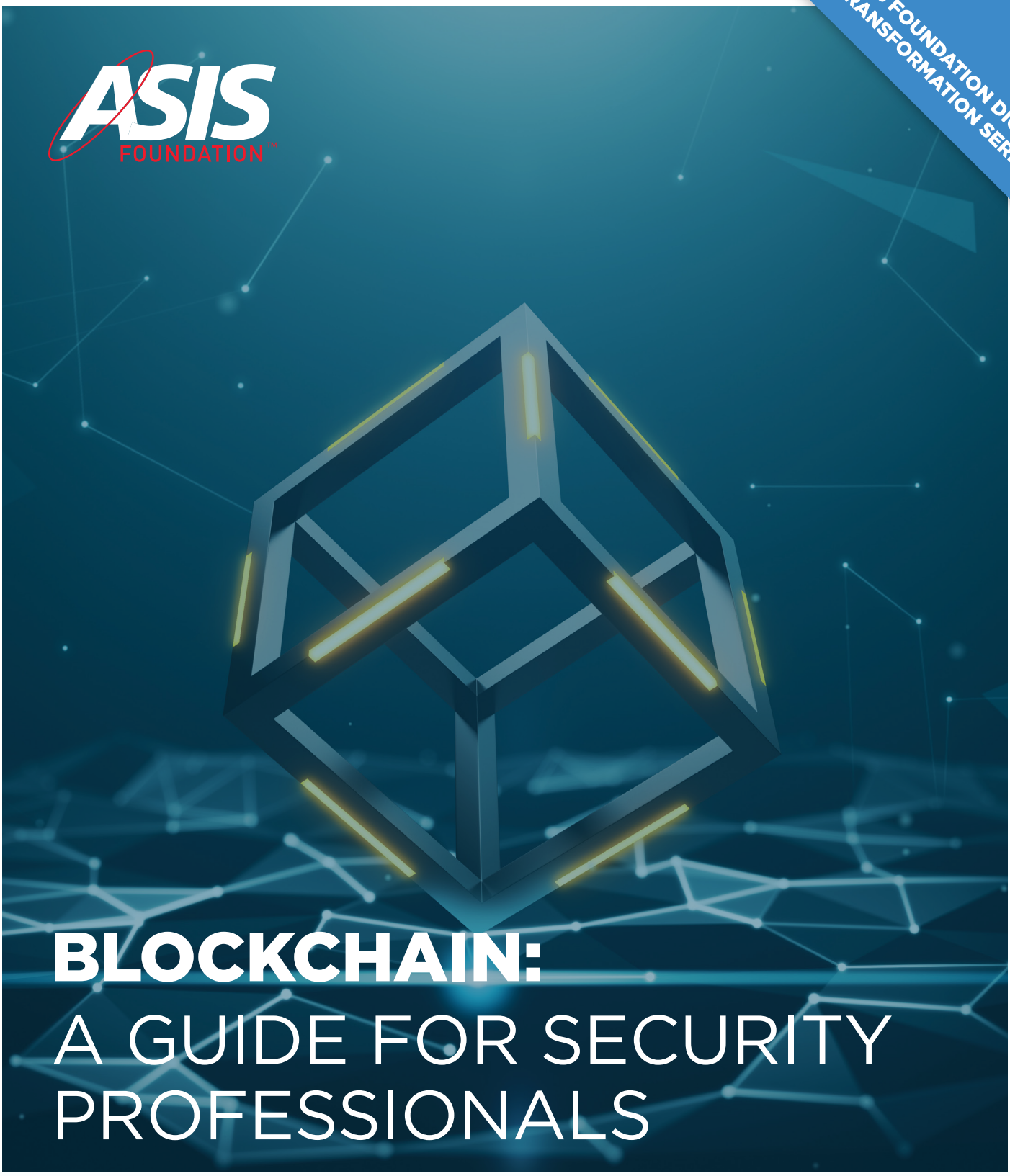
ASIS FOUNDATION DIGITAL TRANSFORMATION SERIES

ASIS FOUNDATION™



BLOCKCHAIN: A GUIDE FOR SECURITY PROFESSIONALS

EXECUTIVE SUMMARY

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.

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).

ASIS International
1625 Prince Street
Alexandria, Virginia, USA 22314

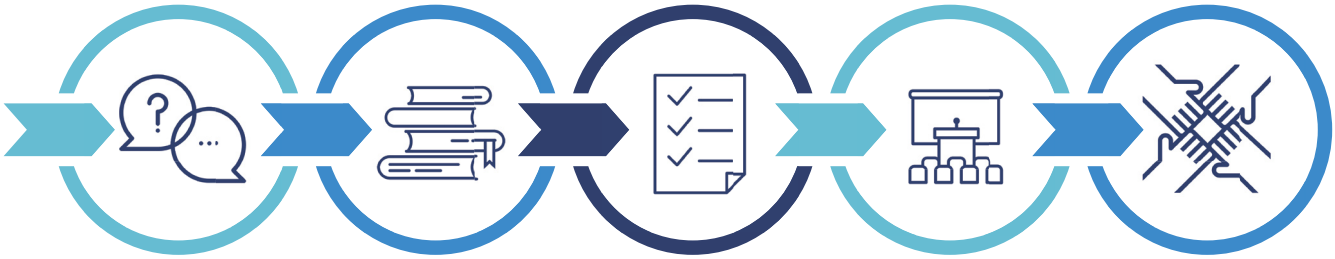
In late 2019, the ASIS Foundation commenced a research study to help security professionals understand blockchain technology and its security impacts.

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 application programming interfaces (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.

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

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. Individuals confirm transactions by doing heavy computational work, and they are rewarded with tokens like Bitcoins. 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.

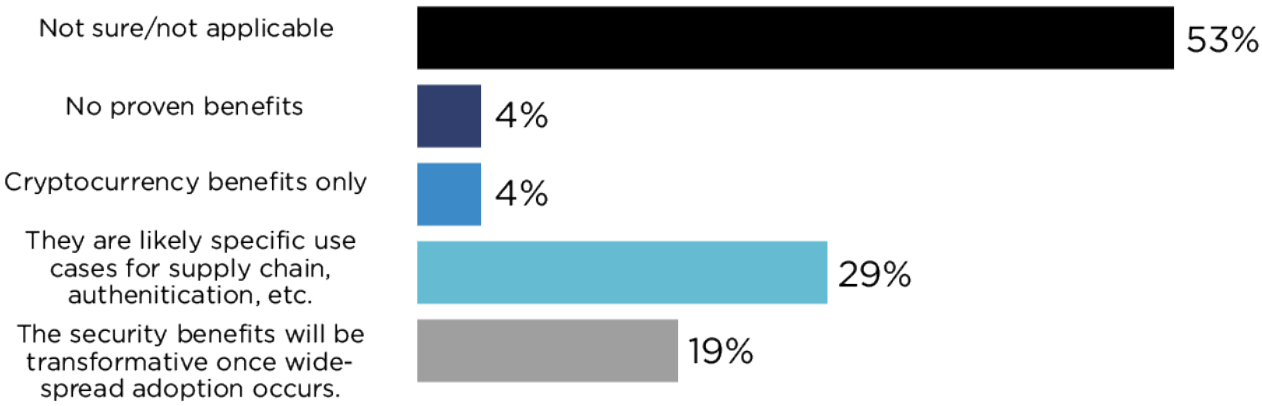
Blockchain may be poised for mass adoption, but it's not quite there yet.

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 Wi-Fi.

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.

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



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

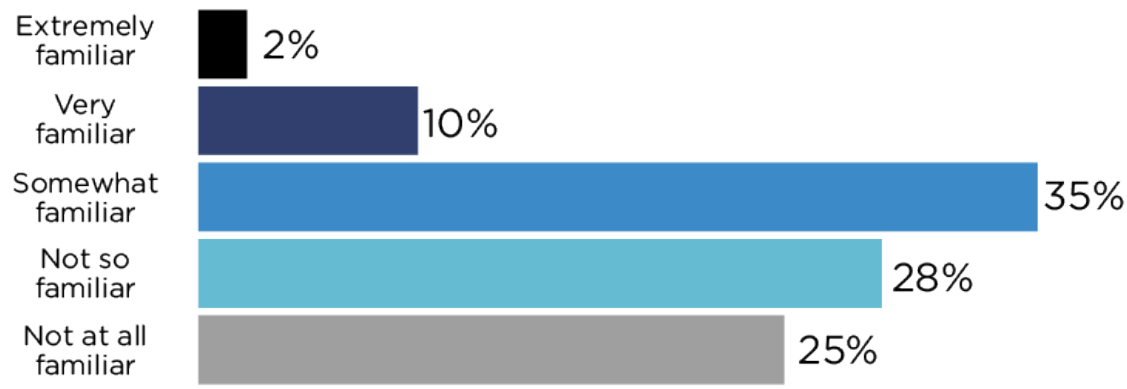
Likewise, most respondents were unsure of blockchain's practical value and had never deployed it. While some security professionals surveyed are avid proponents of the technology, a majority expressed skepticism, pointing out issues such its heavy energy expenditure, the lack of a compelling business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

TRUST IS THE KEY PHILOSOPHICAL ISSUE.

Public blockchains vest trust in technology; private blockchains vest trust in the gatekeepers—organizations or individuals.

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

How familiar are you with blockchain?



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.

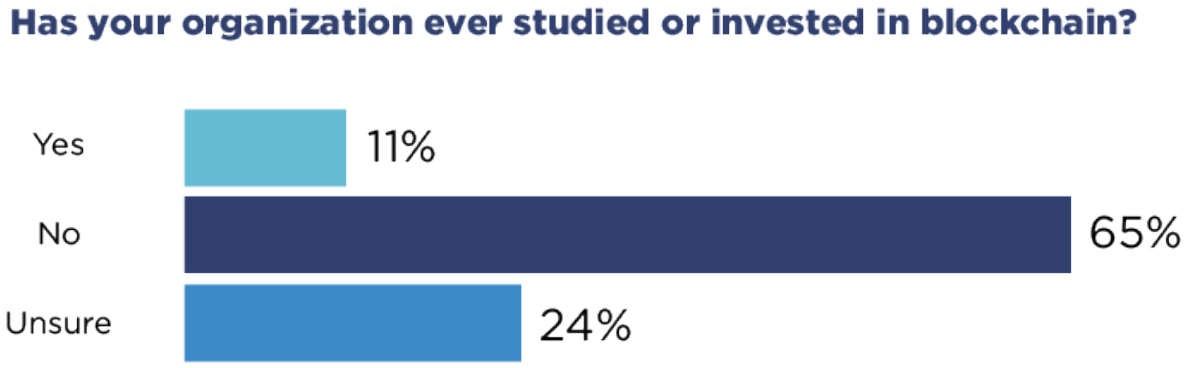
Blockchain offers many security advantages. Advantages include applications in identity management, access control, video verification, private messaging, distributed storage, domain name system integrity, smart contracts, and distributed trust. Some applications, such as identity management and smart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

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.

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.

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. 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 cede 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.

About the ASIS Foundation

The ASIS Foundation, a 501(c)(3) nonprofit affiliate of ASIS International, supports global security professionals through research and education. The Foundation commissions actionable research to advance the security profession. It 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 communities worldwide. To learn more or make a donation, visit www.asisfoundation.org.