Microsoft

Advancing Blockchain Cybersecurity:

Technical and Policy Considerations for the Financial Services Industry

CHAMBER OF DIGITAL COMMERCE

Authors

Erin English, Microsoft
Amy Davine Kim, Chamber of Digital Commerce
Michael Nonaka, Covington and Burling

Contributors

Microsoft
Cameron Birge
Amanda Craig
Dave Dadoun
Michael Glaros
Cristin Goodwin
Craig Hajduk
Trey Herr
Aaron Kleiner
Laura Lindsay
Graham Mosley
Jim Pinter
Jong Hyuk Ro

Chamber of Digital Commerce
Perianne Boring

Covington and Burling
David Stein

Contents

Introduction....4

I. Overview of Blockchain Technology....6

A. Two Categories of Blockchains....6

B. Key Features of Permissioned Blockchains....7

II. Common Forms of Cyber-Attacks Affecting the Financial Services Industry....9

III. Cybersecurity Considerations for Permissioned Blockchains....11

A. Capabilities....11

B. Risks....12

C. Structural Considerations Relevant to Permissioned Blockchains....14

IV. Protecting Permissioned Blockchains from Cyberattacks....17

A. National Institute of Standards and Technology's Cybersecurity Framework....18

B. Payment Card Industry Data Security Standard Requirements....19

C. SOC Audit Standards....19

D. Prudential Regulatory Requirements....20

V. Policy Recommendations....20

A. Financial Services Industry Participants Should Apply a Tailored Version of the NIST Cybersecurity Framework to Permissioned Blockchain Activities....21

B. Encourage Regulator-Industry Dialogue, Including Through Regulatory Sandboxes....22

C. Encourage Policymakers to Acknowledge the Unique Cybersecurity Benefits of Blockchain Technologies....22

D. Foster Harmonization Across Cybersecurity Standards Applied to Permissioned Blockchains....23

VI. Conclusion....23

Introduction

Entrepreneurs, investors, and policymakers are increasingly interested in blockchain technology because of its potential to transform the way businesses communicate and interact with their customers, other businesses, and regulators. As a growing number of companies rush to explore blockchain applications, the blockchain ecosystem becomes more diverse and dynamic and better supports sustainable growth and innovation. One of blockchain's benefits is its inherent resiliency to cyber-attack. While not immune to all forms of cyber risk, blockchain's unique structure provides cybersecurity capabilities not present in traditional ledgers and other legacy technologies.

This whitepaper explores the relationship between cybersecurity and blockchain technologies deployed in the financial services industry. The paper's objectives are to educate policymakers and financial industry participants about how blockchains may fit within broader cybersecurity objectives, create a shared understanding of some of the cybersecurity considerations and risk inherent to blockchain, and form recommendations for policymakers and industry to facilitate blockchain innovations that address extant and emerging cybersecurity threats.

Blockchain is a powerful innovation that is poised to bring substantial positive change to the financial services industry as well as many other industries. Despite such promise, blockchain, like any emerging financial services technology, must be evaluated from the perspective of cybersecurity risk – both to an individual financial institution and to the broader and interconnected financial services industry – because cybersecurity is a primary concern to policymakers and financial institutions.

Blockchains have distinct capabilities in mitigating cybersecurity risk to an information technology ("IT") system. The following examples provide an overview of enhanced security features that are enabled by the blockchain architecture:

- The distributed architecture of a blockchain increases the resiliency of the overall network from being exposed to compromise from a single access point or point of failure.
- Consensus mechanisms – a key feature of blockchains – improve the overall robustness and integrity of shared ledgers, because consensus among network participants is a prerequisite to validating new blocks of data, and mitigates the possibility that a hacker or one or more compromised network participants can corrupt or manipulate the ledger.
- Blockchains also provide participants with enhanced transparency, making it much more difficult to corrupt blockchains through malware or manipulative actions. And blockchains may contain multiple layers of security – both at the network level and installed at the level of each individual participant.
- Finally, blockchains hosted on a cloud platform, such as Microsoft Azure, feature even greater cybersecurity protections due to the platform's access controls and many other protections.

Despite the many cybersecurity benefits inherent in blockchains, the technology, like any other, is subject to cybersecurity risks, including those resulting from human errors. Human errors may include software coding errors and errors that derive from the flaws in participants' information security practices. Blockchain technologies also are susceptible to identity-based attacks in which cybercriminals corrupt the consensus mechanism employed by a particular blockchain by gaining control over a majority of the blockchain's nodes. Mitigating these risks requires prudent cyber risk management practices.

A number of important structural considerations should be taken into account when constructing cybersecurity programs for blockchains. Records added to a blockchain generally are immutable. Immutability prevents tampering and creates an auditable record, but may require a special programming adjustment to restore a blockchain's integrity if fraudulent or malicious transactions are introduced into a blockchain. Blockchain participants' roles and responsibilities also require a thoughtful governance structure in order to achieve an effective balance of access and security.

To explore the intersection between blockchain and cybersecurity in the financial services industry, this paper covers the following topics:

- **Key Blockchain Features.** An overview of blockchain, including key features of blockchains;
- **Common Cyber Attacks.** A discussion of common forms of cyber-attacks faced by the financial services industry;
- **Technology-Specific Considerations.** A review of cybersecurity considerations for permissioned blockchains, including unique capabilities, risks, and technology-specific considerations;
- **Application of Existing Standards.** An examination of existing cybersecurity standards relevant to permissioned blockchains; and
- **Policy Recommendations.** A concluding set of recommendations for regulatory and industry approaches to fostering the development of permissioned blockchains and related internal controls to mitigate cybersecurity risk.

I. Overview of Blockchain Technology

Public blockchains, such as the Bitcoin blockchain or the Ethereum public blockchain, permit any person with the technological capability to access and view the ledger, propose the addition of new blocks to the ledger, and validate transactions by following established protocols.

Anyone who installs certain software is generally granted access and can participate in transactions using the blockchain.

The terms "blockchain" and "distributed ledger technology" ("DLT") are often used interchangeably, but they are distinct innovations. DLT is a family of technologies that employs a shared database architecture to maintain multiple, identical copies of an auditable, up-to-date distributed or decentralized ledger of transactions or data. A "blockchain" is a specific type of DLT and a method of organizing data in aggregated, ordered "blocks" that are "chained" together by a cryptographic hash function.[1] New blocks are added to a blockchain after validation of the integrity of the blocks by a network of participants or "nodes" through a rules-based consensus mechanism. Blockchains are used to create and maintain a shared system of record and platform for tracking transactions or other data. When used in combination, blockchain's complementary technologies provide a powerful toolkit for a broad range of commercial applications. For purposes of this paper, we use the term "blockchain" to refer to the technology under discussion for simplicity and ease of reference.

A blockchain can be tailored to accommodate various types of data, and many industries are exploring blockchain solutions to enhance efficiency, streamline cumbersome or fragmented business processes, and develop trust between counterparties based on the integrity of the technology. In the financial services industry, blockchain developments generally have focused on more efficient alternatives to resource-intensive processes, such as processes that rely on intermediaries to establish trust and facilitate communication between multiple entities, often across geographies. Potential uses for blockchains in the financial services industry include enhancing the efficiency of trade finance; cross-border payments; compliance and audit functions, including the Bank Secrecy Act, anti-money laundering, and know your customer compliance; and the settlement and clearing of securities and derivatives transactions.

A. Two Categories of Blockchains

Permissioned blockchains limit access to the ledger to certain known or trusted parties who generally must participate using their true identities.

Permissioned blockchains may be developed by a single party (private blockchain) or by a consortium of companies, such as a group of banks, with similar interests (consortium-based blockchain).

There are two broad types of blockchains: public and permissioned blockchains. Public blockchains, such as the Bitcoin blockchain or the Ethereum public blockchain, permit any person with the technological capability to access and view the ledger, propose the addition of new blocks to the ledger, and validate transactions by following established protocols. Anyone who installs certain software is generally granted access and can participate in transactions using the blockchain. The consensus mechanisms used in public blockchains to create trust among participants who do not know each other include but are not limited to: (a) proof-of-work, which uses a system of rewards to induce constructive behavior by requiring users to compete for the right to publish the next block by solving computationally intensive puzzles; and (b) proof-of-stake, which uses a system of penalties and the amount that a user has at risk in the blockchain to determine rights to publish new blocks.[2] While public blockchains have an administrative governance structure, they generally operate without any central authority.

---

[1] A blockchain combines two distinct technological innovations: (a) a hash tree, also known in this structure as a "Merkle tree," which is a data structure that combines the hash values of transaction-level data into a single "tree" that is stored within the block and within the next block; and (b) distributed ledger technology. In essence, a blockchain is a DLT that uses a hash tree (Merkle tree) data structure.

[2] Ethereum's founder has suggested that, in the future, the Ethereum public blockchain will move to a proof-of-stake consensus model. *See* https://medium.com/cybermiles/first-impressions-of-ethereums-casper-proof-of-stake-pos-5ce752e4edd9; https://medium.com/@VitalikButerin/a-proof-of-stake-design-philosophy-506585978d51

Permissioned blockchains limit access to the ledger to certain known or trusted parties who generally must participate using their true identities.[3] Permissioned blockchains may be developed by a single party (private blockchain) or by a consortium of companies, such as a group of banks, with similar interests (consortium-based blockchain). Permissioned blockchains rely upon a governance structure to control access, apply and enforce rules, and respond to incidents, including cyber threats. Because there is some degree of trust between participants, permissioned blockchains generally use less complicated or computationally intensive consensus mechanisms. A proof-of-authority consensus model, for example, may allow participating nodes to publish new blocks at will or on a rotating basis, subject to verification of participation rights. Permissioned blockchains can incorporate traditional security features, such as access controls managed through a cloud platform, as well as security features that are customized to the particular blockchain.

From a cybersecurity perspective, both public and permissioned blockchains have certain favorable attributes, including distribution of the ledger, encryption, and a consensus mechanism. Each type of blockchain also presents distinct cybersecurity considerations. An assessment of the relative merits of these two types of blockchains is beyond the scope of this paper. The balance of this paper focuses on the cybersecurity aspects of permissioned blockchains, which have been of greater interest to the financial services industry.[4]

B. Key Features of Permissioned Blockchains

A permissioned blockchain is a network generally comprised of several different types of select participants. Participants may include, for example, a developer; owner-participants that fund development and use of the solution, such as a consortium of banks; non-owner participants or other trusted parties that are granted limited usage rights necessary to the functioning of the system; a managing entity; and a technology service provider including, for example, a cloud service provider ("CSP") or encryption key management service provider. Not all permissioned blockchains include each of these types of participants, as permissioned blockchains are constructed and managed in different ways. For instance, a technology service provider may also serve as the managing entity; or a developer may be the owner and the managing entity, with all other participants classified as non-owner participants. For purposes of this paper, a "network" refers to a simple permissioned blockchain consisting of a developer, a group of owner-participants, and a combined technology service provider/managing entity.

[3] Ethereum, for example, has both a public and a permissioned blockchain.

[4] The Chamber of Digital Commerce has members that explore one or both of these types of blockchains. The Chamber's mission is to promote the acceptance and use of all types of digital assets and blockchain technology.

A blockchain typically includes the following features:

Characteristics of Public and Permissioned Blockchains	
Distributed ledger	Participants or "nodes" maintain one or more current copies of the ledger on their systems. As data is added to the ledger, the nodes receive identical copies of the updated ledger. The use of a shared, distributed ledger offers a measure of resilience by limiting the impact of a cybersecurity incident experienced by any single node and preventing a single point of failure from being used to disable the network, while enabling affected nodes to recover quickly from an incident by obtaining copies of the ledger held by other nodes.
Encryption	Blockchains rely on encryption deployed at several different points in the network. First, participant access rights are managed by employing public/private key encryption. Second, the transactional data within a block is encrypted using cryptographic hashes. Third, blocks of data are linked in chronological order in a blockchain using a cryptographic hash function that securely ties each block to the previous and subsequent blocks. Thus, any attempt to alter data within a block would change the hash values. Cryptographic hashing prevents data within a block from being changed without altering the history of all linked or chained blocks of data. Thus, would-be attackers targeting a particular transaction would need to change the entire blockchain as a result of this form of encryption.
Consensus mechanism or consensus validation procedures	A blockchain's rules establish procedures for validating the integrity of new blocks of data before they are added to the ledger. These rules are known as consensus mechanisms or consensus validation procedures. In a permissioned blockchain, the owner-participants or managing entity establish the rules for validating the integrity of new blocks of data before they are added to the ledger. In general, an authorized participant proposes a new block, and other nodes review and confirm that the proposed block satisfies network rules. A mathematical or consensus algorithm monitors whether a specified number or percentage of nodes have reached a consensus on the integrity of a proposed block. If the nodes reach a consensus, the new block is added to the ledger. Once added, the new block and the data it contains are immutable. There are various models for consensus mechanisms, including proof-of-work, proof-of-stake, and proof-of-authority. Proof-of-authority is the model typically used in permissioned blockchains because it requires the parties to have some degree of trust, while the proof-of-work and proof-of-stake models do not assume such trust and are more commonly used in public blockchains. Consensus mechanisms help to ensure that new transactions added to the blockchain are validated by participants and not introduced fraudulently by cyber-attackers.
Initiation rules and processes	Every blockchain has rules and processes for initiating or proposing new blocks for addition to the ledger. In a public blockchain, any participant may be able to propose new blocks. In a permissioned blockchain, the owner-participants or managing entity establish rules and processes for the initiation or proposed addition of new blocks of data to the ledger. The rules of a permissioned blockchain, for example, identify participants authorized to propose the addition of new blocks of data and when, and the circumstances under which they may have such rights terminated or suspended, and therefore help to detect and prevent access to the network by cyber attackers. For example, if a participant's system is considered vulnerable or has been compromised, or if the participant has submitted a certain number of invalid blocks of data to the ledger, the participant's privileges may be suspended or revoked by the managing entity.
Characteristics of Permissioned Blockchains	
Membership, access, and participation restrictions	Owner-participants of a permissioned blockchain establish rules regarding membership, access, and participation rights, including the criteria for granting and terminating such rights. The owner-participants generally delegate responsibility for implementing and enforcing such rules to a managing entity and may authorize the managing entity to amend the rules to address evolving conditions. In addition to membership, access, and participation restrictions, data on the network could be compartmentalized to prevent intentional or inadvertent access to the sensitive commercial and customer data of other participants.

II. Common Forms of Cyber-Attacks Affecting the Financial Services Industry

The financial services industry faces evolving and dynamic cyber threats intended to exploit vulnerabilities, disrupt systems, and steal data and funds. These attacks continue to increase in frequency and sophistication.[5] A number of high profile cyber-attacks against banks in recent years have served to highlight the escalating threats to the security of customer funds and financial data.[6] The attacks described in this section generally target all types of financial institutions systems, not just blockchains.[7] The range of cyber-attacks targeting the financial services industry include:

- **Malware.** Malicious software or "malware" that compromises an institution's data or damages the institution's information systems can be introduced in a variety of ways.[8] For example, phishing campaigns are used by hackers to induce a person to click on a link to a malicious URL or attachment that installs malware on the person's IT system. Such campaigns also can be used to obtain customer log-in credentials and other sensitive information by installing malware to record customer information entered into fake sources that appear legitimate, leading to the direct compromise of data.

- **Web Application Attacks / Credential Stuffing.** Attacks targeting web applications are often an initial step in mining personal data and credentials that are used by hackers to compromise data on other systems. Depending on the volume of data that is being used to gain further access, data gleaned from a web application attack can form part of an advanced brute force attack that leverages stolen usernames and passwords to gain access to customer accounts. In this type of attack – known as "credential stuffing" – stolen login credentials are systematically and repeatedly input into the login fields of a website using automated scripts or modified software in order to gain access. Once the hacker successfully accesses an account using a stolen username and password, the hacker has access to the account funds and financial data.

- **Distributed Denial of Service (DDoS) Attacks.** DDoS attacks primarily target large organizations. Using botnets[9] or other compromised systems, a DDoS attack sends a stream of traffic and data to a targeted website to overload the system and temporarily or permanently disrupt system operations. In a blockchain network, the cybersecurity controls established at each node provide an additional layer of security that contributes perimeter defense and defense in depth for the network.

---

[5] *See* Office of the Comptroller of the Currency, Semiannual Risk Perspective from the National Risk Committee, p. 2 (Fall 2017) ("The speed and sophistication of cybersecurity threats are increasing. Banks continually face threats seeking to exploit bank personnel, processes, and technology. These threats target large quantities of personally identifiable information and proprietary intellectual property and facilitate fraud and misappropriation of funds at the retail and wholesale levels.").

[6] For example, in 2016 hackers stole more than 2 billion rubles (US $31 million) from customer accounts at the Central Bank of Russia using compromised customer credentials. *See* Jeremy Kirk, Reports: *Hackers Steal $31 Million from Russia's Central Bank*, Reuters (Dec. 5, 2016). In July 2017, UniCredit reported a data security breach that compromised client data of approximately 400,000 customers and resulted from infiltration of one of the bank's commercial partners. *See* Paola Arosio & Gianluca Semeraro, *Italy's UniCredit reveals data attack involving 400,000 clients,* Reuters (July 26, 2017). In February 2018, City Union Bank in India was subject to a cyberattack resulting in the transfer of nearly $2,000,000 in remittances using the SWIFT payment network. This is just one in a series of hacks involving the SWIFT network, including $81 million from the Bangladesh central bank. *See* Devidutta Tripathy, *India's City Union Bank CEO says suffered cyber attack via SWIFT system,* Reuters (Feb. 18, 2018); and see Michael Corkery, Hackers' $81 Million Sneak Attack on World Banking, New York Times (Apr. 30, 2016)

[7] As described in the next section, characteristics of blockchains may make them more resistant to certain types of attacks.

[8] *See* SANS Institute, *Securing Against the Most Common Vectors of Cyber Attacks* (August 2017), *https://www.sans.org/reading-room/whitepapers/riskmanagement/securing-common-vectors-cyber-attacks-37995.*

[9] A "botnet" is a group of compromised computers connected in a coordinated fashion and controlled by cybercriminals for malicious purposes.

For all systems, the theft of passwords or other access devices through various forms of attack is a common and recurring problem.

Blockchains are no different.

The majority of attacks related to blockchains have been designed to steal cryptographic keys, not necessarily attack the blockchain itself.

- **Man-in-the-Middle (MITM) Attack.** Much like eavesdropping, a MITM attack involves an unauthorized actor positioning its system or access tool in transmissions between a user and a trusted party in order to capture or intercept data. There are two types of MITM attacks. A standard attack involves an unauthorized actor within physical proximity of the target who can gain access to an unsecured network, such as a Wi-Fi router. The second type is commonly referred to as a "Man-in-the-Browser" attack and involves the use of malware, which is injected into an unsuspecting user's system and, without the knowledge of the user, records the data that is being sent to a trusted third party website, such as a bank.

- **Ransomware Attack.** Ransomware attacks threaten to block an institution's access to its own data unless the institution makes a payment to the hackers. Ransomware attacks are especially pernicious in the financial services industry given the importance of customer data and the broader risks if it is compromised. Ransomware attacks pose reputational risk for targeted financial institutions because depositors may withdraw funds en masse based on concerns that their funds are not secure. Ransomware attacks are popular because they can be carried out anonymously.

- **Theft of Keys.** For all systems, the theft of passwords or other access devices through various forms of attack is a common and recurring problem. Blockchains are no different. The majority of attacks related to blockchains have been designed to steal cryptographic keys, not necessarily attack the blockchain itself. This experience underscores the importance of enterprise key management to reduce the risk of stolen or compromised keys.

- **Attacks on process.** Blockchain also introduces different attack vectors that malicious actors may seek to exploit. For example, advanced attackers will look to influence decision-making processes around the blockchain in order to add new parts to the chain, change rules or policies, or manipulate a managing entity in such a way that is not transparent or is fraudulent. Attackers will also seek to create new fraud through mechanisms that will need to be created to adjudicate and remediate fraud. Ultimately, an integrity control system will be needed to ensure that those in control of decision-making in relation to the chain are acting as fiduciaries of the chain, rather than as self-interested owners of the chain.

Financial regulators identify cybersecurity as one of the most pressing risks to the financial services industry because banks are frequently under attack and customers are increasing their reliance on technology to obtain banking services. Moreover, due to the interconnectedness of the global financial system, a cyber-attack at one bank may affect other banks and financial institutions.[10] These considerations apply with equal force to permissioned blockchains, which rely upon ongoing interconnections.

[10] *See*, e.g., Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, Office of the Comptroller of the Currency, Enhanced Cyber Risk Management Standards, 81 Fed. Reg. 74315, 74316 (Oct. 26, 2016).

III. Cybersecurity Considerations for Permissioned Blockchains

Permissioned blockchains present unique opportunities in managing cybersecurity risks. As the financial services industry explores the use of permissioned blockchains to enhance services and operations, industry participants should recognize and take into account a number of cybersecurity capabilities, as well as risks and other considerations relating to this technology.[11]

A. Capabilities

The features of permissioned blockchains provide for a number of capabilities in mitigating cybersecurity risks and detecting, preventing, and combating the types of cyber-attacks that are often directed at financial institutions. The capabilities include the following features:

- **Distributed architecture.** The distributed architecture of a permissioned blockchain is an advantage that can deter or minimize the effect of cyber-attacks. Threat actors generally prefer to target a centralized database that, once compromised, would infect and destabilize the system as a whole. A distributed network structure, however, provides inherent operational resilience because there is no single point of failure. With the risk of compromise dispersed among various nodes, an attack on one or a small number of participants would not result in the loss or compromise of the ledger stored on computer nodes not subject to attack. This distributed architecture, for example, makes permissioned blockchains less appealing targets for ransomware attacks since a ledger securely stored in multiple nodes is less susceptible to lock down by a hacker than centrally stored information. To be successful, a ransomware attack would need to compromise all or most nodes in the network. Nevertheless, restoring full service after an individual node or handful of nodes has been compromised will not be instantaneous, and there will be some latency effects on the network in recovery.

- **Consensus validation mechanism.** The use of consensus mechanisms for validating new blocks of data confers another key cybersecurity advantage on a permissioned blockchain network. A consensus mechanism requires a prescribed number of nodes to reach a consensus on whether a new block of data is valid and suitable for inclusion in the shared ledger and whether the ledger itself, with its entire history, is correct, pursuant to the network's validation rules. A consensus mechanism provides a continuous check on the integrity of past transactions identified on the ledger and on the integrity of new blocks of data. An attacker attempting to compromise the ledger would be required to co-opt the consensus mechanism by compromising enough nodes to manipulate the consensus validation process and thereby corrupt or tamper with the ledger. A permissioned blockchain network may prevent such an attack from being effective if the network contains a sufficient number of nodes and network rules require a significant degree of consensus among nodes.

- **Encryption.** Permissioned blockchain networks employ multiple forms of encryption at different points, providing multilayered protections against cybersecurity threats. Participant access rights are secured through asymmetric-key cryptography or public/private key encryption. The linked lists or blocks are also encrypted by a combination of cryptographic hashing and digital signatures, with the latter based on public/private key encryption.

[11] Many of the capabilities, risks, and other considerations discussed throughout Section III apply to all blockchains. For purposes of this paper, however, the discussion in Section III focuses on permissioned blockchains.

Strong key management preserves the integrity of the public/private key encryption mechanism, and helps fortify the ledger and the network against cyberattacks.

- **Transparency.** Transparency in permissioned blockchain networks provides another degree of cybersecurity protection. For example, the transparency of a permissioned blockchain among participants makes it more challenging for hackers to place malware in the network to collect information and to transmit it covertly to another database managed by the hacker.[12] Because each participant has an identical copy of the ledger, the network creates the opportunity for deploying enhanced compliance processes including, among other things, real-time auditing or monitoring by other participants or by regulators granted limited access to the network. As a result, vulnerabilities and threats may be identified quickly if good risk management and compliance controls are implemented.

- **Administrator Risk Controls.** Permissioned blockchains often are hosted on cloud platforms that have robust cybersecurity controls across different layers of the technology stack. Moreover, major CSPs like Microsoft voluntarily submit to periodic independent audits led by internationally-accredited firms, which focus on the CSP's adherence to industry-leading standards from the International Standards Organization (ISO), the U.S. National Institute of Standards and Technology (NIST), and others. Cloud computing offers participants an easily accessible and highly fault-resistant platform, resulting in less downtime, less risk of lost transactions, and less risk of failure to reach consensus. CSPs also have the ability to implement system-wide updates and patches in a much more rapid and comprehensive manner, while leveraging maximum threat intelligence detection across the network.

B. Risks

Notwithstanding the significant capabilities described above, permissioned blockchains, like all computer systems or Internet-based technologies, remain subject to inherent cybersecurity risks that require thoughtful and proactive risk management. Many of these risks involve a human element. Therefore, a robust cybersecurity program remains vital to protecting the network and participating organizations from cyber threats, particularly as hackers develop more knowledge about permissioned blockchains and their vulnerabilities.

A sample of cybersecurity risks associated with permissioned blockchains include:

- **Key management.** Perhaps the single most important risk to blockchain security is key management. Maintaining the confidentiality, integrity, and availability of private keys requires thoughtful and robust cybersecurity controls. Some individuals reportedly have lost or misplaced their private keys, resulting in the loss of assets stored on a blockchain because private keys, by design, are not recoverable. To minimize individual mistakes, service providers, including digital wallet providers and CSPs, have emerged to provide key management services, which has become a critical feature of all types of blockchains. To date, the majority of cyber-attacks related to blockchains have not attacked the blockchains themselves, but have targeted providers of key management services in attempts to steal private keys.

[12] Transparency in a permissioned blockchain network is not absolute. For competitive and privacy reasons, transaction-level data generally is not included in the ledger; rather, a representation of such data is included in the ledger with the underlying transaction-level data stored off-chain. For the same reasons, participants usually incorporate privacy overlays into permissioned blockchains.

- **Software coding errors/protocol vulnerabilities.** As with any computer IT system, human coding errors can introduce cybersecurity risk into blockchains. Permissioned blockchains are built on software code, as are numerous off-chain applications that interface with such blockchains. No software is 100% free from defects, and any defect has the potential to be exploited to compromise a cybersecurity program. For example, hackers in 2016 exploited a coding defect in the source code of a virtual company, known as the Distributed Autonomous Organization (DAO), which resulted in the theft of $55 million.[13] The DAO was a virtual organization operated through smart contracts[14] and built on the Ethereum public blockchain. Secure coding procedures, the application of security by design principles, a robust quality assurance ("QA") program, extensive security testing, and the avoidance of rushed coding processes and production schedules can help to minimize coding defects. These best practices are particularly important where network protocols implement unusual or novel functionality for which potential vulnerabilities may not be well understood.

- **External data sources and endpoint risk.** Permissioned blockchains are only as secure as the information they ingest and consume. Such blockchains do not operate in a vacuum but incorporate, interface with, and rely upon external data sources. From a cybersecurity perspective, these interactions introduce risk into the blockchain network.

  The legacy systems of participants are one external data source. These off-chain legacy systems provide the transactional data from which the representational data stored on a blockchain is constructed. The importation of such off-chain, legacy system data presents one endpoint risk. As noted previously, for competitive, privacy, and other reasons, financial institutions typically include only a small amount of representational data in a block while maintaining full records in off-chain legacy systems. It is critical that network rules require participants that introduce data from such legacy systems ensure that the cybersecurity protections applied to those systems meet defined cybersecurity standards.

  "Oracles" or "smart oracles" are another type of external data source. These off-chain applications from trusted sources submit data and provide reference points, such as pricing data, to trigger smart contract performance. Oracles, however, fall outside the consensus validation mechanism of a permissioned blockchain. Therefore, the data contributed by oracles is not subject to the structural protections inherent to the network and is more susceptible to tampering or malicious alteration.[15]

- **Identity-based attacks.** Permissioned blockchains are not immune from identity-based attacks like those targeting other IT systems, such as spoofing or Sybil attacks. Such attacks could be employed to take over a majority of the nodes in a network and undermine the consensus validation and distributed architecture protections of a network. This risk can be mitigated using a trusted multi-tenant cloud-based directory and identity management service that certifies the identities of persons

[13] David Siegel, *Understanding The DAO Attack*, Coindesk (June 25, 2016), https://www.coindesk.com/understanding-dao-hack-journalists/.

[14] "Smart contracts" are computer code representing an agreement between parties that tracks state changes with the potential to result directly in transfers of data, assets, rights, or liabilities

seeking to participate in the network.[16] Any external threat actor that attempts to take over nodes on the network would be identified by the service and refused access to the network. These cloud-based services deploy their own cybersecurity protections and provide an additional layer of protection for the network.

- **Evolving attack vectors.** It is reasonable to expect new strategies and threats to emerge to exploit unforeseen vulnerabilities in blockchains. One longer-term risk that is gaining attention among observers is the possibility of quantum computing-based attacks that leverage enhanced computational power to weaken or compromise existing cryptographic algorithms used in existing IT systems and in blockchains.[17] As a general matter, all participants in blockchain systems need continuing education to anticipate and protect against threats from new attack vectors, and to adapt and upgrade security protocols as necessary to ensure the success and viability of the network.

C. Structural Considerations Relevant to Permissioned Blockchains

Permissioned blockchains have structural characteristics that are relevant to technology officers who are tasked with designing information security systems for such solutions or adapting existing systems to such solutions. These characteristics include:

- **Immutability.** The immutability of blockchain records is an essential attribute of permissioned blockchains. Immutability prevents tampering with records in the ledger and creates a final auditable record. But immutability also limits recovery options when fraudulent or malicious transactions are introduced into a blockchain ledger. In most cases, a hard-fork is needed to isolate such transactions and redirect the ledger around such transactions. Participants in a permissioned blockchain can establish governance structures and procedures to address incidents in which fraudulent or malicious transactions are introduced into the ledger. It is nonetheless incumbent upon network participants to weigh the pros and cons of immutability, and the efficacy of workarounds, when developing permissioned blockchains, particularly for financial services applications.

- **Network effects.** The distributed network structure of permissioned blockchain creates inherent operational resilience because there is no single point of failure in the network. On the other hand, the participation of multiple entities, each with their own firewalls, is a source of external vulnerability. This structure poses challenges in managing identities, participation rights and limitations, public/private key storage, maintenance, and issuance, and security configurations across multiple external parties. Moreover, financial industry participants in permissioned blockchains each have their own cybersecurity programs and follow their own

[15] One Microsoft solution that addresses the risks inherent in oracles is the use of "cryptlets." Cryptlets operate outside of the permissioned blockchain network and are designed to provide a secure, trustworthy way to serve as an oracle to a smart contract and reduce data quality risks.

[16] More broadly, Microsoft is exploring decentralized digital identity solutions that leverage public blockchains in order to create a secure encrypted digital hub where individuals can store their identity data and easily control access to it. Microsoft likewise has been promoting integrity and security in digital ID solutions using its cloud computing services. *See* Alex Simons, *Decentralized Digital Identities and Blockchain – The Future as We See It,* Microsoft Enterprise Mobility + Security (Feb. 12, 2018).

[17] Yaga, Mell, Roby and Scarfone, *Blockchain Technology Overview, Draft NISTIR 8202* at 34 (National Institute of Standards and Technology, January 2018).

cybersecurity risk reduction techniques. This structure provides perimeter defense and defense in depth, but also requires additional planning to make sure these programs are not inconsistent with, and indeed complement, the blockchain network's cybersecurity program.

The use of a CSP with a mandate to implement comprehensive network security using cloud technology and to enforce participants' compliance with network rules is an effective way to manage a permissioned blockchain in accordance with prevailing cybersecurity standards. CSPs can manage a formal process for key issuance, revocation, and rotation; manage, adjust, and terminate participant permissions; compartmentalize blockchain data to reduce security and competitive risks; establish gateways and other access controls to shield the permissioned blockchain from the public internet; and conduct audits of participants. In this way, CSPs can act as a trusted technology platform to support permissioned blockchains that are reliable, resilient, and scalable.

- **Roles and responsibilities of participants.** To maintain strong network security, the roles and responsibilities of each type of participant must be clearly defined and enforced, and the cybersecurity risks posed by each type of participant must be identified and managed. It is also essential to anticipate the security consequences of participants leaving and entering the network over time.

  Blockchain developers are frequently start-up firms, although many are led by seasoned industry veterans. Regardless of a developer's size or the experience of its personnel, all blockchain developers, particularly those developing solutions for the financial services industry, must conduct their design and development activities at a high level of sophistication relative to security threats.

  All developers should incorporate the principles of the Systems Development Life Cycle ("SDLC") or "security-by-design" and internalize those principles into its culture. For this purpose, the SDLC principles outlined in ISO/IEC 27034-1:2011 are particularly appropriate. The SDLC and security-by-design principles in ISO/IEC 27034 incorporate security controls, referred to as "application security controls," into all aspects of the software and into all aspects of the design-to-production phases. The use of "hardened libraries" and other controls for securing code and software-related information and testing is critical. In addition, all blockchain coding should undergo and pass QA testing that satisfies the ISO/IEC 27034 standards – including testing of all application security controls as part of an application security verification process – to identify and fix bugs, as well as security testing, before rollout.

  Working with network participants, developers need to understand the full range of potential threats that arise from financial institutions interoperating with third parties, including third parties not evaluated when initial design decisions were made. Blockchain developers should anticipate threats resulting from interoperability, conduct threat modeling, conduct penetration testing using various attack scenarios and vectors, document the development process, and obtain independent audits of the design and development process. A sophisticated managing entity with extensive network development expertise can help vet, educate, and oversee developers to ensure adherence to these principles.

  Owner-participants tend to be established financial services firms. The roles and responsibilities of these firms can vary, but generally include the following: developing the structure of the permissioned blockchain; selecting a developer

Blockchain developers are frequently start-up firms, although many are led by seasoned industry veterans.

Regardless of a developer's size or the experience of its personnel, all blockchain developers, particularly those developing solutions for the financial services industry, must conduct their design and development activities at a high level of sophistication relative to security threats.

and exercising appropriate oversight over the developer consistent with existing regulatory expectations; selecting a managing entity qualified to manage the network and exercising appropriate oversight over the managing entity consistent with regulatory expectations; and developing and agreeing to network rules and protocols. From the perspective of cybersecurity, these firms should agree on common cybersecurity standards applicable to all participants and a mechanism to verify compliance with those standards, and establish protocols for how to integrate external data from legacy systems into permissioned blockchains without introducing cyber threats or compromising security.

The managing entity implements and enforces network rules and protocols. Network rules should address what data to include and not to include on the blockchain in view of competitive considerations, participant turnover, and best practices for security and privacy. The managing entity's roles and responsibilities may include the following: enforcing agreed upon cybersecurity standards; providing secure and compartmentalized platforms to facilitate collaboration and interoperability without undermining security or competitive interests; managing participant access and permissions; managing the public/private key infrastructure; conducting validation audits on participants; and responding to cybersecurity incidents that impact the network.

IV. Protecting Permissioned Blockchains from Cyberattacks

Because permissioned blockchains continue to evolve, the cybersecurity controls that best mitigate risk also continue to evolve. The architecture, deployment, and operation of a permissioned blockchain impact the network's inherent cybersecurity risks and determine the controls best able to mitigate those risks. Key considerations include the number and types of participants in the network; the ability of untrusted or unauthorized persons to participate in the network; the design and robustness of the initiation and consensus validation rules and processes; the strength of the encryption protocols (including the cryptographic hash algorithms); the extent of reliance on externally-sourced data; the sensitivity of the records or transactions recorded in the electronic ledger; and the ability to correct fraudulent, malicious, or erroneous records.

Cybersecurity principles and controls from existing laws, regulations, and industry guidance are critical components to an effective cybersecurity program for a permissioned blockchain.

Many financial regulators have issued detailed guidance for financial institution cybersecurity programs, and this guidance likewise should inform the controls established for permissioned blockchains used by financial institutions.

Cybersecurity principles and controls from existing laws, regulations, and industry guidance are critical components to an effective cybersecurity program for a permissioned blockchain. Many financial regulators have issued detailed guidance for financial institution cybersecurity programs, and this guidance likewise should inform the controls established for permissioned blockchains used by financial institutions. These principles and controls include:

i. Access controls on customer information systems, including controls to authenticate and permit access only to authorized individuals and controls to prevent employees from providing customer information to unauthorized individuals who may seek to obtain this information through fraudulent means;

ii. Threat modeling conducted by software developers who best understand the technology and can analyze threats and mitigation in a detailed, granular fashion;

iii. Encryption of electronic customer information, including while in transit or in storage on networks or systems to which unauthorized individuals may have access;

iv. Procedures designed to ensure that customer information system modifications are consistent with information security programs;

v. Dual control procedures, segregation of duties, and employee background checks for employees with responsibilities for or access to customer information;

vi. Systems and procedures to detect actual and attempted attacks on or intrusions into customer information systems;

vii. A well-planned, properly structured audit program to evaluate cybersecurity risk management practices, internal control systems, and compliance with laws, regulations, and corporate policies concerning IT-related risks; and

viii. Response programs that specify actions to be taken when the financial institution suspects or detects that unauthorized individuals have gained access to customer information systems, including appropriate reports to regulatory and law enforcement agencies.

Existing cybersecurity standards and guidance remain highly relevant for ensuring the security of permissioned blockchains. Most CSPs, particularly those that support the financial services industry, should already have these controls in place. Subject to certain adjustments to take into account specific attributes of permissioned blockchains, existing standards and guidance provide a strong foundation for protecting permissioned blockchains from cyber-attacks.

In addition to these general principles and controls, certain specific cybersecurity standards widely-used in the financial services industry have particular relevance to permissioned blockchains:

A. National Institute of Standards and Technology's Cybersecurity Framework

In 2014, the National Institute of Standards and Technology ("NIST") published a Framework for Improving Critical Infrastructure Cybersecurity (the "Cybersecurity Framework" or the "Framework").[18] NIST recently published a proposed update to the Cybersecurity Framework in December 2017.[19]

The NIST Cybersecurity Framework is a voluntary framework designed to help organizations better understand, manage, and reduce their cybersecurity risk. It provides a high-level, strategic view of the lifecycle of an organization's cybersecurity risk management and can be tailored to specific business sectors and companies. Although it is voluntary, many companies across industries, particularly financial institutions, are developing cybersecurity programs aligned with the Framework.[20]

The Framework describes five broad functions – identify, protect, detect, respond, and recover – that define the high-level goals of a cybersecurity risk management program. It also identifies specific categories of cybersecurity outcomes that elaborate on the functions and are tied to particular activities. The functions and categories represent a helpful way to evaluate and comprehensively think about mitigating the cyber risk of a blockchain solution in the context of an organization's broader technology decisions and overall risk. In many cases, blockchain may facilitate the goals or activities specific in the functions and categories. For example, the detect function focuses on detecting anomalous behavior, and blockchain lends itself to the deployment of new threat detection technologies. Specific categories underlying the functions, including risk assessment, access controls, data security, and response planning, also align well with the unique cybersecurity capabilities of permissioned blockchains. For example, the ability to create strong encryption protocols for a blockchain is consistent with the Framework's emphasis on protective technology solutions that are designed to ensure the security and resilience of IT systems and assets.

As part of a review of their cybersecurity capability maturity, companies often will use the Framework to do a regular self-assessment or engage outside auditors or consultants to assess their maturity against the Framework's "tiers." The guidance outlines four implementation "tiers" that are based on an organization's cybersecurity risk management priorities as well as its investments and processes in place to manage that risk.

---

[18] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity Version 1.0* (Feb. 12, 2014).

[19] NIST, *Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 Draft 2* (rev. Dec. 5, 2017).

[20] NIST recently issued in draft a "Blockchain Technology Overview" that is indicative of the standard-setting body's interest in the technology and likely intent to consider standards in the future. *See* Yaga, Mell, Roby and Scarfone, *Blockchain Technology Overview, Draft NISTIR 8202* at 34 (National Institute of Standards and Technology, January 2018).

The Framework expressly states that it is "not a one-size-fits-all approach to managing cybersecurity risk" because "[o]rganizations will continue to have unique risks – different threats, different vulnerabilities, different risk tolerances – and how they implement the practices in the [Framework] will vary." With that said, even though the Framework was not designed for permissioned blockchains specifically, its standards, as described above, are broad enough to cover permissioned blockchains and to help institutions develop cybersecurity frameworks that identify and control risks affecting blockchains.[21]

B. Payment Card Industry Data Security Standard Requirements

The Payment Card Industry Data Security Standard ("PCI-DSS") consists of requirements imposed in connection with the use of network-branded payment cards that apply to an organization's storage, processing, and transmission of sensitive payment card information such as account number, expiration date, and magnetic stripe information.

Covered organizations must take specific steps to ensure the security of payment data, such as installing and maintaining firewalls, encrypting cardholder data (when transmitted), protecting against malware, and implementing and updating anti-virus programs.

To the extent the PCI-DSS requirements apply to payment data reflected on certain permissioned blockchains, the requirements generally are consistent with the cybersecurity principles relevant to blockchains. For example, an organization is required to implement access controls to limit access to sensitive payment card information to only those employees who have a need to know such information. This approach to access can be implemented in the context of a permissioned blockchain, which should only allow employees for a given participant with the requisite expertise and job responsibility to add transactions to the blockchain.

C. SOC Audit Standards

The American Institute of Certified Public Accountants has issued standards for auditor attestation engagements that are followed by many industries and companies, including publicly-traded companies. Service corporations to these companies are audited based on Service Organization Control ("SOC") reports, and particular SOC reports are designed for auditing a service corporation's information security. SOC audit standards include in scope the controls in place to protect the integrity and accuracy of information and the security of IT systems. As described above, blockchains facilitate real-time auditing and analysis of whether SOC standards are satisfied.

[21] *See,* e.g., Financial Conduct Authority, *Distributed Ledger Technology: Feedback Statement on Discussion Paper 17/03*, p. 10 (Dec. 2017) (summarizing industry feedback stating that the NIST Framework is helpful in mitigating vcyber risks for DLT networks).

D. Prudential Regulatory Requirements

In addition to the above industry standards, prudential regulators in many countries have broadly applicable cybersecurity requirements that apply to the use of IT systems such as permissioned blockchains. For example, in the United States, the Federal Financial Institutions Examination Council ("FFIEC"), an interagency council of financial regulators that promulgates industry-wide standards for banks, has issued guidance regarding the use of cloud computing services.[22] This guidance applies to a CSP platform that hosts a permissioned blockchain for participating banks.

In addition, the FFIEC developed its "Cybersecurity Assessment Tool" to help institutions identify their cybersecurity risks and determine their cybersecurity maturity. It is designed to provide a measurable and repeatable process for assessing an institution's level of cybersecurity risk and preparedness. The FFIEC's tool helps to promote regulatory harmonization by mapping to the NIST Cybersecurity Framework.

These types of cybersecurity requirements typically have been informed by prudential regulators' experience with financial services industry participants over time through examinations and other interactions. Prudential regulators also have started to view regulatory sandboxes (described below) as a unique opportunity to learn about emerging technologies that regulated financial services providers may consider using in order to evaluate the regulatory requirements that should apply to such technologies.[23]

V. Policy Recommendations

Permissioned blockchains have certain inherent cybersecurity capabilities but are not immune to cyber-attacks. By describing the cybersecurity capabilities and risks of blockchains, this paper intends to spur a dialogue, further exploration of the technology, and, eventually, a consensus between industry and regulators regarding the appropriate cybersecurity standards to apply to blockchain solutions in the financial services industry. A principles-based approach to cybersecurity regulation – one that many global regulators have taken to regulate cybersecurity more broadly – will do well in mitigating cybersecurity risk in permissioned blockchains while allowing the technology to continue to evolve through innovation.

In addition to this broad recommendation, we have the following specific recommendations for policymakers and industry participants regarding a smart and coordinated approach to promoting the development of secure blockchain applications through workable cybersecurity standards:

[22] *See* FFIEC, Outsourced Cloud Computing (July 10, 2012).

[23] *See* Financial Conduct Authority, *Regulatory sandbox lessons learned report,* p. 8 (Oct. 2017) (stating that the sandbox has given regulators a unique insight into the types of firms that request support, the technologies underpinning their innovations, and the common risks facing them and their prospective customers).

A. Financial Services Industry Participants Should Apply a Tailored Version of the NIST Cybersecurity Framework to Permissioned Blockchain Activities

The NIST Framework is highly relevant and applicable to the establishment of cybersecurity policy and best practices for permissioned blockchains used in the financial services industry. We recommend that financial services industry participants should apply the Framework in developing cybersecurity programs for permissioned blockchain networks, subject to a few modifications tailored to the distinct attributes of permissioned blockchains:

1. The Framework is properly focused on core functions: Identify, Protect, Detect, Respond, and Recover. Focusing on these core functions will help industry participants in developing cybersecurity programs for permissioned blockchains, giving particular emphasis to "prevention" and the incorporation of prevention strategies within the Protect, Detect, and Respond functions.
2. Industry participants should optimize the Framework for permissioned blockchains by shifting the focus from organization or enterprise-level cybersecurity to network-level cybersecurity. Such a shift would recognize that permissioned blockchains are networks consisting of multiple participants who share responsibility for cybersecurity. All participants in a permissioned blockchain, including the developer, owner-participants, and managing entity, should be required to adhere to network-level cybersecurity standards.
3. In draft v1.1 published in December, the Framework Tiers have been revised to give greater emphasis to external participation, specifically whether the organization understands its role, dependencies, and dependents in the larger ecosystem; collaborates and shares information with other entities; and understands and acts upon cyber supply chain risks. The emphasis on external participation in the Framework Tiers is especially relevant to the collaborative environment of permissioned blockchains. Industry participants should consider whether to admit network organizations that fall within less mature Framework Tiers for relevant categories into a permissioned blockchain given the shared risks and external dependencies in a blockchain ecosystem. In the context of permissioned blockchains, entities that are Tier 1 and Tier 2 for categories focused on prevention strategies and the network level may not have the operating history or scale to satisfy network cybersecurity expectations and therefore may generate significant risk for other network participants. Blockchain network rules, for example, could require every participant in the network to satisfy Tier 3 standards for relevant categories and require the managing entity and any technology service provider to satisfy Tier 4 standards for relevant categories.

Participants in permissioned blockchains should make it a priority to apply the NIST Cybersecurity Framework to cybersecurity programs for such blockchains, making adjustments tailored to the structural attributes of permissioned blockchains. By doing so, industry participants would adopt strong cybersecurity programs for the permissioned blockchains they use and set a positive example that may help establish an industry-based global cybersecurity standard for such blockchains.

For regulators to understand cybersecurity risk in permissioned blockchains, they first must have a detailed understanding of the technologies and how they operate.

Industry participants can help provide this understanding by maintaining an open dialogue with regulators regarding permissioned blockchains, their opportunities, and their risks.

B. Encourage Regulator-Industry Dialogue, Including Through Regulatory Sandboxes

For regulators to understand cybersecurity risk in permissioned blockchains, they first must have a detailed understanding of the technologies and how they operate. Industry participants can help provide this understanding by maintaining an open dialogue with regulators regarding permissioned blockchains, their opportunities, and their risks.

Testing is one way to give regulators helpful insight. Testing is an important part of the development lifecycle for permissioned blockchains and an opportunity for regulators to obtain information about them in a live environment. Regulators and industry could, for example, work together to determine the appropriate level of testing necessary to give regulators confidence in the security and resiliency of blockchain technologies. To accomplish this objective, industry should engage in a dialogue with regulators regarding test results and test protocols so that regulators can become comfortable with the cybersecurity features of permissioned blockchains. Such an iterative testing process provides a roadmap through which regulators and industry could arrive at a common understanding of accepted testing standards for blockchain technologies.

Certain foreign governments and U.S. state governments also are currently evaluating regulatory sandboxes and other testing programs that create limited production environments with scaled back regulatory requirements.[24] If properly structured, these sandboxes can align incentives between regulators and industry by giving regulators insights into blockchain technologies and industry the ability to test new technologies in a limited live environment without doing a full-scale roll-out subject to the litany of regulatory requirements.[25]

C. Encourage Policymakers to Acknowledge the Unique Cybersecurity Benefits of Blockchain Technologies

While blockchain technologies are continuing to evolve for an expanding range of applications and industries, policymakers should be attuned to these technologies' unique benefits, including cybersecurity benefits. Acknowledging these benefits, as well as the risks, will focus attention on blockchain and encourage regulated industries, such as financial services, to look to these technologies and their underlying concepts for ways to augment their cybersecurity programs and to better mitigate cybersecurity risk. Such consideration needs to occur at the highest levels of federal agencies to help drive their perspective in regulating specific industries such as financial services.

[24] *See*, e.g., Office of the Arizona Attorney General, Draft Legislative Proposal of Arizona Attorney General Mark Brnovich to Establish a "Fintech" Regulatory Sandbox in Arizona (Sept. 5, 2017).

[25] *See* Chamber of Digital Commerce, Global Regulatory Sandbox Review: An Overview on the Impact, Challenges, and Benefits of Regulatory FinTech Sandboxes (Nov. 21, 2017).

D. Foster Harmonization Across Cybersecurity Standards Applied to Permissioned Blockchains

Prudential regulators and industry should analyze cybersecurity standards that are applied to blockchains, particularly permissioned blockchains, to make sure that such standards are harmonized.[26] For example, industry participants' application of the Framework to permissioned blockchains should be coordinated with the cybersecurity standards that prudential regulators have established for financial institutions' IT systems more generally. Convening interagency councils and public-private governing bodies are helpful steps to making sure that cybersecurity guidance applicable to blockchain technology is consistent and does not impede innovation.

VI. Conclusion

The financial services industry stands to benefit tremendously from the growth of blockchain given the technology's many financial services applications, including in effecting transactions and storing data in a more secure manner. As cyber threats to the industry continue to evolve in complexity and intensity, emerging technologies such as permissioned blockchains can contribute to the important goals of combatting cybersecurity risk and adequately protecting consumers' financial information and the integrity of the global financial system. Permissioned blockchains offer significant cybersecurity capabilities, share some of the same cyber risks that affect other IT systems, and have unique characteristics, all of which merit further evaluation by regulators and industry. We encourage further conversation about the cyber security benefits of blockchain systems and ways to encourage appropriate government policies.

[26] The U.S. Department of the Treasury released a report last summer with recommendations for reforming the regulatory framework for banks and credit unions. One of the recommendations stressed the need for better coordination among U.S. financial regulatory agencies in supervising the banking industry's cybersecurity risks and controls. *See* U.S. Department of the Treasury, A Financial System That Creates Economic Opportunities: Banks and Credit Unions (June 12, 2017) ("Better coordination on cybersecurity regulation is needed to achieve this goal and enhance the resiliency of the sector. Given the risk of fragmentation and overlap, Treasury recommends that federal and state financial regulatory agencies establish processes for coordinating regulatory tools and examinations across sub-sectors.").


Microsoft
CHAMBER OF
DIGITAL
COMMERCE