CUTTER CONSORTIUM
Access to the Experts

Cutter Business Technology JOURNAL

Vol. 31, No. 4, 2018

Management, Innovation, Transformation

"Industries across the board hope to capitalize on block-chain technology whose potential goes well beyond cryptocurrencies — with mil-lions if not billions of dollars being spent on pilot projects and startups."

— Philip O'Reilly,
Guest Editor

Blockchain: Where Are We Now? Where Are We Headed?

Cutter Business Technology JOURNAL

As business models for creating value continue to shift, new business strategies are constantly emerging and digital innovation has become an ongoing imperative. The monthly *Cutter Business Technology Journal* delivers a comprehensive treatment of these strategies to help your organization address and capitalize on the opportunities of this digital age.

Cutter Business Technology Journal is unlike academic journals: Each monthly issue, led by an expert Guest Editor, includes five to seven substantial articles, case studies, research findings, and/or experience-based opinion pieces that provide innovative ideas and solutions to the challenges business technology professionals face right now — and prepares them for those they might face tomorrow. *Cutter Business Technology Journal* doesn't water down or delay its content with lengthy peer reviews. Written by internationally known thought leaders, academics, and practitioners — you can be certain you're getting the uncensored perspectives of global experts.

You'll benefit from strategic insight on how the latest movements in digital innovation and transformation, IoT, big data analytics and cloud, to name a few, are changing the business landscape for both new and established organizations and how cutting-edge approaches in technology leadership, enterprise agility, software engineering, and business architecture can help your organization optimize its performance and |transition to these new business models.

As a subscriber, you'll also receive the *Cutter Business Technology Advisor* — a weekly bulletin featuring industry updates delivered straight to your inbox. Armed with expert insight, data, and advice, you'll be able to leverage the latest business management thinking to achieve your organization's goals.

No other journal brings together so many thought leaders or lets them speak so bluntly — bringing you frank, honest accounts of what works, what doesn't, and why. Subscribers have even referred to *Cutter Business Technology Journal* as a consultancy in print and likened each month's issue to the impassioned discussions they participate in at the end of a day at a conference!

Get the best in thought leadership and keep pace with the technologies and business models that will give you a competitive edge — subscribe to *Cutter Business Technology Journal* today!

Cutter Business Technology Journal®

Founding Editor: Ed Yourdon
Publisher: Karen Fine Coburn
Group Publisher: Christine Generali
Managing Editor: Cindy Swain
Copy Editors: Jennifer Flaxman, Tara Meads
Production Editor: Linda Dias
Client Services: service@cutter.com

Cutter Business Technology Journal® is published 12 times a year by Cutter Information LLC, 37 Broadway, Suite 1, Arlington, MA 02474-5552, USA (Tel: +1 781 648 8700; Fax: +1 781 648 8707; Email: cbtjeditorial@cutter.com; Website: www.cutter.com; Twitter: @cuttertweets; Facebook: Cutter Consortium). ISSN: 2475-3718 (print); 2475-3742 (online).

Subscription rates are US $485 a year in North America, US $585 elsewhere, payable to Cutter Information LLC. Reprints, bulk purchases, past issues, and multiple subscription and site license rates are available on request.

☐ Start my print subscription to *Cutter Business Technology Journal* ($485/year; US $585 outside North America).

Name _____ Title _____

Company Address _____

City _____ State/Province _____ ZIP/Postal Code _____

Email (Be sure to include for weekly *Cutter Business Technology Advisor*) _____

Fax to +1 781 648 8707, call +1 781 648 8700, or send email to service@cutter.com.
Mail to Cutter Consortium, 37 Broadway, Suite 1, Arlington, MA 02474-5552, USA.

Request Online License Subscription Rates

For subscription rates for online licenses, email or call: **sales@cutter.com** or **+1 781 648 8700.**

CUTTER CONSORTIUM
Access to the Experts

Opening Statement

by Philip O'Reilly

Blockchain is gaining prominence. Originally developed as the distributed ledger technology underlying Bitcoin, it is now being recognized as a foundational technology providing a legitimate transaction platform that will likely transform how the world does business. Industries across the board hope to capitalize on this technology whose potential goes well beyond cryptocurrencies — with millions if not billions of dollars being spent on pilot projects and startups to find the blockchain solution that will improve efficiencies, transparency, security, business costs, and, ultimately, trust.

Blockchain pilots being launched by governments and private organizations encompass a range of initiatives, such as improving food and drug traceability, automating share trading, expediting insurance claims processing, improving access to electronic medical records, securing and validating voting processes, and ensuring the delivery of humanitarian aid.

But even with this push toward a blockchain breakthrough, many remain skeptical of its potential and worry about its risks and shortcomings, including scaling, higher energy and processing costs, speed issues, and the current lack of regulations, to name a few. In addition, the new EU General Data Protection Regulation (GDPR), effective 25 May of this year, poses some challenges on the data privacy front that could stall the public blockchain adoption progress.

This issue of *Cutter Business Technology Journal* sheds some light on the status of blockchain technology adoption. With perspectives from eight different authors, the articles detail some of the opportunities, challenges, applications, and use cases, as well as the industry and business implications associated with a blockchain technology initiative.

First, Robin Renwick argues that the tension between blockchain's promise of openness and transparency and the use of cryptographic algorithms that allow the anonymization of information may cause disjunctive rifts between stakeholder groups. Renwick identifies five key stakeholder groups within blockchain and distributed ledger technology and discusses each group's approach to privacy. He proposes "a distinct body that informs and educates stakeholder groups, acting as intermediary between them" to manage tensions as blockchain becomes more established.

Next, Steven Kursh, Arthur Schnure, and Natalia Gold provide us with a comprehensive discussion of smart contracts and how they work within a blockchain. They also consider the benefits of using the cryptocurrency app Ethereum for building and using smart contracts, detail the advantages and limitations of smart contracts, and impart some cautionary advice.

Next, Johannes Ahlmann proposes that blockchain technology has the potential to disrupt the food industry. He describes how blockchain can help gain better insight into and improve the management and transparency of end-to-end food supply chains. Ahlmann also demonstrates how blockchain is particularly suited to benefit the food industry by providing examples of current projects in the pilot and proof of concept stages.

The concept of privacy returns in our next article — but with a very different take. Stephen Walsh envisions "a fundamental shift in the Internet business model from its current status," with users retaining control of their data. His vision of the "New Internet" relies on blockchain. While Walsh recognizes that this New Internet is still in its early stages and faces imposing obstacles, he offers hope that it's closer than we might think with a review of some interesting blockchain platforms and apps, including revolutionary newcomer Blockstack.

Finally, Maciej Jędrzejczyk and Karolina Marzantowicz paint a bright picture for blockchain's commercial adoption, facilitated by the use of integrated private blockchain platforms. They see blockchain disrupting established business models via ecosystems that include the entire value chain and make it possible for competitors to voluntarily cooperate.

We hope the articles in this issue provide you with new perspectives on blockchain's potential as a game-changing technology now and in the future.

BUILDING BRIDGES

Privacy, Blockchain, and Why the Industry Needs a Spanner

by Robin Renwick

The promise of a distributed ledger that is shared, stored, secured, and readily accessible from across the globe heralds a brave new dawn for a host of areas: financial services, identification systems, provenance verification, tracking and tracing databases, and product lifecycle monitoring, to name a few. Information storage using distributed consensus methods is a key evolutionary step in the business ecosphere, especially when deployed in conjunction with platforms for programmable, executable, and externally verifiable business logic (i.e., smart contracts). These technologies offer leveraged innovation, effectiveness, efficiency, and security — all of which are sources of valuable competitive advantage.

When harnessed correctly, technologies are key instigators for the evolution of business process and practice. However, at the center of this revolution sits a concept that weighs heavily on the blockchain industry from several angles. A concept that, if understood, managed, and integrated incorrectly, has the potential to disrupt the seemingly unstoppable global adoption of distributed ledger, blockchain, and smart contract technology. This concept is *privacy*, and, more importantly, *information privacy*.

On one side of the coin appears a technology promising openness and transparency; a technology that affords access from anywhere in the world, as agents[1] draw data from an immutable store. On the reverse side of the same coin, we see the development and application of complex, sophisticated, unbreakable cryptographic algorithms that allow users to obfuscate and anonymize information; an affordance that, if leveraged, encroaches on the regulatory and legislative powers of governments. Understanding how to manage this tension is going to be one of the most important matters of the 21st century.

As businesses adopt blockchain technologies, the ecosphere is going to need a specified intermediary agent whose core function is to manage disparate motives, ideologies, and inclinations. If left unaddressed, tensions may morph into enacted tribalism, and a major disjunct will appear between stakeholder groups — potentially stopping the so-called revolution in its tracks.

Why Is This Important?

The blockchain industry comprises practitioners continuously interacting with notions of privacy from differing perspectives: data obfuscation, data science, information technology, information science, data encryption, data storage, information security, blockchain protocol development, cryptography, privacy legislation, and privacy regulation. Understanding how each group operates is an essential part of any system design process.[2] Comprehending how distinct groups operate will allow the industry to create "bridges," or "spans," between them — allowing technology to mature in a cohesive, rather than divisive, fashion.

The industry needs to understand what similarities and differences exist between groups — whether found in motives, desires, ideologies, or political inclinations. These may concern how privacy is enacted in the technology, who should govern it, or how much power should be afforded to users of the technology. Divergence will surface neither from similarities nor benign differences — but disjunctive differences have the potential to cause upheaval and disruption, as groups battle for what they believe privacy is, what it should be, how it should be enacted, and how technologies should, or should not, leverage it.

Privacy Is Multilayered and Multidimensional

There is a wonderful line in an article by H. Jeff Smith et al. that says, "Privacy has been described as multidimensional, elastic, and dynamic in the sense that it varies with life experience."[3] This description accepts that social consensus around the concept of privacy

may be a moving target, continually evolving as time passes and contexts arise and dissipate. Most people understand some concept of privacy, but in reality, it means different things for different people, contexts, or situations.

We all enjoy drawing our curtains in the evening for a small bit of extra privacy in our living rooms or bedrooms, but do we all view privacy through the same lens when thinking about financial transactions, information storage, or how data is shared across the Internet? Do we ever wonder why there is no figurative curtain for Facebook? Do we question why there is no curtain to shield information from our banks about our week's monetary incomings and outgoings?

Remember, there is no single definition of privacy. It is a concept that straddles domains, cultures, contexts, and industries. It has been discussed within philosophy, sociology, law, computer science, and a host of social sciences for many years.[4] The fact remains that consensus has not been reached on exactly what privacy is. Privacy is viewed, by some, as a legal right; a right that agents should engage with, and one that must be protected by governments through legislation and regulatory bodies.

Economic theorists and practitioners view privacy as a commodity — explicitly related to the supply-and-demand-driven market for information. This view is especially pertinent in the 21st century, as data science and big data emerge as valuable sources of competitive advantage, and market value is built through insight extraction — a process where firms gather, store, analyze, and extract information from user-generated data. Privacy, in this context, relates to what is expected from users, customers, or firms when involved in location-based tracking, targeted ads, email scanning, Google search monitoring, and so on. Should user privacy be protected? If so, what is the cost? If not, what is the benefit? Who owns the data? Who should be able to monetize it, and who is responsible for protecting and/or securing it?

Privacy may also be understood solely as a cognitive concept — a state of being that an entity (living or not) is perceived to be, move through, or become. An example of this is the unambiguous "private property" declaration, which proposes a certain "existive" state on a piece of land, building, or object. A second cognate-based understanding is the perspective of "privacy as control," which attests that privacy is a mechanism through which agents assert or remove control from a situation, artifact, or person. An example of this perspective is a walled garden that remains private as long as the entrance gate remains locked. The person who controls the key controls access — ultimately asserting governance on the persons wanting to enter or exit.

Economic theorists and practitioners view privacy as a commodity — explicitly related to the supply-and-demand-driven market for information. This view is especially pertinent in the 21st century.

Blockchain Technology and Privacy

Understanding certain perspectives of privacy allows us to detail why it is important in the context of blockchain, distributed ledger, and smart contract technology. Thus, questioning the importance of privacy to anyone deploying the technology, using the technology, or regulating the technology, is important. How is a blockchain different than any database? How is it used differently than normal databases? What are the implications of deploying an immutable record of information in a distributed consensus network? How is the technology used in blockchains different from any other information or data storage technology? These are the questions firms should be asking as they attempt to understand the concept and its implications on an active, and evolving, basis.

At its heart, a blockchain is a data store. For the most part, access to this data storage is either open and transparent (i.e., permissionless blockchains) or controlled and monitored (i.e., permissioned blockchains). With permissioned blockchains, users must understand what levels of privacy they are agreeing, and adhering, to. They must understand what information is private or not private. They need to be made aware of what is being done with the information stored on the chain, who is accessing it, and for what purpose. Users may not be aware they are engaging in the market for privacy as a user, consumer, or customer — a source for valuable, marketable, and saleable information. They must be educated on the implications and accepted (or not) modes of interaction. They need to be explicitly made aware that information stored in the blockchain may be immutable,[5] destined to remain stored and accessible for the rest of time.

Users must be made aware that those who control access to the data store hold responsibility to users — whether they are individuals whose data is stored and secured on a ledger, firms that hold information on their user base, or regulators and legislators monitoring or accessing data for legislative or regulatory purposes. If groups have different perspectives of what privacy is, or is not, there may be tensions with respect to how stakeholders access, use, hold, share, secure, analyze, or transmit data. Users may be unaware that their information is being used in certain ways or accessed by a host of external agents, or unaware that one entity (the owners and controllers of the blockchain) may have veto of what is, and what is not, kept private.

We have seen how data analysis and sharing can lead to high-profile investigations and potential libel cases, as in the recent Facebook/Cambridge Analytica data privacy breach.[6] With the deployment of blockchain data stores, the potential for data breaches arguably increases as data is distributed across the globe and is designed by nature to be both accessible and transparent. Firms that store data using these technologies need to be cognizant of potential attack vectors and operational security requirements.

On the other hand, permissionless chains are usually open source, fully transparent, and accessible by anyone. Users must understand how to monitor, control, and engage with aspects of their own privacy. They need to ask whether they want, or even understand, that specific information may be linked directly to them and/or is traceable directly to them or to specific situations. Do users know how to protect certain aspects of their information as it is recorded to this immutable and traceable store of data? Do they know, or are they even aware, that any information stored on the blockchain may be used for any purpose, by any agent, as ledgers are open source and, by design, do not place rules, constraints, or regulations on those that wish to access them?

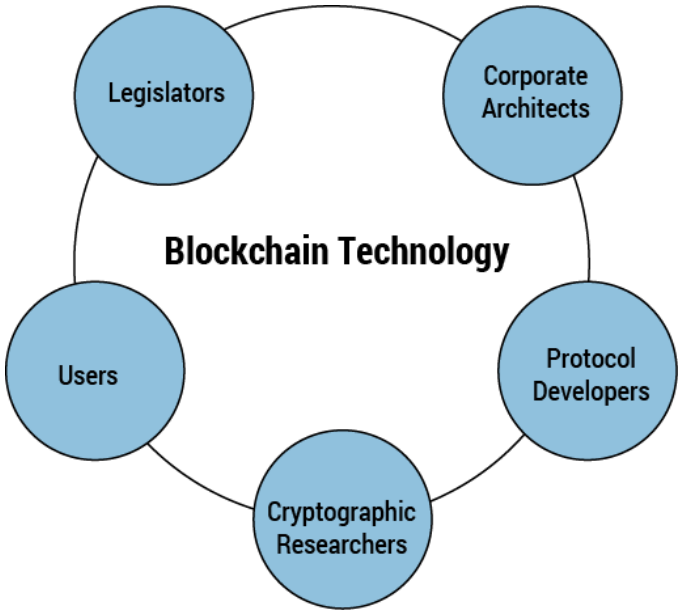

Figure 1 — Stakeholder groups within blockchain and distributed ledger technology.

Stakeholders in Blockchain Technology

The blockchain technology industry comprises many interacting and interrelated groups. There is no single justification as to why they are involved, and no single argument why privacy is of concern to them. Each group approaches the technology, and privacy, from a different perspective, and has differing motives driving their involvement. Figure 1 illustrates some of the key stakeholder groups.

Cryptographic Researchers

The first group is composed of cryptographic researchers. These are individuals who create the mathematically based algorithmic procedures on which a lot of the technology rests. A simple example of this would be the private/public key cryptography systems used in a host of blockchain technologies. It is essentially these researchers' job to ensure the cryptographic algorithms and processes are error-free, unbreakable, stress-tested, and resistant to attack from malefactors. We can liken their role to a lock and key maker. The cryptographers are the ones who ensure the lock and key mechanisms work as intended, and that the lock cannot be opened by anyone without a key, or by anyone with the incorrect key.

These individuals will have varying motives for working in the field and, more importantly, have varying perspectives of how algorithms should enact, afford, or even restrict, information privacy. They may feel that encryption should always be strong, resistant to any backdoor entry regardless, whether by malefactor or state agency, and that cryptography should be enacted as a protector of individual privacy and autonomy.[7] Alternatively, they may feel that cryptography should be monitored by government or state, and that these agents should be afforded avenues for breaking

encryption when personal, or national, security are at stake.

Protocol Developers

Protocol developers are individuals who integrate cryptographic algorithms into distinct blockchain, distributed ledger, or smart contract–based projects. A protocol developer may make decisions on which cryptographic methods are most suited (strong versus weak), the technological roadmap of the specific blockchain (how cryptography will evolve as technology and procedures evolve), and the overarching rules that govern the system. These decisions will be informed by a host of factors, of which understanding of privacy will be one. Returning to the example of the private garden earlier (one whose entrance and exit is controlled by an individual), the protocol developer is in charge of fitting the lock to the door and ensuring that it works as the intended control device for entry and exit.

Corporate Architects

Corporate architects are viewed as system designers in charge of permissioned blockchain technologies. They oversee choosing certain technologies and deploying them within firms, usually for specific contexts. They must ensure that specific information privacy policies are integrated into deployed technologies, and that the levels of enacted privacy are correct for the intended purpose. The architects are also in charge of ensuring the firm is compliant with any regulatory and legislative frameworks that exist. Returning to the metaphor of the curtain in a bedroom or living room, the corporate architect must decide how the curtain is fitted, what material to use, and whether the curtain adheres to legal requirements and legislative regulations.

Legislators

This brings us to the next stakeholder group: legislators. Essentially, this group has one of the most important roles in the multifaceted arrangement of social worlds and is arguably the group that has lagged the evolution of blockchain technology the most. Legislators define the legal and regulatory framework for privacy in the context of blockchain technology. They lay the legal framework for deciding what privacy is and what privacy isn't. They define what rights users have and what responsibilities firms have when dealing with user data or customer information. In essence, they decide the rules to which the walled garden owners and operators must adhere. They may set overarching rules concerning the degrees of control the key holder may assert, or overarching rules about who can enter or exit. The legislators are also in control of deciding whether people should have the right to a curtain, whether the curtain should always afford restricted visibility, or whether some regulatory or policing agent should have ultimate veto on whether the curtain can hide potentially illegal activity.

Sadly, the stakeholder group is now playing catchup, having failed to understand, adapt, or even realize the disruption blockchain technology will have on business processes further into the 21st century. Whether they understand the technology well enough to form able legislation is a valid question yet to be answered. Perhaps more worrying is the question of whether rule-making bodies can adapt quickly enough as the technology develops and evolves and as our understanding of privacy (especially in the context of it as a basic human right) morphs as society itself develops.

> *With the deployment of blockchain data stores, the potential for data breaches arguably increases as data is distributed across the globe and is designed by nature to be both accessible and transparent.*

Users

The final stakeholder group comprises the users. Arguably, this group contains the most diverse set of individuals, who interact with blockchain technology for myriad reasons. Understanding why and how users engage with the technology would be an extremely difficult task. What we can say with certainty is that they will engage with aspects of privacy, regardless of whether they realize it or not. Returning to our walled garden example, users may be able to enter and exit a private garden without realizing that someone is controlling or even monitoring their passage.

When discussing the figurative curtain of privacy, some users may feel they have a fundamental right to privacy in their living room, but are unsure of the rules surrounding it, whether they are free to draw the curtains whenever they please, or whether the legislative body has the right to ask them to draw back the

curtains if they are suspected of foul play or libelous action.

Users may have very different perspectives on the powers afforded to legislative bodies. An example of this may be seen with the recent Clarifying Lawful Overseas Use of Data Act (CLOUD Act) passed in the US Senate.[8] Some may feel they have nothing to hide, while others may feel that the right to privacy should outweigh a government's right to visibility.

Sweeping one-size-fits-all legislation is going to be extremely difficult to deploy — as blockchains can be used for a multitude of purposes and by a whole stratum of individuals and agents.

What Now?

Blockchain technology has emerged and evolved quickly, developing at a staggering pace since it emerged circa 2009. However, governments have failed to create an unambiguous stance on regulation and legislation. They now face a difficult task, as they need to regulate and legislate across the board, as the technology has proliferated into many industries, modes, and mediums. Sweeping one-size-fits-all legislation is going to be extremely difficult to deploy — as blockchains can be used for a multitude of purposes and by a whole stratum of individuals and agents.

Impending privacy legislation like the EU General Data Protection Regulation (GDPR) outlines modes of practice, process, and legislative concerns for firms, enterprises, states, and persons interacting with and storing data or information. Not understanding privacy from the context of the GDPR, or failing to interpret its definitions and legislations correctly into business process, may be extremely dangerous. Disjuncts between how privacy is understood by legislation such as the GDPR or by complementary and corresponding regulatory bodies, and how it is implemented at a technical, operational, or ideological level within specific instances of blockchain technology will have substantial impact on firms in the 21st century.

We are in an era where information is valued highly, while data privacy, security, and safety are foregrounded. There exists an ongoing battle between users' rights and commercial interests, a battle that needs to be moderated closely to avoid clashes that may cause upheaval and disruption in a wide range of industries.

Issues inevitably arise between stakeholders with differing ideologies. Groups may view aspects of privacy through the same lens, agreeing that all should have the right to curtains. However, imagine if they did not all agree on whether the curtains may be drawn continuously, regardless of activity behind the protective veil. Ideological differences must be managed carefully, as they may lead to legal liability. A user may feel he or she has the right to financial privacy and thus leverage blockchain technology to afford this — while the government may feel that such tools and technologies should not be allowed, as critical and potentially incriminating information can be obfuscated through cryptographic methods.

Another example may be user perception of how privacy is enacted within the blockchain. Users may feel that data is safe and secure as a firm interacts with them through a blockchain-based ledger, completely unaware of the fact that the blockchain is only pseudo-anonymous. Forensic techniques enacted by states, firms, or even individuals may reveal distinguishing, valuable, libelous, or even harmful information about use case, while users remain completely unaware of this privacy breach.

Why the Industry Needs a Spanner

The blockchain industry, as I have described, consists of a host of differing stakeholders, each with disparate motives, goals, motives, ideologies, and responsibilities. Aligning them is going to be a major concern for the industry. It will not be enough to formally state: "This is what privacy is." Indeed, privacy is known to mean different things in different contexts, different things to different people, and even to differ over time, morphing and evolving with society. Ultimately, privacy is a fluid and dynamic notion that informs both conceptual and physical artifacts — and this must not be forgotten.

There must be something, or someone, that "spans" disparate stakeholder groups, navigating tensions that arise as blockchain technology becomes a standardized (but evolving) mode of operation for peer-to-peer, peer-to-business, and business-to-business interactions. Stakeholders' opinions will need to be heard as legislation gets enacted and deployed. Users and firms will

need to be educated on what privacy is, what privacy is not, and how notions of privacy can interrelationally affect the spectrum of groups. No one stakeholder group is isolated in this issue.

One view may be that legislators cannot indoctrinate a single stance on privacy, or that protocol developers should not enact strong cryptographic tools, leveraging privacy and secrecy to the detriment of safety. Perhaps users cannot rationally expect information to be kept private while firms simultaneously seek to monetize insight extraction, or perhaps users should be included in the market for their information in a more transparent and fair fashion, with users ultimately being rewarded for foregoing aspects of their own information privacy. These are all valid concerns that jurisdictions need to navigate now — and on an ongoing basis.

There needs to be a distinct body that informs and educates stakeholder groups, acting as intermediary between them — negotiating aspects of privacy as, and when, they are encountered. This "spanner" needs to build bridges by understanding differences, navigating tensions, and smoothing disturbances. There must be a spanner in the works. This spanner will not create a clunking, clanking, heaving, sputtering, smoking mess — but will attempt to tighten up any loose nuts and bolts that threaten to bring the whole "revolutionary" machine to a grinding halt.

Endnotes

[1]For a detailed explanation of agent theory, see: Luck, Michael, Nathan Griffiths, and Mark d'Inverno. "From Agent Theory to Agent Construction: A Case Study." *Proceedings of the Third International Workshop on Agent Theories, Architectures, and Languages*, Springer-Verlag, 1997 (https://warwick.ac.uk/fac/sci/dcs/research/pcav/publications/pubs/from_agent_theory_to_agent_construction_-_a_case_study.pdf).

[2]For a more detailed analysis and perspective of divergent groups involved in cooperative design processes, see: Huvila, Isto, et al. "Boundary Objects in Information Science." *Journal of the Association for Information Science and Technology*, Vol. 68, No. 8, August 2017 (https://onlinelibrary.wiley.com/doi/pdf/10.1002/asi.23817).

[3]Smith, H. Jeff, Tamara Dinev, and Heng Xu. "Information Privacy Research: An Interdisciplinary Review." *MIS Quarterly*, Vol. 35, No. 4, December 2011 (https://misq.org/information-privacy-research-an-interdisciplinary-review.html).

[4]For an overview of privacy, see: Wacks, Raymond. *Privacy: A Very Short Introduction.* 2nd edition. Oxford University Press, 2015.

[5]Blockchains are viewed as immutable data stores. However, instances have occurred where immutability has been questioned, or where decisions have been made to alter the history of specific blockchains. For a more detailed discussion, see: Comben, Christina. "Are Blockchains Actually Immutable?" *The Merkle*, 7 April 2018 (https://themerkle.com/are-blockchains-actually-immutable/).

[6]Cadwalladr, Carole, and Emma Graham-Harrison. "Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach." *The Guardian*, 17 March 2018 (https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election).

[7]For an overview of cryptography, including a discussion of the difference between strong and weak cryptography, see: "Guide to Cryptography." Open Web Application Security Project (OWASP) (https://www.owasp.org/index.php/Guide_to_Cryptography).

[8]For a more detailed discussion of the implications of the CLOUD Act, see: "Coalition Letter on Cloud Act." ACLU (https://www.aclu.org/letter/coalition-letter-cloud-act).

Robin Renwick is a researcher with the University College Cork (UCC)/State Street Advanced Technology Centre. He is currently researching privacy in blockchain technology. Dr. Renwick earned a PhD from Queen's University Belfast, where his research focused on developing, designing, and analyzing specific topologies for network music. He can be reached at 117223923@umail.ucc.ie.

JUST YOU WAIT ...

Should You Use Smart Contracts?

by Steven Kursh, Arthur Schnure, and Natalia Gold

One of the major use cases for blockchain is smart contracts. Does it make sense for your organization to use smart contracts? In this article, we describe smart contracts, including a discussion of how they work and the possible benefits of using them. We also examine the downsides of their use and offer further considerations for the reader.

What Are Smart Contracts and How Do They Work?

So what are smart contracts? Imagine an agreement among multiple parties where certain, predetermined actions are agreed upon by the parties and executed per logic and when specific circumstances exist. There are many formal definitions as well. Back in the 1990s, cryptographer and legal scholar Nick Szabo described smart contracts as:

> A computerized transaction protocol that executes the terms of a contract. The general objectives of smart contract design are to satisfy common contractual conditions (such as payment terms, liens, confidentiality, and even enforcement), minimize exceptions both malicious and accidental, and minimize the need for trusted intermediaries.[1]

Szabo also stated that smart contracts enumerate "a set of promises, specified in digital form, including protocols within which the parties perform on the other promises."[2] His definition is certainly comprehensive, and for the purposes of this article we ask that you note the contractual provisions clause and how actions are enumerated. Of course, those of us who work with and implement electronic data interchange (EDI) as well as many enterprise software applications are generally familiar with other software that does some of what smart contracts do (i.e., use workflow rules to take specific actions previously agreed to among the parties).

An important distinction though: smart contracts work within the blockchain — a cryptographically protected distributed ledger. They use cryptocurrency as consideration for promises. Although Bitcoin — the first cryptocurrency app to use blockchain as its foundation — is the leading cryptocurrency app today, the leading app for building and using smart contracts is Ethereum and its cryptocurrency is Ether. There are also other cryptocurrency apps available that you can use with smart contracts.

Moreover, you may have heard about smart contracts under one or more other labels. Some companies and people who work with them use the term "computerized transaction protocols." Another frequently used label is "conditional transactions" since they feature conditional logic.

Both Bitcoin and Ethereum rely on the data storage and security foundation of blockchain. So, in effect, smart contracts use and benefit from blockchain to enable parties to have agreements that automatically execute specific, predetermined actions under predefined circumstances.

Bitcoin's software is hard-wired to do financial transactions, but Ethereum, in contrast, supplies an environment to host many kinds of application functionalities, ranging from games and gambling to smart contracts. Apps written for Ethereum contain multiple "if xxx, then yyy" statements, and these statements are triggered when users supply variables. A unit in Bitcoin is based on a single financial transaction, but a unit in Ethereum is an account. There are two types of Ethereum accounts: (1) externally owned accounts controlled by private keys and (2) smart contract accounts that can only be initiated by an externally owned account.

Figure 1 shows the main components comprising the Ethereum environment, with its structure approximating the familiar three-tier architecture of: (1) user interfaces, (2) middle-tier functional components with minimal user interfaces within the Ethereum Virtual Machine (EVM), and (3) account data storage and security in the blockchain.

The EVM middle tier, however, is dramatically different from conventional architectures, since the EVM "lives" on each node (or user) connected to the Ethereum network. Thus, every node has access to the same smart

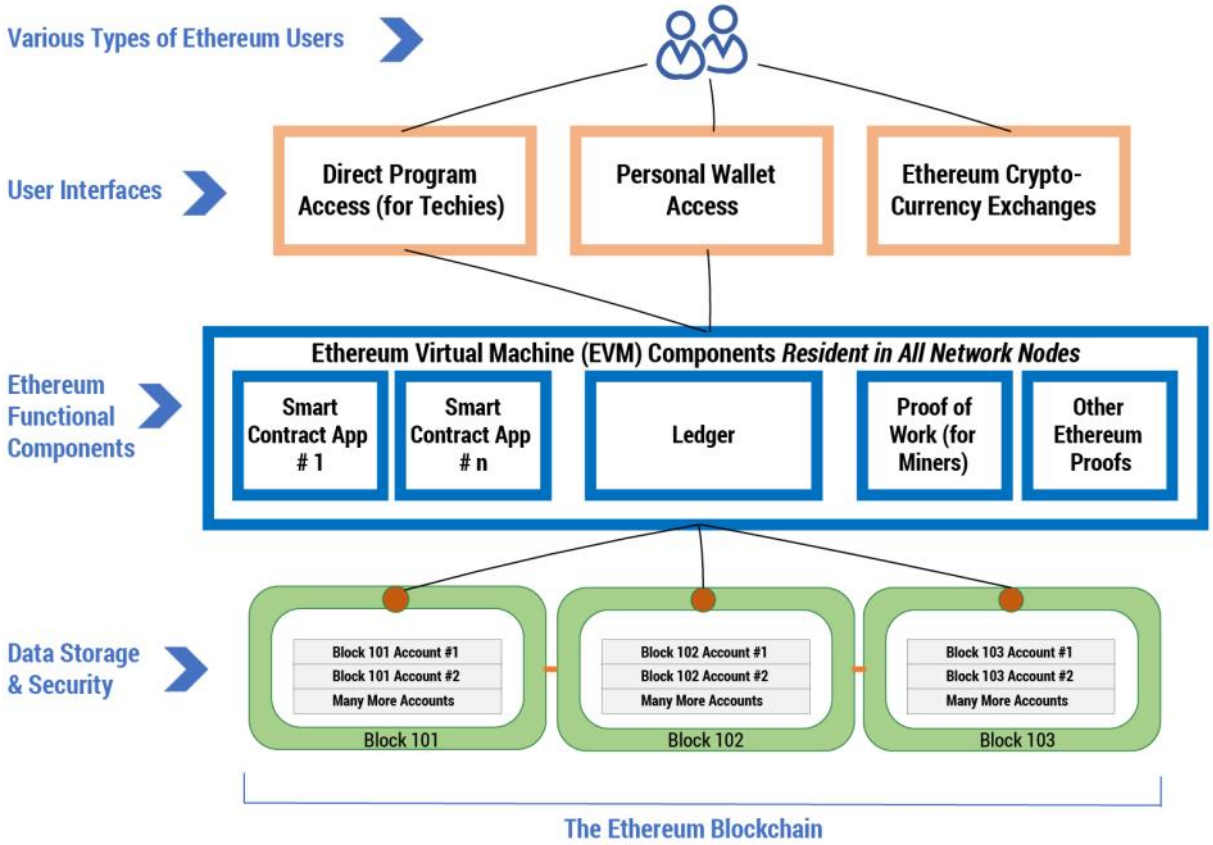

Figure 1 — The Ethereum environment.

contract apps and EVM software as seen by all other nodes on the network. The blockchain data itself is also downloaded to every node on the network.

At the top level of the Ethereum landscape, users are comprised of smart contract developers, smart contract users, and Ethereum blockchain miners. For the user interfaces located just below, programmers who develop smart contract apps can directly access the EVM with development tools to deploy apps to the production EVM. Hence, the environment lends itself to a broad array of applications, particularly smart contracts. Users can securely store the Ethereum cryptocurrency Ether in individual wallets via private keys. Wallets are available in software or hardware. So to implement and use smart contracts, users spend Ether — with Ether effectively being a means of exchange. Ethereum exchanges also store Ether and are quite different from wallets, allowing users to convert cryptocurrencies to other forms of money (including dollars), but they do not offer connections to the EVM.

The EVM middle tier is the runtime environment where Ethereum smart contract apps are deployed to all nodes (users) connected to the network. The process of creating a smart contact app is familiar to many of us. We begin with functional requirements and then move to coding, testing, compiling, testing again, and implementing on the EVM, with Ether expenditures required at certain points in the deployment cycle. Ledger software is at the center of the EVM, containing the required functionality to control the reads and writes of account data to the blockchain. Here we can draw from different ledger software options, some proprietary, others open source.

Finally, data is stored in blocks in the Ethereum blockchain whenever information or value changes for an account. The miners compete to organize the account transactions (written by smart contracts) into blocks, with the winner receiving Ether for their work. Ethereum miners solve complex calculations and, for their effort, can receive Ether for successful solutions. Whenever an account changes, its data is written to the blockchain, but the data is not available to other smart contract users until the entire block is written to a block. While miners race to solve the calculation puzzle, they're also verifying the accuracy of the data as it is entered into the blockchain. Thus, smart contracts are merely an application that uses blockchain.

To round out the financial picture, Ethereum also charges transaction fees to users of the smart contracts and app developers to provide funds to pay the miners.

The Appeal of Smart Contracts

In theory, smart contracts may provide several benefits. In our experience, we've found that the greatest benefit is the process of developing and implementing the framework for smart contracts within an organization. Like many efforts, getting processes in place for the use of automated tools may be difficult, but, ultimately rewarding once over and operational.

> *While smart contracts provide many benefits, they are neither easy to create nor facile to integrate within the blockchain, even for the technically adept.*

Advocates for smart contracts list multiple benefits, most of which are derived from blockchain. Consider first that smart contracts promise *autonomy*; anyone, without consulting with or engaging an attorney can create a contract. Hence, the process for reaching an agreement between parties could go faster and be more efficient than with legal counsel involved. (Of course, this raises several questions as well, including, but not limited to, not having the wisdom and experience of counsel to assist in reaching and executing an agreement. We discuss other related issues regarding the use of legal counsel later in this article.)

Another benefit of smart contracts is *trust*. Since documents are encrypted and stored on trustless public ledgers (TPLs), they offer parties a sense of "trust." A third benefit is consistent *backup*. Due to sharing on TPLs, documents have a multiplicity of immutable "backup[s]." A fourth benefit, while not airtight, is *safety*. TPLs are complex and well coded; furthermore, encryption of documents on the ledger ensures protections against hacking (but not total protection). This benefit is particularly relevant for agreements that are relatively simple and replicable over multiple transactions; by contrast, more complex agreements among parties follow well-established processes where counsel and corporations maintain detailed records and copies of agreements. Fifth, smart contracts offer parties *efficiency*. Instead of people manually processing documents, computers parse the code, eliminating lag and minimizing the risk of human errors. When the specified condition occurs, payment and other actions are automatic. Smart contracts can also bring *savings* from the efficiencies since parties can limit their costs, both through the elimination of middlemen lawyers in contract formation and by obviating the resort to court if there is a breach. Finally, smart contracts offer users *transparency*, which could be a double-edged sword. Dealings, including terms (which some companies may prefer not to be public) are out in the open where "everyone sees."[3] Transparency may not, however, be wanted with certain types of transactions.

Although many of these benefits are already available with other technologies, by combining these technologies with the use of smart contracts, your organization may gain additional value. But like all technologies, the challenges are determining what agreements to automate using smart contracts and, as noted above, the implementation process. There are also other realities that you need to consider.

The Reality of Current Smart Contracts

Simply put, while smart contracts provide many benefits, they are neither easy to create nor facile to integrate within the blockchain, even for the technically adept. Thus, even though a key benefit of smart contracts is autonomy and the ability to avoid middlemen, an industry of intermediaries has emerged to create templates for building smart contracts on the blockchain.

These templates are readily available for use by individuals and corporations, but like templates for some legal documents, there are many limitations to consider. On the plus side, vendors of such templates tout that organizations can accept smart contracts and cryptocurrencies easily. The downsides are that "easily" is a relative term, and in our experience the process of actually using a template is complicated and often constrained by the templates, reducing the alleged benefits of smart contracts.

One of the major constraints we've seen and hear about from clients is that developing and using smart contracts requires experts to modify or build templates. Those "experts" are presently difficult to find. A

talented developer would need expertise in blockchain, general business processes, and some general knowledge of the terms and related customs and practices involved among the parties for the specific smart contract. That individual would have multiple employment opportunities. Indeed, the challenge of finding such talent is a significant barrier to the development and use of smart contracts at many organizations. Ironically, we have found that some of the most active users and proponents of smart contracts are law firms. Some attorneys and staff at these law firms do have the technical expertise and general understanding of agreements relevant to their clients; hence, they can take a leading role in implementing smart contracts at their respective clients.

Here though, the so-called benefit of savings may be less than what some advocates suggest. More specifically, the salaries of developers may be higher than that for lawyers, and the fact that such developers are often difficult to find and keep as employees renders the savings benefit questionable. It's not just the financial cost, but the related cost in time searching for talent. By contrast, finding legal counsel is much faster and easier and given the present oversupply of lawyers, the financial cost may be much lower by simply working with legal counsel that has developed expertise in smart contracts.

Consider the case of Jincor, a platform that allows any business to work with smart contracts and cryptocurrency payments. Jincor claims that users will realize large savings using its templates because the platform will cut the cost of implementation from today's approximate "[US] $5,000-$7,000 — just have a look at blockchain developers' salaries and take into consideration that coding and proper security testing of a smart contract require many working hours of a qualified professional … to roughly $100-$500 per contract by removing the need to program them."[4] Unfortunately, the company does not have readily available data supporting its statements. And given that companies must hire qualified "technical" personnel who could, perhaps, be deployed in other activities that return more for the company, rather than lawyers, where there are many choices, the cost savings may be questionable.

Hence, a fundamental question arises: are smart contracts the best way to deploy your limited technical resources? Plus, consider the fact that your organization benefits from contract law, which has evolved over hundreds of years as society has evolved, too. To turn our backs on that history and on hundreds of years of collective thinking and reasoning and to substitute an automatic system where users lack recourses when issues arise may be foolish.

Modern institutions work well because they're built on centuries of accumulated knowledge. Decentralized blockchain applications are in their infancy, guided mainly by trial and error. A lot of money has poured into the technology, but just because something is technically feasible doesn't mean it's a good idea just yet.[5]

Turning to the benefit of safety, although, theoretically, smart contracts promise safety in practice, the blockchain and wallet apps for cryptocurrencies have, at best, a mixed record with hackers and theft. As one writer at *Bloomberg Businessweek* notes:

> After a string of high-value losses, participants still chose to entrust hundreds of millions of dollars to a vulnerable wallet app. It seems that the friendly interface and accessibility that made Ethereum popular can also lull users into a false sense of security.[6]

A lot of money has poured into blockchain technology, but just because something is technically feasible doesn't mean it's a good idea just yet.

In fact, many of us are well aware that hackers have exposed users' vulnerabilities.[7] Consider the following case: In November of last year, a person known by the pseudonym "DevOps199" stumbled across a critical vulnerability in the code for a subset of Ethereum wallets.[8] DevOps199 made itself the "owner" of this Ethereum code library, called a "smart contract," and destroyed it. This shouldn't have been possible, but DevOps199 nonetheless locked up roughly $150 million worth of other people's digital coins. Once DevOps199 exploited this weakness in the code, the rightful owners had no recourse. While the code on the blockchain can be hacked, it is otherwise immutable, and there is no recourse to a higher authority. What's worse, since activity on the blockchain is transparent, everyone can see as the code is hacked, but can do nothing to change the situation.

Conclusions and Thoughts for Action

We are actively involved in research and practice regarding blockchain and use cases such as smart contracts. At this time, however, despite the hype by advocates of smart contracts and, more broadly, blockchain, we strongly suggest you "watch and wait."

A conversation with counsel, whether in-house, or outside, may be helpful. Keep in mind, too, a hybrid approach: use smart contracts, but add an arbitration clause. The processes your organization has in place regarding contracts likely work well, and while smart contracts may potentially offer benefits, it will take time and numerous steps along the way until you need to focus resources to learning in detail about smart contracts and actively using them.

Endnotes

[1]Szabo, Nick. "Smart Contracts" (http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html).

[2]Szabo, Nick. "Smart Contracts Glossary" (http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_glossary.html).

[3]Rosic, Ameer. "Smart Contracts: The Blockchain Technology That Will Replace Lawyers." Blockgeeks, 2016 (https://blockgeeks.com/guides/smart-contracts/).

[4]Jincor Team. "Costs of Smart Contracts: Can Your Business Afford It?" Medium, 10 November 2017 (https://blog.jincor.com/costs-of-smart-contracts-can-your-business-afford-it-286e76b6355c).

[5]Ou, Elaine. "Smart Contracts Are Still Way Too Dumb." *Bloomberg Businessweek*, 16 November 2017 (https://www.bloomberg.com/view/articles/2017-11-16/smart-contracts-are-still-way-too-dumb).

[6]Ou (see 5).

[7]Pearson, Jordan. "Millions of Dollars in Ethereum Are Vulnerable to Hackers Right Now." Vice Motherboard, 22 February 2018 (https://motherboard.vice.com/en_us/article/8xddka/millions-of-dollars-in-ethereum-are-vulnerable-to-hackers-right-now-smart-contract-bugs).

[8]Pearson, Jordan. "Someone 'Accidentally' Locked Away $150M Worth of Other People's Ethereum Funds." Vice Motherboard, 7 November 2017 (https://motherboard.vice.com/en_us/article/ywbqmg/parity-multi-signature-wallet-vulnerability-300-million-hard-fork).

Steven Kursh is Executive Professor at the D'Amore-McKim School of Business, Northeastern University. His research and consulting focus on the development and execution of innovative technologies, including assessment of financial returns and other benefits. Dr. Kursh has extensive experience in software development, software project management, contract performance, intellectual property, and valuation. He is the author of Minding the Corporate Checkbook: A Manager's Guide for Executing Successful Business Investments *and several articles and cases. Dr. Kursh has received research funding from the GE Foundation, the Kauffman Foundation, and two federal government agencies. He earned a bachelor's degree from Boston College, magna cum laude, Scholar of the College, and a PhD from the University of Pennsylvania. He can be reached at s.Kursh@neu.edu.*

Arthur Schnure is an independent technical consultant focused on large Web-based apps for healthcare, health insurance, and cloud and non-cloud architecture and performance. Mr. Schnure's software startup background provides real-world, practical expertise needed to address the growing challenges in fintech applications. He can be reached at aschnure@gmail.com.

Natalia Gold is Assistant Teaching Professor at the D'Amore-McKim School of Business, Northeastern University, and Principal at GoldNest Partners, a consulting firm focused on strategy and technology. Dr. Gold earned a PhD in strategy and organizational behavior from St. Petersburg State University of Engineering and Economics. She can be reached at natalia.gold@live.com.

WHERE DOES OUR FOOD REALLY COME FROM?

Farm-to-Fork Transparency: Food Supply Chain Traceability

by Johannes Ahlmann

> Now, in the hyper-connected and ever-evolving world, transparency is the new power.
>
> — Benjamin Herzberg, World Bank Institute

> One of the trends we're seeing in food and agriculture is more and more consumers wanting to know things about their food and where and how it's grown and what's in it.
>
> — Dan Glickman, former US Secretary of Agriculture

Blockchain has the potential to transform and disrupt the food and retail industries. Giving access to real-time, auditable, trustworthy information on an immutable ledger about the origin, processing, and handling of food will change how consumers make purchasing decisions, level the playing field for high-quality products, and enable new possibilities in consumer, inventory, and supply chain analytics.

Food Producers Are Under Threat

Food producers are facing massive challenges from shifts in consumer behavior, regulatory pressure, brand damage from food safety incidents, and the difficulty of managing the ever-increasing complexity of the global food supply chain. Blockchain offers a possibility for food producers to gain better insight and control of their end-to-end supply chain (see Figure 1). Four key challenges in the food industry include:

1. Demand for more transparency
2. Increased regulatory pressure
3. Insight into food safety incidents
4. Prevention of food fraud

1. Demand for More Transparency

Consumer preferences are changing in both the developed and developing world, with the most rapid changes occurring in the developing and maturing markets of Asia, Africa, and South America. Consumers want to understand where their food comes from, what goes into it, and how it is produced. They are increasingly driven by new purchasing drivers, such as health, social impact, safety, purchasing experience, and an overarching demand for transparency.[1] Of consumers, 53% shop according to a specific diet.[2] A large percentage of consumers also study food labels and consult third-party sources on their first-time purchasing decision. Producer-independent, immutable information on a trusted ledger could provide much-needed product transparency.

2. Increased Regulatory Pressure

The speed and scope of food regulation is increasing as well, with an emphasis on food safety and food waste. Indeed, it has been predicted that regulatory developments in the food industry will closely mirror those of the highly regulated life sciences industry in the long term.[3] Already, the Food Safety Modernization Act (FSMA) in the US has introduced wide-ranging demands on the food industry to ensure food safety.

Figure 1 — Aspects of the supply chain of highest strategic importance to food producers.

End-to-end supply chain transparency could facilitate compliance and stakeholder management.

3. Insight into Food Safety Incidents

In an ever more complex global food supply chain, the potential impact of food safety incidents is growing. A significant portion of consumers will temporarily cease to buy a brand's product after a recall, leading to massive potential financial and market share losses. Particularly in emerging markets, food safety is becoming a significant purchasing driver. The ability to trace batches and shipments back to their source can increase food producers' ability to target recalls and offer real-time information to consumers.

4. Prevention of Food Fraud

Much of today's food producers' attention is on quality control at the production site to ensure food safety and quality standards of ingredients and the production process. With consumers putting increasing emphasis on the ethical, environmental, corporate social responsibility (CSR), and health-related properties of their food purchases, producers cannot rely solely on physical testing, but need to put in place additional safeguards and processes to prevent future recalls and brand damage on the grounds of ethical, environmental, CSR, religious, or health-related misrepresentation. A trusted ledger can track the provenance of a food product and help establish a chain of custody to combat food fraud.

The Food Industry Today

Today's food industry has little insight into its supply chain and, consequently, receives low consumer trust. Blockchain is an interesting new technology that can be used to establish process transparency across many disparate actors. Food supply chain information is currently held in "one-forward, one-back" silos, in which each company in the supply chain knows only its direct suppliers and customers, and data is often stored in ways that make it difficult to cross-check across companies. Tracing a food product back to all its sources requires significant time and manual effort, causing extensive lead times of days or weeks in discovering the source of ingredients in cases of food safety incidents.

In a complex and long supply chain (see Figure 2), with many semifinished and finished products as ingredients for further processing, there is often no clear "lead organization" held accountable and capable of collecting end-to-end supply chain information. In fact, even in simpler supply chains like container or parcel shipment, the administrative effort of tracking all stakeholders, the bill of lading, and handovers can at times exceed the cost of the actual physical shipment.

According to Kairos Future, "the food supply chain is the most complex and fragmented of all supply chains."[4] And just three years ago, McKinsey found that agriculture, as a central part of the food supply chain, "remains one of the world's least digitized industries."[5] This clearly poses a challenge and threat to the food industry, especially in the context of shifting consumer preferences and new regulation. End-to-end transparency is essential to combat various obstacles; blockchain is a strong candidate to facilitate and enable such transparency.

In terms of consumer trust, various recent reports reveal some interesting numbers:

- "75% of consumers do not trust the accuracy of food labels."[6]
- "Only 16% of consumers find food producers trustworthy."[7]
- "Consumers are 3.4 times more likely to harbor negative sentiments about food companies than a cross-industry average."[8]

Consumers' low trust in food producers and product labels suggest that a new, producer-independent

Figure 2 — A simplified visualization of the food supply chain.

mechanism is needed to convey substantiated product attributes in a trustworthy and auditable way. Such a mechanism would need to be producer-independent to regain consumer trust as well as being auditable and tamper-resistant, all of which apply quite well to a blockchain solution.

Is End-to-End Supply Chain Transparency the Solution?

If end-to-end supply chain transparency were feasible and viable, it would address most of the threats the food industry faces and would, moreover, enable additional use cases and benefits. Capturing information about supply chain transactions — the transfer of materials between any two parties — on a trusted, shared ledger would allow:

- Real-time farm-to-fork access for consumers to the provenance details of their food products
- A faster response to new regulation and legislation, by leveraging already existing supply chain data and workflows
- The provision of better brand protection by quicker, more proactive, and more precise handling of food safety incidents in terms of recall management, consumer information, and localizing of affected product batches
- The analysis of many attributes of the entire supply chain, allowing better consumer analytics, inventory analytics, logistics analytics, and so on
- More direct and unencumbered communication channels with all supply chain participants, leading to better stakeholder and supplier management

In the past, end-to-end supply chain transparency of a complex food product would have been very difficult to achieve except by producers with exceptionally high vertical integration. The challenge of access control, information security, and managing ever-changing supplier-customer relationships across dozens or even hundreds of participating companies would have been overwhelming.

With the advent of blockchain technology, the organizational roadblocks remain; however, the technology may offer a way for hundreds of companies without direct commercial relationships to interact on a shared, trusted ledger.

Supply Chains as Blockchain Use Case

There is currently massive hype and expectation around blockchain/distributed ledger technology, with blockchain often being touted as the silver-bullet solution for any conceivable problem. As Brock Pierce, then chief strategy officer of the fifth largest cryptocurrency by market cap, EOS, stated: "Everything that exists will no longer exist in the way that it does today! Everything in this world is about to get better!"[9]

At its core, a distributed ledger is just that: a ledger that is held by multiple parties, that is kept synchronized via consensus rules, and that stores transaction data in a tamper-resistant manner.

Surely, blockchain implementation won't immediately solve the world's problems. However, supply chains represent a use case that aligns well with the capabilities and tradeoffs of a distributed ledger, and this use case is already seeing early adoption across industries.

Many business use cases don't lend themselves to a blockchain solution. In some cases, it is far easier to use a traditional database, or to identify a mutually trusted third party to record transactions or to establish trust through legal contracts. Figure 3 outlines some requirements for a blockchain solution to be a viable option and can score the food supply chain according to the following six criteria:

1. **Need for a shared common database?** To provide transparency or insights into the food supply chain process and keep it for later use, it is necessary to maintain a stateful database of products, batches, shipments, handovers, or units.
2. **Multiple parties involved?** Food supply chains include dozens or even hundreds of logically distant participants.
3. **Parties involved have conflicting incentives and/or are not trusted?** Food supply chain participants are not fully known to each other and, as a result, there is no full mutual trust between parties. In many cases, there is no natural trusted third party that could oversee multiple levels of sourcing for several dozens of ingredients, logistics providers, customs processes, and so on.
4. **Need for an objective, immutable log?** Data in the food supply chain needs to be stored immutably for regulators, consumers, and other stakeholders to

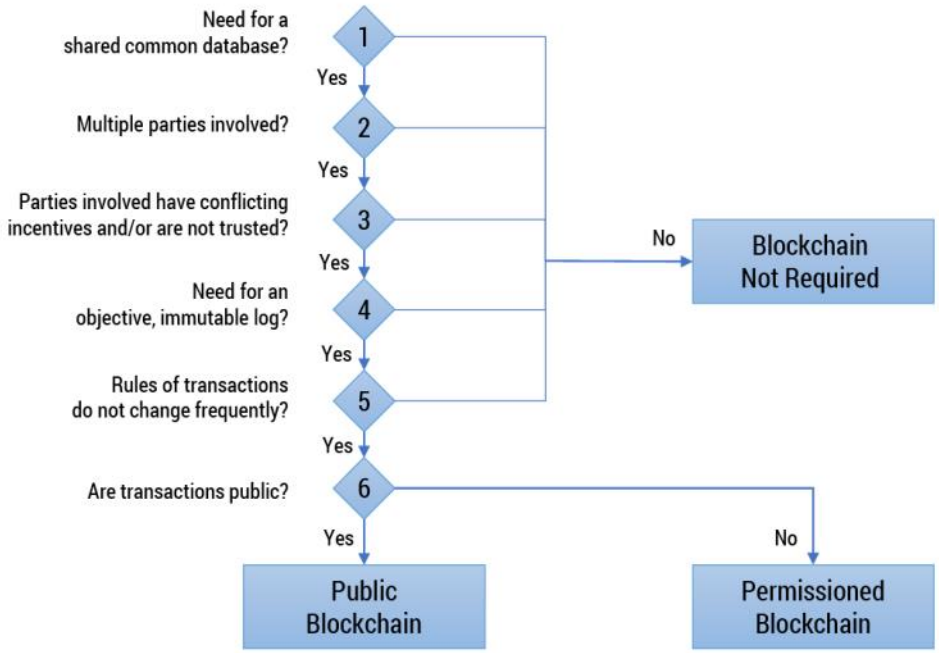

Figure 3 — Criteria for viability of blockchain for a business problem.

have the ability to audit the information and verify its accuracy and internal consistency.

5. **Rules of transactions do not change frequently?** Business logic for party-to-party transactions in a food supply chain is not overly complex and does not change too frequently.

6. **Are transactions public?** Commercial transactions in general are not fully public, leading to the need for a permissioned blockchain.

As illustrated, the food supply chain use case scores very strongly against the given criteria for a possible blockchain solution. Indeed, blockchain appears to be a viable solution to the challenge of capturing supply chain transactions between disparate and distant participants.

The Permissioned Blockchain

Many commercial supply chain use cases will choose a permissioned blockchain. Basically, all the cryptocurrencies discussed in the media and traded on exchanges (Bitcoin, Ethereum, etc.) are public blockchains, meaning that they allow anonymous participants to join, permit all participants to transact and view transaction details, and are censorship-resistant.

Many enterprise and commercial applications do not lend themselves to a public blockchain implementation for reasons of privacy, confidentiality, compliance with the new EU General Data Protection Regulation (GDPR), data governance, and scalability. For these reasons, many companies are exploring the use of *permissioned blockchains*, which restrict which participants can join the network and provide access control mechanisms. Cases where only a single company is part of a blockchain, or where there is perfect trust between participants, are often referred to as private blockchains. These have very little in common with public blockchains and are more akin to traditional databases.

Between public blockchains and private blockchains are several projects seeking to combine the benefits of public blockchains like Bitcoin with the confidentiality, governance, and compliance required for most commercial applications. These solutions are often referred to as "permissioned blockchains" or "consortium blockchains," and consist of a collection of multiple parties that do not fully trust each other and, therefore, have a need for a shared trusted ledger.

Table 1 compares the properties of public and consortium blockchains. As described above, there are several reasons for using permissioned or consortium blockchains in an enterprise context:

- **Confidentiality.** When transaction content cannot be shared publicly, or even with all blockchain participants, privacy and confidentiality controls are needed. To comply with GDPR, data access will need to be permissioned and mechanisms put in place

Public	Consortium
Data is public	Privacy, confidentiality
Transactions are public	Private channels
Pseudonymous	Known participants
Anyone can join	Permissioned
Anyone can access	Permissioned
Trustless nodes	Semi-trusted nodes
Storage unsolved	Storage on chain or integrated key value store
Low transactions/sec	High transactions/sec
No GDPR compliance	GDPR compliance possible

Table 1 — Public vs. consortium blockchain properties.

to be able to manage personally identifiable information (PII).

- **Access.** A public blockchain is open to anyone, both for joining the network and for seeing all transactions. A permissioned blockchain can allow access controls for joining the network and for accessing transactions and data.
- **Data storage.** Data storage is as yet an unsolved roadblock on public blockchains. One can either perpetually store immutable data "on-chain," which is extremely costly, or in other storage mechanisms, but without guarantees for data availability. Permissioned blockchains such as Hyperledger Fabric or Hyperledger Sawtooth provide in-built key-value stores for storage purposes.
- **Scalability.** Currently, scalability is a major obstacle for public blockchains due to their need for "proof of work" consensus mechanisms, with Bitcoin processing only five transactions per second. With consortium blockchains, other consensus algorithms, such as the practical byzantine fault tolerance algorithm, the proof of elapsed time algorithm, or the proof of authority algorithm can be used, achieving rates greater than 1,000 transactions per second.
- **Known parties.** Consortium blockchains can also leverage the fact that participants are known to members of the network and have been authenticated, avoiding the need for proof of work to prevent sybil attacks.[10]

The most common implementations of consortium blockchains include:

- Hyperledger Fabric
- Hyperledger Sawtooth
- JPMorgan Quorum
- R3 Corda

For the reasons stated above, I believe that many blockchain projects undertaken by existing companies in the coming years will use permissioned blockchains, both for compliance reasons and practical considerations, such as transaction costs, storage costs, data governance, and performance concerns.

Blockchain Use Cases and Pilots in the Food Industry

There are several pilot and exploratory projects using blockchain in the food industry, including many that show great promise. So far, however, there are very few, if any, production systems in place using blockchain technology. Here are some sample projects in the food industry:

- Walmart recently completed a pilot for traceability of mangoes using blockchain, reporting that it reduced the time to trace a package of mangoes from the farm to the store from several days to two seconds.[11]

- A group of leading retailers, including Nestlé, Walmart, Costco, Golden State Foods, McCormick, and Tyson Foods, are actively working with IBM to identify and prioritize blockchain use cases.[12]
- Outside the food supply chain, IBM and Maersk have implemented a cross-border supply chain solution on blockchain, showing promise in reducing administrative overhead for container shipment.[13]
- Claru (the author's company) has launched a pilot with sauce producer Rebel Chilli for a blockchain-based traceability solution.[14]
- Vietnamese TE-FOOD is migrating its at-scale solution for animal products in emerging markets to a public blockchain.[15]
- Walmart, Tsinghua University, and Chinese e-retailer JD.com have announced an alliance to enhance food tracking, traceability, and safety in China, achieving greater transparency across the food supply chain.[16]
- UK-based Provenance has completed a pilot tracking Indonesian tuna on the blockchain.[17]
- AgriDigital and Australian agribusiness company CBH have used blockchain technology to successfully execute grain contracts.[18]
- Cargill's brand Honeysuckle White has developed a blockchain-based pilot to trace turkey back to the farm.[19]
- Chinese fintech company ZonghAn Technology has developed a blockchain protocol in partnership with Chinese Internet of Things firm WoPu to track chicken provenance through the supply chain.[20]

Since blockchain technology is new and very novel in much of its technical aspects — and leaves many technical, legal, and organizational challenges yet to be resolved — most if not all the above projects are at the proof of concept stage or are, at most, pilot projects. Overall, blockchain platforms are still quite immature, are rapidly changing, and have yet to be proven in a commercial context.

Challenges Ahead for Blockchain Solutions

To adopt blockchain technology, companies must overcome several challenges and obstacles. Many of these challenges apply equally to the food supply chain and to blockchain projects in general, and many stem from the complexity of any distributed, decentralized system:

- **Distributed systems.** These systems are very complex; effective governance may well be one of the biggest obstacles for nonprivate, nonhierarchical ledgers.
- **Distributed identity and key management.** Both distributed identity and key management need to be solved for participants to exchange public keys and be able to authenticate transactions.
- **Human resources.** There are very few developers and systems architects with significant blockchain work experience, leading to slower adoption due to lack of talent.
- **Multiparty rollout.** One of blockchain's main benefits is the ability for multiple participants to interact without the need for a mutually agreed leader. This also makes the design, implementation, rollout, and governance of such systems much harder, since all participants need to mutually agree on governance and consensus rules.
- **Data privacy.** The new GDPR legislation poses a major challenge, particularly regarding data immutability versus the "right to be forgotten" of PII.
- **Physical-digital gap.** Overcoming the physical-digital gap poses an ongoing obstacle for any digital ledger. How closely can the ledger represent the physical reality, and how are the two kept synchronized in the face of errors, mishaps, and malicious actors?
- **Authentication.** Authenticating participants ("Is this participant who they say they are?") can be very difficult in situations where there is no physical relationship between participants and no organization that can vouch for participants.
- **Fragmentation.** With more and more companies looking into blockchain solutions, fragmentation will be a massive challenge, leading to an urgent need for blockchain standardization and interoperability.
- **Scaling.** Scaling blockchain can be another obstacle, depending on the level of trust between participants, the strategic importance of the ledger data, and the number of validating participants.

- **Risk-aversion.** The benefits of a blockchain project need to significantly exceed the cost, risk, and opportunity costs of its implementation for all participants. For this reason, vertically integrated industries, industries with strong market movers, and industries with few participants are likely to be the first to adopt blockchain.

Conclusion

Blockchain technology holds the promise to disintermediate existing business models, allow untrusting participants to agree on the "state of the world" in real time, and provide more auditability and accountability to supply chains that today are very siloed and opaque. As explored in this article, the food supply chain is certainly a prime example of such a supply chain.

Food supply chain management and transparency seems to be a fantastic use case for blockchain solutions and would allow consumer and supply chain participants real-time access to provenance information and supply chain transactions. Moreover, it will provide the ability to substantiate product claims to consumers, while allowing food producers much more control over potential threats.

Endnotes

[1]Ringquist, Jack, et al. "Capitalizing on the Shifting Consumer Food Value Equation." Deloitte, 2016 (https://www2.deloitte.com/content/dam/Deloitte/us/Documents/consumer-business/us-fmi-gma-report.pdf).

[2]"Driving Long-Term Trust and Loyalty Through Transparency." Label Insight, 2016 (https://www.labelinsight.com/hubfs/2016_Transparency_ROI_Study_Label_Insight.pdf).

[3]"What's on Your Plate?" Deloitte, April 2017 (https://www2.deloitte.com/content/dam/Deloitte/ch/Documents/consumer-business/ch-en-food-safety-POV-whats-on-your-plate.pdf).

[4]"Blockchain Use Cases for Food Traceability and Control." Kairos Future, 2017 (https://www.sklkommentus.se/globalassets/kommentus/bilder/publication-eng-blockchain-for-food-traceability-and-control-2017.pdf).

[5]Manyika, James, et al. "Digital America: A Tale of the Haves and Have-Mores." McKinsey Global Institute, December 2015 (https://www.mckinsey.com/industries/high-tech/our-insights/digital-america-a-tale-of-the-haves-and-have-mores).

[6]Label Insight (see 2).

[7]"Building Trust in What We Eat." FoodThink, 18 March 2013 (https://wehatesheep.com/foodthink/whitepaper/building-trust-eat/).

[8]Ringquist et al. (see 1).

[9]Matyszczyk, Chris. "John Oliver Can't Decide If Cryptocurrency Is a Good Thing." CNET, 12 March 2018 (https://www.cnet.com/news/john-oliver-undecided-if-cryptocurrency-is-a-good-thing-hbo/).

[10]A sybil attack is an attack on a consensus mechanism by injecting a large number of "fake" participants into a network to gain an artificial majority.

[11]Aitken, Roger. "IBM & Walmart Launching Blockchain Food Safety Alliance in China with Fortune 500's JD.com." *Forbes*, 14 December 2017 (https://www.forbes.com/sites/rogeraitken/2017/12/14/ibm-walmart-launching-blockchain-food-safety-alliance-in-china-with-fortune-500s-jd-com/#197f007a7d9c).

[12]Hackett, Robert. "Walmart and 9 Food Giants Team Up on IBM Blockchain Plans." *Fortune*, 22 August 2017 (http://fortune.com/2017/08/22/walmart-blockchain-ibm-food-nestle-unilever-tyson-dole).

[13]Moller, A.P. "Maersk and IBM to Form Joint Venture Applying Blockchain to Improve Global Trade and Digitize Supply Chains." Press release, IBM, 16 January 2018 (https://www-03.ibm.com/press/us/en/pressrelease/53602.wss).

[14]Claru (https://claru.io/).

[15]"Farm to Table Fresh Food Traceability for Emerging Markets." TE-FOOD (https://ico.tefoodint.com/).

[16]"Walmart, JD.com, IBM, and Tsinghua University Launch a Blockchain Food Safety Alliance in China." Press release, IBM, 14 December 2017 (https://www-03.ibm.com/press/us/en/pressrelease/53487.wss).

[17]"From Shore to Plate: Tracking Tuna on the Blockchain." Press release, Provenance, 15 July 2016 (https://www.provenance.org/tracking-tuna-on-the-blockchain).

[18]"Building a Blockchain for Agri-Supply Chains." AgriDigital, 2017 (https://www.agridigital.io/blockchain).

[19]"Honeysuckle White Brand Leads the Way in Food Transparency, Delivering a Farm-to-Table Thanksgiving Featuring First-Ever Traceable Turkeys." Press release, Cargill, 25 October 2017 (https://www.cargill.com/2017/honeysuckle-white-brand-leads-the-way-in-food-transparency).

[20]"Poverty Alleviation by Raising Chickens with ZonghAn Blockchain: Benefiting Thousands of Poor Counties Within the Next 3 Years." Press release, ZhonghAn, 31 August 2017 (https://www.zhongan.io/en/news/article).

Johannes Ahlmann is CTO for Claru, which is engaged with Irish and premium food producers to differentiate and substantiate premium product attributes to end consumers via blockchain traceability. Mr. Ahlmann's area of interest focuses on bringing blockchain and distributed ledger technologies to practical applications, particularly in the supply chain and food industry sectors. He holds a master's of science degree in computer science from Karlsruhe Institute of Technology, Germany, and is currently pursuing a master's of science degree in data business from University College Cork, Ireland. He can be reached at johannes.ahlmann@claru.io.

Privacy Regained: Is Blockstack the Template for a New Internet?

by Stephen Walsh

Blockchain protocols have the potential to facilitate a fundamental shift in the Internet business model from its current status, where the user is the *product*, to a future model, where the user is the *customer* and the user's data always remains in the user's control.

The blockchain paradigm enables this shift in business model because it keeps user-specific data encrypted and visible only to the user who holds a private key. For example, on the Bitcoin blockchain, owners of Bitcoin addresses are not explicitly identified, but all transactions on the blockchain are public. The mask of privacy provided by cryptography allows the service provider access to only the minimum information required for the provision of the service.

A second dynamic at play is the distributed nature of blockchain. Each participant in a blockchain provides resources to that network in accordance with the needs of that particular blockchain — be it computing, storage, security, funding for development, or maintenance services related to the blockchain. The design of blockchain protocols (to varying degrees) ensures that no single participant has outright control of the blockchain. As such, there is a new governance model in which the rights of users, developers, and miners are balanced and distributed.

Thus, blockchain enables the emergence of a "New Internet," in which users pay for access to limited resources by means of tokens that have monetary value. These tokens may be accumulated by founders and early-stage developers; they may be allocated to early adopters to incentivize a particular activity that helps grow the network; or they may be purchased during an initial coin offering (ICO) or on an ad hoc basis by users wishing to access services. Tokens may have differing functions at different phases of the network's development, but generally are designed to provide appropriate incentives to the parties to the network: entrepreneurs, developers, users, and miners.

In 2017, we saw an explosion of activity in the blockchain community — and, notably, we've seen a new model for bootstrapping startups come to the fore. ICO is a new route to market for startups, allowing them to bypass the venture capital circuit using tokens and their public sale. This model was first discussed in blockchain/academic circles in mid-2016, so most people were taken by surprise when it became the highest-profile means for startups to raise funds in 2017. Over the course of 2017, ICOs raised almost US $5 billion in funds for startups in what became a frenzied market rivaling the dot-com boom of the late 1990s.[1]

It is remarkable that the nine-page white paper that set out the rules for Bitcoin and thus created the first blockchain could so radically change business, technology, and governance paradigms.

A new era — and a New Internet — underpinned by blockchain technology is within sight, where:

- Users can access vital Internet services without compromising their personal privacy.
- Startups can bootstrap the early phases of an enterprise without having to bow before venture capitalists.
- The rewards for successful innovation are distributed to the participants.
- The network is a shared resource developed in line with the needs of the users, developers, and miners.

Why Do We Need a New Internet?

The problem with the current Internet is that it requires the most successful tech firms to store massive volumes of personal data on centralized databases in the cloud. Much of this data is repackaged for sale to advertisers. Governments have the capability to monitor entire populations via backdoor servers in cloud data centers. Hackers exploit security weaknesses, enter illegally, and pillage the data, making it available to unknown players who monetize it in nefarious ways.

As long as the Internet maintains this "data honeypot" design, it is inevitable that both privacy issues and personal data breaches will become more frequent and more severe. The scale and frequency of data breaches already are increasing to the point where the current Internet is no longer fit for purpose, secure, or reliable.

All this raises the question: what exactly should the New Internet be?

Let's first consider the evolution of the Internet:

- **Web 1.0** — distributed, static
- **Web 2.0** — centralized, dynamic, social, insecure
- **Web 3.0** — distributed, dynamic, social, secure

Basically, Web 3.0/New Internet should provide all the benefits of the existing Internet but be secure, private, and safe for all to use. How can this be achieved?

Can Blockchain Technologies Underpin a New Internet?

What we learned from Bitcoin's Satoshi Nakamoto is that a great idea, articulated in a succinct white paper, can catch the imagination of innovators and those who desire change. While Bitcoin's reputation is extremely mixed, a grudging respect for the underlying blockchain has emerged, as people have realized the potential there is in crossing a database with a network to resolve some of the most fraught problems relating to Web 2.0.

In 2017, a new generation of blockchain visionaries emerged. In my opinion, the most prescient of these are the founders of Blockstack, Muneeb Ali and Ryan Shea, whose white paper set out in stunning detail the architecture of a New Internet that meets the criteria for the Web 3.0 presented above (see Figure 1).[2]

The five key elements of the New Internet described by Ali et al. include the following:

1. **Decentralized identity system.** This allows individuals and legal entities to purchase a single username that permits them to access every service in the Blockstack ecosystem.

2. **Decentralized domain name system (DNS).** Recognizing the trust deficit that users of Web 2.0 have to place in navigating the Web via DNS, Blockstack has invented a blockchain naming system (BNS). Once an address is validated on the network, it is formed into a block and available in a universal directory distributed to each BNS node on the network.

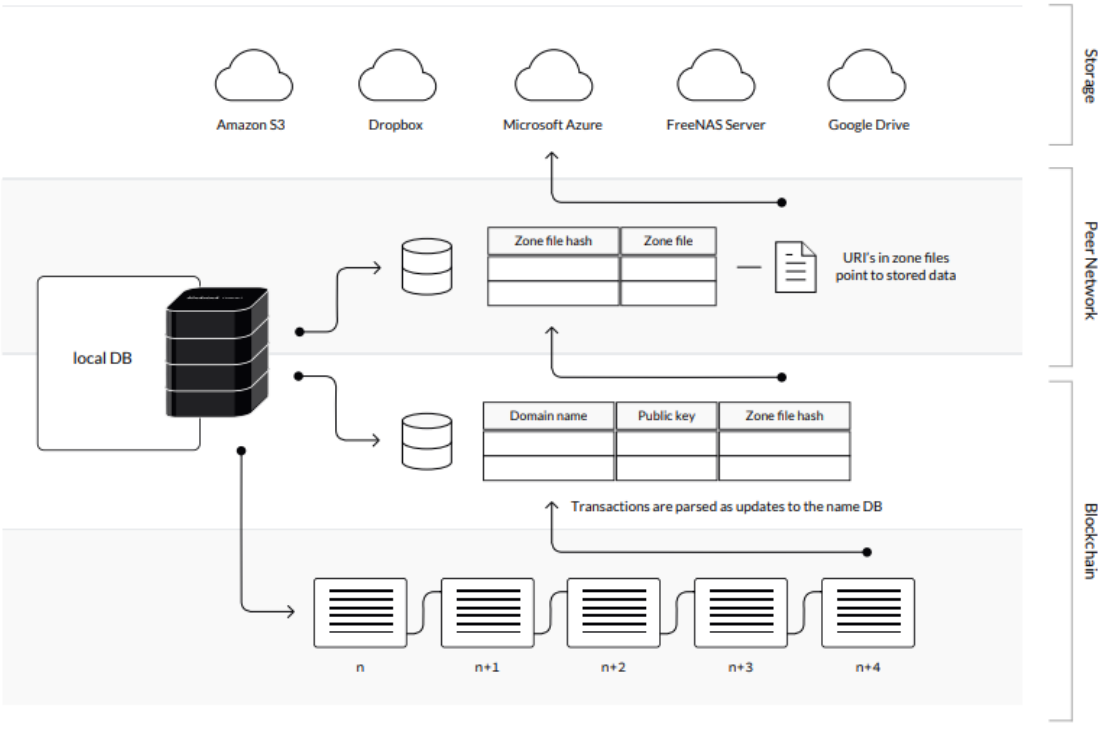

Figure 1 — Blockstack architecture. (Source: Blockstack.)

3. **Decentralized storage network.** The blockchain protocol enables users to leverage existing storage infrastructure on the Internet (e.g., AWS, Google Drive, Dropbox) by using keys to encrypt and store data, which are available only to the rightful owner. This provides scalability while preventing third parties from accessing/manipulating that data as part of the service. The data is encrypted, so the service provider cannot monetize it in any form apart from the simple provision of the storage itself. Should an unauthorized third party gain access to the storage, it is of no use to them, as the data remains encrypted at rest.

4. **Decentralized app platform.** The great success of the dominant players of Web 2.0 has been their ability to excite and mobilize the developer community to build apps on their platforms and to utilize their application programmer interfaces (APIs). Blockstack sets out to provide the ultimate environment for app developers to create next-generation blockchain apps using Blockstack. In addition to providing the platform and tools for app developers, Blockstack is dedicating 30% of the $55 million (Ethereum equivalent) funds raised in its 2017 ICO to incentivize developers to create apps on Blockstack.

5. **Blockchain Web browser.** Users install an app on their computers that enables their Web browser to access all apps and services that exist on the Blockstack platform via a single private key. In effect, this creates a "parallel universe" of a New Internet run by a new set of Internet protocols. For example, navigation is done via block name servers rather than the domain name servers used in Web 1.0 and 2.0. The trouble is that, as of today, there is not that much content in this New Internet. So this may be where lawmakers and regulators need to step in to ensure Web 3.0 has the opportunity to gain critical mass, preventing it from being choked to death by the masters of Web 2.0.

Interoperability between Web 3.0 and Web 2.0 may prove to be an important stepping stone for the success of the New Internet. Blockstack's view on this interoperability is that while it is technically feasible, the incentive models between the two are radically different, and this may be the cause of some friction as people try to migrate to the New Internet. According to Blockstack's Xan Ditkoff, "When you use an application on today's Internet, all of your data — social graphs, photos, messages, and documents — are locked up in their servers, and they use that to build algorithms and target ads at you. The data ownership baked into the Web 3.0 model allows for censorship resistance and true data portability, so people can transfer all of their digital information from app to app."[3]

It would seem likely given the tradeoffs between better personal data control and the need for connectivity with contacts and existing Internet assets that a hybrid Web 2.5 may emerge. It could act as a transition phase for those wishing to get control of their data, while maintaining the existing value of the Internet.

3 Obstacles Facing the New Internet

1. High Switching Costs for Users

Anyone who has spent several years cultivating their profile and social group on a social network knows that the switching costs of moving to another social network are daunting. During the recent #deletefacebook campaign, many people were disturbed by Facebook's lack of respect for privacy. Despite this frustration, many people feel that if they move away from Facebook, they will no longer have the same and easy access to their family and friends that they currently enjoy.

Nonetheless, some 1.1 million social media enthusiasts have taken the leap and set up camp with Mastodon — "the world's largest free, open source, decentralized microblogging network," according to its website.[4] Mastodon's design ensures that individuals have control over their personal data and are not subject to corporate manipulation. Refreshing as this sounds, users who abandon Facebook are cut off from the more than 2 billion strong Facebook community and, at least for the time being, Mastodon is not really a good substitute for Facebook.

2. Metcalfe's Law and Critical Mass

Metcalfe's law states that the effect of a telecommunications network is proportional to the square of the number of connected users of the system (n2).[5] Likewise, in social networks, the greater the number of users with the service, the more valuable the service becomes to the community.

The utility of a small social network is extremely limited for each new user, as they are entering a domain where most of their peers are not present. There is very little

incentive for individuals to join an obscure social network where they might find very few or none of their peers.

The possibility of an alternative, general-purpose social network accessible to all is simply not possible as the Internet is currently configured. If Tim Berners-Lee, the inventor of the World Wide Web, had included a protocol for mapping our social identity in his original specs, we might not have Facebook.[6]

3. Outside the Walled Gardens

In the years since the mid-2000s, we have seen a growth in the established social networks' use of the "walled garden" model. Users are no longer operating in the open Internet, but rather are accessible only to other members of the same social network.

The gatekeepers to these walled gardens are APIs, which define to third parties the scope, extent, and cost of interaction with these networks. These APIs have been designed to maximize the commercial value of the networks to the network owners, rather than for the benefit of the users.

The APIs to Facebook, Twitter, and Instagram are ideal for marketers seeking to hone advertising campaigns based on user data. They provide almost no scope for social network interoperability, thus maintaining the status quo of the dominant networks and choking off any innovation outside the narrow scope defined by their own commercial interests.

Government Intervention for a New Internet, Pronto!

Creating the conditions for a secure, reliable, and open Internet available to all will require a series of policy interventions on the part of lawmakers in the US, EU, and elsewhere, including:

- **Regulation of ICOs and cryptocurrencies to make investment-raising models safe for investors.** The great Bitcoin bubble of 2017 and unregulated investment in ICOs have tainted blockchain technologies and created unacceptable risks for investors. Governments must ensure that appropriate regulation is put in place for cryptocurrencies, ICOs, and fintechs in the blockchain space. This would facilitate more mainstream participation in the sector, bring greater legal certainty, and create appropriate legal sanctions for criminal activity relating to ICOs and cryptocurrencies.

- **Government adoption of blockchain-based identity initiatives.** As demonstrated by the Blockstack white paper, blockchain offers an excellent use case for validation of individuals' identities. Governments should leverage blockchain technology to issue unique IDs to enable citizens to access public services.

- **Use of antitrust laws to break Facebook, Amazon, and Google into their constituent parts.** At a recent US Senate hearing, Facebook CEO Mark Zuckerberg struggled to name a single competitor,[7] and, according to the *Financial Times*, many senior US politicians would favor a breakup of Facebook.[8] By most definitions, Facebook is controlling a monopoly, or, at the very least, is abusing a dominant position in a number of markets. The tech sector should be held to the same standards as companies operating in other industries and placed under the active scrutiny of antitrust laws in both the US and Europe. Likewise, regulators must prevent further consolidation of messaging apps and social networks in the future by refusing to sanction further acquisitions by dominant players in the market.

- **The US adoption of the EU's General Data Protection Regulation (GDPR).** The EU provides leadership in consumer data protection through GDPR, which places onerous responsibilities on data processors by requiring explicit permission from users regarding the processing of their personal data.

  The stinging financial penalties set out by GDPR prompted LinkedIn and Facebook to tweak their terms and conditions, shifting responsibility for all users outside the US, Canada, and the EU from its international headquarters in Ireland to the US.[9] US companies operating in the EU should operate under the laws of the EU, and the US government should consider adopting tougher data protection laws similar to GDPR.

Blockchain Apps and Platforms to Watch

Let's look at a few decentralized platforms, protocols, and apps of interest. The first of these, of course, is Blockstack and two apps that live on that platform (Graphite, Stealthy). Overall, Blockstack's white paper

is striking in how it applies a clarity of thought to the design of a New Internet with a radically different approach to identity, navigation, and data storage. Next, we have dock.io, a working example of how users can extract their data to an encrypted hub, and then leverage that to access different cloud services. Finally, we examine Mastodon, the open source microblogging platform. The Mastodon model may provide a template for a future where social networking is decentralized and personal data is controlled by the user.

Significant barriers to moving to a safer New Internet exist, since the winners of Web 2.0 have accumulated vast wealth, power, and personal data, which they can use to protect their profitable business models.

Blockstack

Blockstack has taken the identity-first approach. Its designs implement services for identity, discovery, and storage that remove any centralized trust points and rely on blockchains for key data bindings. Its protocol defines a New Internet that exists as a parallel universe to the existing Internet. Blockstack provides a platform upon which privacy-enhanced products and services can be based and is readily available to enterprises, developers, and governments.

Its architecture is designed for single-identity per user, scalability, and interoperability between different blockchains. These attributes may make it a good bet for corporations or banks wishing to maintain their position within the "know your customer" and trust infrastructure.

After 25 May of this year, when GDPR goes into effect in EU countries, Blockstack may have a particular appeal to app developers who need to ensure privacy by design. Ditkoff, who's responsible for growth at Blockstack, asserts, "While Blockstack wouldn't be a cure-all for GDPR compliance (a data officer would still need to be hired, for instance), it would drastically reduce the regulatory burden to a business operating under that framework."[10]

Blockstack recognizes the need for users to experience an aha moment, as Facebook users did 12 years ago, when Facebook made every effort to ensure that each new user would find at least 10 friends within their first seven days on the app. It worked then, and aha moments are still needed today for apps to succeed with a wide global audience.

Graphite and Stealthy: Decentralized Apps Built on Blockstack

Graphite is a decentralized set of apps with functionality similar to Google's G Suite,[11] and Stealthy is a fully decentralized P2P chat app.[12] These tools offer the basic functionality of an online word processor and a messaging app. Blockstack founder Ali notes, "We're going back to the world where it's like the old-school Microsoft Word — where your interactions are yours, they're local, and nobody's tracking them."[13]

The main issue for most users will be their ability to migrate to these apps. First, users must install Blockstack on their computer and register an ID (which may take a fair bit of effort, even for those who are reasonably tech savvy). The next issue is the lack of integration with users' legacy Web 2.0 assets; for example, network of contacts, content on G Suite, and social history. Finally, users looking to interact with colleagues, friends, and family may find the lack of interoperability with Web 2.0 messaging and social apps means that the utility of this next generation of apps is limited due to a low number of users and the resulting lack of value.

dock.io

dock.io connects user profiles, reputations, and networks into one sharable source using blockchain technology.[14] It has streamlined the process of extracting users' personal data from LinkedIn and Google and storing it on an encrypted-distributed database. The dock.io app creates a fully-fledged professional profile using the data input from LinkedIn.

The app may appeal to people on a few levels. First, due to the Facebook/Cambridge Analytica scandal, people have become more aware of the value of their personal data and wish to be in better control of it. dock.io apparently ticks that box. Users can export their data from Google and LinkedIn and store it using the dock.io protocol. The data can then be used to socially bootstrap other applications, such as networking apps, job marketplaces, and HR management systems. To date, dock.io is in the alpha stage of development, and integration with third-party apps is limited to almost none. The app is clearly at an early stage of its

development and requires extensive investment in the product, partnerships, and community.

Mastodon

Mastodon claims to be the world's largest free, open source, decentralized microblogging network with circa 1.1 million active users as of April 2018.[15] The network provides an open source instance as a starting point for community organizers. Each community can have its own rules, interests, members, and branding. According to its founder, Eugen Rochko, "As a decentralized alternative to commercial platforms, it avoids the risks of a single company monopolizing your communication."[16]

The Mastodon model has been touted as a possible replacement for Twitter.[17] Whether Mastodon indeed reaches its full potential as an alternative model for social networks, it will be interesting to see if this model is viable. Detractors of Mastodon have pointed to its convoluted naming convention for users as a critical weakness. Were Mastodon to outsource the identity question to Blockstack's identity protocol, the overall viability of it might be improved, as each user globally would have a single secure identity.

Conclusion

The recent Cambridge Analytica/Facebook scandal has raised the consciousness of data privacy issues for Internet users everywhere. It may even have provoked Internet users to consider how they might enhance their privacy in practical ways. The key question now is this: how can we move to a New Internet that offers the benefits of the existing model, but is safe and secure for all users?

Significant barriers to moving to a safer New Internet exist, since the winners of Web 2.0 have accumulated vast wealth, power, and personal data, which they can use to protect their profitable business models. Regulators need to use existing antitrust and privacy laws to disrupt the monopolistic behavior of players such as Google, Facebook, Twitter, and Amazon.

There are encouraging signs that blockchain technology may be able to deliver on the promise of a secure and private Internet for all, but it is clear that it is still in the early stages of development. There are significant engineering and design challenges for the blockchain sector that remain to be overcome. As the scale and frequency of data breaches in Web 2.0 escalate in the coming years, interest in blockchain will clearly rise, too.

Endnotes

[1]Mullin, John Patrick. "ICOs in 2017: From Two Geeks and a Whitepaper to Professional Fundraising Machines." *Forbes*, 18 December 2017 (www.forbes.com/sites/outofasia/2017/12/18/icos-in-2017-from-two-geeks-and-a-whitepaper-to-professional-fundraising-machines/#54e6dec9139).

[2]Ali, Muneeb, et al. "Blockstack: A New Internet for Decentralized Applications." Blockstack Technical Whitepaper, 12 October 2017 (https://blockstack.org/whitepaper.pdf).

[3]Xan Ditkoff, conversation with author.

[4]Mastodon (https://joinmastodon.org).

[5]Metcalfe's law (https://en.wikipedia.org/wiki/Metcalfe%27s_law).

[6]Johnson, Steven. "Beyond the Bitcoin Bubble." *The New York Times Magazine*, 16 January 2018 (https://www.nytimes.com/2018/01/16/magazine/beyond-the-bitcoin-bubble.html).

[7]Jeong, Sarah. "Zuckerberg Struggles to Name a Single Facebook Competitor." *The Verge*, 10 April 2018 (https://www.theverge.com/2018/4/10/17220934/facebook-monopoly-competitor-mark-zuckerberg-senate-hearing-lindsey-graham).

[8]Luce, Edward. "Donald Trump's War on Jeff Bezos Is More Than Just Bluster." *Financial Times*, 4 April 2018 (https://www.ft.com/content/fe829992-372c-11e8-8b98-2f31af407cc8).

[9]Hern, Alex. "Facebook Moves 1.5bn Users Out of Reach of New European Privacy Law." *The Guardian*, 19 April 2018 (https://www.theguardian.com/technology/2018/apr/19/facebook-moves-15bn-users-out-of-reach-of-new-european-privacy-law).

[10]Xan Ditkoff, conversation with author.

[11]Graphite (https://www.graphitedocs.com).

[12]Stealthy (https://www.stealthy.im/).

[13]Fung, Brian. "The New Technology That Aspires to #DeleteFacebook for Good." *The Washington Post*, 23 March 2018 (https://www.washingtonpost.com/news/the-switch/wp/2018/03/23/the-new-technology-that-aspires-to-deletefacebook-for-good/).

[14]dock.io (https://dock.io).

[15]Mastodon (https://mastodon.social/about).

[16]Burgess, Matt. "Could Mastodon Be the Social Network to Replace Twitter?" *Wired*, 5 April 2017 (http://www.wired.co.uk/article/mastodon-social-network-what-how-create-account).

[17]Burgess (see 16).

Stephen Walsh is a technology entrepreneur from Ireland. He is CEO of Keeper Solutions, a software services firm that provides outsourced development services to clients in the UK, US, and Ireland. Mr. Walsh's background is in banking systems, software services, and outsourcing, and he has played key roles in Misys, Perot Systems, and Dell. He can be reached at stephen@keepersolutions or on Twitter @keepersolutions.

BEYOND THE STATUS QUO

Toward Ecosystems: How Blockchain Disrupts the Business Model

by Karolina Marzantowicz and Maciej Jędrzejczyk

2018 is a defining year for the commercial adoption of blockchain. Initiatives in various industries have reached a maturity threshold, marked by a transition of focus from experimental proof of concept projects toward production use. A breakthrough is visible at all levels. Indeed, the size of the blockchain technology market worldwide jumped from US $210 million in 2016 to $548 million in 2018 and is projected to reach $2,312 million within the next three years.[1] Moreover, it is estimated that 66% of organizations that have implemented blockchain initiatives are now experimenting with more integrated business models that connect people, resources, and organizations in a distributed value chain.[2]

The Internet and digitalization are slowly modifying established business models and the way companies do business.

Ecosystems: From Competition to "Co-opetition"

Technology advances fast. Globalization increases. It is in these conditions that market participants evolve and adapt to change. While technology is now absorbed as an integral part of a business model, the foundations upon which companies are built have not changed much. One of the contributing factors to this situation is that the Internet, which now serves as a backbone of modern markets, was not built with security in mind. Thus, the need to preserve trust in business dealings has persisted and, as a result, the need for established trusted third parties has continued uninterrupted.

However, the Internet and digitalization are slowly modifying established business models and the way companies do business. The modus operandi for such evolution takes the form of integration into a network of interrelated parties around centers of gravity, with trusted (or dominant) decision makers (governors) placed in the center with their subsidiaries (or less powerful counterparties) orbiting around them. In practice, relationships between different centers of gravity have not changed all that much — the different centers remain competitive in nature and interact with each other only through trusted third parties. However, the lowered costs provided by digitization have allowed for more integrated networks, or ecosystems, to flourish and slowly disrupt the traditional relationships.

Ecosystems — integrated networks focusing on the production of goods or services, thus generating value to customers — can be compared to a network of interlinked companies and other participants that interact with each other. Participants in an ecosystem can compete or collaborate to grow sales, revenue, and profit, or toward other goals. The main differentiator between an ecosystem and a network is that an ecosystem usually includes the entire value chain (i.e., suppliers, producers, partners, competitors, and stakeholders). A new wave of digital revolution, however, is integrating end users or final customers into the ecosystem, too.

In an ecosystem, parties previously unrelated to each other or even in direct competition must overcome difficulties to access the low-hanging fruits the newly created value chain provides. Although modern digital ecosystems have been with us for a while, they were often focused around a single dominant player, surrounded by accountable subsidiaries or consumers. Some notable examples of dominant players with integrated ecosystems are Amazon, Google, and Facebook. The difference brought by blockchain is that decentralized consensus mechanisms now make it possible to achieve similar business results while preserving a relationship between participants based on equitable rights enforced by decentralized governance. In other words, modern cryptography saves us

the time normally needed to develop trust in each other in the absence of a trusted third party.

Moreover, blockchain helps in driving new collaborations among participants within an ecosystem to address rising social and environmental challenges. This technology helps lower operational costs due to a higher level of digitalization and automation of business-to-business (B2B) processes. As a result, it allows ecosystem members to reach new partners, customers, and markets through blockchain platforms. With the arrival of private blockchain platforms that integrate nonfunctional requirements arising from typical market conditions (i.e., privacy, confidentiality, controlled access), the barriers to creation of a digital economy become less significant and easier to overcome.

Why Blockchain Makes a Difference for Ecosystems

The intrinsic value residing in blockchain can only be unleashed if more than one participant uses it to execute or take part in a multiparty business process. In the past, a multiparty business process typically required a trusted third party to govern the process execution. By design, such processes require not only continuous checks and balances from counterparties but also a guarantee of privacy and confidentiality whenever executing sensitive business elements of the process. In more complex situations, this model meant that parties resorted to a paper trail to avoid revealing too much about their secrets to an unwanted audience. Blockchain's cryptographic capabilities, however, can be applied directly to the business process, via the distributed ledger and data flow, obviating the need for third parties and ensuring privacy and confidentiality. Consequently, almost end-to-end business process automation between external parties can be achieved across the value chain. This automation eliminates some intermediaries, while others take on new roles and provide additional value in the ecosystem.

In 2017, there were already signs of progress, with competitors voluntarily cooperating and using blockchain as the means to easily guarantee transparency for the duration of that relationship. Fast-forward to today, and many of these endeavors are showing their first measurable results, encouraging early adopters to move forward toward production. In the following sections, we present examples from different industries.

Blockchain Ecosystems in the Financial Sector

Trade Finance

A principal example where blockchain is being elevated to the status of a go-to platform for cooperation between competitors is we.trade — the consortium that includes Deutsche Bank, HSBC, KBC, Natixis, Rabobank, Société Générale, UniCredit, and Nordea.[3] We.trade is being built as a digital platform for managing, tracking, and protecting trade transactions between micro, small, and medium-sized enterprises operating in the EU. It harnesses both distributed ledger technology and smart contracts and links the parties involved in trade (i.e., buyer, buyer's bank, seller, seller's bank, and the logistics companies). The entire trade process, from order to payment, will be registered in a blockchain platform — which will display the process via an at-a-glance, user-friendly interface — and will guarantee automatic payment when all contractual agreements have been met. The we.trade platform is being built with application programming interface (API) layers, which will allow each participating bank to be onboard either through cloud software as a service (SaaS) or on-premises (computer or server-based) software, depending on the bank's capabilities. The platform is powered by open source blockchain platform Hyperledger Fabric 1.0.

The intrinsic value residing in blockchain can only be unleashed if more than one participant uses it to execute or take part in a multiparty business process.

To use the platform, European small and medium-sized enterprises (SMEs) must be clients of the banks involved, and the banks need to have performed the appropriate know-your-customer (KYC) procedures on all the companies that transact on the platform. A chief benefit for companies in this blockchain ecosystem is the ability to identify any known counterparts in their supply chains, in addition to real-time tracking and tracing of shipment and conditional settlement through the banking system. It is expected that the platform will be rolled out into production in the third quarter of 2018.

Regulatory Compliance

Various EU regulatory provisions require that a company provide certain information to a client in writing, either on paper or in another "durable medium." Many record-keeping requirements require organizations to store information in a durable medium. A durable medium must adhere to the following requirements:

- Allow information to be addressed personally to the recipient.
- Enable the recipient to store information in a way that is accessible for future reference and for a period of time adequate for the purposes of the information.
- Allow the unchanged reproduction of the information stored.

> *In a blockchain solution, performance is often mentioned as one of the main challenges and unknown factors.*

Technologies such as blockchain can be used to satisfy a regulatory obligation to guarantee the integrity of issued documentation (or information provided to customers). In 2017, the Polish Office of Competition and Consumer Protection made a statement that refers to the Court of Justice of the EU ("CJEU") judgment in a case concerning the interpretation of articles 36(1) and 41(1) of the Payment Services Directive 2007/64/EC.[4] The ruling requires greater transparency from banks and credibility in communication with customers. One of banks' primary challenges with regard to the CJEU ruling is the need to prove the immutability of the documents they publish, both public and private, directed to their clients. The methods that banks use to publish and store those documents at present do not comply with the requirements of the durable medium definition. To be in legal compliance, both parties — the bank and the client — should have the ability to verify, at any point in the future, that the original versions of the documents have not been modified in any unauthorized way.

Krajowa Izba Rozliczeniowa (KIR), the national clearinghouse in Poland, proposed an innovative solution to the problem. Together with IBM and Accenture, KIR has built a new service for the Polish banking sector that responds to the regulatory requirements.[5] This blockchain-based platform provides a proof of existence service that allows for registration and verification of documents via timestamped transactions saved on a distributed ledger. With this solution, the lifecycle of documents issued and exchanged between banks and their clients, as well as the documents' integrity, can be traced and audited. KIR is able to access online the status of a document and validate its content by using the self-operated banking channel or via the provided application — both of which are integrated with the blockchain-based platform.

In a blockchain solution, performance is often mentioned as one of the main challenges and unknown factors. This becomes extremely important if a platform must sustain service for a large number of documents published in a short period of time by many organizations within a network. The project team made a great effort during tests to streamline and seek the optimal configuration for the platform.

The executed performance tests gave a promising outcome. The blockchain network was benchmarked on the document publishing and on the verifying and downloading rates. The publishing result was 400 documents per second, which is sufficient to publishing almost 32 million documents per day. The verifying and downloading performance was even better, with the platform capable of verifying 600 documents per second with a download rate of 2,500 documents per second. The blockchain technology is not recommended for real-time systems, but from these results, we can see that the technology is mature enough for a production implementation to support B2B processes, automation, and digitalization.

More Blockchain Ecosystems

Food Tracking

According to the World Health Organization, access to sufficient amounts of safe and nutritious food is key to sustaining life and promoting good health globally. Unsafe food containing harmful bacteria, viruses, parasites, or chemical substances causes more than 200 illnesses and diseases worldwide — ranging from diarrhea to cancers. Almost one in 10 people in the world fall ill after eating contaminated food every year. Food safety and food security are inextricably linked.

Urbanization has increased the number of people buying and eating food prepared in public places. Globalization results in an increasingly more complex and longer global food chain, crossing multiple national borders. Good collaboration between governments, producers, and consumers helps ensure food safety.

A group of 10 food producers and retailers — Dole, Driscoll's, Golden State Foods, Kroger, McCormick, McLane, Nestlé, Tyson Foods, Unilever, and Walmart — is working together to address food safety in the global food supply chain. It is a collaborative effort to create a blockchain-based food safety platform. The blockchain technology enables different parties in the supply chain to share details, such as the date an animal was slaughtered or the weather conditions at harvest time. Data can be stored through a photograph on a smartphone that is transmitted onto a dedicated platform. The blockchain ledger is immediately updated, and all the parties within this ecosystem have access to the latest information.

One great virtue of blockchain is enhanced transparency by letting consumers look up key information on where food comes from, an asset amid growing concerns about genetically modified crops and artificial ingredients. Blockchain is ideally suited to help address these challenges because it provides a trusted and secure environment for all transactions. All participants — farmers, growers, suppliers, processors, distributors, retailers, regulators, and consumers — can gain permissioned access to known information regarding the origin and state of food for their transactions. Food providers and other members of the ecosystem can use the blockchain platform to trace product to its source in a short amount of time to ensure safe removal from store shelves in the event of contamination, thereby stemming the spread of illness.

General Meetings of Shareholders

Historically, there is an ongoing challenge to grow investor engagement, with general meetings of shareholders (GMSs) having very low participation from retail shareholders. One of the reasons for low participation is the limited number of participation modes. For instance, one can participate in person in a GMS or engage proxies as representatives. The extent of this issue is not limited to a specific territory or jurisdiction; last year, the European Council gave a green light to Directive (EU) 2017/828, which encourages long-term shareholder engagement.[6]

One particular institution took this issue quite seriously. The Polish Central Securities Depository, Krajowy Depozyt Papierów Wartościowych (KDPW), launched a project for mapping the entire lifecycle of a GMS onto a blockchain platform.[7] Since KDPW's role is crucial in the trading of financial instruments in Poland, it was clear that such a solution would attract an ecosystem of participants in the capital markets industry. The ecosystem's foundation provided the capability for several actors with dissimilar interests to be integrated in a multiparty process. Issuers, investors, registrars, auditors, and regulators can now see an ongoing GMS in its entirety while different steps of the process that require privacy remain protected by the smart contract. The latter governs the moment when sensitive information is revealed to all relevant participants.

One great virtue of blockchain is enhanced transparency by letting consumers look up key information on where food comes from.

Preliminary tests show that the blockchain-based platform for a GMS builds trusted cooperation between participants because access to the distributed ledger is controlled, registered events are indisputable, and security ensures confidentiality. Moreover, the decision to use the Hyperledger Fabric platform was based on a premise that it will serve as a private consortium ledger for the capital market industry and therefore will allow the linking of events related to a particular GMS to the identity of a particular participant.

Maritime Transport

One of the main challenges in the cross-border shipping industry is the number of interactions that must take place before a shipment can proceed. According to some estimates, a single shipment of goods from one continent to another may require more than 200 unique interactions with 30 individuals and organizations.[8] Many of these do not have a digitized documentation flow and therefore operate on the basis of a paper trail. This makes the administrative burden a considerable part of overall shipping costs.

Since around 80% of consumer goods are shipped through maritime transport, it became obvious that

Maersk (an international leader in the maritime shipping industry) would look for possibilities to optimize the administrative and communication exchange in the shipment process. A blockchain-based pilot ran over 18 months and provided evidence that digitization and automation of the documentation flow between Maersk and the ecosystem of participants in international maritime trade could significantly reduce costs and thus remove many of the financial barriers to growth in trade. Notably, the pilot has proven that a 15% increase in trade volume can be achieved by integrating participants and multiparty processes, as well as digitizing tracked assets.[9]

The future of ecosystems is bright but will flourish more with integrated private blockchain platforms.

As a result of this initial success, a decision was made to extend the reach of this ecosystem and invite new participants to a newly created joint venture that IBM and Maersk announced at the beginning of this year. Among companies expressing an interest in joining are GM, Procter & Gamble, Agility Logistics, Singapore Customs, Peruvian Customs, APM Terminals, PSA International, and Guangdong Inspection and Quarantine Bureau for trade corridors in and out of China. The objective of this endeavor is to integrate all parties involved at any stage of the shipping process, private and public organizations or institutions alike. [10]

Conclusion

The future of ecosystems is bright but will flourish more with integrated private blockchain platforms. The examples presented in this article confirm that blockchain will play a significant role in the reduction of friction and the emergence of new ecosystems focused around a particular industry. Many projects will reach full maturity and enter into production this year, in particular, in financial services and logistics. We expect that other industries will follow, with one of the main drivers being a need for regulatory compliance. Disruption in the area of personal data protection (e.g., the EU's General Data Protection Regulation [GDPR]) or protection of consumers against counterfeit drugs could provide a trigger for new blockchain ecosystems. The future also looks promising for the creation of cooperative networks in multiparty processes that extend beyond a particular industry. Examples of ongoing efforts can be found in the use of sovereign digital identity issued to those who lack one (e.g., refugees, stateless persons) or digitization of life events (e.g., birth of a child, death of a person).

From a technical perspective, it is crucial that a chosen blockchain platform be capable of materializing typical market conditions, such as complex transaction execution, preservation of privacy and confidentiality, access control, transparency, and scalability. Perhaps it comes as no surprise that all the ecosystems described in this article are based on Hyperledger Fabric — an open source, openly governed blockchain platform ready for production use. Open access to the source code provides much-needed transparency and clarity at both the business and technical layers. Moreover, controlled access to a distributed network based on a private blockchain reduces the risk of malicious attacks from unidentified parties. The latter means that incentives toward network maintenance such as cryptocurrency issuance or resource-intensive mining processes all become obsolete. This minimizes legal uncertainty related to territoriality of data and compliance with anti-money laundering laws. The use of private blockchain platforms also lowers the operational cost related to the use of computing resources (i.e., no mining required), execution of the business logic based on smart contracts (i.e., no limitation imposed on what tasks can be executed), and registration of new content on a distributed ledger (i.e., no inherent cost as no platform token is used for settlement of transactions). Therefore, the use of private blockchains is the direction to go for any enterprise use of distributed ledger that takes this endeavor seriously.

Endnotes

[1]"Size of the Blockchain Technology Market Worldwide from 2016 to 2021 (in Million US Dollars)." Statista, October 2016 (https://www.statista.com/statistics/647231/worldwide-blockchain-technology-market-size).

[2]"First on the Block: Learn from Early Blockchain Business Networks." IBM Institute for Business Value, 2017 (https://public.dhe.ibm.com/common/ssi/ecm/gb/en/gbe03903usen/first-on-the-block.pdf).

[3]we.trade (www.we-trade.com).

[4]"The Statement of the President of the Office of Competition and Consumer Protection Containing Crucial Point of View on an Issue." (Translated from Polish.) Urząd Ochrony Konkurencji i Konsumentów (Poland Office of Competition and Consumer Protection), January 2017 (https://www.uokik.gov.pl/download.php?plik=19511).

[5]"KIR Has Developed Prototype Solutions for a Durable Medium of Information." (Translated from Polish.) Press release, Krajowa Izba Rozliczeniowa (KIR), 1 February 2018 (https://www.kir.pl/o-nas/aktualnosci/kir-opracowal-prototypowe-rozwiazania-dla-trwalego-nosnika-informacji,219.html).

[6]"Directive (EU) 2017/828 of the European Parliament and of the Council of 17 May 2017 Amending Directive 2007/36/EC as Regards the Encouragement of Long-Term Shareholder Engagement." EU Publications, 17 May 2017 (https://publications.europa.eu/en/publication-detail/-/publication/9b871b38-3d20-11e7-a08e-01aa75ed71a1/language-e).

[7]"New Blockchain Solution to Enhance Investors' Customer Experience and Streamline Shareholder Meeting Preparation Process." Press release, KDPW Group, 13 October 2017 (http://www.kdpw.pl/en/kdpw/news/pages/NewsDetails.aspx?idn=436).

[8]van Kralingen, Bridget. "IBM, Maersk Joint Blockchain Venture to Enhance Global Trade." *THINK Blog*, IBM, 16 January 2018 (https://www.ibm.com/blogs/think/2018/01/maersk-blockchain).

[9]van Kralingen (see 8).

[10]van Kralingen (see 8).

Karolina Marzantowicz is IBM's CEE Banking Technical Leader and CEE WiT Leader and is a member of the IBM Academy of Technology leadership team. She stands in between the worlds of technology, business innovation, and psychology. Ms. Marzantowicz acts as a catalyst and fosters curiosity to help lead the adaptation to rapidly changing environments and to help drive organizational agility (internally and externally). She is continually learning from and contributing to the growing community of tech/fintech innovators and disruptors. Ms. Marzantowicz is passionate about digital transformation (and its impact) and innovation trends within IT. She can be reached at karolina.marzantowicz@pl.ibm.com.

Maciej Jędrzejczyk is a Blockchain Technical Leader at IBM Blockchain iLab, where he focuses on developing cross-industry distributed ledger technology (DLT) solutions in the CEE region. Mr. Jędrzejczyk has in-depth expertise in conceptualizing, designing, architecting, prototyping, scaling, and roadmapping DLT solutions. He works with clients from the public sector, financial services, capital markets, and telecommunications on vision and strategy for blockchain, technology, and digitization. Mr. Jędrzejczyk also leads the effort in building a critical mass of support by evangelizing the general adoption of innovative technologies via public forums, regulatory bodies, conferences, trade shows, standards groups, media, meetups, and universities. He has represented IBM in the Blockchain/DLT Stream and Digital Currencies initiative led by the Polish Ministry of Digital Affairs and is a member of the Blockchain working group within the Polish Chamber of Information Technology and Telecommunications. He can be reached at maciej_jedrzejczyk@pl.ibm.com.

Cutter Membership
The Ultimate Access to the Experts

Cutter Consortium Membership opens up multiple avenues to interact with Cutter's experts to brainstorm and gain guidance to transform your organization and boost success.

Like everything business technology, one size does not fit all.

That's why we encourage you to choose the Membership that's right for your organization. Whether you choose Digital Transformation & Innovation, Enterprise-wide, Practice-specific, or CIO Membership you'll see a strong return.

Contact us at +1 781 648 8700 or sales@cutter.com to arrange a sample inquiry call with a Cutter expert and see for yourself how quickly your return on Membership can be realized.

What Do You Get from Cutter Membership?

- Get guidance in leveraging new strategies, emerging technologies, and business management practices to enable digital transformation and boost competitive advantage.
- Learn how to mine data to create new products and services and improve customer experience.
- Get input on how to reduce expenses through more cost-effective strategies.
- Gain insights and get ideas on achieving sustainable innovation, successful change management, and prudent risk management.
- Get coaching and insights on leadership and team-building practices that boost productivity.
- Discover vendor-agnostic advice to ensure unbiased purchasing decisions.

Test Drive Cutter Today

Have a question? A challenge you're trying to overcome? Have you reached a bottleneck and need some expert advice? Find out for yourself how valuable Cutter Membership can be — request a sample inquiry with a Cutter expert now.

Call +1 781 648 8700 or email sales@cutter.com.

CUTTER CONSORTIUM
Access to the Experts

37 Broadway, Suite 1
Arlington, MA 02474 USA
Tel: +1 781 648 8700
Fax: +1 781 648 8707
Web: www.cutter.com
Email: sales@cutter.com

"I have personally been able to leverage Cutter's services since 1999. Among the attributes that differentiate Cutter from other firms, two remain at the top of my list: **Thought Leadership and Real Value**. Thought Leadership is driven by Cutter's experts. Real Value, driven by 'Access to the experts,' pushes us beyond just understanding the options. We can develop relationships with the experts, and tailor the options they present so that they can be quickly and practically executed within our organization, enabling our Business Technology team to continually improve, engage, and contribute to business growth."

— Doug Mikaelian,
VP Business Technology,
Dairy Farmers of America

"The Information Technology revolution continues to change how businesses work and how people work in and with them. Today's demands on software to provide useful, usable, secure, and scalable services stress all aspects of systems development. These include architecture, technology selection, product development and lifecycle management. Cutter provides comprehensive coverage for these crucial topics — through research reports and customized virtual training delivered globally — helping us to understand needs and solutions that span traditional silos."

— Eric Schoen
Director of Engineering, i2k Connect LLC;
Former Chief Software Architect,
Schlumberger

"Thanks to Cutter´s experts, in a short time we have been able to:

- Improve our capabilities, using the contract scorecard for outsourcing.
- Gain key insights and practical strategies for responding to challenges we face in building trust and partnerships within the organization and outside our institutional borders.
- Improve our methods for working with people and anticipating the challenges of cultural transformation within our organization.
- Have immediate access to key 'experts' at critical times, who spend quality time with our teams, provide state-of-the-art orientation, and help us implement projects.
- Implement agile, effective, and articulated innovation around a common vision for achieving quality education in Mexico."

— Arturo Cervantes
Director General of Information Systems for Evaluation Results, National Institute for Educational Evaluation, Mexico

Cutter Business Technology JOURNAL

About Cutter Consortium

Cutter Consortium is a unique, global business technology advisory firm dedicated to helping organizations leverage emerging technologies and the latest business management thinking to achieve competitive advantage and mission success. Through its research, training, executive education, and consulting, Cutter enables digital transformation.

Cutter helps clients address the spectrum of challenges technology change brings — from disruption of business models and the sustainable innovation, change management, and leadership a new order demands, to the creation, implementation, and optimization of software and systems that power newly holistic enterprise and business unit strategies.

Cutter pushes the thinking in the field by fostering debate and collaboration among its global community of thought leaders. Coupled with its famously objective "no ties to vendors" policy, Cutter's *Access to the Experts* approach delivers cutting-edge, objective information and innovative solutions to its clients worldwide.

For more information, visit www.cutter.com or call us at +1 781 648 8700.

CUTTER CONSORTIUM
Access to the Experts