each transaction must be independently validated by multiple stakeholders, and digitally signed using each stakeholder's cryptographic keys. It is incumbent upon each stakeholder to guard the security of their keys. Theft of a set of keys would give the thief the ability to authorize new transactions in the name of the stakeholder, but would not allow them to alter previous transactions. Loss of one's keys has the potential to prevent a stakeholder from accessing any of the value stored in a blockchain, although newer systems have ways to recover from this. In many systems, there is a fee associated with each transaction, which is used to cover the costs of transaction validation similar to how credit-card companies charge a percentage of each transaction they process.

A "block" is a batch or collection of validated transactions. The number of transactions in a block is usually determined by one of several means. A new block is created when either:

- A predetermined number of transactions have been accumulated, or
- A predetermined period of time has elapsed, or
- Whichever of the above two events comes first, or
- Some other event occurs, such as the solving of a proof-of-work puzzle, or the random selection of a block creator via lottery, voting, or some other process

Each block is created by a single stakeholder in the network, but is subsequently verified by other stakeholders to be correct. In some applications (like Bitcoin) the creation of a block is referred to as "mining" and is associated with the receipt of some form of reward, which is used to incentivize mining. All blockchains use some form of cryptographic hashing algorithm to verify the contents of a block. Each subsequent block incorporates the hash from the previous block, except the very first block, typically called the "genesis" block. Since it is impossible to correctly calculate the hash of a new block without relying on the hashes from all of the blocks that came before it, the blocks are said to form a "chain"—hence, a "blockchain."

"Consensus" is the process by which a network of stakeholders validates each block and then incorporates it into the blockchain. Since no block can be added to the blockchain without achieving consensus on the network, and since each block is cryptographically linked to all of the blocks before it, it is extraordinarily costly for the ledger to be tampered with once it has been written. There is no way to alter any earlier block (or any transaction within it) without immediately changing the hash value, therefore corrupting all of the blocks that come after it. As such, a blockchain represents a virtually tamper-proof ledger of historical transactions between independent stakeholders.

TRUST VS. CONSENSUS MECHANISMS

To understand trust vs. consensus, the authors describe the actors in a typical transactional economy *without* blockchain. The relationship between these stakeholders is adversarial, meaning that transactions between them represent a zero-sum game in which one stakeholder could potentially obtain a disproportionately larger benefit from the transaction through cheating, misrepresentation, or falsification of the digital artifacts mediating the transaction. This characterization is not meant to imply that such cheating is by any means typical or expected, nor that bad actors are the norm. To the contrary, a key characteristic of highly functioning economies is that a high proportion of participants in the economy play by the rules; cheating and corruption are relatively rare. Rather, the key here is that the possibility of cheating always exists. In the absence of cheap, effective, and objective means to verify participants' faithfulness to the terms of the transaction, each must rely upon either the trustworthiness of the other, or upon the reliability of the society's systems of accountability and redress, for example, the legal system.

Clearly this is not a perfect system. Some actors enter the economy expecting to be cheated some percentage of the time, and they adjust their behavior to mitigate loss. An easy example is the consumer credit scoring system. Lenders assign a score to individuals designed to approximate the likelihood that someone will not honor the terms of a lending agreement. The higher the credit score (that is, the probability of paying back the loan to the bank), the lower the costs of the transaction in terms of fees and interest rates charged. Lenders assume they will make some bad bets and factor the cost of the losses into their business model. Frequently, they will not even bother to pursue the legal remedies available to them, and instead, sell bad debt to debt collection agencies or other actors who will pursue debtors.

In the days before credit scores, it was common for banks to have personal relationships with borrowers. Loan decisions were made locally. The lender and the borrower were members of the same community and were likely to know each other personally. The rules for determining creditworthiness were much more flexible and largely depended on the judgment of the lender. For better or worse, this way of doing business has become too expensive, and other ways to determine who is creditworthy have been developed.

Technically speaking, however, trust is neither the goal, nor promise, of blockchain. The goal is to achieve consensus around one particular version of the truth, that is, one version of reality that can be described or recorded digitally. Stakeholders and/or entities within a blockchain-based system do not rely upon trust; rather, they work to achieve agreement around the veracity of a shared set of digital artifacts. The algorithms by which such agreement is achieved are called consensus mechanisms or consensus algorithms. The existence and operation of these mechanisms is why blockchain-based systems are sometimes referred to as "trustless" systems, that is, because they facilitate transactions that don't rely upon trust.

Generally, there are two broad contexts in which these consensus mechanisms must operate: 1) trustless environments; and 2) permissioned consensus environments.

TRUSTLESS CONSENSUS ENVIRONMENTS

Most of the recent news about blockchain has been about trustless environments. This is the context in which blockchain-based systems like Bitcoin and Ethereum operate. The key assumption of trustless environments is that the transactors have little to no opportunity and zero need to actually know each other. In other words, there is no opportunity for a trust-based relationship to develop between the participants, and thus algorithms must replace trust.

A typical online purchase is an example of a trustless context. When purchasing a product on a website, it is extremely uncommon for the purchaser to actually know the merchant, and vice versa. They do not have the means or opportunity to meet and get to know one another, and in many, if not most, cases, the effort required to form such a relationship would defeat the purpose of having online stores in the first place, that is, the ability to buy things from anyone and anywhere on the planet without the need for the transactors to be colocated. But if this is the case, how is it that there is currently a robust online economy when there is no blockchain to obviate trust?

The answer is: trustworthy governments and banks. Since the medium for most online exchanges is government-backed fiat currencies, behind every transaction is the threat that the governments backing the currencies will impose stiff penalties to anyone caught attempting to violate the terms of the deal. Likewise, banks (credit card companies) also facilitate these transactions by serving as a proxy for trust. MasterCard trusts that a consumer will pay his or her credit card bill, the merchant trusts that MasterCard will front the cash for the purchase, and through this intermediary, one is able to complete the transaction. To participate in this economy, both merchants and consumers must establish their trustworthiness by developing credit histories. The alternatives to this process (cash-on-demand or mailing checks) have their own associated costs, and none of them are entirely free of intermediaries.

Of course, there are costs associated with these systems of trust. Governments collect taxes to operate and maintain a society where economies can flourish. Credit card companies collect a percentage of every transaction that is completed. One of the revolutionary aspects of blockchain-based systems is that they have the potential to remove the need for either governments or banks in the practice of commerce. This simultaneously creates a great deal of excitement on the part of merchants and consumers (no taxes! no fees!), and a great deal of fear on the part of governments and banks (no taxes! no fees!). While the prospect of getting rid of banks and government-backed currencies clearly excites most people (after all, people who work for governments and banks are consumers, too), dismantling these enormous infrastructures will almost certainly cause great disruption. (That discussion, however, is beyond the scope of this article.)

One aspect of trustless environments that is rarely discussed is where the computing power comes from. In the previous example, in addition to serving as a trust broker by providing credit, banks provide another crucial service: they maintain a massive global infrastructure of computing power that is used to process and clear all of the monetary transactions that occur. If society gets rid of banks, where will money "reside" and where will the computing power needed to validate and clear transactions come from? First, with cryptocurrencies, an individual's "money" will live in a cryptographically secure "wallet," which is really just a piece of software that keeps track of the transaction history and balance. It is very important to back up one's wallet, as a hard drive crash could make all of these funds inaccessible.

Second, computing power will be provided by the stakeholders in the network. Each of the consensus strategies described next provides some sort of incentive for a significant subset of the stakeholder network to keep their computers on and connected to the network at all times. If people only connected to the network when shopping or otherwise making transactions, the networks would likely never get off the ground due to lack of computing power. The method of incentivization varies dramatically and is one of the key defining factors of each strategy.

What are the mechanisms for achieving consensus in a trustless environment? The two most commonly talked about algorithms are called proof-of-work (PoW) and proof-of-stake (PoS). These two algorithms have some significant shortcomings, which will be addressed in the next section. However, given the enormous number of transactions that require a trustless environment (think e-commerce), there is a great deal of effort currently being devoted to coming up with other new alternatives to PoW and PoS. As a result, there is tremendous volatility in the trustless blockchain space right now, and the authors recommend that developers avoid this space for the time being.

Proof-of-Work Consensus

In a PoW system, potential block-creators, called "miners," have their computers solve mathematical puzzles of arbitrary difficulty. The puzzles also serve as the computational means of validating the transactions in the block. If a miner successfully "mines" a block, that is, is the first node in the network to solve the puzzle, the solution is sent out to all of the other nodes in the network that verify the solution, thereby achieving consensus. The successful miner receives a reward or bounty of some form. In the case of Bitcoin, the current bounty for successfully mining a block is 12.5 BTC, currently valued at just under $90,000 (early April 2018), and almost $250,000 at Bitcoin's peak price of $19,783.06 (Morris 2017).

There are two main downsides to PoW. The first is that it's slow. The Bitcoin PoW algorithm is tuned so a new block is mined about every 10 minutes. Given that most credit-card transactions happen in milliseconds, and stock trades in nanoseconds, most people believe a PoW algorithm could not currently handle the pace of transactions necessary to support the global economy. The second downside is that it is power hungry. Currently, the Bitcoin PoW algorithm is expected to consume about 60 TWh of electricity this year. That is approximately the same amount of energy that the entire country of Columbia uses in the same period (Digiconomist 2018). Given these issues, developers have been working on other consensus mechanisms like proof-of-stake (PoS).

Proof-of-Stake Consensus

In PoS, there is no mining; all available coins are "minted" or "forged" and distributed to "investors" at the moment the network is created. "Investing" usually involves giving some amount of a fiat currency, like U.S. dollars, to the creators of the blockchain with the promise that those creators will work to create something of value with that money in which the investor will have a stake. This investment opportunity is referred to as an "initial coin offering" or ICO. After minting, the value of the coins will fluctuate along with their perceived value.

Block-creators, called "validators," are chosen pseudo-randomly on a set schedule, for example, every 10 seconds, and rewarded with the fees from the transactions bundled in the created block. To be selected as a validator, members of the network must set aside some or all of their coins as their "stake." Staked coins cannot be spent until all transactions backed by the stake have been validated and cleared. Validation requires receiving a majority vote from the entire network. The likelihood of being chosen as a validator increases in proportion to the number of coins being staked. If validators try to cheat, they risk losing their entire stake. One cannot earn more in fees than one has staked, so the penalty for cheating is always much greater than potential reward, thus deterring bad behavior.

PoS largely solves the problems of PoW; it is relatively fast and doesn't consume massive amounts of energy. However, because the validation process requires vote tallies to be sent to every node on the network, as the network grows, latency increases. As such, PoS is not as scalable as some other strategies. Also, if not designed correctly, PoS disproportionately rewards the "rich," which will eventually lead to centralization and power imbalance. Lastly, PoS is relatively difficult to understand, especially if validator selection and voting are designed to avoid the centralization problem. As such, developing the software is more error-prone.

Other Trustless Algorithms

Conceptualizing and developing trustless algorithms is an area of active research (for example, Hawlitshek, Notheisen, and Teubner 2018). Proof-of-activity is a hybrid between PoW and PoS designed to combine the best aspects of both approaches. Proof-of-burn incentivizes churn with a stake that decays over time. Proof-of-capacity uses empty hard-drive space in place of coins for your stake. There are many variations on these themes, and more are being developed all the time. There is a lot of speculation (both cognitive *and* monetary) on which, if any, the market will choose. As a result, the authors advise that SCM developers avoid trustless environments, and instead look toward permissioned consensus environments to be described next.

PERMISSIONED CONSENSUS ENVIRONMENTS

Humans still have a significant advantage over automated systems in determining who is trustworthy and who is not. It is a skill developed and honed over millennia of human evolution. In permissioned environments, trust is not based solely on PoW or PoS or any other algorithm. Ledgers are not automatically open to the world as in trustless environments. While companies are open to a measure of decentralization (which means giving up some control over what is known about them), they don't want to just open their books and all their operations for the whole world, especially their competitors, to see. To a large extent, trust will still need to be built, at least at first, the old-fashioned way: through personal relationships over time. However, by using blockchain, companies will take great comfort in knowing that it is virtually impossible for anyone involved in the network to cheat. Any attempt to violate the terms of a contract will immediately be flagged in the system, and the source of the violation will be immediately identifiable. Actors who violate trust can be ejected from the network and lose the ability to participate in the economic system, either for a specified period of time or forever.

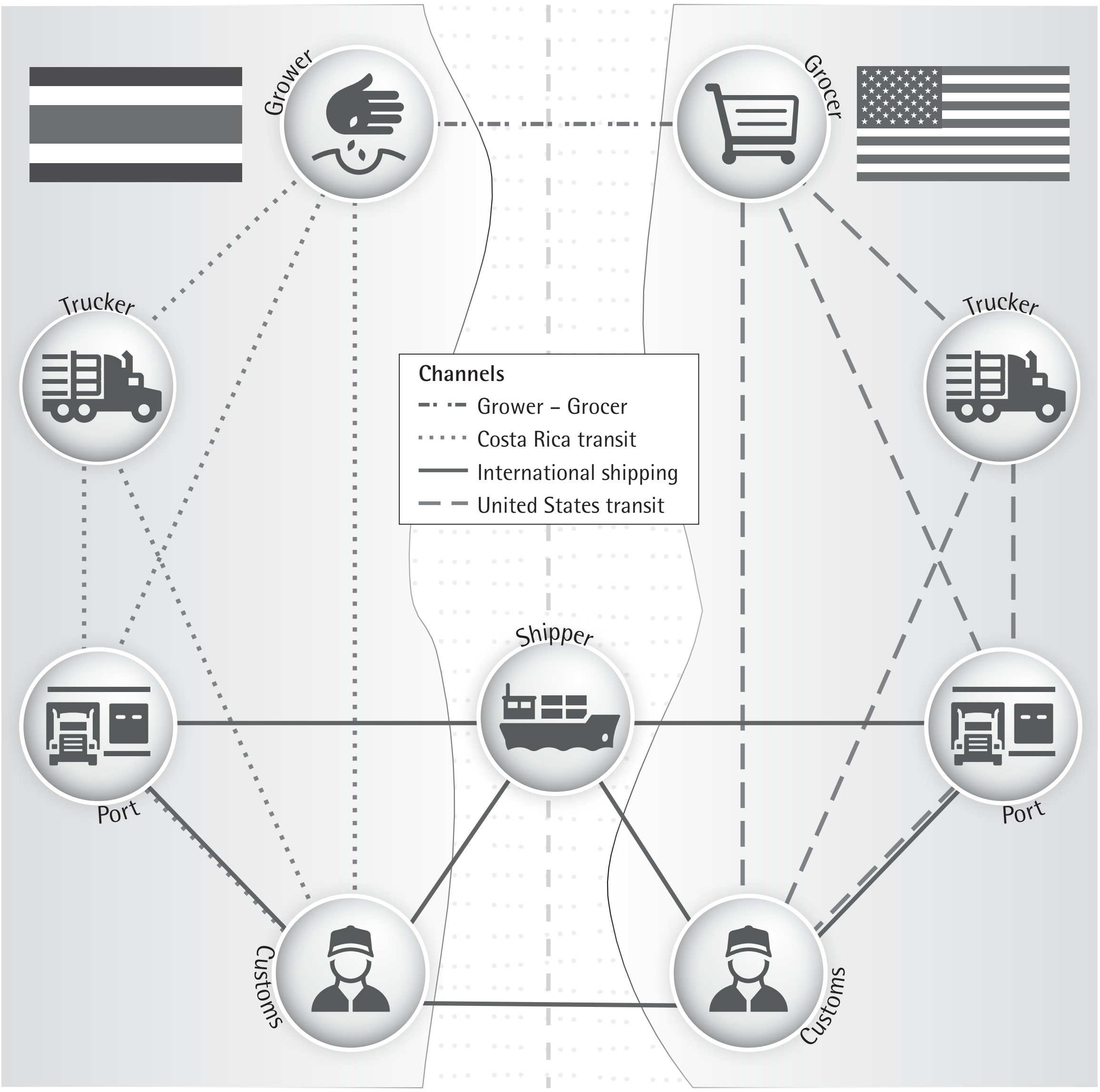
Complex strategies for convincing individuals to contribute computing power to the network are not necessary. Participants in permissioned networks will purchase and maintain their own computing resources in much the same way as companies currently pay to host websites and their own corporate networks. Another key difference is the kinds of transactions that will take place. In trustless environments, almost all of the transactions involve transferring digital currency of some form from one stakeholder to another. In permissioned environments, a "transaction" is simply the act of recording some piece of data relevant and necessary to facilitating the operation of the entire supply chain.

To illustrate these differences more concretely, consider an imaginary series of transactional use cases involving:

- A banana grower in Costa Rica
- A Costa Rican trucking company that will deliver the bananas to port
- Customs officials, food-safety inspectors, and other governmental agency employees
- Dock workers and other employees of the port who will move the bananas from the truck to the ship
- A shipping company that will move the bananas from the Port of Caldera to Los Angeles
- More customs officials, food-safety inspectors, and governmental regulators on the U.S. side
- Port and dock workers in Los Angeles
- A California trucking company that will pick up and deliver the bananas
- A grocery store where they will be sold to consumers

This network is depicted in Figure 1 on the next page and models the kind of network that can be built with Hyperledger, an open-source platform

FIGURE 1 A hypothetical permissioned consensus environment



©2018, ASQ

for blockchain development with broad support from a growing number of large companies spanning a wide variety of industries, governments, and academic institutions. Hyperledger will be described in greater detail later in the article.

Figure 1 depicts a simplified version of an international network for food production and distribution. It consists of four overlapping blockchain-based subnetworks called "channels." Membership in a channel is restricted to only relevant stakeholders. In this case, there are two domestic transit channels, an international transit channel, and a channel connecting a grower in Costa Rica with a grocer in California.

In this network, imagine that a grocer in California orders a shipment of bananas from a grower in Costa Rica. At any point during their journey, the quantity and condition of the bananas could be ascertained by a number of electronic means:

- Cameras to take photographs
- Scales to weigh the produce
- Thermometers and humidity sensors in storage containers to ensure produce was kept in optimal conditions throughout transit
- GPS to keep track of the physical location of the produce

- Digital signatures from every key person who takes responsibility for the shipment at some point in time
- Documentation of every transaction from the first order by the grocery store to the grower, to every service or inspection that took place in between

Any and all of these digital records can and will become part of the immutable digital ledger that will record every aspect of the entire process. If at any point during transit the bananas were damaged, or if some of them "fell off the truck" (an industry euphemism for theft), it would be immediately apparent at the next checkpoint. Responsibility for the damage could immediately be assigned to the guilty party. The terms for how such damage is to be handled can be programmed right into the "smart contracts," and penalties immediately and automatically applied. One of the most developed solutions for implementing a blockchain-based SCM system currently available in the market is Hyperledger.

HYPERLEDGER

Hyperledger is:

> "an open source collaborative effort created to advance cross-industry blockchain technologies. It is a global collaboration, hosted by The Linux Foundation, including leaders in finance, banking, Internet of Things, supply chains, manufacturing and technology" (Hyperledger 2018)

Hyperledger is led by Brian Behlendorf, co-creator of the Apache web server, the open-source software that, at its peak, powered more than 80 percent of the websites on the planet. He is also cofounder of the Apache Free Software Foundation, and recently a member of the board for the Mozilla Foundation where he has helped lead the effort to make HTTPS the default for new websites, and incorporate industry-leading privacy protections into the Firefox web browser. Premiere partners in the Hyperledger project include companies such as American Express, Cisco, IBM, Intel, and J.P. Morgan. At its core, Hyperledger is an incredibly broad coalition of powerful partners led by some of the most successful and experienced players in the open-source world.

Given the immaturity of the blockchain space, rather than devote all of their energy to a single platform, the Hyperledger project has decided to support development and experimentation with a broad range of promising frameworks, each of which will be attractive to different subsets of industry. Less than two years into the project, they have created a number of tools designed to give developers a robust sandbox in which to gain experience with building and deploying blockchain-based solutions. For example, the Hyperledger Composer Playground is a website (https://composer-playground.mybluemix.net/login) where even nondevelopers can quickly get their hands dirty and get a sense for what development in the blockchain space looks like. Given the relative complexity and steep learning curve of trustless blockchain environments like Ethereum, the authors were pleased to find that application development in the blockchain space is not terribly different from the more traditional application development people were used to. IBM, one of the biggest contributors to Hyperledger, is also working to convince other major industry players, like Maersk, that blockchain is an important place to invest their time, energy, and money.

IBM/MAERSK STUDY

In January 2018, IBM and Maersk, the world's largest shipping company, announced a joint venture to revolutionize the global shipping industry with blockchain-based technology. During an 18-month-long study, they discovered opportunities for the improvement of supply-chain operations that could reduce costs by approximately 10 percent, and increase total global trade volume by approximately 5 percent. For example, in examining the shipping of a single container of flowers from Kenya to the Port of Rotterdam, they discovered that it required more than 200 communications, sign-offs, and approvals, mostly paper-based, from a wide variety of entities along the journey. They found that such documentation can account for up to 20 percent of total shipping costs, and that the cost of shipping frequently equals or exceeds the raw cost of the goods being shipped. The opportunities for process improvement were immense. Although the study didn't directly estimate the cost of waste, fraud, and abuse, this is another area in which streamlined processes supported by blockchain are expected to have a significant impact (IBM 2018, van Kralingen 2018).

What the IBM/Maersk study and the rapid innovation demonstrated by Hyperledger teach is that there is a better than average chance that blockchain-based technologies are poised to become fundamental to how businesses, including supply chains, operate. While it is still very early in the process, it appears clearer every day that the world is on the brink of adopting a new way of interacting driven by and arising from the hyperconnectivity brought by 30 years of intense investment in the internet.

DISCUSSION AND RECOMMENDATIONS FOR DEVELOPERS

If a person is responsible for developing and maintaining one or more supply chains for a company, or for creating and maintaining the software that does so, what actions should that person be taking right now with respect to blockchain? Is it a fad? If not, what should that person be doing to prepare for adopting and incorporating this new technology into the company's systems? The authors believe that blockchain is not a fad, and that the best thing for SCM professionals to be doing right now is educating themselves about permissioned blockchains. For the rest of this section, whenever they refer to "blockchain" they are specifically referring to *permissioned* blockchains.

What gives the authors confidence that blockchain technology will become important for the foreseeable future? There are two relatively straightforward answers to these questions. The first is that the actual implementation details of blockchain-based systems have been around for a while and are not that difficult for developers to understand. Hashing functions have been around since the 1950s, and Merkle trees since the 1970s (Knuth 2000). The concepts surrounding transaction processing and database management are extremely well-understood across industry, and Merkle-tree-based systems (like Git) are used daily by developers, which will make them feel very comfortable as they begin to explore and discover how to implement blockchain-based solutions within their own systems. The key ideas that comprise blockchain have been around since the early 1990s. The reason they were not implemented sooner, perhaps, is that society needed 20 years to build out and experiment with the internet before it was ready. In short, a big reason the authors think blockchain is not a fad is that the key underlying concepts are relatively straightforward and have been around a long time.

The second reason they think blockchain is not a fad is the competitive advantages that emerge from the efficiencies blockchain promises to bring. Sustainable, IT-based, competitive advantage is well studied and notoriously hard to maintain since it is relatively easy for competitors to mimic (Piccoli and Ives 2005). On the other hand, given that the overall impact of technology-based solutions is a tendency to magnify the properties of an organization, companies that already have a strong track record of continuous improvement via seeking and implementing efficiency measures stand to benefit greatly. Particularly in the SCM space, blockchain promises to streamline regulatory and documentary processes, and potentially even remove the need for audits in many situations. The authors believe the 10 percent efficiency gain predicted by the IBM/Maersk study is likely to be a conservative estimate. Given that open-source organizations like Hyperledger have already been able to roll out proof-of-concept systems in a short, two-year window, it seems reasonable that the more progressive players in the SCM market will be inclined to pursue blockchain aggressively.

As such, SCM professionals would do well to begin educating themselves on the details of incorporating permissioned blockchain into their current operations, for example, find places within the organization where blockchain could be incorporated into internal workflows. As experience is gained, it will become possible to expand these practices more broadly within the company, and eventually to begin looking for ways to use blockchain to streamline the interactions between companies.

People and organizations care a great deal about the provenance of the goods and services they consume. Although the term itself is relatively recent, the importance of traceability can be tracked back at least to the Middle Ages. While for some time already the technological capacity to monitor and track the origin, condition, and handling of materials in supply chains has existed, there has never been a mechanism for guaranteeing that these data are reliable and trustworthy. The advent of blockchain likely signals a fundamental shift in the way supply chains will be managed, and how data quality and traceability can be ensured for SCM applications.

REFERENCES

Baker, A. 2015. The fight against blood diamonds continues. *Time* (August 27).

Benton, M., and N. Radziwill. 2017. Quality and innovation with Blockchain technology. *Software Quality Professional Magazine* 20, no. 1.

Berry, D. 2002. The market for tradable renewable energy credits. *Ecological Economics* 42, no. 3:369-379.

Bosona, T., and G. Gebresenbet. 2013. Food traceability as an integral part of logistics management in food and agricultural supply chain. *Food Control* 33, no. 1:32-48.

Chamayou, G. 2014. History and philosophy of traceability. Historicizing Big Data Working Group. Sciences of the Archives Project. Berlin, Germany: Max Planck Institute for the History of Science. Available at: http://bit.ly/2qf82ZO.

Digiconomist. 2018. Bitcoin Energy Consumption Index. Available at: http://bit.ly/2GPjvpq.

ElAmin, A. 2006. Japan re-opens doors to US beef. BakeryAndSnacks.com. Available at: bakeryandsnacks.com/Article/2006/07/27/Japan-re-opens-doors-to-US-beef.

Epstein, S. A. 1995. *Wage labor and guilds in medieval Europe.* Chapel Hill, NC: UNC Press Books.

Eribon, D. 1991. *Michel Foucault.* Betsy Wing (translator). Cambridge, MA: Harvard University Press.

GS1. 2017. GS1 Global Traceability Standard (Issue 2.0). Available at: http://bit.ly/gs1gts2 on 2018-04-08.

Hannan, M. T., and M. Kranzberg. 2017. History of the organization of work. *Encyclopædia Britannica.* Available at: http://bit.ly/2qfLVCE.

Hawlitschek, F., B. Notheisen, and T. Teubner. 2018. The limits of trust-free systems: A literature review on blockchain technology and trust in the sharing economy. Electronic Commerce Research and Applications.

Hyperledger. 2018. About Hyperledger. Available at: https://www.hyperledger.org/about.

IBM. 2018. News release: Maersk and IBM to form joint venture applying Blockchain to improve global trade and digitize supply chains. Available at: https://ibm.co/2uZm0DP.

Knuth, D. E. 2000. *Sorting and searching*, second edition. Boston, MA: Addison-Wesley, 547–548.

Melcher, F., M. A. Sitnikova, T. Graupner, N. Martin, T. Oberthür, F. Henjes-Kunst, E. Gäbler, A. Gerdes, H. Brätz, D. Davis, and S. Dewaele. 2008. Fingerprinting of conflict minerals: columbite-tantalite ("coltan") ores. *SGA News* 23, no. 1:7-14.

Morris, D. Z. 2017. Bitcoin hits a new record high, but stops short of $20,000. *Fortune.com.* Available at: https://for.tn/2uWWi2T.

O'Neill, K. 2005. How two cows make a crisis: US-Canada trade relations and mad cow disease. *American Review of Canadian Studies* 35, no. 2:295-319.

Piccoli, G., and B. Ives. 2005. IT-dependent strategic initiatives and sustained competitive advantage: A review and synthesis of the literature. *MIS Quarterly* 29, no. 4: 747-776.

Schurman, R. 2004. Fighting "Frankenfoods": Industry opportunity structures and the efficacy of the anti-biotech movement in Western Europe. *Social problems* 51, no. 2: 243-268.

Tian, F. 2016. An agri-food supply chain traceability system for China based on RFID & blockchain technology. In *Proceedings of the 2016 13th International Conference on Service Systems and Service Management (ICSSSM)*, 1-6. New York: IEEE.

van Kralingen, B. 2018-1-16. IBM, Maersk joint blockchain venture to enhance global trade. *IBM Think Blog.* Available at: ibm.com/blogs/think/2018/01/maersk-blockchain/.

Weber, C. L., and H. S. Matthews. 2008. Food-miles and the relative climate impacts of food choices in the United States. *Environmental Science & Technology* 42, no. 10:3508-3513.

Ying, Z. 2006. The transformation of traditional Chinese guilds in modern times. *Frontiers of History in China* 1, no. 2:292-306.

Zorzini, M., L. C. Hendry, F. A. Huq, and M. Stevenson. 2015. Socially responsible sourcing: Reviewing the literature and its use of theory. *International Journal of Operations & Production Management* 35, no. 1:60-109.

BIOGRAPHIES

Morgan Benton is co-founder of the Burning Mind Project, and an associate professor in the Department of Integrated Science and Technology at James Madison University in Harrisonburg, Virginia. He holds doctorate and master's degrees in information systems from the New Jersey Institute of Technology, and a bachelor's degree in leadership studies/sociology/physics from the University of Richmond. His research focuses on innovation in learning, higher education, and transformation. Benton can be reached by email at: morgan.benton@gmail.com.

Nicole Radziwill is an associate professor in the Department of Integrated Science and Technology at James Madison University in Harrisonburg, Virginia. She is an ASQ Fellow and is a Certified Six Sigma Black Belt (CSSBB) and Manager of Quality/Organizational Excellence (CMQ/OE). She has a doctorate in quality systems from Indiana State University, and her research focuses on the quality and innovation in cyber-human production systems. She is one of ASQ's Influential Voices and blogs at http://qualityandinnovation.com.

Austin Purritano is a senior studying the social impacts of computing in the Department of Integrated Science and Technology at James Madison University. For his capstone, Purritano developed a predictive algorithm designed to alert type 1 diabetics when their blood glucose levels were likely to fall out of the normal range as part of a mobile application designed to help diabetics manage and track their condition.

Cole Gerhart is a senior studying social impacts of computing in the Department of Integrated Science and Technology at James Madison University. Gerhart's capstone focused on mitigating the social and environmental impacts of commuting via an app to promote ridesharing.