ASIS FOUNDATION DIGITAL TRANSFORMATION SERIES

ASIS FOUNDATION™

BLOCKCHAIN:
A GUIDE FOR SECURITY PROFESSIONALS

Table of Contents

About the Author

Michael Gips, CPP, CSyP, is principal at Global Insights in Professional Security, Inc., a firm providing security strategy, content, research, and thought leadership. He was formerly the Chief Global Knowledge & Learning Officer at ASIS International, and has written more than a thousand articles on all aspects of security. He contributed prominently to industry research including "The State of Security Convergence in the United States, Europe, and India (ASIS Foundation, 2019), "The United States Security Industry: Size and Scope, Insights, Trends, and Data (ASIS and IOFM, 2012 and 2014), "Leveraging Corporate Security for Business Growth and Improved Performance: The Transformative Effect of 9/11" (The Conference Board, 2012), and "Enterprise Security Risk Management: How Great Risks Lead to Great Deeds" (CSO Roundtable, 2010).

Complimentary for ASIS Members
Non-Members: $125

ASIS International | 1625 Prince Street | Alexandria, Virginia, USA 22314

EXECUTIVE SUMMARY

In late 2019, the ASIS Foundation commenced a research study to help security professionals understand blockchain technology and its security impacts.

The study—which included 30 interviews, a literature review, a survey, and additional research—found that blockchain has a firm foothold in cryptocurrencies and is gaining use in financial applications. The technology has been tested in hundreds of other use cases from creating corporate currency to tracking refugees from the war in Syria. But despite enormous amounts of hype, promise, and positive results from the use cases, industry and government have rarely committed to blockchain with large investments or implementations. Reasons for this reluctance range from lack of a business case to make the transition to questions over how blockchain deals with third-party trust.

For security professionals, many other issues arise. For all the benefits that blockchain can provide—improved identity management, access control, private messaging, smart contracts, and so on—equal challenges present themselves. These include vulnerabilities to blockchain's APIs, the threat of manipulation to the underlying ledger, and lack of a governance scheme, to name a few.

Still, blockchain is coming. It's making inroads all around the security industry. Security practitioners can no longer ignore it and wait for it either to go away or become relevant. Blockchain may well be at the tipping point where it starts to feature in cyber and physical security applications, and security professionals will be expected to understand it, leverage it, and protect it.

KEY FINDINGS

Blockchain is simply a type of database, though a powerful one.

Blockchain is a shared database among a group of individuals or organizations. It doesn't exist in a central repository, but rather in a network of computers around the world. Advocates of blockchain say that the technology is immutable, decentralized, secure, irreversible, distributed, and anonymous. To a large extent, all those claims are true; the challenge is that none of them is 100 percent true.

By removing a central authority, a blockchain relies on the crowd to verify transactions, and they are rewarded for their troubles. A transaction is entered into the system and is typically stored with many other transactions within a block. Subsequent transactions form new blocks, and each new block is linked to the previous block via a unique digital signature. If someone tampers with a transaction recorded in a block, it alters the digital signature and unlinks that block. That's what makes it so difficult to alter data on blockchain.

Blockchain may be poised for mass adoption, but it's not quite there yet.

Billions of dollars are pouring into blockchain. LinkedIn says blockchain will be the most in-demand hard skill in the workplace in 2020. Blockchain has been called the Internet 2.0 and the harbinger of a paperless society. Use cases are legion.

Yet, the technology hasn't quite reached mainstream use. Questions persist about its value compared to a simple database, its vulnerabilities, its enormous power expenditure, and so on. However, some experts predict that in several years blockchain will be as ubiquitous as wifi.

And blockchain weariness has set in. Gartner has been tracking blockchain's progress through its hype cycle. As of late 2019, analysts there said that blockchain was entering the "Trough of Disillusionment" after summiting the "Peak of Inflated Expectations." The trough is where "interest has waned as experiments and implementations fail to deliver," according to Hype Cycle for Blockchain Technologies, 2019, and the technology will languish there until 2021.

Blockchain shouldn't be a technology seeking an application.

As with any security application, things go awry when security experts look for a solution that a

technology can handle rather than the other way around. A fundamental tenet of good security is that you assess an application first, then add the appropriate technology.

There are applications where blockchain is a good fit, but it needs careful selection and a clear system-level view as to 'why' coupled with a clarity of upsides and downsides. It requires a clear-eyed perspective of what issue needs to be solved and what hurdles blockchain introduces. It's a tradeoff.

Security professionals around the globe are generally unfamiliar with blockchain, nor are their companies using the technology.
The results of a survey of ASIS members indicate that blockchain is still shrouded in mystery, if not obscurity. Fifty-three percent of respondents said that they were either "Not at all familiar" or "Not so familiar" with blockchain. Just more than a third said they were "Somewhat familiar." And only 11 percent reported that they were "Very familiar" (9 percent) or "Extremely familiar" (2 percent) with blockchain.

Likewise, most respondents were unsure of blockchain's practical value and had never deployed it. While some security professionals surveyed are avid proponents of the technology, a majority expressed skepticism, pointing out issues such its heavy energy expenditure, the lack of a compelling business case, and regulatory issues.

When blockchain is a good solution, any one of four different types of blockchain might be the best choice.
Several different types of blockchain exist: public, private, hybrid, and consortium. Public blockchains, such as Bitcoin, are the choice for cryptocurrencies and applications where users are willing to vest the issue of trust in the technology. The three types of restricted-access blockchains—private, hybrid, and consortium-based—place more trust in humans. Private blockchains, which are by invitation only, are controlled by a single individual or organization. Hybrid blockchains place private blockchains on a public platform to achieve the benefits of each. Consortium blockchains are jointly controlled private blockchains in which organizations with like interests collaborate for a specific purpose.

Blockchain offers many security advantages.
Advantages include applications in identity management, access control, video verification, private messaging, distributed storage, domain name system integrity, smart contracts, and distributed trust. Some applications, such as identity management and smart contracts, are fairly mature. Others, such as video verification, are relatively nascent.

Blockchain must confront various security issues and other challenges.
Challenges include questions of trust, lack of governance, software vulnerabilities, aging encryption, private blockchain manipulation, regulatory uncertainty, negative associations, the lack of a compelling use case, better alternatives, antitrust implications, implementation issues, data migration concerns, interoperability hurdles, enormous power use, and the "trash in, trash out" factor.

Trust is the key philosophical issue.
Public blockchains vest trust in technology; private blockchains vest trust in the gatekeepers—organizations or individuals.

Successful blockchain use cases have yet to transform into lasting implementations.
Hundreds of blockchain use cases, most of them declared successes, have been undertaken. The report documents such cases in finance, government, corporate currency, copyright, global trade, food sourcing, pharmaceuticals, ticketing, legal privilege, conflict minerals, cryptoassets, health records (including Coronavirus response), and art provenance. Yet these represent the relatively small percentage that have moved beyond the proof-of-concept phase.

RECOMMENDATIONS

Before implementing blockchain, security professionals should consider the following recommendations.

Don't try to force-fit blockchain into your application. Determine whether your organization or application truly needs a blockchain solution. Be able to make the business case for blockchain implementation

Determine whether blockchain will fit with your current IT architecture or a systems overhaul will be necessary. Ensure that your technical team has a strong background with blockchain. Consider working with industry partners that have experience with blockchain. Beware using blockchain with physical assets.

Rigorously check the trustworthiness of both the organization that manages the blockchain and the technology itself. Determine whether you can beta-test a blockchain solution before making the investment. Establish specific goals and timelines for your blockchain implementation. Consider blockchain's impacts on issues such as business processes, governance, and talent management. Consider whether regulation exists that will influence your use of blockchain.

RESEARCH METHODOLOGY

This research is the result of hundreds of hours of interviews, literature reviews, discussions, observations, and analysis. More than 80 professionals were contacted who have experience with and insight into blockchain and cryptocurrencies, including: developers, investors, consultants, blockchain project managers, analysts, futurists, attorneys, lobbyists, academics, technologists, systems engineers, cryptocurrency miners, journalists, and security professionals (physical, cyber, converged). Those contacts resulted in 30 interviews.

A brief survey was also conducted to focus the research on security professionals including their level of familiarity with blockchain, their use of the technology, and their impressions of its value. The survey was sent to 10,000 members of ASIS International who hold senior level positions—CSOs, CISOs, deputies, principals, business owners, and other executives. The 21 percent response rate exceeded expectations. Follow-up interviews with six respondents ensued.

The author also attended conferences, exhibits, and presentations featuring blockchain, including the Consumer Electronics Show in Las Vegas in January 2020 and (virtually) RSA in San Francisco in February 2020. Blockchain experts demonstrated how to encode transactions and messages on blockchains as well.

Finally, the research encompassed a thorough literature review that included studies, reports, and surveys by management consulting firms and analysts such as Gartner, McKinsey, PwC, Accenture, and Deloitte. It included dozens of books, survey results, articles, webinars, podcasts, and other materials from both mainstream sources and specialty sources. A complete bibliography and list of interviewees are included in the full research report.

INTRODUCTION

Blockchain. A compound word comprised of two elemental terms. A block is sturdy and impenetrable. A chain links and secures component parts. Therein lies the essence of blockchain, a system that encodes and records transactions in a way that is impenetrable, binds these transactions together, and secures the series of transactions as a whole. But while a physical chain exists in a specific geographical location, blockchain records are virtually distributed across a multinodal network. Hundreds of articles, white papers, reports, press releases, blog posts, marketing pieces, case studies, videos, and podcasts available on the Internet explicate almost every possible aspect and capability of a blockchain. There's seemingly no problem that a blockchain can't solve. That exuberance has been countered by extreme fatigue and jaundice by more skeptical observers.

So what is blockchain, how does it help security practitioners, what vulnerabilities and issues does it raise, who is using it, and to what benefit? These questions are all addressed in the following pages.

Here's why you should care: Blockchain is coming. It's making inroads all around the security industry. Security practitioners can no longer ignore it and wait for it either to go away or become relevant. Blockchain may well be at the tipping point where it starts to feature regularly and prominently in cyber and physical security applications, and security professionals will be expected to understand it, leverage it, and protect it. This report will serve as a thorough introduction to the technology, its benefits, its challenges, and its uses, and it will offer guidance for getting started with blockchain. Promising use cases—from food supply to conflict minerals—appear in call-out sections throughout the report.

A good place to start, before plunging into the origins and technical aspects of blockchain technology, is a level-headed observation by futurist and technologist Scott Klososky:

"Blockchain to me is a technology concept that basically is a more advanced form of a database. Just as a database has fields, can be searched, and has a structure for storing data, so does a blockchain. The way it's built, it has some unique characteristics in how it stores data. It's more encrypted. It allows more people to participate in anonymous transactions.

"People overcomplicate what it is.

"Some people think it's cryptocurrency, or cryptoassets. It's just a platform we can do things with, a unique way to store information."

THIS STUDY IS THE RESULT OF:

- 30 interviews with blockchain and cryptocurrency experts
- Review of more than 150 reports, studies, research papers, books, surveys, presentations, articles, blog posts, webinars, videos, and podcasts
- 2,093 responses to a survey of security professionals about blockchain
- Attendance at two conferences covering blockchain
- Performing blockchain transactions with three organizations

BLOCKCHAIN BASICS

Among the scores of explanations of blockchain, one of the best is offered by McKinsey in a June 2018 article:

> *Blockchain is a distributed ledger, or database, shared across a public or private computing network. Each computer node in the network holds a copy of the ledger, so there is no single point of failure. Every piece of information is mathematically encrypted and added as a new "block" to the chain of historical records. Various consensus protocols are used to validate a new block with other participants before it can be added to the chain. This prevents fraud or double spending without requiring a central authority.*[1]

In essence, blockchain is a database that is shared among a group of individuals or organizations. It doesn't exist in a central repository, but rather in a network of computers around the world. It has been the cause for enthusiasm, investment, and downright hyperbole because of what it offers—or promises to offer. Advocates of blockchain say that the technology is immutable, decentralized, secure, irreversible, distributed, and anonymous. To a large extent, all those claims are true; the challenge is that none of them is 100 percent true.

ORIGINS

Blockchain was developed in 2008 by a person or persons calling themselves Satoshi Nakamoto. The goal was to create a digital payment system that allowed the parties to trust each other in the absence of a third-party intermediary. It would also prevent double spending and create a record that anyone could see but not change. The result was Bitcoin, the first public blockchain.

Since Bitcoin was born, the world has spawned more than 5,000 traded cryptocurrencies.[2] That dwarfs the mere 180 "fiat" currencies in existence—currencies established and backed by government authorities—such as the U.S. dollar, European Union euro, British pound, and Japanese yen.

Part of the explosion of cryptocurrency is due to the leveling, libertarian appeal of a system of payment that is not controlled by a centralized authority. However, governments are scrambling to get into the act. Countries such as Bolivia, Algeria, and Vietnam ban cryptocurrency outright. Argentina, Israel, South Africa, and others now tax cryptocurrency transactions, while nations such as Singapore, the Czech Republic, and Costa Rica subject cryptocurrency to anti-money laundering and anti-terrorism financing regulations. And China, Ireland, Dominica, and Lithuania are going so far as to issue their own national or regional cryptocurrencies.[3,4]

HOW IT WORKS

A technical description of how blockchain operates is beyond the scope of this research. However, certain basic principles are essential to understand.

By removing a central authority, a blockchain relies on the crowd to verify transactions, and crowd members are rewarded for their efforts. A transaction is entered into the system and is typically stored with many other transactions within a block. Subsequent transactions form new blocks, and each new block is linked to the previous block via a unique digital signature. A digital signature is made from a cryptographic hash function that creates a 64-digit string. If someone tampers with a transaction recorded in a block, it alters the digital signature and unlinks that block, indicating trouble. In fact, altering just one block would change the digital signature for every other block down the chain. That's what makes it so difficult to alter data on blockchain.

Many of the principles underpinning blockchain aren't new, points out Roger Shepherd, an Internet of Things (IoT) consultant. "It packages

By removing a central authority, a blockchain relies on the crowd to verify transactions, and crowd members are rewarded for their efforts.

USE CASE: CRYPTOCURRENCY

Blockchain was invented to facilitate decentralized, secure, immutable, and transparent transactions via cryptocurrency. Samson Williams calls cryptocurrency "the porn of blockchain," by which he means the easiest application for the then-fledgling technology.

As mentioned, thousands of cryptocurrencies exist, with a constant churn of births and deaths. Some experts, such as Jimmy Song, believe cryptocurrencies are the ideal use for blockchain. He doesn't see much value otherwise, especially as private blockchains fall under centralized control. Other experts, however, counsel patience as the hype subsides and the business uses catch up.

"Blockchain will be more transformative than the Internet because it is built on top of the Internet and will allow us to take it to a new level," says Gerard Dache, CEO of the Government Blockchain Association. In a blog post called "The Blockchain Chinese Bamboo Tree" on his organization's website, Dache says blockchain turned the corner in 2019, but more tending to the "tree" is needed:

Before the widescale adoption of blockchain and cryptocurrency can be achieved, organizations will have to offer blockchain-related services in asset management, accounting, financial, healthcare, identity, law, security, and systems development. Support services will have to be provided by associations, conference/event management, data analytics, and media organizations to support this new industry.

up various technologies to make them useful and comprehensible," he says. For example, ledgers, cryptography, and blocks (which are based on Merkle Trees—structures that verify content in a sea of data) have existed for a long time, while blockchain adds novelties such as decentralization. The Web did the same thing. "It brought together lots of existing technologies that were just becoming functional and bundled them together in a very usable form," explains Shepherd." Those technologies included Internet Protocol, File Transfer Protocol, Gopher, browser software, and HTML. "Blockchain can be like that."

BLOCKCHAIN VS. DISTRIBUTED LEDGER TECHNOLOGY

Blockchain and distributed ledger technology (DLT) are often used interchangeably, but they have key differences. Essentially, blockchain is a subset of DLT. Both are distributed, decentralized ledgers. But classic DLTs don't store data in blocks and link them together through hashes. In addition, blockchains can be public or permissioned—open or by invitation only. DLTs are permissioned systems used for groups with common interests.

TYPES OF BLOCKCHAINS

Although various typologies exist, blockchains can be organized into four categories: public, private/permissioned, hybrid, and consortium-based. While they share technology, the philosophies underlying the different approaches, as well as benefits and shortcomings, vary significantly.

PUBLIC BLOCKCHAINS

Bitcoin is the first, most well-known, and most successful public blockchain. Others include Ethereum (for decentralized applications and smart contracts), EOS (for industrial-scale decentralized applications), TRON (for sharing entertainment content), and Stellar (for banking in underserved areas). Anyone with Internet access can participate, and no one is in charge of the network. Since it's not possible to personally know everyone on a public blockchain, the technology substitutes for the element of personal trust.

A public blockchain contains five components: a database, encryption, a token (cryptocurrency), a consensus mechanism, and a peer-to-peer network.

Tokens and the consensus mechanism are typical of public blockchains. A consensus algorithm means that everyone on the network agrees that a transaction added to the blockchain is unique and legitimate. Proof of Work (PoW) and Proof of Stake (PoS) are the two most popular consensus algorithms.[5] In both cases, users on the network—called "miners," because they mine for cryptocurrency—seek to verify a bundle of transactions that are grouped in a block.

In PoW, miners solve difficult mathematical puzzles to confirm the transactions. Doing so gives them a reward, such as a cryptocurrency token. Once verified by at least 51 percent of the nodes in the network, the block of data can be attached to the blockchain. The upside is that the system generally works well without needing a central authority. The downside is that it expends enormous amounts of computational power, and thus energy. In addition, large mining operations could end up dominating the verification process, which undercuts decentralization. With PoS, by contrast, the user who puts up the most stakes—such as the most coins—is more likely to get first crack at validating the block. This approach is much more energy efficient, but it also may be less reliable and secure because it favors majority stakeholders.

PRIVATE BLOCKCHAINS

Also called "permissioned" blockchains, private blockchains depend on the same technology and mechanisms as public blockchains do. The key difference is that a single entity typically controls access and allows only certain parties to participate in and view transactions, and these members are known to each other. That means private blockchains are more centralized than public blockchains. Moreover, private blockchains have much less "traffic" so operate much faster than public blockchains and are more scalable because they incorporate fewer nodes. Whereas in public blockchains the trust resides in the technology, in permissioned blockchains it resides in the individual members of the blockchain: Who should we allow in? Knowing the users also allows role-based access to information and ability to conduct transactions.

Well-known permissioned blockchains include Hyperledger (which promotes collaboration in developing blockchains), Corda (an open-source platform to manage contracts and transfer value), and Ripple (a currency exchange and remittance network).

While mining can occur on private blockchains, it isn't necessary because there is no incentive to reward tokens to get people join the network and verify blocks of transactions. And since private blockchains are usually smaller than public ones, they are faster, more efficient, and less energy-dependent.

According to technologist Rick Bawcum, who is working with a trade association to implement a blockchain for purposes to include smart contracts and chain of custody verification, permissioned blockchains are the way to go for maximum security. "Who you are is handled outside the blockchain, in real life," he says. "With

USE CASE: STOCK EXCHANGES

A 2020 report by J.P.Morgan Chase sees blockchain technology taking root most firmly in global stock exchanges. It says:

> *Payments, trade finance, and custodial services remain the clearest use cases for blockchain. The adoption of blockchain technology among stock exchanges to improve the efficiency around settlement/clearing and collateral management has been noteworthy. Exchanges around the world are embracing blockchain technology in their operations and seeking to launch new digital asset trading platforms. The potential beneficiaries of the new Distributed Ledger Technology (DLT)-based settlement/clearing systems include banks and brokers who would see lower reconciliation costs and lower capital requirements (from potential real-time settlement), while registry service providers may be negatively impacted.*

cryptocurrency [on public blockchains], I don't have to trust," he adds. "In a business application like access control on a data center, trust has to exist beyond the blockchain." (For more analysis of blockchain and trust, see pages 24-27.)

HYBRID BLOCKCHAINS

Though private and public blockchains each have their ardent advocates—public blockchain enthusiasts often bridle at the corporate control of private blockchains—benefits can accrue by combining the two approaches.

Hybrid blockchains involve creating a private network on a public blockchain[6]: they blend a public-facing side with a back-of-house side, and the speed of private with the security of public. For example, XinFin joined forces with Ramco Systems to create a hybrid system for aviation, logistics, and human resources that combines Ethereum (public) and Quorum (private) blockchains.[7] The companies say that the system will prevent users from sending tokens to incompatible addresses or nonexistent addresses. They expect it to reduce congestion to the benefit of security, speed, and scalability.

The hybrid model allows system users to conduct transactions that are invisible to both the outside world and to participants in the blockchain that are not parties to the transaction. They protect privacy (a feature of private blockchains) while allowing users to connect with the outside world (a cornerstone of public blockchains).[8]

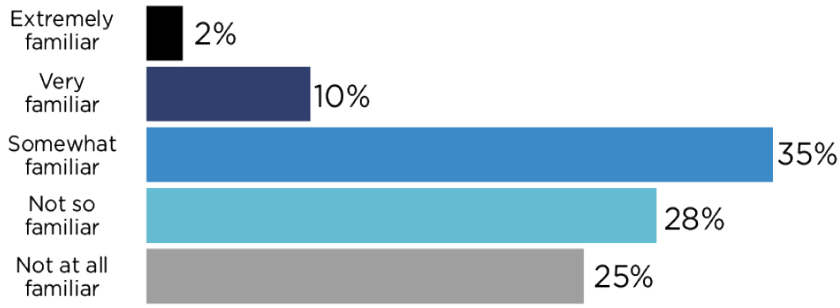
Another zealous advocate of a hybrid solution is Andre De Castro, CEO of Blockchain of Things. Using Catenis Enterprise as a Web services layer, the company provides application programming interfaces (APIs)—software that allows two applications to communicate with each other—and development tools for companies that want to build on or integrate with the Bitcoin platform. "I believe the answer is going to be a hybrid solution on the most robust, only proven blockchain in the world," De Castro says.

Not only does a hybrid blockchain share the benefits of public and private blockchains, he contends, but it also eliminates some downsides. For example, he says that DLTs like HyperLedger can be manipulated and that a simple database can essentially perform the same functions with far less cost and trouble.

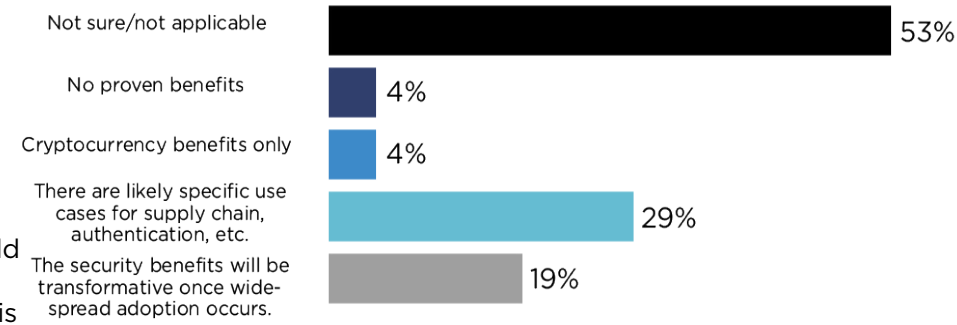
CONSORTIUM BLOCKCHAINS

Consortium blockchains represent a type of private blockchain governed by a group of individuals or organizations with common interests. They spread the development and cost burden among multiple bodies. These organizations may compete with each other but wish to partner and collaborate on specific initiatives.[9] For example, the IBM Food Trust—

How familiar are you with blockchain?



What are your thoughts on the security benefits of blockchain? (select all that apply)



USE CASE: PHARMACEUTICALS

One of the most enthusiastically pursued blockchain applications involves the integrity of the prescription drug supply chain. Fintech attorney Christian Auty explains why this use makes sense. "The Drug Supply Chain Security Act [DSCSA] mandates a digital pedigree from manufacturer to wholesaler to pharmacy," he says, "but there are regulatory silos" between those groups. For many industries, blockchain is just an inefficient database. "To justify that inefficiency, you need preconditions—people who need to communicate information to each other and are divided somehow such that they cannot fully trust each other, yet they share a common goal that can't be achieved individually." Plus, the parties wish to talk about drug authenticity and diversion without veering into trade secrets or antitrust activity. Hence, pharma is a fitting application, Auty says.

And that application is moving forward. Under the Drug Supply Chain Security Act, the U.S. Food and Drug Administration (FDA) must put requirements in place to enhance drug supply chain security. The FDA asked for proposals for accomplishing this, and one proposal that it accepted, the MediLedger Project, brought together 24 major pharmaceutical manufacturers, distributors, retailers, logistics partners, and solution providers, including Amgen, Pfizer, Walmart, McKesson, and FedEx. Their mission: to look at the feasibility of blockchain for tracking and tracing prescription medicines.

The project issued a report in February 2020. The principal findings were:

- Blockchain has the capability to be the technology underlying an interoperable system for the pharmaceutical supply chain, as mandated by DSCSA. When using a single blockchain solution, transaction throughput, speed, and reasonable cost can be achieved to meet stakeholder needs.

- Data privacy requirements of the pharmaceutical industry can be met using "zero knowledge proof" technology, where all transactions posted to the blockchain are fully obfuscated, ensuring no confidential information or business intelligence is shared. The design allows for nodes in the blockchain system to be hosted by multiple unique parties while maintaining strict transactional privacy and still ensuring immutability of the transactions.

- A blockchain system can be capable of validating the authenticity of product identifiers (verification) as well as facilitating the provenance of saleable units back to the originating manufacturer.

- The authenticity of the drug transaction information can be confirmed with each transaction allowing for expedited suspect investigations and recalls.

USE CASE: PHARMACEUTICALS CONTINUED

- If a blockchain ecosystem is created as a possible solution to the DSCSA interoperable solution requirement, it should have an open system architecture with an appropriate governance to oversee the function of the system and ensure compliance with industry-agreed business rules and standards of operation.
- Governance should come from the industry itself.
- The trust established by a blockchain system can be leveraged for additional business applications to the pharmaceutical industry, allowing for compounding benefits for this industry once such a platform is established.
- This is a complex solution that will require a stabilization period. The implementation date and the FDA enforcement date could be separate and planned in advance.
- The long-term success of a truly interoperable blockchain-based solution will require strong participation and adoption from all industry stakeholders (manufacturers, wholesalers, dispensers, service providers, etc.).
- There are clear challenges with making disparate track and trace systems interoperable. The project group is concerned that no standards currently exist to make the multiple systems interoperable, and without appropriate standards, it is not likely that disparate systems can be made successfully interoperable.[10]

which includes organizations such as Walmart, Carrefour, Albertsons, Smithfield, and Nestle—allows entities all along the food supply chain to share information related to food origin, process, and shipping. Consortium blockchains solve the lack of governance issue that bedevils open blockchains, because the members need to agree on a common set of rules. For example, IBM Food Trust's governance model is a joint effort to ensure that members comply with common rules. To avoid fears arising from loss of intellectual property or competitive intelligence, consortium members own their data and control the sharing of their data. Consortium-based blockchains may raise antitrust issues, however; these are discussed on page 31.

SECURITY PROFESSIONALS AND BLOCKCHAIN

To measure security professionals' familiarity with and use of blockchain, the ASIS Foundation conducted an online survey in early February 2020. It targeted 10,000 ASIS International members with director-level titles and higher, including CSO, CISO, president, vice president, owner, principal, senior director, and so on. The survey yielded 2,093 responses—an almost 21 percent response rate. (The survey questions can be found in Appendix III.)

FAMILIARITY WITH BLOCKCHAIN

The results indicate that blockchain is still shrouded in mystery, if not obscurity. Fifty-three percent of respondents said that they were either "Not at all familiar" or "Not so familiar" with blockchain. Just more than a third said they were

"Somewhat familiar." And only 12 percent reported that they were "Very familiar" (10 percent) or "Extremely familiar" (2 percent) with blockchain.

BENEFITS OF BLOCKCHAIN

Not surprisingly, when asked about their thoughts on the benefits of blockchain, 53 percent—the same percentage that were "Not at all familiar" or "Not so familiar" with the technology—indicated that they were unsure or that the question was not applicable. Another 29 percent believed that "There are likely specific use cases for supply chain, authentication, etc." Nineteen percent were downright bullish, agreeing that "The security benefits will be transformative once widespread adoption occurs." Very few respondents considered blockchain to have "No proven benefits" (4 percent) or "Cryptocurrency benefits only" (4 percent).

PRACTICALITY OF BLOCKCHAIN

Queried about how practical blockchain is, the majority (61 percent) said they didn't know or were unsure, providing further evidence that the technology barely registers for many security professionals. Twenty percent said that blockchain "Is as practical as the specific application." Another 20 percent said that "It will take off once the real-life benefits are in substantial evidence," which closely tracks the 19 percent who think blockchain will be transformative. Less than 5 percent chose the option, "It does little more than a database does, at greater cost and complexity." One U.S.-based security consultant who is very familiar with the technology commented that blockchain "is good for limiting unauthorized changes to data, but the initial entry is critically important and users should include protection of their [intellectual property] as part of their sharing."

STUDY OR INVESTMENT IN BLOCKCHAIN

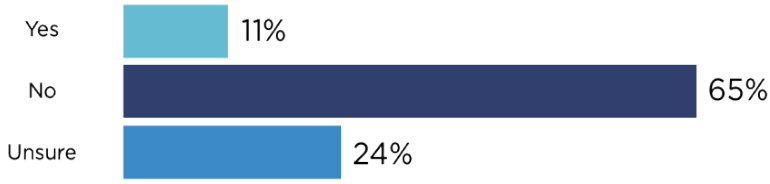
Only 11 percent indicated that their organization has ever studied or invested in blockchain. Of those, one-third said that they are "Participating in one or more use cases," 30 percent are biding their time until the technology becomes more mainstream, 20 percent are taking no further actions because costs exceed benefits, 17 percent are developing or partnering on a permissioned (or private) blockchain, and 6 percent are participating in a public blockchain such as Bitcoin. Some respondents were enthusiastic about blockchain despite not having had their organizations roadtest it. "For the purposes of multifactor verification," said one African physical security professional, "quite frankly I believe it's the future."

BLOCKCHAIN CHALLENGES

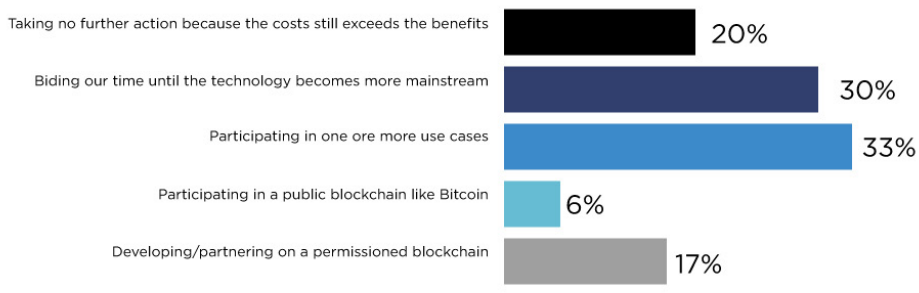
Many respondents' comments crystallized the challenges posed by blockchain. Several mentioned that it is computationally and energy intensive. One U.S.-based healthcare/pharmaceutical company security executive who sees blockchain as a transformative technology conceded that "The complexity of the supply chain requires all entities to participate in order to achieve the benefit. Until all participants commit, [I] don't see any business investment."

An Asia-based security consultant in the transportation and delivery industry who is unsure

Has your organization ever studied or invested in blockchain?



If you answered yes above, which of the following actions have you taken?



What are your thoughts on the security benefits of blockchain? (select all that apply)

Practitioner Responsibility	Not sure/not applicable	No proven benefits	Cryptocurrency benefits only	There are likely specific use cases for supply chain, authentication, etc.	The security benefits will be transformative once widespread adoption occurs
Physical Security	57%	4%	4%	27%	17%
Cybersecurity	15%	8%	3%	67%	21%
Business Continuity	52%	0	13%	23%	23%
Safety	52%	0	9%	30%	12%
Combination	49%	4%	4%	31%	21%

about blockchain's future said, "Blockchain has been used by my company in its supply chain operations but the opportunities to apply the same in security-related local operations are rare." A U.S.-based executive in a business support firm expressed reluctance due to issues arising from the European Union's General Data Protection Regulation (GDPR). And a security executive in the technology space—who is extremely familiar with blockchain and believes that it has no proven benefits and does little more than a database—spurns blockchain because "It is prone to attack, fraud, and theft as easily as any other medium. We prefer other security methodologies."

EFFECT OF FAMILIARITY

The more familiar the respondents were with blockchain, the more optimistic they were about its implementation. For those who said they were very familiar or extremely familiar with blockchain, 58 percent replied that there are specific use cases for it (compared to 30 percent for all respondents), and 47 percent said the technology will be transformative (compared to 19 percent of all respondents).

The same held true about their views on the practicality of blockchain. Forty-three percent of respondents who were very or extremely familiar with blockchain predicted that blockchain is poised to take off, compared to 20 percent of all respondents, and 49 percent said it's as practical as the specific application, as opposed to 20 percent of all respondents. Tellingly, even among the blockchain cognoscenti, only 40 percent of their companies have ever studied or invested in blockchain or are participating in or partnering on a blockchain.

INDUSTRY BREAKDOWN

Broken down by industry, the professionals most likely to know about blockchain work in finance, insurance, technology, the military, management consulting, retail, and transportation. Those least familiar work in education, nonprofit, security services, utilities, and entertainment/leisure.

ROLE/RESPONSIBILITY BREAKDOWN

As might be expected, respondents with cybersecurity responsibilities were the most knowledgeable about blockchain—36 percent were extremely or very familiar, versus 11 percent for all respondents. Business continuity/disaster recovery professionals followed with 16 percent extremely or very familiar. Respondents with a combination of responsibilities (12 percent) were the next group in order of familiarity with blockchain. Physical security practitioners and safety professionals (9 percent each) pulled up the rear.

USE CASE: GOVERNMENT INITIATIVES

Government Initiatives

Some countries are dipping a toe in the water. Others are diving right in. Here's a world tour of some state-sponsored blockchain initiatives that have broad impact or have significant security ramifications.

UAE

Dubai has pledged to be the first government in the world to conduct all its transactions in blockchain, making it "the happiest city on Earth." Smart Dubai estimates that the emirate will save $1 billion in document processing alone, and it reports that the government and private sector there are currently piloting 24 use cases in eight industries.[19]

Samson Williams adds that the United Arab Emirates and Saudi Arabia have joined forces to boot up their own cryptocurrency, called Aber. Initially it will be used for interbank transactions, not for retail use.

Other Middle Eastern governments are pouring money into blockchain, artificial intelligence (AI), and other technology, as well. According to a February 2020 report by the International Data Corporation (IDC), Middle Eastern nations consider blockchain to be "a powerful government tool for reducing fraud, boosting security, and establish new relationships with citizens. And while MEA [Middle East and North African] governments only directed $21 million towards blockchain last year, IDC expects that figure to top $105 million by 2023, representing a phenomenal CAGR [Compound Annual Growth Rate] of 49.2%." [20]

INDIA

Led by the states of Telangana and Andhra Pradesh, the Indian government has 40 blockchain initiatives underway, with 92 percent in the pilot phase.[21] Applications include land registry, identity management, cybersecurity, power distribution, and the agricultural supply chain, among others.

As far as cryptocurrency is concerned, the Central Bank of India banned trading in virtual currencies in April 2018. But in March 2020, the Supreme Court of India overturned that prohibition. According to Indian blockchain expert Ajit Tripathi, the court's ruling "paves the way for measured and progressive regulation that will allow India, a leading software exporter and market for fintech, to benefit from rapid innovation in blockchain technology and digital assets."[22]

AUSTRALIA

A recently released roadmap of how Australia can leverage blockchain technology over the coming years focuses on finance, educational credentialing, and wine production and export. The document explains that the wine industry would benefit from blockchain's "transparency, data-sharing, and efficiencies. It can assist in inventory tracking, facilitate automated payments between supply chain members, and reduce counterfeiting through provenance transparency."[23]

USE CASE: GOVERNMENT INITIATIVES CONTINUED

GHANA

The governor of Ghana's largest bank has announced plans to unveil a digital form of currency for the nation's country in the "near future."[24]

UNITED KINGDOM

UK's Food Standards Agency successfully ran a blockchain pilot in a slaughterhouse to provide more transparency in the food chain. Land registration and pension payments are other applications in the works.[25]

VENEZUELA

Venezuela's petro is first the digital currency issued by a government. But it's been banned in the United States and been called a scam by some risk-rating agencies. To revive the struggling currency, President Nicolas Maduro has ordered Venezuelan airlines to pay for fuel in petros.[26]

UGANDA

Lookalike fake drugs result in a reported 158,000 deaths per year in sub-Saharan Africa. The government of Uganda has joined forces with healthcare startup MediConnect to track legitimate drugs along the supply chain and identify dangerous fakes.[27]

EUROPEAN UNION

The European Blockchain Partnership, established in April 2018, is building a European Blockchain Services Infrastructure. Four use cases were trialed in 2019: notarization, educational credentials, self-sovereign identity, and data sharing. New use cases will roll out in 2020.[28]

SPAIN

The Port of Valencia uses blockchain to provide security and visibility into the supply chain. A "paperless port" is the objective.[29]

SIERRA LEONE

Most citizens of Sierra Leone don't have bank accounts. San Francisco startup Kiva is using blockchain to store biometrics such as fingerprints so lenders can reliably look up residents' credit histories.[30]

THAILAND

The Thai government recently greenlighted an e-visa plan to speed up and reduce fraud in its visa on arrival service. Visitors from China and India will be the first enrolled.[31]

USE CASE: GOVERNMENT INITIATIVES CONTINUED

BRAZIL

The state of Bahia is using blockchain to track bidding on government contracts, with a focus on the agriculture industry. Bahia says more than 1,000 organizations are lined up to use the new bidding system.[32]

SINGAPORE

Singapore may be one of the first nations to tokenize its national currency. The government is also looking into blockchain to help prevent bank fraud by cargo importers and exporters. It has been implementing blockchain in many industries, including healthcare, air travel, energy, real estate, and food.[33]

USA

Among many initiatives, the U.S. Department of Homeland Security (DHS) recently awarded a grant to startup Factom to use blockchain to secure camera and sensor data at national borders. Since 2016, the DHS has been experimenting with blockchain to protect Internet of Things (IoT) devices. The Department of Defense is exploring authenticating 3-D printing via blockchain and is researching blockchain for secure troop communications, and the U.S. Army and the Department of Treasury are applying blockchain to track medical devices and track mobile devices, respectively.[34,35]

Cybersecurity professionals were much more likely to see specific use cases (67 percent) than their peers in related fields; the other groups hovered between about 25 and 30 percent. Perhaps defying expectations, cybersecurity professionals were no more likely to say that blockchain will be transformative (about 21 percent) than were professionals with combined responsibilities or business continuity/disaster management practitioners, with physical security close behind (17 percent).

GEOGRAPHICAL BREAKDOWN

Some geographical differences manifested themselves. The region that was most positive about blockchain (i.e. respondents see specific use cases for blockchain or think it will be transformative) was Europe/United Kingdom at 62 percent, followed by South America (60 percent) and Asia (59 percent). Most skeptical were respondents from the United States (41 percent) and Oceania (42 percent). Europe/UK had the most respondents say that their employer has studied or invested in blockchain (19 percent, compared to 11 percent overall).

WILL BLOCKCHAIN FULFILL ITS PROMISE?

The survey shows a dichotomy between optimistic and skeptical views about blockchain that is reflected in the literature and the interviews conducted for this research study. Blockchain has been called the new Internet. Some have said it could lead to the paperless society that we have been promised for at least three decades. Governments have rolled out ambitious plans that include everything from virtual currencies to identity authentication. LinkedIn says blockchain will be the most in-demand hard skill in the workplace in 2020, although it did not appear in the top ten in 2019.[11] It leapfrogged such buzzworthy trends as cloud computing, artificial intelligence, and UX design. Though

levels decreased in 2019, plenty of venture capital is flowing into blockchain startups. And perhaps the cultural capstone: a recent episode of *The Simpsons* included a segment in which an animated version of Jim Parsons—Sheldon Cooper from *The Big Bang Theory*—explained cryptocurrencies and blockchain.[12]

Yet blockchain weariness has set in. Gartner has been tracking blockchain's progress through its hype cycle. As of late 2019, analysts there said that blockchain was entering the "Trough of Disillusionment" after summiting the "Peak of Inflated Expectations."[13] The trough is where "interest has waned as experiments and implementations fail to deliver," according to *Hype Cycle for Blockchain Technologies*, 2019, and the technology is predicted to languish there until 2021.[14]

When will blockchain's time come then? According to Gartner Vice President of Research Avivah Litan, "By 2023, blockchain platforms will be scalable, interoperable, and will support smart contract portability and cross-chain functionality."[15]

Respondents to *Deloitte's 2019 Global Blockchain Survey* seem ambivalent, divided, or even schizophrenic about the technology. While 53 percent of respondents said that blockchain would be a top five strategic priority, 43 percent said it is overhyped.[16] And different surveys yield contrasting results. A 2019 KPMG survey revealed that 67 percent of corporations don't use blockchain,[17] but a PwC survey from a year before indicated that 84 percent of companies had at least some involvement with blockchain.[18]

Ben Rothke, senior information security specialist at New York technology firm Tapad, agrees that blockchain has been wrongly lauded as a panacea. "It's a great new technology and it has its use cases, but it's seen as a solution to every problem," he says. While Rothke sees a bright future for blockchain, it's still not ready for widespread use, he says. "There are auditing problems, implementation problems, interoperability problems," Rothke explains. "Organizations have to understand what their problems are and see how blockchain can solve them, not other way around. It's like going into a pharmacy and picking a random drug and saying how can it help me. No one in their right mind would do that."

"What I'm careful about is someone who says blockchain is the biggest thing to happen to security and it will solve all hacking problems," says Scott Klososky, a technologist and futurist. "That isn't true. It's another tool that can improve the security of information, transactions, and contracts."

USE CASE: TICKETING

Having analyzed blockchain and other technologies for years, Geoff Revill still isn't convinced that it has found a natural fit beyond cryptocurrencies. "The best use case I've seen is tickets for an event," he says. Blockchain enforces logging of subsequent transfer of tickets, which would undercut ticket "touting," or scalping. "It's a short blockchain, me and you, it's documented, traversed one more time upon entry to the venue, then never used again," he explains. No long-term issues of trusting data over time, and no heavy use of processing power.

Boston-based startup True Tickets recently announced a deal with the Shubert Organization, which owns 17 Broadway theaters, to run a pilot project of its digital ticketing software. It is designed not only to track who sits in which seat, but also to diminish fraud and tailor services to patrons. The system could also leverage dynamic pricing to ensure that, say, when a show unexpectedly becomes a hit, the venue benefits instead of the scalper.[42]

Plenty of other startups see ticketing as a lucrative niche for blockchain. They include GUTS Ticketing, Aventus Systems, Blocktix, EventChain, and EventX.

SECURITY APPLICATIONS

Inherent to blockchain, though to different extents depending on the type of blockchain, are immutability, transparency, unhackability, and decentralization. All can be considered security features in and of themselves, but blockchain

offers a host of other security benefits and, as will be discussed later, distinctive challenges.

"I'm a big proponent of blockchain for security," says Brent Barker, a cryptocurrency and blockchain security adviser for Barker Global Security. In his estimation, industry must use private (or consortium) blockchains. "Businesses don't necessarily want every Tom, Dick, and Harry to see their transactions," Barker says. He points to TradeLens, the blockchain created by Maersk and IBM to document shipping transactions (a description of that program appears on page 30). "You want people to see only certain things," he says. "You don't want Company A to see what its competitor Company B is doing."

IDENTITY MANAGEMENT

Barker views identity management, such as for travelers or refugees, as a fitting application for blockchain. In the case of travelers, a permissioned blockchain would limit organizations such as airlines and immigrations and customs officers in countries around the world to access only information necessary for them.

Myn Kyriannis, a cybersecurity and technology expert at engineering firm Jaros, Baum & Bolles, agrees that blockchain can streamline identity management. She points out that governments currently use blockchain to verify the identity of refugees. Finland, for example, provides asylum seekers with prepaid debit cards. It links the cards, as well as the refugees' identities, with a blockchain.[36]

Jordan has been deploying blockchain for those purposes as well. In that case, it's to identify dwellers in the country's refugee camps, which have been overflowing since civil war in Syria began.[37]

But identity management via blockchain applies to institutions and corporations as well. Ethereum allows users to create digital identities via decentralized identifiers, identity management, and embedded encryption. At least 33 startups sell blockchain solutions for identity management. For example, V-ID helps prevent document fraud. Object Tech enables individuals to obtain digital visas. Hub uses blockchain to identify levels of users' trustworthiness. And Vetty uses blockchain to conduct background checks.[38]

Some need more convincing that blockchain answers the identity issue. Geoff Revill, CEO of UK-based Krowdthink, has spent years assessing technology and now runs a startup that "brings the digital value proposition into a real-world security context," as he puts it.

He says that he worries about using blockchain for personal identity. "...from a privacy point of view, I get concerned about the application beyond its capability to deliver value," he says.

Lewis Werner, cofounder at Quill Security Technology, which specializes in facility protection, finds the type of reputation management promised by Hub to be one of the most intriguing facets of blockchain's identity management capabilities. "When you combine identity management with reputation, it can affect how much you believe what a person said," he notes. "You can determine a person's level of credibility based on their interaction with other people."

BATTLING CORONAVIRUS/COVID-19

Coronavirus was beginning to rampage around the world as this report was being prepared for publication, with particularly grave situations in Italy, Iran, and New York City. Chinese news agencies issued statements that officials used blockchain to help manage the fallout of that contagion. As GCN reported,

> *"Blockchain technology helped the Chinese government and medical agencies battle against the coronavirus, according to Xinhuanet, China's official news outlet. In the first two weeks of February, at least 20 blockchain-based applications were launched to tackle the emerging challenges, including health records management, securing gated communities for residents, managing relief supplies along and tracking logistics of epidemic prevention materials."*

Various other blockchain applications have emerged in response to the COVID-19 pandemic.[52]

ACCESS CONTROL

Closely related to identity management is access control: Are we letting the proper individual into the appropriate physical or virtual space at the right time and with the correct permissions?

In January 2019, a research team from the University of Saskatchewan issued a paper documenting their test of an access control application based on HyperLedger Fabric Blockchain and HyperLedger Composer. Their conclusion: "We found blockchain as an improvement for storing and managing [the] software layer of physical access control."[39]

Security consultant Steve Surfaro sees blockchain as a natural component of access control. "The obvious case is to use blockchain with permissions for a logical and physical access control system," he says. Then one could add sensors and inputs for location management, geolocation, and multifactor authentication to verify someone's permission to be in a certain location. By using artificial intelligence and security configuration management tools, Surfaro adds, an integrated access control system could learn and identify relationships between individuals and, say, parts of warehouse and shipping processes. "Access transactions would be stored securely and would leave a supreme audit trail," Surfaro says.

Although companies are developing blockchain solutions for physical and logical access control, Surfaro says, they do not always improve on the prevailing technologies. "They aren't necessarily doing it in an agile or scalable way. You have to prove it's better than other methods."

Masseh Tahiry, a technology strategist at Toffler Associates, is not yet witnessing any significant move to blockchain-based access control. "I haven't seen a macro application or enterprisewide deployment, something like, 'we've done away with our identity management system and are replacing it with a blockchain solution' that perhaps tokenizes each person's identity," Tahiry says. "It hasn't happened yet."

Some products are emerging, however. A solution by Russia-based REMME uses blockchain to replace solutions based on public key infrastructure.[40] Everledger deploys an IBM blockchain product to control virtual access to its diamond certification system.[41]

INTERNET OF THINGS

Enhanced authentication and data management offered by blockchain makes its application to secure the Internet of Things (IoT) and the Industrial Internet of Things (IIoT) attractive. The key to the effective functioning of the IoT and IIOT is the transfer of massive amounts of data in almost real time—which requires edge devices.

Blockchain expert Brent Barker sees blockchain as an effective way of confirming that an IoT sensor records reliable, specific data from, say, a power plant. If AI is used, he says, blockchain could solve the issue that AI is a "black box—information is sent in, no one knows what happens, and a decision emerges," he says. "Maybe you can confirm the validity of a decision if you can confirm the data that came into the system via blockchain," he adds. "The AI receives data from IoT sensors that is secured on blockchain to confirm and verify the information."

A 2019 article by Stevan Mcgrath in *Hackernoon* posits two possibilities for using blockchain to protect the IoT. In one case, "a company integrates its connected devices to get and transmit data, then it connects them to a blockchain network." This enables smart devices "to exchange messages, make orders, and complete transactions. In the second, Mcgrath writes, "Ethereum smart contracts are implemented by a company in order to automate the process. This will provide seamless and safe exchanges of messages between connected devices, just as it is in blockchain-based financial transactions."[43]

Indeed, blockchain for IoT protection has progressed from the theoretical to the actual. The U.S. Air Force, for example, recently awarded Xage Security a contract to protect the many physical devices used in its network—from the server room to the battlefield.[44]

Xage is also working with San Jose, California-based ABB Wireless, a network technology provider, to secure edge devices at power utility substations. According to Vish Ganpati, a cofounder of the Global Security Risk Management Alliance, "A blockchain app allows field workers to log into any device, even if the substation is disconnected from a utility's central data center due to an accident, such as a wildfire." [45]

However, a blog post by Arnab Chattopadhyay of Sogeti UK, a provider of digital transformation

services, makes a crucial observation that may limit the effectiveness of blockchain in these kinds of applications. As previously mentioned, the IoT relies on the movement of massive amounts of data in real time. Chattopadhyay writes: "Strong cryptographic processes introduce latency. The latencies are not acceptable in a near-time and real time service situation. Hence, the blockchain is not best suited in a recording of raw data at the source."[46]

The author does present a solution—introducing an "aggregating caching node" near the sources that "can be used as a broker between source and blockchain services." But, he adds, "this will be a deviation from the key strength of blockchain and must be used after careful consideration."[47]

Whether or not blockchain is best suited for raw data at the source, companies are combining them in a big way, according to Gartner. A December 2019 Gartner survey showed that 75 percent of U.S. IoT technology adopters have already adopted blockchain or plan to by the "close of 2020. Two-thirds of those doing so cited "increased security and trust" as either a primary or secondary driver, with more than half also citing increased efficiency and lower costs.[48]

According to the survey, IoT implementers adopt blockchain most frequently in pharmaceuticals, energy, natural resources, and transportation—all sectors that involve transport of goods.[49] In addition, the forecaster Research and Markets projects that the global market for blockchain use for the IoT will balloon from $37 million in 2018 to $9 billion in 2027, which calculates to a whopping 60.6 percent compound annual growth rate.[50]

VIDEO

More experimental at this point is blockchain use to verify video integrity and chain of custody. Research has begun, for example, on using blockchain to counter "deepfakes," the use of AI to create or manipulate convincing video and audio to present something that didn't actually occur. "There are lots of challenges to successfully doing this," says Peter Tan, a security consultant and lecturer at Temasek Polytechnic in Singapore. "You have to ascertain the source of the video, yet there are so many sources of video out there. But you can put in a hashing algorithm [which works in a way like email authentication] to verify if a video has been changed."

At the forefront are Amber Authenticate and the Media Forensics Program of the Pentagon's Defense Advanced Research Projects Agency (DARPA). According to a 2 November 2019 article in *Wired,* Amber Authenticate generates hashes "that then get indelibly recorded on a public blockchain. If you run that same snippet of video footage through the algorithm again, the hashes will be different if anything has changed in the file's audio or video data—tipping you off to possible manipulation."[53]

DARPA has been testing blockchain technologies for the same end. According to a statement by Dr. Matt Turek of DARPA's Media Forensics (MediFor) Program, "If successful, the MediFor platform will automatically detect manipulations, provide detailed information about how these manipulations were performed, and reason about the overall integrity of visual media to facilitate decisions regarding the use of any questionable image or video."[54]

USE CASE: COPYRIGHT PROTECTION

Many companies and organizations are working on blockchain solutions to protect copyrights in films, television programs, books, cartoons, music, photographs, and so on. The nonprofit Content Blockchain Initiative, for example, is working on standards for content identification, licensing, and attribution.

Using the Ethereum platform, the startup OPUS is targeting the music royalty quagmire. Custos Media targets pirates and leakers of video and other media.[59]

In late 2019, the Italian Society of Authors and Publishers (SIAE) announced it will use the blockchain-based Algorand network for copyright management.[60] And in China, the Hangzhou Internet Court receives uploaded evidence of copyright infringement of written works on a blockchain platform. As of late 2019, that platform had already received 2.1 billion pieces of data.[61]

USE CASE: CRYPTOASSETS/STORES OF VALUE

Cryptocurrency is only a legitimate application if it's a viable store of value. People assign value to fiat currencies—of which there are fewer than 200—because regulations underpin them. In the United States, the Federal Deposit Insurance Corporation backstops the greenback, and the Internal Revenue Service likewise requires taxpayers to deal in U.S. dollars.

Cryptocurrency is only one type of cryptoasset. Others include utility tokens (Golem, for example), platform tokens (such as EOS), and tokenized securities. While no one is sure whether cryptocurrency has a robust future, many people consider it to represent a reasonably stable store of value. Despite wild fluctuations on the exchanges, Bitcoin is still a viable investment at the time of this writing. Says Christian Auty, an attorney with Bryan Cave Leighton Paisner who specializes in blockchain and fintech, "Bitcoin, inasmuch as it is a store of value, is the only true use case because I can buy it and I can sell it." Time will tell whether the public will decide that cryptocurrency is too ephemeral and unsupported to have value, but that moment doesn't seem imminent.

Scott Klososky is a fan of cryptoassets, via Initial Coin Offerings (ICOs) or Security Token Offerings (STOs). As explained in a November 2018 article in Deloitte's *Inside* magazine, "An STO can be used to create a digital representation—a security token—of an asset, meaning that a security token can represent a share in a company, ownership of a piece of real estate, or participation in an investment fund. These security tokens can then be traded on a secondary market."[63]

Dina Ellis Rochkind, a fintech and cryptocurrency lobbyist, adds that cryptoassets "unlock equity in things that are hard to fractionalize, like wine collections, art collections, and patents."

"If I want to sell my land and don't want to borrow against it, I can create my own cryptoasset on the market," Klososky explains. "I see a real future in that—getting value out of an asset without forming a corporation, creating shares, and selling them to the public."

EWitness has also joined the cause. The company, which is currently testing its product, says that its "system consists of a smart-phone application that computes robust hash of pictures or videos taken from a phone camera, a local attestation service, and a public blockchain which contains ledger entries to preserve the evidence file's hash and location certificate."[55]

A 72-page report by WITNESS Media Lab, an organization that curates citizen videos of abuse from around the world, discusses the pros and cons of using blockchain to prevent and detect deepfakes. Among the questions they pose for blockchain applications are:

Do you really need a blockchain? Could timestamps be delivered at a fraction of the cost by a company like Google? Could you use PGP signing (encryption) of images in order to generate proofs that live off the blockchain?

Are you considering a permissioned chain? What benefits are you gaining by running a chain instead of merely having a consortium-run, distributed database with time-stamping provided by Google or another nonchain service and, potentially, PGP signing of data?

Do you have a strategy for how your tool will be able to evolve with the blockchain that you're working with? How will you accommodate the subsequent infrastructure changes?[56]

In fact, these are excellent questions for any blockchain application.

PRIVATE MESSAGING

Private messaging services frequently deploy

end-to-end encryption. Via its decentralized nature, blockchain offers a valuable alternative. Because data is held in nodes across the network, messages are harder to intercept.

A company called Obsidian released an alpha version of its public-blockchain-based Secure Messenger tool in December 2018, when it became available in the Google Play Store. The platform is powered by its own cryptocurrency, Obsidian Coin. Other startups in the field include SENSE, BeeChat, Dust, Crypviser, and Sylo.

DISTRIBUTED STORAGE

Cloud storage may have a new competitor. Several startups have focused on safely storing transactions on the blockchain.

Stacey Peterson of *SearchStorage* explains how blockchain storage works:

> *A blockchain-based storage system prepares data for storage by creating data shards or segments, encrypting the shards, generating a unique hash for each shard, and creating redundant copies of each shard. The replicated shards are then distributed across the decentralized nodes in the blockchain infrastructure. The transactions are recorded in the blockchain ledger, and the system validates and synchronizes the transactions across the nodes in the blockchain.*[57]

Blockchain storage can be cheaper than cloud storage, plus it offers additional transparency and availability.

Not so fast, says writer Natalya Dyatko. Most startups use the public Ethereum blockchain and its ERC20 token standard, she says. She calculates that storing a single 1-megabyte insurance policy on one of these systems would cost a staggering $747.52. And it would take 14 minutes to save, she adds. A better solution would be a permissioned blockchain, though that exposes the system to a greater threat of hacking.[58]

DNS

The Internet's Domain Name System (DNS) has been called the Internet's phonebook, linking domain names with their IP addresses. It is a prime target for hackers, who can take down websites, create fraudulent websites, and so on. Blockchain's decentralized approach makes it harder for hackers to identify single points of vulnerability.

Among efforts trying to decentralize the DNS is Handshake (an Ethereum protocol that uses its own coin for name registration), Blockstack (based on Bitcoin), and Ethereum Name Service.

USE CASE: CONFLICT MINERALS

Charles Dumbrille is based in Vancouver, where about two-thirds of mining companies in the world are listed in the local stock exchange, making that city a major mining entrepot. Mining companies there are concerned about "conflict minerals," says Dumbrille, who is president of the Mining Security Working Group and Chief Risk Officer of IN-D-TEL International. Conflict, he explains, can designate minerals acquired through exploitation and trade associated with significant adverse impacts, such as organized crime, slave labor, militant activity, or other human rights abuses.

Companies such as BMW have pledged to adhere to ethical practices.[67] To assist in that effort, blockchain startups have sprung to life to ensure responsible sourcing of precious minerals such as titanium, tin, and tungsten. MineSpider attaches digitally encrypted certificates to specific amounts of minerals in the supply chain.[68] Similarly, Lucara Diamond acquired blockchain-provider Clara Diamond Solutions to ensure provenance, integrity, and transparency of its precious stones.[69]

De Beers is using the Tracr system to monitor diamonds on their journey from mine to consumer. The system registers both a diamond's physical attributes—such as karat, cut, color, and clarity—and metadata.[70]

SMART CONTRACTS

Smart contracts, sometimes referred to as Blockchain 2.0, constitute one of the most popular features of blockchains. Technology advisor Mayank Pratap, who defines smart contracts as "automatically executable lines of code that are stored on a blockchain which contain predetermined rules," provides a good overview in *Hackernoon:*

> *A smart contract is a set of computer code between two or more parties that [runs] on the top of a blockchain and [consists] of a set of rules which are agreed upon by the involved parties. Upon execution, if these...pre-defined rules are met, the smart contract executes itself to produce the output. This piece of code allows decentralized automation by facilitating, verifying, and enforcing the conditions of an underlying agreement. Smart contracts allow you to exchange anything of value including money, shares, property, etc., in a transparent manner eliminating the need for a middleman and keeping the system conflict-free.*[62]

No lawyers, no notaries, no professional fees.

Futurist Scott Klososky and Quill's Lewis Werner believe that smart contracts are among the most viable features of blockchain, especially when a contract involves intellectual property or code. "With untrusted third-party work, it's a way that encryption is both compensation and product," Werner says. In other words, by fulfilling a smart contract, an individual automatically gets paid. Fulfillment and payment are linked.

Things are trickier with contracts for items or actions in the physical world, because an action to fulfill a contract in the real world does not automatically trigger fulfillment of the smart contract. That's an extra step, and one that doesn't prove that the terms of the contract were truly fulfilled.

Others take a dimmer view of smart contracts. "A smart contract is neither smart nor a contract," says Andre De Castro, CEO of the Blockchain of Things. "It's an if-then condition on conditionally receiving and releasing Ether [from the Ethereum blockchain]." He notes a litany of problems with smart contracts, including, what recourse you have if you are not paid, and whether the contract is enforceable.

TRUST

In an interview with McKinsey & Company, Don Tapscott, cofounder of the Blockchain Research Institute, elegantly laid out the argument for trust embedded in the fabric of blockchain:

> *This is a platform for truth and it's a platform for trust. The implications are staggering, not just for the financial-services industry but also right across virtually every aspect of society. Most blockchains—and Bitcoin is the biggest—are what you call permission-less systems. We can do transactions and satisfy each other's economic needs without knowing who the other party is and independent from central authorities.... But to me, the blockchain, the underlying technology, is the biggest innovation in computer science—the idea of a distributed database where trust is established through mass collaboration and clever code rather than through a powerful institution that does the authentication and the settlement.*

SECURITY CHALLENGES

For all the promise—and fulfilled promise—offered by blockchain, the technology can't escape security weaknesses that are either inherent to it or sneak up alongside. In February 2020, the Depository Trust & Clearing Corporation (DTCC) issued a report on security for DLTs in the financial industry. The document compiles 15 categories of threats to DLTs and blockchains, offering "high-level insight into the most commonly researched and utilized security considerations."[65]

Another source of insight is a presentation by Kurt Callewaert of Howest University developed for the 2020 RSA Conference (though not presented). It explores threats and vulnerabilities such as consensus mechanism vulnerabilities, including Vector 76 attacks, and membership services vulnerabilities, including Sybil attacks.[66]

Some of the threats and vulnerabilities discussed by DTCC and Callewaert are among the ones discussed below.

USE CASE: CORPORATE CURRENCY

Corporations printing their own currency? It sounds antithetical to modern society. But the practice has deep antecedents and is still common today.

"Historically, the Dutch East India Company [1602-1799] and the Hudson Bay Company [1820-1870] had charters to coin or print money," observes lecturer and blockchain aficionado Samson Williams.

During the Free Banking Era in the United States, between 1837 and 1866, private railroads, retailers, churches, engineering firms, restaurants, insurance companies, banks, and even private individuals could print and issue their own currency. Up to 8,000 different types were in circulation up to 1860.

During this time, coal mining and logging companies often paid employees in scrip, which they could use only in company-owned stores. The system persisted, due to the lack of U.S. currency in remote areas, until the early 1950s.

Many Americans remember collecting S&H green stamps and dutifully pasting them into special booklets so they could be redeemed—yet another type of corporate currency.

Today, corporate currency takes the form of gift cards, gift certificates, and private money such as Disney Dollars. We may be well be entering the corporate cryptocurrency age. Facebook plans to introduce its own permissioned blockchain-based digital currency, called Libra, in 2020. Regulators from around the world have put those plans into question, however; France, for instance, has declared that only governments can mint money, and the United Kingdom has warned that it will hold Libra to high financial standards. In late December 2019, Switzerland rejected Libra in its then-current form. And at least eight companies have withdrawn from a Libra consortium, including PayPal, Visa, eBay, and Vodafone.

Samson Williams condones the pushback against Libra, but for a different reason. "It's giving a company the right to print money without taking on any social responsibility," he contends. "A dictator who might not be able to get a loan from the World Bank would be able to get a loan from a cryptocurrency like Libra."

Cointelegraph reports that other organizations are lining up to develop cryptocurrencies of their own, including AirAsia, Google, and Walmart.[73]

Though Amazon hasn't confirmed any plans, many industry analysts believe that the online retail behemoth will be announcing its own cryptocurrency. It would be a shrewd move for the company, Williams says. "Amazon might say, we will give you four tokens for a dollar, with each token worth a dollar of Amazon goods," he postulates. "People will flock to it for the 75 percent discount. Amazon won't care because it will have created, say, 100 million new users. They may lose $750 million in the short term but they have the lifetime value of those new customers."

TRUST

Yes, trust is included as a security advantage of blockchain. It's also an inherent weakness.

Trust is the metaphysical elephant in the virtual room called blockchain. One of the cherished features of an open blockchain is that it alleviates the need to have a monitor at the door. The technology enforces trust. Discussing public blockchains on his blog, cryptographer and cybersecurity guru Bruce Schneier pointedly presents the problem with this approach:

> *What blockchain does is shift some of the trust in people and institutions to trust in technology. You need to trust the cryptography, the protocols, the software, the computers, and the network. And you need to trust them absolutely, because they're often single points of failure.*
>
> *When that trust turns out to be misplaced,*

USE CASE: LEGAL PRIVILEGE

Both the Dutch Public Prosecution Service and the Netherlands State Secretary of Finance have advocated for narrowing attorney-client privilege. That privilege, explains e-discovery and cyber forensic expert Bas Sluijsmans, applies more narrowly than it does in the United States and various other jurisdictions. Questions surround whether it applies when lawyers are involved in transactions and related services.

Enter blockchain. Sluijsmans asked the Ministry of Justice and the Dutch Bar to create a database containing historical information on who has ever held legal privilege as an attorney or part of a firm. "We want to design a register that is available to view and is trackable and traceable," he says. "It would enable everyone to determine whether a certain communication would fall under attorney-client privilege." Only attorneys would be included on the blockchain. Clients and law enforcement could check to see which attorneys are covered.

Sluijsmans says that the biggest concern is criminal evidence. "Authorities might collect a digital mailbox that they can't search unless the privilege is waived," he says. And in antitrust investigations, a firm can make a claim on privileged information within five working days. "Having a list of law firms that can claim privilege on information collected by authorities is a big advantage," he says.

The next question to be addressed is the type of blockchain to use—public or permissioned. Anyone can enter information on an open blockchain, which taints its reliability. Sluijsmans says that attorneys are looking to the Dutch Bar to govern the system.

there is no recourse. If your bitcoin exchange gets hacked, you lose all of your money. If your bitcoin wallet gets hacked, you lose all of your money. If you forget your login credentials, you lose all of your money. If there's a bug in the code of your smart contract, you lose all of your money. If someone successfully hacks the blockchain security, you lose all of your money. In many ways, trusting technology is harder than trusting people. Would you rather trust a human legal system or the details of some computer code you don't have the expertise to audit?

Blockchain enthusiasts point to more traditional forms of trust—bank processing fees, for example—as expensive. But blockchain trust is also costly; the cost is just hidden. For bitcoin, that's the cost of the additional bitcoin mined, the transaction fees, and the enormous environmental waste. Blockchain doesn't eliminate the need to trust human institutions. There will always be a big gap that can't be addressed by technology alone. People still need to be in charge, and there is always a need for governance outside the system.[71] [Underlines removed from original]

Geoff Revill, CEO of Krowdthink, agrees. "My biggest concern is that the climate of trust it promises to convey is way beyond its capacity to deliver," he says.

Jimmy Song, a lecturer at the University of Texas and a Bitcoin Fellow at Blockchain Capital, questions whether you can trust blockchain to digitally verify a physical transaction. "Like anything in the real world, like real estate or a shoe, when you put it into a database there's no guarantee that the data is correct about the item in the real world," he contends. "You can't force these things to be the same. Most solutions are trying to solve metaphysical problems with technological tools," he adds. "You can't prove a shoe was produced in China. You can only have mere attestation."

That argument closely resembles the criticism of smart contracts documenting real world transactions. Song concedes, however, that blockchain can accurately verify "digitally native assets that are part of that particular blockchain. It has to be a native token to that blockchain because it knows the accounting."

At the February 2020 RSA Conference in San Francisco, a presentation by Charles Kaufman and Radia Perlman of Dell EMC questioned whether blockchain constitutes the best approach to distributed trust. Kaufman and Perlman argued that there are other methods of providing distributed trust that are far more effective and efficient than blockchain—and don't expend massive amounts of computing power. For example, they favor "Shamir's secret sharing," a cryptographic algorithm in which a secret is split into multiple parts and distributed to multiple parties. To reconstruct the secret, either all of the parts or a certain number of parts must be provided. "This technology is simple and efficient," they said in their presentation, "and forms the basis of many schemes that want to guard against some subset of participants being flaky."[72]

By contrast, Gerard Dache, CEO of the Government Blockchain Association, might subscribe to the credo of "In Public Blockchain We Trust." According to Dache, blockchain gets its power because "you don't need a trust intermediary. It's a feature of the technology." Just like the job of pumping gas at service stations has largely been phased out, blockchain makes the middleman unnecessary, he says. "It's a more efficient way of doing things."

USE CASE: ART PROVENANCE

Tracing the provenance of art can be a murky business, perhaps to include slogging through histories of raided antiquities and Nazi confiscation, finding elusive or hidden documents, tracking down forgers' workshops, or squinting at faint marks under special lamps.

Blockchain can establish a secure digital ledger for art provenance and make "art ownership more transparent and fair," according to Peter Langela, CEO of Fluidensity, who exhibited his company at the 2020 Consumer Electronics Show. Fluidensity is one of several startups aiming to convert art ownership into digital certificates; others include FRESCO, Artory, Verisart, and the Blockchain Art Directive.

DECENTRALIZATION/LACK OF GOVERNANCE

Another of blockchain's biggest strengths—its decentralized nature and lack of governance—can be considered a significant weakness. Being distributed throughout many nodes, data on blockchain is difficult to hack, manipulate, or corrupt.

Yet who's in charge when everyone is in charge? That prospect troubles many experts. Scott Klososky believes that public blockchains must be overseen by some entity. "Someone has to have created the rules," he says. "If anything goes wrong, someone is going to have to branch the blockchain, like with Ethereum."

Klososky is referring to instances when blockchains have had to figuratively pull the emergency brake and shut everything down, then create a brand-new ledger that exists side by side with the previous version. That is called a "hard fork." As described by *Cointelegraph,* "After a hard fork, the previous version and the new one are completely split, there is no communication or transaction option between the two. Usually, the new version inherits all the historic transactions and, from now on, each version will have its own transaction history."[74] Hard forks, which require drastic changes to the blockchain's protocol code, typically occur to reverse fraudulent or invalid transactions or to fix holes in the earlier protocol.

Min Kyriannis believes that for blockchain to become mainstream, a governance model has to exist. "I think there will be a blockchain regulatory scheme," she says. "But it won't be a country. It has to be a collaborative effort across different nations and businesses. Someone has to back it to make people comfortable using blockchain." When regulation falls into place, big institutions will follow, Kyriannis predicts.

The flip side of the contention that someone has to be in charge is the argument that public blockchains aren't really distributed and decentralized; there is often a secret hand involved. Says Geoff Revill, "I've yet to see the business model that doesn't insert a management agency between the user and the service. You end up with a platform that claims to be distributed and secure but is managed with techniques that are no different than any other platform."

USE CASE: FOOD

Begun in 2017 with 11 founding members, the IBM Food Trust digitizes transactions on every link of the food chain for its now 200-plus members, from growers to retailers. A lettuce leaf or wild scallops, for example, can be traced virtually from farm to table, documenting information such as holding temperatures, shipping dates, and certifications.

According to Offering Director Suzanne Livingston, the Food Trust uses a permissioned HyperLedger blockchain. To get buy-in from major companies such as Carrefour and Walmart, IBM assured potential partners that it does not own the data on the system. That decision eliminated issues over competition and trade secret protection. "That's probably the number one reason this works," Livingston says. "Because we don't own the data."

Participants can only view certain transactions, she explains. For example, Carrefour can't see what Walmart is buying from a certain apple farm.

What if there's a discrepancy between the record and an actual shipment? "We ask the parties to resolve their differences," Livingston responds. IBM doesn't change the ledger. "A company might send an auditor who can then upload documents to blockchain to support their hypothesis," she continues, "but more often they talk to each other and resolve it."

Most surprising to Livingston is the number of transactional mistakes that happen naturally but don't get resolved. "The issue is lack of communication," she says. But, she adds, "We've accomplished our goal of growing a food ecosystem in an industry that didn't want to share."

SOFTWARE VULNERABILITIES

Blockchains may be extremely difficult to hack, but there are plenty of associated attack vectors.

In a paper titled "A Survey of Blockchain from Security Perspective," Dipankar Dasgupta, John M. Shrein, and Kishor Datta Gupta highlight specific security threats—some actual, some still theoretical—to blockchain. The authors identify more than 20 attack vectors, including cryptographic key vulnerabilities, hashing operation vulnerabilities, identity vulnerabilities, manipulation-based attacks, quantum vulnerability, reputation-based attacks, vulnerability-in-service attacks, malware attacks, and application vulnerabilities.[75]

All of these intrusions are plausible, says Samson Williams. "In any technical system, however, the weakest link is the human," he says. "It's easier to socially engineer than to use technical attacks. Blockchain doesn't really get hacked; it's on the on-ramps, the APIs.

The odds of successfully hacking into a public blockchain are infinitesimally small. The soft underbelly is the intermediaries, Williams says. Software flaws, social engineering, and malware all contribute to these vulnerabilities.

Williams' opinion is borne out by the aforementioned blockchain security paper. "By far the weakest link in blockchain security so far is the result of third-party applications that either run on or interact with the blockchain," write the authors, such as exchanges, wallets, and decentralized apps.[76] Hot wallets (which are connected to the Internet, as opposed to cold wallets) have been particularly targeted on cryptocurrency exchanges. A 2014 attack netted 850,000 Bitcoins by accessing the private keys stored in a wallet accessible over the Internet, and a 2016 attack yielded 120,000 Bitcoins by targeting a vulnerability in multisignature wallets (wallets requiring multiple parties to sign transactions involving that wallet).[77]

Through the first half of 2019, seven cryptocurrency exchanges had been victimized by large-scale hacks. Gatehub reported a loss of $10 million worth of tokens via accessing a database holding user tokens. About 90 Bitrue users lost a collective $5 million when hackers accessed

their hot wallets. And the hot wallets of 55,000 Bitpoint users were hacked in July to the tune of $19 million.[78]

Perhaps the most well-known vulnerability comes via a 51% attack. That occurs when some person or group obtains the majority of the mining power on blockchain, preventing others from reversing transactions. Someone pulling this off can double spend their coins or prevent the confirmation of transactions. Bitcoin Cash (May 2019), Ethereum Classic (January 2019), Vertcoin (December 2018), Verge (April 2018), and Bitcoin Gold (January 2020 and May 2018) have been among the victims.[79]

Eddie Schwartz, CSO of block.one—which both develops blockchain software and invests in blockchain projects—taps storage of keys as blockchain's biggest vulnerability. "If someone accesses your key, they can get your information and trade it," he says. "The big question is how keys are stored and managed," he continues, adding that they are typically stored in a virtual wallet or written down. "For blockchain to be truly adopted, people need to know the opsec around it, like they do for passwords. They need to treat keys like critical assets."

IT security expert Ben Rothke agrees. "People focus on the 'bulletproof-ness' of blockchain, which is the mathematics," he says. "No one will try to crack the crypto—that's too hard—but how it is implemented," such as how keys and data are shared.

Wired calculated that the odds of correctly guessing an Ethereum private key is 1 in 115 quattuorvigintillion, or 1 in 2 to the 256th power.[80] Yet hackers have successfully used brute force attacks to burglarize blockchains via software errors or poor key-creating practices. An account called the Blockchain Bandit defied the imposing odds and stole more than 45,000 ether from Ethereum. As explained by James McDowell, a senior securities analyst at the Alabama Securities Commission,

> *By creating user wallets with identical private keys, the 'Blockchain Bandit' was able to misappropriate victim funds. It appears fraudsters, such as the "Blockchain Bandit," could generate lists of weak private keys by breaking the 256-bit private key into eight separate 32-bit subsections. Then, one could scan and run them in parallel to increase the speed. By breaking the key into smaller bits and running them in parallel, [a hacker could] generate roughly 34.3 billion keys in an 8-hour period. [They] could then use automated processing to scan the blockchain and steal cryptocurrencies from these weak keys within milliseconds of the generation of accounts with the same, weak private key.*[81]

The cause of such weak keys could be as simple as coding errors by wallet developers or allowing novice users to generate their own keys. The Blockchain Bandit illustrates the importance for developers to audit their code and correct issues. Additionally, it reinforces the importance of investor's conducting due diligence prior to participating in the cryptocurrency market and serves as a cautionary tale for newcomers who may want to create their own private keys.

AGING ENCRYPTION

Encryption is a bastion of blockchain security. But not if it isn't regularly updated, says Geoff Revill. "What is the methodology to update the encryption?" he asks. "No one has a good answer."

His concern: while blockchain encryption can't be defeated today, that day will come. "Time always breaks encryption," he says. For example, a nation-state may acquire quantum computing abilities, which are expected to make child's play out of today's cryptographic algorithms. "How will it be upgraded by then? Blockchains are distributed; what's the method to update the encryption on all the links without risking the security it's meant to embody? It may not be possible."

The U.S. National Institute for Standards and Technology has been addressing this very issue in its Post-Quantum Cryptography Standardization project, where it has winnowed 82 candidates to 26 contender algorithms to withstand tomorrow's attacks.[82] Microsoft, Google, and many other companies likewise are working on the issue. In fact, in February 2020, Texas-based Futurex announced a hybrid solution that combines conventional cryptographic methods with a post-quantum security solution.[83]

PRIVATE BLOCKCHAIN MANIPULATION

By definition, blockchain is decentralized. But that's not the case when a single organization manages a private blockchain. In a report on

USE CASE: GLOBAL TRADE

Begun by Maersk and IBM, TradeLens describes itself as "a global supply-chain ecosystem made up of shippers, freight forwarders, ports and terminals, ocean carriers, intermodal operators, government authorities, customs brokers, and more." Major ports or terminals integrated into the system are in Long Beach (California), Mumbai, Hong Kong, Singapore, Buenos Aires, and Sydney. Each party has access only to their information as well as a secure audit trail of their transactions.

TradeLens struggled early on due to concerns of prospective members about sharing sensitive information with competitors and about IBM and Maersk running the program, but in recent months the membership has soared, picking up 100 new entrants. The initiative still faces regulatory hurdles, however. For example, the U.S. Federal Maritime Commission must approve the collaboration due to potential anti-competitive effect. However, in February 2020, that commission granted an antitrust exemption to five of its U.S.-based members, allowing them to share information.[94]

private blockchains, Moody's wrote that private or centralized blockchains are more exposed to fraud risk because their system design and administration remain concentrated with one or few parties.[84]

The report also weighs in on business continuity ramifications. It says that risk will be mitigated by decentralized ledger structures that facilitate data recovery while preserving a comprehensive audit trail. However, the number of gateways for attacks increases and the blockchain application will frequently shorten process execution times (payments).[85]

GENERAL CHALLENGES

With the exception of major projects such as the IBM Food Trust and TradeLens, many of the foregoing applications are pilot projects, tests, proofs of concept, or startup initiatives. Will they go into mainstream use?

It's questionable, at least in the short run. In 2019, Deloitte observed a drop in the number of organizations that have already initiated a blockchain deployment compared to the year before—from 34 percent to 23 percent.[86]

Roger Shepherd describes attending a presentation by a blockchain expert who ran corporate research for financial institutions. The presenter said there were a lot of proof-of-concept trials that were successful, but none were pursued. "The follow up is really telling you whether the trial was successful or not," he says.

Reasons include regulatory uncertainty, negative associations, a lack of a compelling reason to adopt blockchain, the availability of better alternatives, the cost and burden of a system overhaul/implementation concerns, data migration issues, interoperability issues, vast computing power expenditure, and the "trash in, trash out" factor.

REGULATORY UNCERTAINTY

Governments are split on their views of blockchain and cryptocurrencies. Some are at the forefront of blockchain use, others are slamming on the brakes, while still others are trying to sort things out. A 2020 article for the World Economic Forum puts it this way:

> *Regulation represents by far the most significant hurdle for blockchain innovators, according to a survey of hundreds of executives and entrepreneurs, co-conducted by the Chamber of Digital Commerce Canada and the Blockchain Research Institute. Existing regulations favor incumbents over disruptors. Blockchain presents new challenges to regulators looking to protect consumers and markets, but the rigidity with which regulators in the world's major economies have approached blockchain has served to stifle innovation and growth.*[87]

NEGATIVE ASSOCIATIONS

In the public mind, cryptocurrency is often associated with money laundering, criminal enterprises, and terrorist financing. Hamas, al Qaeda, ISIS, and many other terrorist groups accept Bitcoin donations. An October 2019 article in the *National Law Review* predicted that "cryptocurrency use to fund terrorism and crime will increase over time as adoption in general increases and technology enables easier access unless regulations continue to be put into place."[88] And the Swiss Financial Market Supervisory Authority has linked blockchain use to increased risk of money laundering.[89]

However, Samson Williams says that the risk of money laundering through cryptocurrencies is exaggerated. "It's easy to figure out who conducted a transaction," he says. "Cryptocurrency leaves a digital footprint."

NO COMPELLING CASE

Experts interviewed for this research often mentioned that blockchain hasn't yet become indispensable, just a "nice to have." Because of its technical nature and its confusion with cryptocurrencies, it puts some people off.

BETTER ALTERNATIVES

Many critics assert that blockchain often is no better than a standard database—which is much cheaper, quicker, and easier to use. Andre De Castro of the Blockchain of Things says using a permissioned blockchain "makes no sense. Just use a database."

ANTITRUST IMPLICATIONS

Competing organizations that partner in a consortium-based blockchain risk running afoul of antitrust laws. Specifically, antitrust law prevents organizations from working together to fix prices or eliminate competition. Sharing price, cost, or output information, for example, could draw scrutiny, as could restricting membership. According to attorney Sergei Zavlasky, the following factors help determine the risk of an antitrust violation:

- The more indispensable access to the blockchain is to the rivals' ability to compete, the higher the risk.
- Existence of a legitimate business reason for excluding certain competitors reduces risk.
- Independent action by a company carries far less risk than an agreement between competitors to exclude a common rival.
- For a company acting independently, risk rises if the company is a monopolist (or has a reasonable shot of becoming one) and the exclusion of a rival is a break from prior course of dealing.[90]

The U.S. Maritime Commission recently granted an antitrust exemption to five U.S.-based companies participating in TradeLens, the IBM-Maersk global shipping blockchain[91] (see page 31).

IMPLEMENTATION ISSUES

Deloitte's 2019 blockchain survey found that the most frequently cited barrier to investment in blockchain was implementation.[92] "To build your whole application on blockchain is too expensive," says Dustin Laun, CEO and CTO of Mobohubb, which makes software for security officer reporting and other uses. He recommends a blended model, meaning building an application with a very specific use of blockchain and the rest with traditional tools.

"I've been an adviser to CIOs," Laun says. "Most people don't have teams to keep up with the speed of technology." In fact, 28 percent of respondents to the 2019 Deloitte survey cited lack of in-house capabilities as operational barriers to adopting blockchain.[93] "The change management is very hard to do," Laun continues. "Until you sort that out, those cool technologies will be used by 10 percent of organizations and everyone else will be 8 to 10 years behind."

DATA MIGRATION CONCERNS

Massive data migration requirements also pose a significant obstacle. Imagine CVS and Cardinal Health overhauling how they receive doctors' prescriptions, posits blockchain attorney Christian Auty. "Electronic health records are huge. To move the pharmaceutical industry to blockchain, you would need a federal mandate."

INTEROPERABILITY HURDLES

Interoperability is another issue, according to Ben Rothke, especially with the public sector. "The federal government has mainframe applications that are over 40 years old," he points out.

ENORMOUS POWER USE

And then there is energy expenditure. Public blockchains burn massive amounts of power—anathema in an age of sustainability. "Blockchain causes horrendous amounts of energy consumption," emphasizes Geoff Revill. He points out that Internet and digital services are responsible for 3 percent of global emissions today, a number that is expected to balloon to 21 percent in 10 years. "These algorithms have a societal impact."

THE TRASH IN, TRASH OUT FACTOR

Next, there's the "trash in, trash out" problem that comes with immutability. "Blockchain only shows the transaction, not the quality of the transaction," says Brent Barker. Masseh Tahiry agrees: "If we put trash in the system, we will have secure trash—let alone the downside of intentionally inserting trash, false, or malicious information within a blockchain, which is a serious problem."

RECOMMENDATIONS

It is clear that blockchain offers tremendous possibilities. But adopters should proceed cautiously. We present the following recommendations for security professionals involved in developing, using, or partnering on a blockchain application.[95]

- Don't try to force-fit blockchain into your application. While blockchain is a powerful technology, it adds costs, latency, and complexity in many situations.
- Determine whether your organization or application truly needs a blockchain solution. What is your application?
- Be able to make the business case for blockchain implementation.
- Check whether other organizations have tested use cases similar to yours, evaluate the results, and determine how they fit your situation.
- Determine whether you need one or more of the following blockchain advantages.
  - Are you trying to remove intermediaries or brokers?
  - Do you need immutability, decentralization, traceability, and transparency?
  - Do you wish to issue tokens or corporate currency?
  - Are smart contracts a priority?
- Determine whether blockchain will fit with your current IT architecture or a systems overhaul will be necessary.
- Ensure that your technical team has a strong background with blockchain.
- Consider working with industry partners that have experience with blockchain.
- Beware using blockchain with physical assets. There is no guarantee that a blockchain transaction accurately represents a physical transaction. Digital-only assets are a better case for blockchain.
- For uses requiring lightning-fast processing, there may be more cost-effective options than blockchain.
- If blockchain is the best solution for you, determine what type of blockchain is best—public, permissioned, hybrid, or consortium-based. Consider factors such as:
  - The need for decentralization
  - Power and cost considerations
  - The size of the universe that will use the system
  - The level of trust in the users
  - The alignment of users' goals
  - Intellectual property and antitrust issues
  - Experience of other blockchain users
- Do your homework. Dozens of blockchain developers, architects, startups, and solution providers exist and specialize in distinct industries and use unique approaches.
- Rigorously check the trustworthiness of both the organization that manages the blockchain and the technology itself. Does the management system give effective control to any one entity or person and, if so, what checks are in place to prevent exploitation or compromise?
- Determine whether you can beta-test a blockchain solution before making the investment.
- Establish specific goals and timelines for your blockchain implementation. Key performance indicators could include time per transaction or cost per transaction.
- Consider blockchain's impacts on issues such as business processes, governance, and talent management.
- Consider whether regulation exists that will influence your use of blockchain.

CONCLUSION

Billions of dollars are pouring into blockchain, but the technology hasn't quite reached mainstream use yet. Questions persist about its value compared to a simple database, its vulnerabilities, its ability to live up to advertised potential, its enormous power expenditure, and so on. Yet many experts agree with the likes of Samson Williams, who says that in several years blockchain will be as ubiquitous as Wi-Fi: No one cares how Wi-Fi works. They just want the password. No one will care how blockchain works. They'll just expect it does and does so securely.

As with any security application, things go awry when security experts look for a solution that a technology can handle rather than the other way around. A fundamental tenet of good security is that you assess an application first, then add the appropriate technology.

"There are applications where blockchain is a good fit," says Geoff Revill, "but it needs careful selection and a clear system-level view as to 'why' coupled with a clarity of upsides and downsides." He urges security professionals to banish both the hype and the cynicism. "You need a clear-eyed perspective of what issue you need to solve and what new issues you introduce," he adds. "It's a tradeoff."

ENDNOTES

[1] Carlson, Brant, et al. *Blockchain Beyond the Hype: What is the Strategic Business Value?* McKinsey Digital, June 2018.

[2] Bagshaw, Rick. "Top Ten Cryptocurrencies by Market Capitalisation," *Yahoo! Finance*, April 22, 2020.

[3] Macaulay, Tom. "How Governments Around the World Are Using Blockchain," *Computerworld*, 19 September 2019.

[4] "Which Governments Are Using Blockchain Right Now?" ConsenSys, 18 November 2019.

[5] At least 14 blockchain consensus algorithms exist, including Practical Byzantine Fault Tolerance, Proof of Burn, Proof of Capacity, Directed Acyclic Graphs, and Proof of Elapsed Time. See Hary, Zaara. "What Is Blockchain Consensus Algorithms," Bitdeal, available at https://www.bitdeal.net/blockchain-consensus-algorithms, 11 January 2019

[6] Singh, Nitish. "Hybrid Blockchains: The Best of Both Worlds," *101 Blockchains,* 6 October 2018.

[7] Chitra, Rachel. "Ramco Systems, XinFin to Develop Hybrid Blockchain Solutions," *Times of India,* 14 February 2018.

[8] Singh, "Hybrid Blockchains."

[9] Anwar, Hasib. "Blockchain Consortium: 20 Consortia You Should Check Out," *101 Blockchains*, 16 November 2019.

[10] Sample, Matt. *MediLedger DSCSA Pilot Project, MediLedger,* February 2020.

[11] Partz, Helen. "Blockchain Will Be Most In-Demand Hard Skill in 2020: LinkedIn," *Cointelegraph*, 14 January 2020.

[12] "Frinkcoin," *The Simpsons,* Season 31, Episode 13, Fox, 23 February 2020.

[13] "Gartner 2019 Hype Cycle Shows Most Blockchain Technologies Are Still Five to 10 Years Away From Transformational Impact," Gartner, 8 October 2019.

[14] *Hype Cycle for Blockchain Technologies, 2019,* Gartner, October 2019.

[15] "Gartner 2019 Hype Cycle."

[16] *Deloitte's 2019 Global Blockchain Survey: Blockchain Gets Down to Business,* Deloitte Insights, 2019.

[17] Perez, Yessi Bello. "KPMG Survey: 67% of Corporates Are Not Using Blockchain Technology," *Hard Fork*, 9 April 2019.

[18] *PwC's Global Blockchain Survey 2018,* PwC, August 2018.

[19] "Smart Dubai Announces Achievements of Dubai Blockchain Strategy 2020," Smart Dubai, 26 January 2020.

[20] "Digital Transformation to Fuel Government ICT Spending Growth, Says IDC," International Data Corporation, 12 February 2020.

[21] *NASSCOM Avasant India Blockchain Report 2019*, NASSCOM and Avasant, March 2019.

[22] Tripathi, Ajit. "India's Supreme Court Ruling Is a Win for the Whole Blockchain Industry," *Coindesk*, 4 March 2020.

[23] "Beyond Bitcoin: Australia Releases 52-Page Blockchain Roadmap to Power Its Future Economy," *The Daily Hodl*, 7 February 2020.

[24] Dzawu, Moses Mozart. "Bank of Ghana Set to Issue Digital Currency in "Near Future," *Bloomberg News*, 27 November 2019.

[25] Macaulay, Tom. "How Governments Around the World Are Using Blockchain," *Computerworld*, 19 September 2019.

[26] "Maduro Bids to Revive Venezuela's 'Petro' Cryptocurrency," *France 24*, 15 January 2020.

[27] Vitáris, Benjamin. "African Country Turns to Blockchain to Stem Deadly Fake Drug Epidemic," *Cryptocurrency News*, 25 July 2019.

[28] "European Countries Join Blockchain Partnership," European Commission, 10 April 2018, available at https://ec.europa.eu/digital-single-market/en/news/european-countries-join-blockchain-partnership.

[29] "Valenciaport Expone en Rotterdam que Utilizará el Blockchain Para Dar Visibilidad 'Extremo a Extremo' de la Cadena Logística," Autoridad Portuaria de Valencia, 3 October 2019.

[30] Inveen, Cooper. "San Francisco Crowdfunder Kiva Sets Up Sierra Leone Credit Database," *Reuters*, 21 August 2019.

[31] Akilo, David. "Thailand E-Visa Blockchain System for Indian and Chinese Tourists," *Business Blockchain HQ*, 31 December 2019.

[32] Boddy, Max. "Brazilian State Launches Blockchain Platform for Government Contract Bids," *Cointelegraph*, 13 July 2019.

[33] Lago, Cristina. "How Singapore Is Using Blockchain Outside of Cryptocurrencies," *CIO*, 17 October 2018.

[34] Baydakova, Anna. "Factom Blockchain Project Wins Grant to Protect U.S. Border Patrol Data," *Coindesk*, 18 June 2018.

[35] Gatto, James. Bourne, Townsend. "Blockchain Tech Has Numerous Applications for Defense," *National Defense*, 11 December 2019.

[36] Suberg, William. "Finland Solves Refugee Identity with Blockchain Debit Cards," *Cointelegraph*, 5 September 2017.

[37] Hempel, Jessi. "New Refugees Are Helping Create Blockchain's Brand New World," *Wired*, 14 March 2018.

[38] Mire, Sam. "Blockchain for Identity Management: 33 Startups to Watch in 2019," *Disruptor Daily*, 8 February 2019.

[39] Rouhani, Sara. Deters, Ralph. Pourheidari, Vahid. *Physical Access Control Management System Based on Permissioned Blockchain*, available via ResearchGate, January 2019.

[40] "How Blockchain Addresses Public Key Infrastructure Shortcomings," Remme, available at https://remme.io/blog/how-blockchain-addresses-public-key-infrastructure-shortcomings, 27 January 2020.

[41] O'Neal, Stephen. "Diamonds Are Blockchain's Best Friend: How DLT Helps Tracking Gems and Prevents Fraud," *Cointelegraph*, 6 February 2019.
[42] Hayward, Andrew. "How True Tickets Is Bringing Blockchain to Broadway," *Yahoo! Finance*, 18 October 2019.

[43] Mcgrath, Stevan. "Resolving IoT Security Issues with Blockchain Technology," *Hackernoon*, 21 January 2019.

[44] "Xage Security to Implement Blockchain Security System for U.S. Air Force," *Asia Blockchain Review*, 1 January 2020.

[45] Ganpati, Vish. "Blockchain: Implications for the Security Professional," Security Industry Association, available at https://www.securityindustry.org/2018/09/04/blockchain-implications-for-the-security-professional/, 4 September 2018.

[46] Chattopadhyay, Arnab. "IoT Security Using Blockchain," Sogeti UK blog, available at https://www.uk.sogeti.com/content-hub/blog/iot-security-using-blockchain/, 2019.

[47] Ibid.

[48] "Gartner Survey Reveals Blockchain Adoption Combined With IoT Adoption Is Booming in the U.S.," Gartner, 12 December 2019.

[49] Ibid.

[50] *Global Blockchain IoT Market Size, Market Share, Application Analysis, Regional Outlook, Growth Trends, Key Players, Competitive Strategies and Forecasts, 2019 To 2027,* Research and Markets, January 2020.

[51] Rockwell, Mark. "Blockchain Protects IP, Tracks Tires, Supports Coronavirus," *GCN*, 13 March 2020.

[52]On a different COVID-19 front, stay-at-home orders and social-distancing mandates have raised the possibility of U.S. citizens voting at home, via a system with a blockchain backbone, in the November presidential election. But in a letter dated 9 April 2020 to governors, secretaries of state, and state election directors, the American Association for the Advancement of Science's (AAAS) Center for Scientific Evidence in Public Issues warned officials to not allow Internet voting, pointing out that e-voting via blockchain would raise concerns about privacy, ballot manipulation, and vote counting. Wright, Turner. "Online Voting Not Secure Even with Blockchain, Says U.S. Association," *Cointelegraph*, 10 April 2020.

[53] Newman, Lily Hay. "A New Tool Protects Videos from Deepfakes and Tampering," *Wired*, 2 November 2019.

[54] DARPA Media Forensics website. Available at https://www.darpa.mil/program/media-forensics.

[55] Samanta, Priyanka. Jain, Shweta. *E-Witness: Preserve and Prove Forensic Soundness of Digital Evidence*, MobiCom '18: Proceedings of the 24th Annual International Conference on Mobile Computing and Networking, October 2018.

[56] *Ticks or It Didn't Happen: Confronting Key Dilemmas in Authenticity Infrastructure for Multimedia*, WITNESS Media Lab, December 2019.

[57] Peterson, Stacey. "What You Need to Know About Blockchain Storage," *SearchStorage*, 10 April 2019.

[58] Dyatko, Natalya. "No, You Don't Store Data on the Blockchain—Here's Why," *JAXenter.com*, 16 December 2019.

[59] Yadav, Gaurav. "Blockchain Meets the Film Industry: Beginning of a New Avatar," *Hackernoon*, 2 July 2018.

[60] Aurora, Jenny. "Blockchain-enabled Ecosystem for Copyright Management Introduced by Italian Agency," *The Cryptosight*, 7 December 2019.

[61] "China Using Blockchain Evidence for Copyright Infringement," *Ledger Insights*, November 2019.

[62] Pratap, Mayank. "Everything You Need to Know About Smart Contracts: A Beginner's Guide," *Hackernoon*, 27 August 2018.

[63] Laurent, Patrick, et al. "The Tokenization of Assets is Disrupting the Financial Industry. Are You Ready?" *Inside*, Deloitte, November 2018.

[64] "How Blockchains Can Change the World," McKinsey & Company, May 2016.

[65] Scharf, Stephen. Koutras, Chris. Izzo, William. *Security of DLT Networks*, Depository Trust Clearing Corporation, February 2020.

[66] Callewaert, Kurt. "Blockchain and DLT: Security Risks, Threats and Vulnerabilities," Presentation prepared for RSA Conference, 27 February 2020, available at https://www.rsaconference.com/usa/agenda/blockchain-and-dlt-security-risks-threats-and-vulnerabilities.

[67] Fawthrop, Andrew. "BMW Becomes First Car Manufacturer to Join IRMA Mining Standards Initiative," *NS Energy*, 9 January 2020.

[68] Jacobsen, Jax. "Can Blockchain Apps Ensure a Responsible Mineral Supply Chain," *Forbes*, 22 March 2019.

[69] "Lucara Diamond Replaces CEO, Invests in Blockchain Platform," *Financial Times*, 26 February 2018.

[70] Bates, Rob. "De Beers' Blockchain Platform Hopes to Track Every Diamond," *JCK*, 12 June 2019.

[71] Schneier, Bruce. "Blockchain and Trust," Schneier on Security, 12 February 2019.

[72] Kaufman, Charles. Perlman, Radia. "Distributed Trust: Is 'Blockchain' the Best Approach?" Presentation at the 2020 RSA Conference, 25 February 2020.

[73] Shawdagor, Jinia. "10 Global Enterprises Looking to Issue Their Own Crypto," *Cointelegraph*, 12 August 2019.

[74] "What Is Hard Fork?" *Cointelegraph*, available at https://cointelegraph.com/bitcoin-cash-for-beginners/what-is-hard-fork.

[75] Dasgupta, Dipankar. Shrein, John M. Gupta, Kishor Datta. "A Survey of Blockchain from Security Perspective," *Journal of Banking and Financial Technology*," 3 January 2019.

[76] Ibid.

[77] Williams, Sean. "The Biggest Cryptocurrency Hacks in History," *The Motley Fool*, 9 May 2018.

[78] Young, Joseph. "Round-Up of Crypto Exchange Hacks So Far in

2019—How Can They Be Stopped?" *Cointelegraph*, 18 June 2019.

[79] Canellis, David. Bitcoin Gold Hit By 51% Attacks, $72K in Cryptocurrency Double-Spent," *Hard Fork*, 27 January 2020.

[80] Greenberg, Andy. "A 'Blockchain Bandit' Is Guessing Private Keys and Scoring Millions," *Wired*, 23 April 2019.

[81] McDowell, James. "Beware of the Blockchain Bandit," Government Blockchain Association, accessed at https://www.gbaglobal.org/blockchainbandit/, 6 May 2019.

[82] "NIST Reveals 26 Algorithms Advancing to the Post-Quantum Crypto 'Semifinals,'" U.S. National Institute of Standards and Technology, 30 January 2019.

[83] "Futurex Announces Post-Quantum Hybrid Certificate Authority Solution," *Yahoo! Finance*, 20 February 2020.

[84] Cerveny, Frank, et al. *Blockchain Improves Operational Efficiency for Securitisations, Amid New Risks*, Moody's Investors Service, 25 April 2019.

[85] Ibid.

[86] *Deloitte's 2019 Global Blockchain Survey: Blockchain Gets Down to Business*, Deloitte Insights, 2019.

[87] Tapscott, Dan. "These Are the Challenges Blockchain Faces in 2020," World Economic Forum, 17 January 2020.

[88] Teperdjian, Raffi. "Examining the National Security Implications of Cryptocurrencies," *National Law Review*, 26 October 2019.

[89] Zmudzinski, Adrian. "Blockchain Makes Money Laundering Risks Greater, Says Swiss Regulator," *Cointelegraph*, 11 December 2019.

[90] Zaslavsky, Sergei. "Blockchain and Antitrust: How Counsel Can Reduce Risk," *Bloomberg Law*, 9 January 2019.

[91] Huillet, Marie. "Standard Chartered Joins IBM and Maersk's Blockchain Shipping Platform," *Cointelegraph*, 13 March 2020.

[92] Deloitte's 2019 *Global Blockchain Survey*

[93] Ibid

[94] Huillet. "Standard Chartered Joins IBM and Maersk's Blockchain Shipping Platform."

[95] Compiled with assistance from Geoff Revill.

Appendix I: Works Consulted

Ajiboye, Tolu. "Amazon Will Likely Announce Cryptocurrency to Threaten Facebook's Libra," *Coinspeaker*, 4 February 2020.

Akilo, David. "Thailand E-Visa Blockchain System for Indian and Chinese Tourists," *Business Blockchain HQ*, 31 December 2019.

Anwar, Hasib. "Blockchain Consortium: 20 Consortia You Should Check Out," *101 Blockchains*, 16 November 2019.

Arnold, Andrew. "4 Promising Use Cases of Blockchain in Cybersecurity," *Forbes*, 30 January 2019.

Aurora, Jenny. "Blockchain-enabled Ecosystem for Copyright Management Introduced by Italian Agency," *The Cryptosight*, 7 December 2019.

Bagshaw, Rick. "Top Ten Cryptocurrencies by Market Capitalisation," *Yahoo! Finance*, April 22, 2020.

Banking Is Only the Beginning: 55 Big Industries Blockchain Could Transform, CB Insights, 11 June 2019.

Baraniuk, Chris. "Blockchain: The Revolution That Hasn't Quite Happened," *BBC News*, 11 February 2020.

Barber, Gregory. "What's Blockchain Actually Good for, Anyway? For Now, Not Much," *Wired*, 28 October 2019.

Bates, Rob. "De Beers' Blockchain Platform Hopes to Track Every Diamond," *JCK*, 12 June 2019.

Baydakova, Anna. "Factom Blockchain Project Wins Grant to Protect U.S. Border Patrol Data," *Coindesk*, 18 June 2018.

Beedham, Matthew. "Here's the Difference Between Blockchain and Distributed Ledger Technology," *Hard Fork*, 27 July 2018.

Beigel, Ofir. "51% Attack Explained: A Beginner's Guide," *99Bitcoins,* updated 14 November 2019.

"Beyond Bitcoin: Australia Releases 52-Page Blockchain Roadmap to Power Its Future Economy," *The Daily Hodl*, 7 February 2020.

Birch, Joseph. "The State of Blockchain: Experts Weigh In On Adoption Around the World," *Cointelegraph*, 23 February 2020.

Blockchain and the Decentralization Revolution: A CFO's Guide to the Potential Implications of Distributed Ledger Technology, JPMorgan, May 2018.

"Blockchain, Digital Currency, and Cryptocurrency: Moving Into the Mainstream?" *J.P. Morgan Perspectives*, 21 February 2020.

Boddy, Max. "Brazilian State Launches Blockchain Platform for Government Contract Bids," *Cointelegraph*, 13 July 2019.

Burg, John. Murphy, Christine. Petraud, Jean Paul. "Blockchain for International Development: Using a Learning Agenda to Address Knowledge Gaps," Merl Tech, 29 November 2018.

Callewaert, Kurt. "Blockchain and DLT: Security Risks, Threats & Vulnerabilities," Presentation prepared for RSA Conference, 27 February 2020, available at https://www.rsaconference.com/usa/agenda/blockchain-and-dlt-security-risks-threats-and-vulnerabilities.

Canellis, David. Bitcoin Gold Hit By 51% Attacks, $72K in Cryptocurrency Double-Spent," *Hard Fork*, 27 January 2020.

Carlson, Brant, et al. *Blockchain Beyond the Hype: What is the Strategic Business Value?* McKinsey Digital, June 2018.

Carlson, Jill. "Trust No One. Not Even a Blockchain," *Slate*, 25 January 2020.

Cerveny, Frank, et al. *Blockchain Improves Operational Efficiency for Securitisations, Amid New Risks*, Moody's Investors Service, 25 April 2019.

Chain Reaction: Blockchain Enters the Mainstream: The GBBC 2020 Annual Report, Global Blockchain Business Council, 2020.

Chandler, Carson. "What Is the Difference Between Blockchain and DLT?" *Cointelegraph*, 2 August 2019.

Chatterjee, Rohit. "The Future of Identity Management Using Blockchain," *Hackernoon*, 3 August 2019.

Chattopadhyay, Arnab. "IoT Security Using Blockchain," Sogeti UK blog, available at https://www.uk.sogeti.com/content-hub/blog/iot-security-using-blockchain/, 2019.

"China Using Blockchain Evidence for Copyright Infringement," *Ledger Insights*, November 2019.

Chitra, Rachel. "Ramco Systems, XinFin to Develop Hybrid Blockchain Solutions," *Times of India*, 14 February 2018.

Comben, Christina. "China Turns to Blockchain as Coronavirus Spins Out of Control," www.bitcoinist.com, 14 February 2020.

Cosgrove, Emma. "TradeLens Blockchain Platform Awaits Antitrust Clearance by FMC," *Supply Chain Dive*, 10 January 2020.

Dache, Gerard. "The Blockchain Chinese Bamboo Tree," Government Blockchain Association, accessed at https://www.gbaglobal.org/china-bc-tree/, 14 December 2019.

Daley, Sam. "Wallets, Hospitals, and the Chinese Military: 19 Examples of Blockchain Cybersecurity at Work," Built In, accessed at https://builtin.com/blockchain/blockchain-cybersecurity-uses, updated 7 January 2020.

DARPA Media Forensics website. Available at https://www.darpa.mil/program/media-forensics.

Dasgupta, Dipankar. Shrein, John M. Gupta, Kishor Datta. "A Survey of Blockchain from Security Perspective," *Journal of Banking and Financial Technology*," 3 January 2019.

De Filippi, Primavera. Wright, Aaron. *Blockchain and the Law: The Rule of Code*, Harvard University Press, 9 April 2018.

Deign, Jason. "Energy Blockchain's Most Obvious Use Case Is Not What You Think, *Greentech Media*, January 27, 2020.

Deloitte's 2019 Global Blockchain Survey: Blockchain Gets Down to Business, Deloitte Insights, 2019.

"Digital Transformation to Fuel Government ICT Spending Growth, Says IDC," International Data Corporation, 12 February 2020.

Drinkwater, Doug. "6 Use Cases for Blockchain in Security," *CSO*, 6 February 2018.

Dzawu, Moses Mozart. "Bank of Ghana Set to Issue Digital Currency in "Near Future," *Bloomberg News*, 27 November 2019.

Dyatko, Natalya. "No, You Don't Store Data on the Blockchain—Here's Why," *JAXenter.com,* 16 December 2019.

Efrima, Adam. "Five Predictions for the Future of Blockchain and Cryptocurrency," *Forbes*, June 13, 2019.

"European Countries Join Blockchain Partnership," European Commission, 10 April 2018, available at https://ec.europa.eu/digital-single-market/en/news/european-countries-join-blockchain-partnership.

Fawthrop, Andrew. "BMW Becomes First Car Manufacturer to Join IRMA Mining Standards Initiative," *NS Energy*, 9 January 2020.

Febrero, Pedro. "How Does Public Blockchain Technology Work?" *Yahoo! Finance*, 10 May 2019.

Franklin, Jr., Curtis. "7 Ways Blockchain is Being Used for Security," *Dark Reading*, 5 September 2018.

"Frinkcoin," *The Simpsons*, Season 31, Episode 13, Fox, 23 February 2020.

"Futurex Announces Post-Quantum Hybrid Certificate Authority Solution," *Yahoo! Finance*, 20 February 2020.

Ganpati, Vish. "Blockchain: Implications for the Security Professional," Security Industry Association, available at https://www.securityindustry.org/2018/09/04/blockchain-implications-for-the-security-professional/, 4 September 2018.

"Gartner 2019 Hype Cycle Shows Most Blockchain Technologies Are Still Five to 10 Years Away From Transformational Impact," Gartner, 8 October 2019.

"Gartner Survey Reveals Blockchain Adoption Combined With IoT Adoption Is Booming in the U.S.," Gartner, 12 December 2019.

Gatto, James. Bourne, Townsend. "Blockchain Tech Has Numerous Applications for Defense," *National Defense*, 11 December 2019.

Gazdecki, Andrew. "Proof-of-Work and Proof-of-Stake: How Blockchain Reaches Consensus," *Forbes*, 28 January 2019.

George, Rohith P., et al. "Blockchain for Business," *Journal of Investment Compliance*, 2019.

Global Blockchain IoT Market Size, Market Share, Application Analysis, Regional Outlook, Growth Trends, Key Players, Competitive Strategies and Forecasts, 2019 To 2027, Research and Markets, January 2020.

Greenberg, Andy. "A 'Blockchain Bandit' Is Guessing Private Keys and Scoring Millions," *Wired*, 23 April 2019.

Global Legal Research Directorate Staff. "Regulation of Cryptocurrency Around the World," Library of Congress, available at https://www.loc.gov/law/help/cryptocurrency/world-survey.php, June 2018

Grieg, Jonathan. "10 Ways the Enterprise is Using Blockchain," ZDNet, 2 December 2019.

Grieg, Jonathan. "MIT Finds Massive Security Flaws with Blockchain Voting App," *Tech Republic*, 14 February 2020.

Hary, Zaara. "What Is Blockchain Consensus Algorithms," Bitdeal, available at https://www.bitdeal.net/blockchain-consensus-algorithms, 11 January 2019

Hayward, Andrew. "How True Tickets Is Bringing Blockchain to Broadway," *Yahoo! Finance*, 18 October 2019.

Hempel, Jessi. "New Refugees Are Helping Create Blockchain's Brand New World," *Wired*, 14 March 2018.

"How Blockchain Addresses Public Key Infrastructure Shortcomings," Remme, available at https://remme.io/blog/how-blockchain-addresses-public-key-infrastructure-shortcomings, 27 January 2020.

"How Blockchains Can Change the World," McKinsey & Company, May 2016.

"How Does Blockchain Work in 7 Steps: A Clear and Simple Explanation," available at https://blog.goodaudience.com/blockchain-for-beginners-what-is-blockchain-519db8c6677a, 6 May 2018.

Huillet, Marie. "Standard Chartered Joins IBM and Maersk's Blockchain Shipping Platform," *Cointelegraph*, 13 March 2020.

Hype Cycle for Blockchain Technologies, 2019, Gartner, October 2019

"Inclusive Deployment of Blockchain: Case Studies and Learnings from the United Arab Emirates," United Arab Emirates Centre for the Fourth Industrial Revolution and the World Economic Forum, January 2020.

"Introducing the European Blockchain Services Infrastructure (EBSI)," The European Union, available at https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/ebsi.

Inveen, Cooper. "San Francisco Crowdfunder Kiva Sets Up Sierra Leone Credit Database," *Reuters*, 21 August 2019.

Jacobsen, Jax. "Can Blockchain Apps Ensure a Responsible Mineral Supply Chain," *Forbes*, 22 March 2019.

Kaaru, Steve. "2019 Year in Review: Blockchain and Crypto Take Root in Africa," *Coingeek*, 31 December 2019.

Kaufman, Charles. Perlman, Radia. "Distributed Trust: Is 'Blockchain' the Best Approach?" Presentation at the 2020 RSA Conference, 25 February 2020.

Kolisko, Lukas. "Do We Need Mining in Private and Permissioned Blockchains?" *Medium*, 14 May 2018.

Kshetri, Nir. "I Study Blockchain. It Shouldn't Be Used to Secure Our Elections," *Fast Company*, 19 October 2019.

Kuchar, Michael. "What Does 2020 Have in Store for the Blockchain?" *Yahoo! Finance*, 11 February 2020.

Lago, Cristina. "How Singapore Is Using Blockchain Outside of Cryptocurrencies," *CIO*, 17 October 2018.

Laurence, Tiana. *Blockchain for Dummies, 2d. Edition*, John Wiley & Sons (2019).

Laurent, Patrick, et al. "The Tokenization of Assets is Disrupting the Financial Industry. Are You Ready?" *Inside*, Deloitte, November 2018.

"Lucara Diamond Replaces CEO, Invests in Blockchain Platform," *Financial Times*, 26 February 2018.

Macaulay, Tom. "How Governments Around the World Are Using Blockchain," *Computerworld*, 19 September 2019.

"Maduro Bids to Revive Venezuela's 'Petro' Cryptocurrency," *France 24*, 15 January 2020.

Massessi, Demiro. "Public Vs. Private Blockchain in a Nutshell," *Coinmonks*, 12 December 2018.

McDowell, James. "Beware of the Blockchain Bandit," Government Blockchain Association, accessed at https://www.gbaglobal.org/blockchainbandit/, 6 May 2019.
Mcgrath, Stevan. "Resolving IoT Security Issues with Blockchain Technology," *Hackernoon*, 21 January 2019.

Mearian, Lucas. "IoT Could Be the Killer App for Blockchain," *Computerworld*, 25 June 2018.

Mearian, Lucas. "What is Blockchain? The Complete Guide," *Computerworld, 29 January 2019.*

Menon, Jai. "10 Questions to Ask Before You Use Blockchain," *Forbes*, 11 September 2018.

Miller, Hugo. "Facebook's 'Failed" Libra Cryptocurrency Is No Closer to Release," *Bloomberg*, 20 January 2020.

Mire, Sam. "10 Startups Using Blockchain to Transform Messaging," *Disruptor Daily*, 24 December 2018.

Mire, Sam. "12 Startups Using Blockchain to Transform the Art Industry," *Disruptor Daily*, 25 December 2018.

Mire, Sam. "Blockchain for Identity Management: 33 Startups to Watch in 2019," *Disruptor Daily,* 8 February 2019.

Mire, Sam. "Blockchain in Ticketing and Events: 9 Startups to Watch in 2019," *Disruptor Daily*, 11 February 2019.

Mulligan, Cathy, et al. "These 11 Questions Will Help You Decide Whether Blockchain Is Right for Your Business," World Economic Forum, 23 April 2018.

Myrlea, Michael. Gourisetti, Sri Nikhil Gupta. "Blockchain: Next Generation Supply Chain Security for Energy Infrastructure and NERC Critical Infrastructure Protection (CIP) Compliance," *Systemics, Cybernetics and Informatics*, vol.6 no. 6, 2018.

NASSCOM Avasant India Blockchain Report 2019, NASSCOM and Avasant, March 2019.

The National Blockchain Roadmap: Progressing Toward a Blockchain-Powered Future, Department of Industry, Science, Energy and Resources, Australian Government, February 2020.

Navedo-Perez, Steffan. "Blockchain Could Save a Country Billions, Report Says," *Chief Investment Officer*, 17 January 2020.

Newman, Lily Hay. "A New Tool Protects Videos from Deepfakes and Tampering," *Wired*, 2 November 2019.

"NIST Reveals 26 Algorithms Advancing to the Post-Quantum Crypto 'Semifinals,'" U.S. National Institute of Standards and Technology, 30 January 2019.

Ometoruwa, Toju. "IBM and Maersk's Struggles Cast a Shadow Over Private Blockchains," *Hackernoon*, 2 November 2018.

O'Neal, Stephen. "Diamonds Are Blockchain's Best Friend: How DLT Helps Tracking Gems and Prevents Fraud," *Cointelegraph*, 6 February 2019.

Orcutt, Mike. "How Secure is Blockchain Really?" *MIT Technology Review*, 25 April 2018.

Partz, Helen. "Blockchain Will Be Most In-Demand Hard Skill in 2020: LinkedIn," *Cointelegraph*, 14 January 2020.

Perez, Yessi Bello. "KPMG Survey: 67% of Corporates Are Not Using Blockchain Technology," *Hard Fork*, 9 April 2019.

Peterson, Stacey. "What You Need to Know About Blockchain Storage," *SearchStorage*, 10 April 2019.

Phillips, Gavin. "The 5 Best Decentralized Messaging Apps," *Blocks Decoded*, 23 October 2019.

Popper, Nathaniel. "Terrorists Turn to Bitcoin for Funding, and They're Learning Fast," *The New York Times*, 18 August 2019.

Pratap, Mayank. "Everything You Need to Know About Smart Contracts: A Beginner's Guide," *Hackernoon*, 27 August 2018.

PwC's Global Blockchain Survey 2018, *PwC*, August 2018.

Rathore, Heena, et al. "A Survey of Blockchain Enabled Cyber-Physical Systems," *Sensors*, 3 January 2020.

Rockwell, Mark. "Blockchain Protects IP, Tracks Tires, Supports Coronavirus," *GCN*, 13 March 2020.

Rosenbaum, Leah. "Anthem Will Use Blockchain To Secure Medical Data for Its 40 Million Members in Three Years," *Forbes*, 12 December 2019.

Rouhani, Sara. Deters, Ralph. Pourheidari, Vahid. *Physical Access Control Management System Based on Permissioned Blockchain*, available via ResearchGate, January 2019.

Samanta, Priyanka. Jain, Shweta. *E-Witness: Preserve and Prove Forensic Soundness of Digital Evidence,* MobiCom '18: Proceedings of the 24th Annual International Conference on Mobile Computing and Networking, October 2018.

Sample, Matt. MediLedger DSCSA Pilot Project, *MediLedger*, February 2020.

Scharf, Stephen. Koutras, Chris. Izzo, William. *Security of DLT Networks*, Depository Trust Clearing Corporation, February 2020.

Schneier, Bruce. "Blockchain and Trust," Schneier on Security, 12 February 2019.

Shawdagor, Jinia. "10 Global Enterprises Looking to Issue Their Own Crypto," *Cointelegraph*, 12 August 2019.

Schumann, Turner. "Consensus Mechanisms Explained: PoW vs. PoS," *Hackernoon*, 5 April 2018.

Shapiro, Gary. "Blockchain Promises A Future of Security," *Detroit News*, 7 October 2019.

Singh, Nitish. "Hybrid Blockchains: The Best of Both Worlds," *101 Blockchains*, 6 October 2018.

"Smart Dubai Announces Achievements of Dubai Blockchain Strategy 2020," *Smart Dubai*, 26 January 2020.

Stalinsky, Steven. "The Coming Storm: Terrorists Using Cryptocurrency," *MEMRI Jihad and Terrorism Threat Monitor*, 21 August 2019.

Suberg, William. "Finland Solves Refugee Identity with Blockchain Debit Cards," *Cointelegraph*, 5 September 2017.

Swinhoe, Dan. "4 Blockchain Security Lessons from Euroclear's CISO," *CSO*, 22 October 2019.

Tapscott, Alex. Roque, Oscar. "Webinar: Building New Business Networks," *Blockchain Research Institute,* 16 December 2019.

Tapscott, Dan. "These Are the Challenges Blockchain Faces in 2020," *World Economic Forum*, 17 January 2020.

Tariq, Hira. "Public Blockchains You Should Know About," https://xord.one/different-public-blockchain-platforms-you-should-know-about/, 25 October 2019.

Taylor, P.J., et al. "A Systematic Literature Review of Blockchain Cybersecurity," *Digital Communications and Networks*, 21 January 2019.

Taylor, Phil. "Despite Benefits, Blockchain Adoption Is Slow in Life Sciences, Says Report," Pharmaphorum.com, January 17, 2020.

Teperdjian, Raffi. "Examining the National Security Implications of Cryptocurrencies," *National Law Review*, 26 October 2019.

Thind, Gurpeet. "Saudi-UAE Leaders Confirm Aber Digital Currency Launch," *Cryptopolitan*, 28 November 2019.

Ticks or It Didn't Happen: Confronting Key Dilemmas in Authenticity Infrastructure for Multimedia, WITNESS Media Labs, December 2019.

Tripathi, Ajit. "India's Supreme Court Ruling Is a Win for the Whole Blockchain Industry," *Coindesk*, 4 March 2020.

Vinayak, Heena. "Crypto Under Attack: The Five Worst Hacks that Shook the Crypto World," *Cointelegraph*, 4 November 2019.

Vitáris, Benjamin. "African Country Turns to Blockchain to Stem Deadly Fake Drug Epidemic," *Cryptocurrency News*, 25 July 2019.

"Valenciaport Expone en Rotterdam que Utilizará el Blockchain Para Dar Visibilidad 'Extremo a Extremo' de la Cadena Logística," Autoridad Portuaria de Valencia, 3 October 2019.

Volpicelli, Gian. "What Is Libra? Facebook's Cryptocurrency, Explained," *Wired*, 14 August 2019.

Wachsman, Melanie Wolkoff. "Research: Blockchain Must Overcome Hurdles Before Becoming a Mainstream Technology," ZDNet, 2 December 2019.

Wang, Junyao, et al. "A Summary of Research on Blockchain in the Field of Intellectual Property," 2018 International Conference on Identification, Information and Knowledge in the Internet of Things, IIKI, 2018.

"What Is Hard Fork?" *Cointelegraph*, accessed at https://cointelegraph.com/bitcoin-cash-for-beginners/what-is-hard-fork.

"Which Governments Are Using Blockchain Right Now?" ConsenSys, 18 November 2019.

Williams, Sean. "The Biggest Cryptocurrency Hacks in History," *The Motley Fool*, 9 May 2018.

Wilson, Bernadette. "6 Physical Security Trends Creating Opportunities for ISVs," *DevPro Journal*, 1 August 2018.

Wright, Charles. Joshi, Rakesh. "Blockchain in Healthcare and Life Sciences," PreScouter, January 2020.

Wright, Turner. "Online Voting Not Secure Even with Blockchain, Says U.S. Association, *Cointelegraph*, 10 April 2020.

"Xage Security to Implement Blockchain Security System for U.S. Air Force," *Asia Blockchain Review*, 1 January 2020.

Yadav, Gaurav. "Blockchain Meets the Film Industry: Beginning of a New Avatar," *Hackernoon*, 2 July 2018.

Yang, Lu. "The Blockchain: State-of-the-Art and Research Challenges," *Journal of Industrial Information Integration*, 9 April 2019.

Young, Joseph. "Round-Up of Crypto Exchange Hacks So Far in 2019—How Can They Be Stopped?" *Cointelegraph*, 18 June 2019.

Young, Reginald. "A Brief History of Private Money and Crypto: This Time is Not Different," *Medium*, 17 January 2018.

Zaslavsky, Sergei. "Blockchain and Antitrust: How Counsel Can Reduce Risk," *Bloomberg Law*, 9 January 2019.

Zmudzinski, Adrian. "Blockchain Makes Money Laundering Risks Greater, Says Swiss Regulator," *Cointelegraph*, 11 December 2019.

Appendix II: Experts Consulted

Christian Auty, Esq., Counsel, Bryan Cave Leighton Paisner

Brent Barker, Cryptocurrency and Blockchain Security Adviser, Barker Global Security

Rick Bawcum, Technologist, Futurist, and CEO, CIMATRI

Howard Belfor, CPP, President, Belfor & Associates

Gerard Dache, Executive Director, Government Blockchain Association

Andre De Castro, CEO, Blockchain of Things

Charles Dumbrille, Chief Risk Officer, IN-D-TEL International

Scott Klososky, Founding Partner, Future Point of View

Alissa Knight, White Hat Hacker, and Partner, Knight Ink

Min Kyriannis, Associate, Cybersecurity/Technology Business Development, Jaros, Baum & Bolles

Peter Langela, CEO, Fluidensity

Dustin Laun, CEO, CTO, Mobohubb

Suzanne Livingston, Offering Director, IBM Food Trust

Ben Rothke, Senior Information Security Specialist, Tapad

Geoff Revill, CEO, Krowdthink

Dina Ellis Rochkind, Esq., FinTech Counsel, Paul Hastings

Stephen Scharf, CSO, Depository Trust Clearing Corporation

Bruce Schneier, Security Technologist

Eddie Schwartz, CSO, block.one

Roger Shepherd, Managing Director, Chipless

Bas Sluijsmans, Partner—E-Discovery & Cyber Forensic Expert, Forcyd

Jeff Snyder, Cybersecurity Recruiter and Executive Coach

Jimmy Song, Bitcoin Fellow, Blockchain Capital; Lecturer, University of Texas at Austin

Don Southerton, Global Head of Corporate Communications, Hancom Group

Steve Surfaro, Chairman, Public Safety Working Group, Security Industry Association

Masseh Tahiry, Senior Risk Strategist, Toffler Associates

Peter Tan, Security Consultant and Lecturer, Temasek Polytechnic

Mirena Taskova, Privacy and Cybersecurity Advisor and Attorney, Fieldfisher

Lewis Werner, Co-Founder, Quill Security Technology

Samson Williams, Blockchain Consultant; Adjunct Professor UNH School of Law and Columbia University

Appendix III: Blockchain Survey Questions

1. WHICH OF THE FOLLOWING BEST DESCRIBES YOUR ORGANIZATION'S PRINCIPAL INDUSTRY?

a. Advertising and Marketing
b. Agriculture
c. Airlines and Aerospace
d. Automotive
e. Business Support & Logistics
f. Construction, Machinery, and Homes
g. Education
h. Entertainment & Leisure
i. Finance & Financial Services
j. Food & Beverages
k. Government
l. Healthcare & Pharmaceuticals
m.Houses of Worship
n. Insurance
o. Law Enforcement
p. Management Consulting
q. Manufacturing
r. Military
s. Nonprofit
t. Retail & Consumer Durables
u. Real Estate/Facilities
v. Security Services
w. Telecommunications, Technology, Internet & Electronics
x. Transportation & Delivery
y. Utilities, Energy, and Extraction
z. I am currently not employed

2.WHAT IS YOUR PRIMARY AREA OF RESPONSIBILITY?

a. Physical security
b. Cyber security
c. Business continuity/disaster recovery
d. Safety
e. Combination/multiple areas of responsibility
f. Other (please specify)

3.WHICH OF THE FOLLOWING BEST DESCRIBES YOUR ROLE?

a. CEO/President/Vice President
b. Chief Information Security Officer (CISO)
c. Consultant
d. Chief Security Officer/Deputy CSO
e. Director
f. Distributor/Supplier
g.Integrator
h. Partner/Principal/Owner

4. WHERE ARE YOU LOCATED?

a. United States
b. Canada
c. Mexico, Central America, Caribbean
d. South America
e. Europe/UK
f. Africa
g. Middle East
h. Asia
i. Oceania

5. HOW FAMILIAR ARE YOU WITH BLOCKCHAIN?

a. Extremely familiar
b. Very familiar
c. Somewhat familiar
d. Not so familiar
e. Not at all familiar

6. WHAT ARE YOUR THOUGHTS ON THE SECURITY BENEFITS OF BLOCKCHAIN? (SELECT ALL THAT APPLY)

a. Not sure/not applicable
b. No proven benefits
c. Cryptocurrency benefits only
d. There are likely specific use cases for supply chain, authentication, etc.
e. The security benefits will be transformative once widespread adoption occurs

7. HOW PRACTICAL IS BLOCKCHAIN? (SELECT ALL THAT APPLY)

a. It does little more than a database does, at greater cost and complexity
b. As practical as the specific application
c. It will take off once the real life benefits are in substantial evidence
d. Don't know/Unsure

8. HAS YOUR ORGANIZATION EVER STUDIED OR INVESTED IN BLOCKCHAIN?

a. Yes
b. No
c. Unsure

9. IF YOU ANSWERED YES ABOVE, WHICH OF THE FOLLOWING ACTIONS HAVE YOU TAKEN?

a. Taking no further action because the costs still exceed benefits
b. Biding our time until the technology becomes more mainstream
c. Participating in one or more use cases
d. Participating in a public blockchain like Bitcoin
e. Developing/partnering on a permissioned blockchain

10. ARE YOU WILLING TO BE INTERVIEWED BY AN ASIS FOUNDATION RESEARCHER ON BLOCKCHAIN?

a. Yes
b. No

11. IF YOU ARE OPEN TO BEING INTERVIEWED, PLEASE PROVIDE YOUR CONTACT INFORMATION.

About the ASIS Foundation

The ASIS Foundation, a 501(c)(3) nonprofit affiliate of ASIS International, supports global security professionals worldwide through research and education. The Foundation commissions actionable research to advance the security profession and awards scholarships to help chapters and individuals—including those transitioning to careers in security management—achieve their professional and academic goals. Governed by a Board of Trustees, the Foundation is supported by generous donations from individuals, organizations, and ASIS chapters and councils worldwide.

Support future security research with a gift to the ASIS Foundation. Online at *www.asisfoundation.org*.