Cybersecurity Tech Basics: Blockchain Technology Cyber Risks and Issues: Overview

JARED R. BUTCHER, STEPTOE & JOHNSON LLP, AND CLAIRE M. BLAKEY, PAUL HASTINGS LLP, WITH PRACTICAL LAW DATA PRIVACY ADVISOR

A Practice Note providing an overview of blockchain cybersecurity risks and issues, including a brief review of blockchain technology basics and a discussion of cyber threats to and common vulnerabilities in blockchain applications. This Note also addresses the tension between using blockchain technology and general data privacy obligations and potential uses of blockchain technology to improve overall cybersecurity and minimize cyberattacks.

Blockchain technology increasingly receives attention as a next-generation solution to a wide variety of transactional and recordkeeping problems. As often occurs with innovative technologies, many struggle with understanding its implementation details and potential risks. Organizations considering using blockchain technology and their counsel must:

- Understand basic blockchain technology concepts.
- Assess how its cyber risks may apply to them.
- Make reasonable implementation decisions as the technology and its applications mature.

This Note provides an overview of blockchain technology, highlights how it works from a cyber risk perspective, and examines vulnerabilities that can occur in end-user and blockchain application environments. This Note also discusses emerging issues, such as the tension between using blockchain applications and general data privacy obligations, and applying blockchain technology to better secure the internet of things (IoT).

BLOCKCHAIN TECHNOLOGY DEFINED

Blockchains are digital online ledgers that typically:

- Are implemented in a distributed fashion.
- Allow users to record transactions in a shared ledger.
- Follow established policies but lack a central authority or data repository.

The National Institute of Standards and Technology (NIST) emphasizes that blockchain technology:

- Groups cryptographically signed transactions into blocks to form a ledger.
- Makes the ledger tamper-resistant and tamper-evident by cryptographically linking each block to the previous entry after validation.
- Resolves conflicts automatically using established rules.
- Replicates copies of the ledger across a network of independent nodes.

(Executive Summary, NISTIR 8202, Blockchain Technology Overview, NIST.)

The core ideas behind blockchain technology emerged in the late 1980s and early 1990s. Software developers combined the blockchain idea with other technologies and computing concepts in 2008 to create modern cryptocurrencies, culminating in Bitcoin's 2009 launch.

Cryptocurrency is the most widely recognized application of blockchain technology. Many industries are also exploring blockchain technology-based solutions to enhance efficiency, streamline business processes, and develop trust between parties with little or no knowledge of each other. For example, blockchain technology can support:

- Smart contracts.
- Identity management systems.
- Supply chain solutions.
- Public records, such as property registers.
- Other applications, especially those that require sharing verified data among multiple geographically distributed parties.

Counsel must understand several core blockchain technology concepts to support clients in assessing risks and making sound implementation decisions. Specifically:

- The distinction between public and private blockchains (see Public Versus Private Blockchains).

- Key blockchain technology characteristics, including:
  - ledger distribution (see Ledger Distribution);
  - security measures (see Blockchain Security Measures); and
  - consensus mechanisms (see Blockchain Consensus Mechanisms).

PUBLIC VERSUS PRIVATE BLOCKCHAINS

Public or permissionless blockchains allow any person or system to:

- Access and view the ledger.
- Propose adding new data blocks to the ledger.
- Validate transactions by following established protocols.

Public blockchains have an administrative governance structure but generally operate without any central authority. Examples of public blockchains include most cryptocurrencies, such as Bitcoin and Ethereum.

Private or permissioned blockchains limit access to the ledger to certain known or trusted parties that generally must participate using their true verified identities. They rely on a governance structure and authority to:

- Control access to the ledger.
- Establish functions and the related code to support them, such as implementing smart contracts or supply chain transactions.
- Apply and enforce rules.
- Respond to incidents, including cyber threats.

Public blockchain applications support the broadest participation among parties having little or no knowledge of each other. However, the lack of privacy and the inability to limit participants in a public blockchain can create an unacceptable risk level for some business transactions. Organizations that wish to collaborate without exposing their transactions and business processes to public scrutiny or uninvited participants can benefit from cooperatively developing and supporting private blockchain applications. For example, IBM's Food Trust solution is a blockchain-based network that includes Walmart and other food supply chain participants to track produce accurately and securely from farm to table.

LEDGER DISTRIBUTION

A blockchain uses a distributed ledger, which is an auditable, real-time digital listing of transactions or data that is made available, or distributed, to network participants. The technology:

- Gathers new transactions or other data into blocks.
- Validates them using a consensus mechanism, usually requiring:
  - the participant adding the block to perform some form of work; or
  - approval from the other participants.

  (See Blockchain Consensus Mechanisms.)
- Connects, or chains, the new validated block to the blockchain using a cryptographic hash function.
- Updates the distributed ledger.

Blockchain participants that maintain a copy of the ledger are generally known as nodes. Each node maintains one or more current copies of the ledger on its system. Each node receives an identical copy of the updated ledger as participants add validated data.

Counsel should consider the potential legal implications, including the laws and regulations that may apply, according to how a particular ledger is geographically distributed. For example, some jurisdictions' data localization and data protection laws and regulations may limit whether and where organizations store certain kinds of transaction data (for more discussion on potential data protection and privacy issues, see Tensions Between Using Blockchain Technology and Data Privacy Obligations). Participants in public blockchains typically can only control their own nodes' locations.

However, organizations considering private blockchain projects may:

- Have some influence over most or all of the nodes.
- Wish to build location requirements into the application's administrative governance structure.

(See Public Versus Private Blockchains.)

BLOCKCHAIN SECURITY MEASURES

Blockchain security measures vary according to each individual application but typically include:

- Public-private key method encryption to manage participant access.
- Transaction data integrity protection within blocks using cryptographic hashes. The technology also chronologically records data blocks by securely tying each block to the previous and later blocks. This measure:
  - prevents data tampering within a block because any attempt to alter the data changes the hash values, which other participants can rapidly detect; and
  - provides the immutability principle widely touted for blockchain-recorded transactions.

Specific blockchain applications may use different security measures that affect risk levels. Potential users should investigate and understand the particular measures a blockchain application uses to avoid unexpected vulnerabilities. Private blockchains require heightened scrutiny because they may not have a robust network of users, which is essential for policing attempts to mistakenly or intentionally introduce erroneous data into a blockchain.

BLOCKCHAIN CONSENSUS MECHANISMS

Each blockchain application establishes rules for creating new data blocks in the ledger (see Ledger Distribution). These rules:

- Establish procedures for validating the integrity of new data blocks before they are added to the ledger.
- Apply across all nodes that participate in the blockchain, collectively known as the blockchain's "network."
- Provide consensus mechanisms, which are validation procedures that allow participants to agree on new data blocks. This agreement takes place in code using algorithms that implement the particular blockchain application's governance structure.

Consensus mechanisms typically require a majority or other prescribed number of nodes to agree on whether:

- A new data block is valid and appropriate for inclusion in the shared ledger.
- The ledger and its entire history is currently correct according to the network's rules.

These functions mean that a properly implemented consensus mechanism provides a continuous check on the integrity of both:

- New data blocks.
- Past ledger transactions.

Public blockchains typically use consensus mechanisms, such as:

- Proof-of-work, which uses a system of rewards to induce users to compete for the right to publish the next block by solving computationally intensive puzzles. For example, cryptocurrency miners invest in extensive data centers and computing resources to:
  - solve these puzzles;
  - gain or "mine" rights; and
  - earn rewards for their efforts, such as fees.
- Proof-of-stake, which determines rights for publishing new blocks according to users' current known investment in the blockchain application.

Private blockchains generally use less complicated or computationally intensive consensus mechanisms, such as:

- Proof-of-authority, which verifies a node's identity.
- Simple delegation of authority for approving new blocks to certain trusted nodes.
- Allowing participating nodes to publish new blocks at will or on a rotating basis, subject to verification.

HOW BLOCKCHAIN TECHNOLOGY WORKS FROM A CYBER RISK PERSPECTIVE

Blockchain technology offers important cybersecurity benefits but is not immune from cyberattack. Blockchain applications provide a strong method for securing networked ledgers. However, they do not guarantee the security of individual participants or eliminate the need to follow other cybersecurity best practices. Organizations must distinguish blockchain technology from the environment in which it operates when assessing cyber risks. A blockchain's edge, which includes its points of intersection with users and other connected systems, offers the most likely opportunity for cyberattack.

Key cybersecurity risks and issues to understand when considering using blockchain technology include:

- How blockchain technology protects transaction data (see Blockchain Transaction Security).
- Transaction validation risks and potential blockchain integrity attacks (see Blockchain Network Governance).
- Whether a blockchain application depends on external data or other at-risk resources (see External Data Dependencies and the Oracle Problem).
- The cyber vulnerabilities that may exist in:
  - a blockchain application's implementing code (see Blockchain Code Vulnerabilities);
  - the environment in which the blockchain technology runs (see Blockchain Platform Vulnerabilities); and
  - end-user environments (see End-User Vulnerabilities).

BLOCKCHAIN TRANSACTION SECURITY

Blockchain technology provides a stronger method than traditional, centralized computing services for securing a networked transaction ledger. For example:

- Cyberattackers generally prefer to target centralized databases that once compromised infect and destabilize entire systems. Distributed ledger technologies increase cyber resiliency because there is no single point of failure. An attack on one or a small number of participants does not affect other nodes, which are able to:
  - maintain ledger integrity and availability; and
  - continue transacting with each other.
- The enhanced transparency of distributed ledgers makes it more difficult for cyberattackers to corrupt blockchains using malware or manipulative actions. Each node holds an identical copy of the ledger so participants can quickly detect any attempt to corrupt or inappropriately modify the historical transaction record. The encryption technologies that blockchain applications use to build and link data blocks protect individual transactions and the entire ledger (for more on blockchain security, see Blockchain Security Measures).
- Consensus mechanisms similarly protect new data blocks by requiring network participants to validate and continually compare them with past transactions, which mitigates the possibility of a cyberattacker or rogue organization inappropriately manipulating new ledger blocks (for more discussion on these methods, see Blockchain Consensus Mechanisms).

BLOCKCHAIN NETWORK GOVERNANCE

A blockchain's integrity depends on its network governance model and the methods it uses to validate transactions. Different blockchain applications choose different mechanisms (for more details on common methods, see Blockchain Consensus Mechanisms). Some have suggested the potential for several blockchain integrity attacks, including:

- **Centralization of miners or the 51% attack.** Any blockchain network that relies on a majority consensus to validate transactions is vulnerable if attackers compromise a sufficiently large group of its nodes. For example, bad actors may compromise a public blockchain application if they acquire or control at least 51% of its mining and consensus power. The same problem may result if multiple miners surreptitiously join forces to create a majority and manipulate the blockchain. This scenario is unlikely in a robust network with many users. Some limited blockchains, especially small private implementations, may be more vulnerable. Private blockchain applications typically vet participants and support user authentication and other controls to address this risk.
- **Selfish miners.** Researchers have suggested a scenario where a self-interested public blockchain miner may fool others into wasting time and computing power on already validated transactions, reducing the number of miners doing real mining work and potentially making it easier to manipulate outcomes.
- **The eclipse attack.** Blockchain technology depends on communications across a network of nodes. Disrupting node communications or disseminating or accepting false information to confirm fake transactions may compromise the network.

These attacks become much more difficult in practice as the number of participants increases. It is hard to compromise a majority if the total participants number in the hundreds, thousands, or more. A large number of participants also significantly increases the likelihood of detecting these types of attacks quickly. Legitimate participants would presumably avoid further activities in compromised blockchain networks.

Organizations that are considering using private blockchain technology applications and their counsel should:

- Understand a particular blockchain application's chosen network governance model, consensus mechanisms, and resulting risks.
- Consider various risk management strategies, as with any new technology, including:
  - conducting thorough upfront due diligence;
  - negotiating contractual protections with other participants;
  - implementing continuous monitoring for security incidents; and
  - obtaining appropriate cyber insurance, if available.

EXTERNAL DATA DEPENDENCIES AND THE ORACLE PROBLEM

Blockchains typically function based on information they receive about real-world events. For example, a simple payment transaction requires information sufficient to accurately identify the payor and the payee. More complex applications, such as managing a supply chain or settling cross-border transactions, require even more information. External data sources can create risks that participants must address. For example:

- "Oracles" or "smart oracles" provide trusted data and reference points for blockchain applications, such as pricing data or other economic terms for smart contracts. These external data sources typically fall outside a blockchain application's network consensus validation mechanisms.
- Blockchain networks and participants must take steps to monitor and ensure data reliability because these elements may be more susceptible to tampering or other malicious actions. Hackers may be able to compromise a blockchain's integrity by breaching an oracle or tricking it into using false information.

BLOCKCHAIN CYBER VULNERABILITIES

Blockchain Code Vulnerabilities

Blockchain applications are like any other computer system from the view that software coding errors can introduce cyber risks. Coding errors may be more likely to occur where network protocols implement unusual or novel functionality for which potential vulnerabilities are not yet well understood.

For example, in 2016, hackers exploited a coding defect in the source code of the Decentralized Autonomous Organization (DAO), a virtual organization operated using smart contracts and built on the Ethereum public blockchain, resulting in the theft of Ethereum tokens valued in excess of $50 million at the time.

Blockchain technology is also highly dependent on encryption algorithms. Commonly used encryption techniques are widely vetted and generally reliable. However, as computing techniques evolve, they may become more vulnerable to attack. Emerging technologies, especially quantum computing, which harnesses the unique properties of quantum particles to efficiently perform computing tasks, may make current encryption techniques much less secure.

Blockchain Platform Vulnerabilities

Blockchain applications typically run on general purpose operating systems and platforms that are subject to known hardware and software vulnerabilities. Even special purpose blockchain platforms often depend on general purpose hardware and software.

Organizations must treat these environments like their other business critical computing resources and follow generally accepted cybersecurity practices. Identifying and managing known vulnerabilities is a core element of any reasonable cybersecurity program. For more information on addressing cyber vulnerabilities, see Practice Note, Cybersecurity Tech Basics: Vulnerability Management: Overview (W-013-3774).

End-User Vulnerabilities

The edge of any blockchain where users interact with the system is often the gateway for cyberattacks. For example:

- Cryptocurrency thefts typically involve exploiting vulnerabilities in connected systems. Perhaps an online wallet is hacked or a user's private key is stolen, allowing hackers to drain account balances, but the blockchain itself remains intact.
- End-user vulnerabilities may allow attackers to infiltrate and compromise private blockchains by impersonating authorized users.

Specific end-user vulnerabilities that organizations considering using blockchain applications should address include:

- **Private key management.** Blockchain network integrity depends on encryption algorithms, typically public-private key methods. Most reported blockchain-related cyberattacks have succeeded by stealing end users' keys, not attacking the blockchain itself. Individuals may lose or misplace their private keys, resulting in the loss of blockchain-stored assets because private keys are not reproducible by design. End users must understand and protect the private keys they hold on their systems or other media.
- **Wallet controls.** Service providers, such as digital wallet providers, have emerged to provide key management services and minimize individuals' risks. However, these services depend on passwords, device authentication, such as using a particular mobile phone, or other user authentication controls. Because they involve human interaction, these controls are vulnerable unless individuals and organizations take due care.
- **Impersonation, phishing, malware, and other end-user attacks.** Attackers can use general end-user attacks to gather user credentials or otherwise infiltrate blockchain applications. These attacks can be especially damaging to private blockchains that operate under less robust consensus mechanisms. For more information on general end-user attacks and how to prevent them, see Practice Note, Cybersecurity Tech Basics: Malware and End User Attacks: Overview (W-003-4711).

CYBERSECURITY USE CASES FOR BLOCKCHAIN TECHNOLOGY

Blockchain technology may be able to help solve difficult general cybersecurity problems that require reliable distributed data and records. Some potential applications include:

- Using blockchain technology to support trusted cybersecurity information sharing across widely distributed unrelated organizations (for more details on cybersecurity information sharing, see Practice Note, Data Security Risk Assessments and Reporting: Cybersecurity Information Sharing Programs (W-002-2323)).
- Allowing organizations to validate their software configurations and component lists against known reliable information to detect malware or tampering.
- Building distributed identity management registers.

These use cases and others are the subject of much debate. Viable real-world applications have yet to become mainstream.

TENSIONS BETWEEN USING BLOCKCHAIN TECHNOLOGY AND DATA PRIVACY OBLIGATIONS

A discussion of general data privacy principles and requirements is beyond this Note's scope. However, some have raised concerns about tensions between using blockchain technology and increasingly common data privacy and data protection obligations.

For example, recent trends in global privacy laws and regulations, such as the EU's General Data Protection Regulation (GDPR), support individuals' rights to request data deletion under some circumstances (for more information on the GDPR, see Practice Note, Overview of EU General Data Protection Regulation (W-007-9580)). This "right to be forgotten" can be seen as in tension with the immutability of blockchain transaction records. Specific blockchain applications can reasonably address this and other related data protection issues in various ways, such as:

- Limiting the use of personal data or storing it separately from the transaction register.
- Supporting data processing agreements in private blockchains.
- Using enhanced encryption techniques, such as additional private keys for handling personal data. Organizations can easily destroy these keys if an individual requests deletion, making personal data unrecoverable.

BLOCKCHAIN AND THE INTERNET OF TRUSTED THINGS

Blockchain technology is widely hyped as able to support a variety of innovative and potentially disruptive applications. One increasingly cited area is the fast-growing, cross-sector IoT and the related struggle to validate and secure connected devices.

Blockchain technology may offer security enhancements to IoT devices and their associated networks, creating an internet of trusted things, using:

- **Device authentication.** Blockchain technology may offer a way for devices in an IoT network to:
  - authenticate each other;
  - ensure that their communications with each other are valid; and
  - quickly detect and report rogue devices.
- **Network resilience.** IoT architectures typically use a central authority to manage devices and the data they generate. Blockchain technology enables individual nodes, or devices, to be more independent. For example, IoT devices participating in a blockchain-enabled network may each:
  - determine what is normal device behavior;
  - identify and quarantine devices engaging in unusual behavior; and
  - flag outlier devices for review by a system administrator or other authority.

Regulators may ultimately drive the development of IoT security solutions, whether using blockchain or other technologies. For example, in late 2018, California enacted CA S.B. 327 (2018 Cal. Legis. Serv. Ch. 886 (S.B. 327) (WEST)) (effective January 1, 2020) which sets minimum security standards for connected devices. For more details on California's requirements, see Practice Note, California Privacy and Data Security Law: Overview: Connected Devices (6-597-4106).

01-19


WHITE LABEL
EXCHANGE
Open your own Cryptocurrency Exchange
WE CAN HELP
www.whitelabel.exchange