Considerations and Guidelines for Advancing Cybersecurity in the Token Economy

Prepared by the Token Alliance – an industry initiative of the Chamber of Digital Commerce

SECOND EDITION • SEPTEMBER 2019
CHAMBER OF DIGITAL COMMERCE

The Chamber of Digital Commerce is the world’s largest trade association representing the blockchain industry. Our mission is to promote the acceptance and use of digital assets and blockchain technology. Through education, advocacy, and working closely with policymakers, regulatory agencies, and industry, our goal is to develop a pro-growth legal environment that fosters innovation, jobs, and investment.

TOKEN ALLIANCE

The Token Alliance is an industry-led initiative of the Chamber of Digital Commerce, developed to be a key resource for the emerging industry surrounding the generation and distribution of tokens using blockchain technology. Comprised of more than 400 global industry participants, the Alliance includes blockchain and token experts, technologists, economists, former regulators, and practitioners from around the globe. The Token Alliance develops community-driven guidelines for the responsible development of tokens.

CHAMBER OF DIGITAL COMMERCE INDUSTRY INITIATIVES & WORKING GROUPS

- **SMART CONTRACTS ALLIANCE**
  Promotes real-world application of smart contracts to enhance the way business is conducted.

- **DIGITAL ASSETS ACCOUNTING CONSORTIUM**
  Developing accounting and reporting standards for digital assets and blockchain-based technologies.

- **GLOBAL BLOCKCHAIN FORUM**
  Working with the world’s leading blockchain policy experts to develop industry best practices and help shape global regulatory interoperability.

- **STATE WORKING GROUP**
  Engaging with state and local governments on the regulation and implementation of blockchain technology.

- **BLOCKCHAIN ALLIANCE**
  The public-private forum for the blockchain community and law enforcement to help combat criminal activity.

- **CHAMBER OF DIGITAL COMMERCE CANADA**
  Promoting the acceptance and use of digital assets and blockchain-based technologies in Canada.

- **BLOCKCHAIN INTELLECTUAL PROPERTY COUNCIL**
  Balancing the protection of proprietary information with the openness necessary for innovation.
# TABLE OF CONTENTS

I. ACKNOWLEDGEMENTS  
II. INTRODUCTION  
III. CONSIDERATIONS AND GUIDELINES FOR ADVANCING CYBERSECURITY IN THE TOKEN ECONOMY  
   A. INTRODUCTION  
   B. CYBERSECURITY CONSIDERATIONS FOR PUBLIC BLOCKCHAINS  
      1. LACK OF CENTRAL AUTHORITIES AND IMPACTS TO ASSET RECOVERABILITY  
      2. COMPROMISE OF DISTRIBUTED CONSENSUS PROTOCOLS  
      3. CRITICALITY OF PRIVATE KEY MANAGEMENT  
      4. PROTOCOL AND SMART CONTRACT VULNERABILITIES  
      5. INACCURATE EXTERNAL DATA SOURCES  
   C. CYBER POLICY AND REGULATORY CONSIDERATIONS  
      1. JURISDICTIONAL CHALLENGES  
      2. SECURITY TOOLS AND MAPPING GUIDANCE  
      3. NEW YORK STATE BITLICENSE  
      4. GDPR CYBER EVENT DISCLOSURE REQUIREMENTS  
   D. GUIDELINES FOR ADVANCING CYBERSECURITY IN A TOKENIZED ECONOMY  
IV. CONCLUSION
I. ACKNOWLEDGEMENTS

TOKEN ALLIANCE CO-CHAIRS

PAUL ATKINS
Chief Executive Officer, Patomak Global Partners

JAMES NEWSOME, PH.D.
Founding Partner, Delta Strategy Group
The Chamber of Digital Commerce would like to recognize the following individuals for their thought leadership, contributions and support to the Token Alliance in the production of this report.

KEVIN BATTEH  
Partner,  
Delta Strategy Group

PERIANNE BORING  
Founder and President,  
Chamber of Digital Commerce

JOE CUTLER  
Partner,  
Perkins Coie LLP

DAX HANSEN  
Partner,  
Perkins Coie LLP

CHRIS HOUSSER  
Co-Founder,  
Polymath

JONATHAN JOHNSON  
President,  
Medici Ventures

AMY DAVINE KIM  
Chief Policy Officer,  
Chamber of Digital Commerce

KARI LARSEN  
Partner,  
Perkins Coie LLP

BRIAN LIO  
Chief Executive Officer,  
Smith + Crown

RUMI MORALES  
Partner,  
Outlier Ventures

MATTHEW ROSZAK  
Chairman and Co-Founder,  
Bloq

BILL SHIHARA  
Chief Executive Officer,  
Bittrex

JOSHUA STEIN  
Chief Executive Officer,  
Harbor

COLLEEN SULLIVAN  
Chief Executive Officer,  
CMT Digital
EXPERT CONTRIBUTORS

The Chamber of Digital Commerce would like to thank the following individuals and organizations for their valuable contributions to the Token Alliance in the production of this report.

We would also like to extend a special thank you to Sal Ternullo and Sam Wyner, Directors and Cryptoasset Services Co-Leads of KPMG LLP, for helping to lead the development of this report.

PAUL BRIGNER
Chamber of Digital Commerce

STEVE BUNNELL
O’Melveny & Myers

DAVID FITZGERALD
O’Melveny & Myers

AMY DAVINE KIM
Chamber of Digital Commerce

OLGA MACK
Quantstamp

RAMESH NAGAPPAN
Harvard University

DIVIJ PANDYA
Chamber of Digital Commerce

STEVEN SPRAGUE
Rivet

COLLEEN SULLIVAN
CMT Digital

DAWN TALBOTT
RiskSpan
II. INTRODUCTION

This new installment of our series of reports is an important addition to the overall regulatory and market consideration of the token ecosystem. The way in which digital tokens operate is complex and can maintain multiple characteristics – from an investment contract, to something necessary for utilizing a digital platform, to a form of payment or exchange, to name just a few. We are in a moment when technological advancement is pushing the boundaries of decades-long established law – law that was made at a time when tokenized assets and instantaneous digital transfers of value were not contemplated. It is exciting to be a part of it, but it also entails risks.

To facilitate the development of token businesses as well as minimize incidents of fraud and compliance challenges, the Chamber embarked on a plan to tackle each of the issues impacting this ecosystem. This journey started with a publication of guidelines for digital tokens that were intended to operate outside Securities and Exchange Commission (SEC) and Commodities Futures Trading Commission (CFTC)-regulated products and services laws (so-called “utility tokens” and associated platforms).

Those Guidelines also sought to provide legal context by detailing the legal landscapes governing digital tokens in five countries – the United States, Canada, the United Kingdom, Australia, and Gibraltar. Taking up a sizeable portion of the Report, the description of the vast number of potential legal requirements and government oversight demonstrated that this is a regulated industry, no matter where you fall in the spectrum of token categorization.

Finally, we provided an economic perspective on the industry with an analysis of market trends. The sheer volume of capital raised demonstrates the passionate interest of so many around the world in the potential of these markets – whether as a way to make money, a way to use new and better services, or other reasons. This installment expands on those initial resources to balance out the conversation around utility tokens to discuss the rules, regulations, and resulting considerations for those who wish to issue or trade tokens that are or otherwise represent securities. This sector of the market is growing with entrants from new technology companies as well as established institutional financial services providers. The securities laws are complex, generated in the 1930s and developing substantial legal and regulatory precedent. In some cases, that precedent has endured because it is principles-based. In others, it has become outdated as it no longer sufficiently contemplates the types of securities that can be created, issued, held, and traded digitally.
We are excited to introduce these guidelines for cybersecurity related to digital tokens. First, these guidelines address cybersecurity considerations for public blockchains. These considerations account for the issues associated with a lack of central authorities, attack vectors in a consensus driven system, and other challenges unique to the blockchain environment. Second, the guidelines explore regulatory considerations from a cybersecurity perspective, addressing the application of both new and existing frameworks. Third, and finally, we provide a set of guidelines for advancing cybersecurity in a tokenized economy.

While this document primarily focuses on cybersecurity risks and associated guidelines to address them, blockchain technology is a major step forward from a cybersecurity perspective. Blockchain is based on the discovery of new ways to leverage existing cybersecurity technologies like public key cryptography, distributed computing, and consensus mechanisms to create ledgers that feature inherent tamper resistance and resiliency never before realized with traditional approaches. Because of its cybersecurity and other benefits, many experts foresee a time when blockchain will underpin all of our enterprise business models, and we anticipate publishing additional papers to further explore the cybersecurity benefits of blockchain technology.

This report complements our recent work on consumer protection and securities and non-securities tokens. But we can’t stop there. More areas need to be considered and addressed with thoughtful analysis. We will be supplementing our legal landscape on a rolling basis with the introduction of additional countries and the laws that apply to digital tokens.

We hope you enjoy these publications and that they serve to help guide your analysis and views of the evolving digital token ecosystem. We look forward to sharing this series as we roll out these publications throughout the coming weeks!

A few words of caution:

**THIS REPORT DOES NOT CONSTITUTE LEGAL ADVICE**

» Specifically, nothing in this report should be construed as advice regarding the law of the United States or any other jurisdiction.

» This report, including its suggested guidelines, merely express the general views of the Token Alliance, and compliance with such guidelines cannot assure that the distribution or trading of tokens will fully comply with the laws discussed herein.

» These views are being offered for discussion purposes only, and they have not been sanctioned by any regulator or government agency.
CONSULT LEGAL COUNSEL BEFORE DISTRIBUTING OR HOSTING TRADES OF DIGITAL TOKENS

» Token Sponsors and associated parties seeking to generate or distribute a blockchain-based token should seek independent legal counsel with expertise in this area before proceeding with their project, particularly given the fast-paced nature of this industry and the quickly evolving legal landscape.

» Counsel can help consider the facts and circumstances surrounding particular issues within the contours of then-current regulatory and enforcement activity.

» This report does not attempt to address any individual case, and the thought leadership contained herein is not appropriate for use as a substitute for independent counsel.

» Further, the digital token market is rapidly shifting and therefore the cases and regulatory interpretations discussed in this report may be overtaken by future events.

The Token Alliance will continue to study the issues surrounding the appropriate regulation for tokens and it will offer additional insights, as appropriate, when new developments arise.
III. GUIDELINES FOR ADVANCING CYBERSECURITY IN A TOKENIZED ECONOMY

A. INTRODUCTION

The digital economy continues expanding across technology domains and industry lines, driving economic growth and enhancing consumer experiences. In this era of digital innovation, blockchain is one of the most progressive examples of technology convergence at the intersection of applied cryptography and distributed systems. Blockchain has inspired the emergence of fundamentally new assets, and, in parallel, has encouraged innovators to reimagine how traditional assets are issued, managed, exchanged, and accounted for. Although still in early days, investment into blockchain innovation and development has increased dramatically with innovators striving to realize blockchain’s potential to become a foundational technology layer of a digitized economy.

While the market continues to place a strong focus on blockchain’s transformative potential, there has been less focus on blockchain cyber risks and benefits. This phenomenon is ironic given blockchain technology is best known for giving rise to “cryptocurrencies,” where “crypto” describes the application of cryptographic functions and mechanisms to support secure transactions recorded on a decentralized ledger. The use of cryptographic functions and distributed architectures enable key blockchain value drivers including tamper resistance and resiliency. The inherent composition and structure of the technology that links blocks of transactions cryptographically — creating the “chain” in “blockchain” — makes them tamper-resistant. In other words, attempts to modify a blockchain ledger (whether maliciously or otherwise) are extremely difficult and, if somehow successful, open and conspicuous. Also, the fact that blocks are cryptographically linked sequentially eliminates the availability of large troves of data such that a malicious actor would need not only modify the transaction they seek to alter, but every transaction thereafter in order to hide the change. The power and rate of computing ability needed to accomplish such a task has thus far proved impossible for the Bitcoin blockchain. These attributes can be widely applied to solve data problems persistent in current computing models across industries in managing data integrity, availability, and transparency.
In 2018, Microsoft partnered with the Chamber of Digital Commerce to publish “Advancing Blockchain Cybersecurity,” which discussed permissioned blockchain “capabilities in mitigating cybersecurity risks and detecting, preventing, and combatting the types of cyber-attacks that are often directed at financial institutions.” The paper discussed distributed architectures, consensus validation mechanisms, encryption (cryptographic immutability), transparency, and administrator risk controls. While these features were discussed in the context of permissioned blockchains, there are unique and nuanced risk considerations when considering permissionless or “public” blockchains and blockchain-enabled assets such as cryptocurrencies.

These unique risk considerations have resulted in a high frequency of cyber events with significant impacts across the tokenized economy. The ecosystem has incurred billions of dollars of cyber-related losses and major insolvency events (e.g., Mt. Gox and Quadriga) which have subsequently led to skepticism in both digital assets and the broader ecosystem. In this report, we will discuss these unique and nuanced risk considerations to help practitioners, policymakers, and investors across the ecosystem better understand and effectively manage cybersecurity to protect tokenized assets.

B. CYBERSECURITY CONSIDERATIONS FOR PUBLIC BLOCKCHAINS

The 2018 paper “Advancing Blockchain Cybersecurity” assessed the cyber risk profile of permissioned blockchains within the financial services industry, laying the foundation for this piece to discuss unique and nuanced risk considerations for public blockchains and enabled digital assets. The risks described in the 2018 paper focus on private key management, software and protocol vulnerabilities, external data sources and endpoint risks, data security and privacy, and evolving attack vectors, which are each applicable and relevant to public blockchains.

This report applies these risks factors and highlights unique and nuanced risk considerations for public blockchains, including:

1. Lack of central authorities and impacts to asset recoverability
2. Compromise of distributed consensus protocols
3. Inappropriate access to private keys and/or endpoints
4. Protocol and smart contract vulnerabilities
5. Inaccurate external data sources

2 See, e.g., Kate Rooney, $1.1 Billion In Cryptocurrency Has Been Stolen This Year, And It Was Apparently Easy To Do, CNBC (June 7, 2018), [https://www.cnbc.com/2018/06/07/1-point-1b-in-cryptocurrency-was-stolen-this-year-and-it-was-easy-to-do.html](https://www.cnbc.com/2018/06/07/1-point-1b-in-cryptocurrency-was-stolen-this-year-and-it-was-easy-to-do.html).
1. LACK OF CENTRAL AUTHORITIES AND IMPACTS TO ASSET RECOVERABILITY

In both traditional technology environments and permissioned blockchains, central authorities control critical technology operations including identity and access management (“IAM”) to control user’s access to read and process information using business applications. The most important scientific breakthrough that Bitcoin provided was the ability for participants in a distributed system to perform trusted transactions and achieve consensus on the state of a distributed ledger without central authorities to facilitate settlement and mitigate counterparty risk. Bitcoin’s consensus mechanism, proof-of-work (“PoW”), provided the first viable solution to achieve consensus on the state of a distributed ledger and transaction history across a network of distributed unknown participants. By doing so, Bitcoin enabled the emergence of blockchain technology unlocking the ability for counterparties to perform trusted transactions directly without central authorities, having wide-reaching implications to many businesses and industries. Within the context of this discussion, then, we focus on the risk implications that a lack of central authorities has to digital assets on public blockchains.

The comparatively rapid settlement of transactions executed on public blockchains enable counterparties to achieve nearly instantaneous settlement finality. Once a transaction is executed, whether authorized by the owner or not, and the transaction is validated by the network through consensus, the asset transfer is final, and the transaction cannot be reversed or recovered. In this regard, the “finality” condition for transactions executed on public blockchains is unique from traditional asset exchanges which are cleared through traditional financial market infrastructure, often including broker-dealers, exchanges, clearing houses and custodian banks. In traditional market infrastructure, asset owners can often pursue remediation through established asset recovery procedures or legal proceedings targeting the central authorities who facilitated the transaction. This type of action is not possible for transactions executed for assets on public blockchains because there are no central authorities. Policymakers and practitioners must consider these risk implications when designing standards and best practices for business models engaging with public blockchains and enabled assets.

There have been historical scenarios where a public blockchain community implemented a solution to achieve asset recovery when a significant negative event occurred. In 2015, following a major asset compromise via a smart contract vulnerability on the Ethereum blockchain, the community deployed a “hard fork” (protocol changes) to facilitate asset recovery. While the asset recovery was effective, the decision to deploy the hard fork was highly contentious and divisive. Moving forward, it is reasonable

---

to assume that hard forks will not be a viable asset recovery method until ongoing efforts in the ecosystem, such as protocol upgrades (e.g., Ethereum Improvement Proposal (“EIP”) #867) are implemented.

In the absence of technical solutions to facilitate asset recovery following a cyber event, asset issuers and owners have pursued global coordination between exchanges to track and trace assets using analytical approaches to flag and recover assets. These approaches focus on eliminating off-ramps for malicious actors to convert compromised assets into fiat currencies.

Although this has led to successful asset recovery in several circumstances, substantial challenges are associated with this type of coordination that impede its effectiveness. It is also important to note that advanced cryptographic implementations (i.e., zero-knowledge proofs or “ZKP”), as well as increasing interoperability across networks (i.e., atomic swaps), may prove substantial challenges for organizations attempting to track and trace compromised assets using analytical approaches over the transaction ledger.

2. COMPROMISE OF DISTRIBUTED CONSENSUS PROTOCOLS

In Section A, we established consensus mechanisms as a major breakthrough and discussed the risk implications that peer-to-peer transactions have to asset recoverability in the event of a compromise due to a cyber event. In this section, we build on the discussion of consensus mechanisms to explore risks directly related to distributed consensus protocols.

Consensus mechanisms in distributed systems have been an area of scientific and academic exploration for decades, however, Bitcoin provided the first production quality solution in Proof-of-Work (“PoW”). While PoW has achieved mass adoption to date, consensus mechanisms are evolving as researchers, scientists, and the private sector focus on investment into consensus innovation. To this point, a number of public blockchain communities, including Ethereum, have communicated intentions to adopt Proof-of-Stake (“PoS”) consensus models where validators “stake” their tokens as security deposits to participate in the consensus process for transaction validation to earn block production rewards. In the PoS model, validators who attempt to manipulate transactions do so at the risk of losing their staked tokens. PoS builds on game theory concepts deployed in PoW to provide a more resource efficient consensus mechanism (i.e., does not consume electricity for “mining” as in PoS). In the future, it is likely that different blockchains will choose consensus mechanism designs based on desired attributes in performance, scalability, and transaction finality, among other considerations.

From a risk perspective, PoW and PoS systems are similar in that they can both be compromised through “51% attacks” where the consensus mechanism is manipulated by an actor seeking to process fraudulent transactions. To date, consideration of 51% attacks has focused on PoW consensus protocols as that consensus model is currently the most widely adopted. In order to better understand a 51% attack, we first provide a brief description of PoW and how the consensus mechanism functions.

At a high level, PoW is a cryptographic, mathematical puzzle that validators on a network aim to solve in order to win a block reward and the right to publish the next “block” of valid transactions to the network. The puzzle is solved by generating an arbitrary random input called a “nonce” (random inputs) into a one-way hash function with the aim of producing a fixed length value which meets a certain outcome condition. The likelihood of achieving the target outcome and solving the puzzle increases proportionally with a validator’s (“miner”) computational resources to produce nonces relative to the total population of computing resources producing nonces to solve the PoW algorithm (“hashpower”). The more rapidly a validator can produce nonces, the higher their probability of solving the PoW puzzle to publish the next block and win the block reward (currently 12.5 BTC on the Bitcoin network). Validators are also paid transaction fees which creates the incentive to collect all transactions to increase economic gain should the validator solve the puzzle and publish the next block. Validators are disincentivized from manipulating transactions because all transactions are shared on the network, creating a condition where an inaccurate transaction would be immediately identified to invalidate the block with the manipulated transaction(s). This consensus attack incurs a substantial opportunity cost to the malicious actor in the form of both forgone block rewards and wasted resources (electricity and computational resources).

A 51% attack against a PoW network requires the majority of a network’s validating hashpower to perform a “double spend” attack by manipulating historical transactions to the malicious validators own economic advantage. This risk to PoW networks has been discussed frequently as hashpower has become more centralized. This is the result of the institutionalization of the mining industry and creation of mining pools, where miners combine their mining capacity to earn block rewards that are then distributed across the mining pool. Successful 51% attacks have been executed against smaller
PoW networks resulting in “double spends” and asset compromise. Most recently, the Ethereum Classic (“ETC”) protocol fell victim to a 51% attack resulting in the compromise of more than 200,000 ETC valued in excess of $1 million USD at the time of the attack.\(^5\)

PoS blockchains are also subject to the risk of a 51% attack where an individual validator or “staker” controls more than half the network assets and stakes more than 51% compromise the PoS consensus process. Discussion of 51% attacks on PoS networks continues to increase alongside adoption, both with regard to newly launched blockchains using PoS and older blockchains transitioning to PoS.

Regardless of the consensus mechanism, public blockchains validated through distributed consensus mechanisms are susceptible to distributed consensus compromise. The risks associated with an attack on a blockchain’s consensus mechanism must be considered by practitioners interacting with native assets. In order to help address risks related to consensus mechanisms’ compromise, practitioners in the ecosystem have developed blockchain threat monitoring solutions to help generate alerts when consensus attacks are attempted or executed. In closing, it is beneficial for practitioners interacting with digital assets on public blockchains to perform consensus attack modeling to understand the security posture of a given blockchain to inform business strategy, operations and risk management efforts.

3. CRITICALITY OF PRIVATE KEY MANAGEMENT

On a public blockchain, identities and the assets they own are not managed or tracked by a central institution. Identities are reflected on the network by the public key address of a defined “key pair.” A key pair consists of a public key, visible to all network participants, and a cryptographically paired private key, which is kept secret and is required to execute transactions on behalf the related public key address. These key pairs are derived from asymmetric cryptographic algorithms which create a unique private key from each public key that is generated.\(^6\) The combination of a private and public key pair composes a “wallet” as discussed within this piece.

Blockchain transactions processed using digital signatures are pseudonymous, meaning that every public key address ultimately correlates to an identity which is unknown. In this model, the counterparty’s information is not recorded in on-chain transaction records, however, advanced analytics have been developed to try to unveil potential identities. Advances in zero-knowledge proof (“ZKP”) cryptography and ring-signatures (e.g., Z-cash, Monero, Dash) will further obfuscate transactional information including public wallets addresses from transaction details recorded on the ledger to further protect user privacy.


\(^6\) It is worthwhile to note that advances in quantum computing will challenge existing approaches to asymmetric cryptography (including blockchain as well as any other use of such cryptography, which is commonly used); however, these considerations fall outside the scope of this discussion.
Private key management is an important consideration in permissioned blockchains; however, it is dramatically exacerbated when considering public blockchains and the factors discussed in Section A centering on the implications that a lack of central authorities has on asset recoverability. In public blockchains, the exposure of a private key fundamentally compromises all of the assets associated with the related public key wallet address. The need to protect private key material to “custody,” or maintain ownership control of tokenized assets, has spurred a massive market with a diverse array of solutions targeting retail and institutional market segments.

From the retail perspective, investors in assets traded on public blockchains may choose to manage their own private keys in a “self-custody” model or opt to utilize a third-party wallet service or exchange. Investors choosing self-custody models should fully understand the risk they are responsible for holding the asset, with an appreciation that there is no path to pursue recourse in the case of asset compromise. As a result of self-custody risks, many users will engage the services of a wallet service, exchange, or brokerage platform to manage their private keys and effect transfers. This can be an option for asset owners to transfer the risk associated with private key management to a third-party to rely on the third-party’s controls and process to mitigate cyber risks to private keys. This approach has resulted in high profile cyber and technology risk events, most recently and notably impacting QuadrigaCX, a Canadian exchange. QuadrigaCX was forced into bankruptcy after two unfortunate developments: QuadrigaCX CEO, Gerald Cotton, died with sole access to wallets containing cryptocurrency worth $137 million USD, affecting 115,000 customers; and, in the process of responding to Cotton’s death, an additional $469,000 dollars was accidentally sent to the wallets that could not be accessed. This risk event, while not directly cyber-related, highlights the criticality of key management and the implications for investors relying on third parties to manage risks related to cryptoasset custody.

"MAINTAINING THE CONFIDENTIALITY, INTEGRITY, AND AVAILABILITY OF PRIVATE KEYS REQUIRES THOUGHTFUL AND ROBUST CYBERSECURITY CONTROLS"

— Erin English, “Advancing Blockchain Cybersecurity”

While retail and institutional custody models have similarities, there are differences in asset owners’ and asset managers’ requirements for risk management, security, and regulatory compliance in regard to both custodial and non-custodial models. To this point, there is strong competition across the
in institutional cryptoasset custody market, with a number of emergent business models and technology solutions being developed and adopted. Across these solutions, cyber risk is a critical consideration driving risk management and control innovation to help securely custody assets. As noted by Erin English in Advancing Blockchain Cybersecurity, “Maintaining the confidentiality, integrity, and availability of private keys requires thoughtful and robust cybersecurity controls.”

These business process and control innovations have laid the foundation for best practice principles to effectively manage and custody private keys. While there are some key nuances, these principles and standards are largely derived from existing standards for cybersecurity and private key management.

Established approaches to cryptographic key management (i.e., NIST 800-57, FIPS 140-2 Level 2/3) should be considered by practitioners providing custody products and services. The implementation of business based on established standards, security policies, operating procedures, and resiliency plans throughout key lifecycles is required to effectively protect private key material. Cyber risks should be considered through the key lifecycle from creation, initialization, distribution, operational utilization (active/inactive), and retirement. These risks encourage practitioners to develop business processes to support private “key sharding,” where a single private key is split into “shards,” or requisite pieces, to decentralize the risk related to the private key. This approach renders each shard useless without assembling a defined number of the other shards. Key sharding has been implemented widely using Shamir’s Secret Sharing (“SSS”) to eliminate single points of failure where a private key can be compromised.

 Similarly, the implementation of multi-signature wallets requiring two or more signers to transact can reduce single points of failure by requiring multiple users to sign transactions. This helps to increase the resiliency of control environments protecting private keys. Multi-signature wallet schemes may also integrate the use of independent, third-party signers who perform identity verification to authenticate transactions. In addition to key sharding and multi-signature schemes, research into the

---

8 English, Kim, and Nonaka, supra note 1.
use of multi-party computation (“MPC”) approaches, which allow multiple parties to compute a function over inputs while maintaining the privacy of the inputs, are being analyzed and incorporated to securely manage private keys. MPC approaches to key management have been deployed in Bring Your Own Key (“BYOK”) models for public cloud infrastructure deployments to prevent key compromise by the cloud service provider (“CSP”). Similarly, MPC-based approaches to cryptographic key management can be integrated into custodial solutions to securely manage private keys to public wallets.

The focus on “crypto custody” has increased substantially through 2018 and 2019, largely due to persistent cyber-attacks on exchanges. While complex in practice and implementation, crypto custody simply refers to the business process and technology infrastructure designed for cryptoassets to securely store and managing the private keys. Crypto custody may be included in a broader suite of services offered by token trading platforms, as a standalone business model, or as a managed service. The technology environment supporting the given business performing the custody function is subject to traditional cyber risks which must be mitigated. These risks are present for all entities operating blockchain nodes, underlying infrastructure, and/or business processes interacting with the network and native assets.

In order to meet rising institutional demand and increasingly sophisticated service requirements, tiered custody models are frequently implemented to provide varying levels of security and availability to meet asset owner requirements. These approaches utilize strong network segmentation, resiliency by design and air-gapped physical vault storage using hardware security modules (“HSMs”) to provide the highest levels of security against cyber risks. Regardless of the custody model and solution, established cyber frameworks (i.e., NIST 800-53) and defense-in-depth principles to cybersecurity should be embraced to help securely manage private keys and protect assets hosted on public blockchains against cyber risks.

4. PROTOCOL AND SMART CONTRACT VULNERABILITIES

Public blockchain protocols and smart contracts are software, and like all software they are susceptible to vulnerabilities. Traditional risks of software vulnerabilities must be considered and mitigated as public blockchains are launched and upgraded and as smart contracts are issued. For example, developer communities and ecosystem participants must perform rigorous software testing procedures and code-level reviews to manage these risks.

At the protocol layer, the responsibility for testing is shared across the community. Developers and actors across the ecosystem have coalesced to develop software testing procedures and code reviews to help manage these risks. These testing procedures are often performed on “test nets” which are replicas of public blockchains where the software updates are deployed and tested. A compromise in a blockchain protocol is a critical risk consideration that must be regarded with the utmost importance by all related parties and reflected as such through integration into incident response policies to address a protocol layer breach.

This reality recently arose in the Bitcoin community with the identification of a protocol vulnerability (Bitcoin CVE 2018-17144) that could have allowed a Denial-of Service driven “double-spend” attack. This scenario exposed a potentially existential risk to Bitcoin as the exploitation of this vulnerability could have deeply eroded trust in the protocol and asset itself. The community rallied to address the software flaw and it was ultimately remediated prior to exploitation. While this protocol risk was successfully addressed, participants quickly realized that the risk exposure extended across a number of other networks that had cloned the Bitcoin protocol.

While the risk of protocol vulnerabilities will always exist, academic institutions including MIT’s Crypto Security Initiative are investing resources and performing security research to identify and patch blockchain protocol vulnerabilities. The institutions and organizations will play a critical role in guaranteeing the security and longevity of blockchain infrastructure and enabled assets.

While protocols serve as the foundational transaction layer, smart contracts provide applications that run on blockchains and, upon the occurrence of specified conditions, automatically execute functions. Automated execution alleviates the need for intermediaries to manage terms and conditions between transacting counterparties, replacing them with programmed logic. Smart contracts can be deployed in a variety of use cases, however, the most frequently deployed use case to date has been to facilitate the issuance of tokens taking a variety of forms (e.g., security, utility, commodity).

While a marvel of innovation, inherent risks to smart contracts exist that must be mitigated to prevent contract and asset compromise. Smart contracts issued on public blockchains are deployed to all nodes on the network, allowing all participants the ability to interact with the contract. The distribution of smart contracts across network participants increases the attack surface to include all network participants. This contrasts with permissioned blockchains where smart contracts are only exposed to the approved members of network limiting the attack surface to only known participants.

As with any software development, flaws and vulnerabilities in smart contract code have led to extensive risk events resulting in the compromise of millions of dollars of assets, most notably through

---

the DAO hack, where 3.6 million ether was siphoned out of a smart contract through an exploited vulnerability (i.e., a bug in the software). In efforts to better understand the prevalence and scope of the issue, different academic studies have performed analytics over historically issued smart contracts. In one example, researchers from University College London (Ilya Sergey) and the School of Computing, NUS Singapore (Ivica Nikolic and Aashish Kolluri) analyzed nearly one million smart contracts deployed on the Ethereum blockchain concluding that thousands of issued contracts contain vulnerabilities that could lead to asset compromise.

In recognition of the risks associated with smart contracts, industry participants and academic researchers continue to develop approaches to perform smart contract security audits and assessment. Frameworks have emerged and are evolving which can be adopted by practitioners to help ensure secure smart contract coding practices. For example, Consensys has released “a guide to smart contract security best practices” on GitHub. In most use cases today, smart contracts undergo exhaustive third-party security audits and code reviews prior to issuance.

Alongside the propagation of smart contract security approaches, standards for specific smart contract use cases have emerged, namely token standards such as ERC20 in the Ethereum ecosystem. This standard has given entities issuing tokens on the Ethereum blockchain an option to rely on a standard contract structure. Participants gained increased comfort over security design due to the rigor of the community’s review and approval process with this approach. In addition, standards enable more effective interoperability across tokens and underlying infrastructure. While token standards like ERC20 have increased security and interoperability, the structure lacks native capabilities to recover tokens in the event of a compromise.

To solve for this problem, developers have designed proprietary token structures to allow for asset recovery. These token structures include built-in mechanisms to facilitate the destruction and re-issuance of outstanding tokens in the event of a compromise. While a powerful feature for responding to theft, the ability to destroy tokens introduces centralization risk which could be exploited by the issuer or a malicious actor.

5. INACCURATE EXTERNAL DATA SOURCES

Smart contracts often rely on external data sources (sources outside the blockchain protocol) or “oracles” in order to execute conditional logic, introducing risk which much be considered and mitigated. In a simplistic model, oracle feeds introduce a central point of failure to smart contracts, an issue which has been called the “oracle problem.”

14 David Siegel, Understanding the DAO Attack, Coindesk (June 25, 2016), http://www.coindesk.com/understanding-dao-hack-journalists/.
Smart contracts are commonly designed to execute based on external oracle data feeds. In this model, the risk of inaccurate external data being fed into a smart contract is critical. As with all technology systems, external data feeds and the supporting infrastructure must be effectively controlled and secured to protect against malicious actors targeting the smart contract. While the risk related to inaccurate external data sources is consistent across smart contract platforms, solutions are actively being designed to decentralize oracle data feed infrastructure.

C. CYBER POLICY AND REGULATORY CONSIDERATIONS

Tokenized assets on public blockchains are borderless by nature causing challenges for global regulatory authorities and complexity for practitioners in the space. Global regulators have been consistent in highlighting cybersecurity risks resulting in specific cybersecurity requirements for certain jurisdictions. In this section, we consider the U.S. cyber-related regulatory requirements at the Federal level, as well as the BitLicense cybersecurity requirements for entities operating within New York State.

1. JURISDICTIONAL CHALLENGES

The token economy is an emergent segment of the digital economy, defined by rapid innovation and an evolving risk landscape which must be managed by proactive adoption of established cybersecurity tools and guidance from governments and standards bodies. Participants in the token economy have worked diligently to rationalize positions across domestic regulators (i.e., SEC, CFTC, FinCEN, IRS) and across international borders. While largely consistent with core intentions, challenges to compliance across multiple regulatory bodies can prove difficult.

2. SECURITY TOOLS AND MAPPING GUIDANCE

Security toolkits and mapping guidance assist organizations dealing with cybersecurity risks. To assist with control mapping efforts, tools and mapping guidance have been developed and released by standards bodies. Specifically, NIST has developed and open-sourced the Security Content Automation Protocol (“SCAP”)


Further, the manner in which a token is regulated will dictate certain cybersecurity requirements. For example, financial institutions must consider the Federal Financial Institutions Examination Council (“FFIEC”) expectations for cybersecurity practices, including its guidance for cloud computing services and authentication of an internet banking environment when applicable. These organizations should consider adopting the FFIEC Cybersecurity Assessment Tool to help identify cybersecurity risks and determine control environment maturity.

3. NEW YORK STATE BITLICENSE

New York State’s BitLicense is a set of regulations administered and enforced by the New York State Department of Financial Services (“NYDFS”) for virtual currency businesses serving New York residents. The regulation, Part 500 of Title 23 of the New York Code, requires companies with virtual currency operations in New York to obtain a license from the NYDFS and to comply with additional requirements as set forth in the regulations. The BitLicense, effective since March 2017, aims to protect customer information as well as the information systems by holding covered entities accountable for their cyber defense responsibilities, among other things.

The regulatory framework requires the implementation of a written cybersecurity program to include five core functions. Licensees must “establish and maintain an effective cybersecurity program to ensure the availability and functionality of their electronic systems and to protect those systems and any sensitive data stored on those systems from unauthorized access, use, or tampering.” Furthermore, each licensee must:

» Designate a Chief Information Security Officer responsible for overseeing the cybersecurity program and policy;

» Comply with certain reporting and audit requirements relating to cybersecurity; and

» Ensure that applications follow written security standards and guidelines.

Similar to industry-leading frameworks such as ISO-27001, NIST SP 800-53r5, and NIST CSF, the BitLicense also requires licensees to establish and maintain a business continuity and disaster recovery (“BCDR”) plan designed to ensure the availability and functionality of services in the event of an emergency or disruption to Licensee’s normal business activities. The rules set forth minimum requirements for each BCDR plan such as annual testing and remediation activities.

19 See FFIEC, Outsourced Cloud Computing (July 10, 2012).
4. GDPR CYBER EVENT DISCLOSURE REQUIREMENTS

In May 2018, the European Union’s General Data Privacy Regulations (GDPR) came into effect establishing specific expectations within Articles 32-34 for security and breach reporting. These domains have been covered extensively and will not be discussed in depth, however, given their applicability to entities within the token economy handling personal data of EU citizens, they warrant reference and inclusion within this narrative.

The security expectations established in GDPR require organizations to implement appropriate technology controls and procedures to ensure security commensurate with the entities’ respective risk environment. The prevalence of cyber risk across actors in this space will establish foundational requirements including pseudonymization and encryption; ensuring confidentiality, integrity, availability, and resiliency of all systems; the ability to recover availability and access to personal data in the event of an incident; and the regular testing/evaluation of technological and operational controls to ensure security of data processing.

Further, GDPR has established requirements for breach documentation following any incident related to confidentiality, integrity, and/or availability. In addition, when a breach results in risk to the rights and freedoms of citizens, they must be reported to the Supervisory Authority (“SA”) within 72 hours of breach identification. Specific reporting requirements must be included within the breach report to the SA.

Finally, we must acknowledge the clash between blockchain technology and its cryptographic immutability, and regulatory expectations regarding data deletion, namely GDPR Article 32’s “Right to Be Forgotten.” By design, transactions written to a blockchain are tamper-resistant. The data attributes of these transactions can, in some circumstances, contain identity information and/or cryptographic representations of an underlying identity (i.e., public key address). If such information is written to a public blockchain, it cannot be removed. The application of the regulatory expectation to on-chain data has not been clearly defined, and, as such, it is a consideration that must be explored.²⁰

---

D. GUIDELINES FOR ADVANCING CYBERSECURITY IN A TOKENIZED ECONOMY

In order to advance security across the ecosystem, practitioners and policymakers should consider the following guidance:

1. Practitioners interacting with digital assets on public blockchains should consider the challenges associated with asset recovery when developing policies, procedures, and technology infrastructure to develop robust preventative controls to prevent asset compromise. These policies may include the recommendations for “crypto custody” and key management, below.

2. Practitioners should develop policies, procedures, and technical infrastructure for crypto custody to securely manage digital assets throughout their lifecycle. These policies should limit the exposure of assets by balancing security and availability across tiered storage architectures to meet customer availability needs while limiting risk exposure to the assets. Practitioners may mitigate risk exposure by adopting key sharding techniques, multi-party computational approaches (“MPC”), multi-signature wallets, and third-party signers for identity validation/transaction authentication.

3. Practitioners must understand the risks to distributed consensus protocols by performing economic attack modeling to understand cost and likelihood of consensus mechanism attacks. These risks should inform business strategy and plans to integrate services with new public blockchains and assets.

4. Practitioners and participants choosing to self-custody their assets or to use a non-custodial solution must understand the implications of losing private keys and develop processes and approaches to mitigate these risks. These approaches may include utilizing specialized hardware for private key management, storing private keys in secure physical vaults, and creating resilience by backing up key replicas or recovery phrases in a geographically distributed and physically secure vault.
When using or building on public blockchains, protocol integrity and security must be guaranteed through robust testing procedures prior to production deployment through a “hard fork.” Blockchain communities have taken and should continue to take conservative approaches to deploying software upgrades via hard forks to avoid inadvertently introducing new software vulnerabilities. Historically, the majority of protocol level testing procedures have been executed by developer communities; however, to the extent permitted by the relevant regulatory frameworks or conducted under the appropriate regulatory oversight, practitioners may consider investing resources into pre-launch testing procedures on “test nets” prior to adopting and deploying software upgrades.

Smart contract code is susceptible to vulnerabilities and requires a robust secure software development lifecycle including extensive testing and security auditing. As smart contracts (and associated code) become more complex, the risk of unintended outcomes for malicious attacks will increase. Practitioners must enforce comprehensive controls to carefully review, test, and monitor smart contract implementations to detect and prevent anomalies from being exploited. Smart contract code and ongoing outcomes should be continuously monitored to ensure that new vulnerabilities are identified and that outcomes are consistent with the contract’s intended outcomes.

Practitioners must leverage established industry frameworks like NIST’s Cybersecurity Framework (“CSF”) to implement effective cybersecurity programs. In addition to the CSF, NIST provides the 800-53 control framework and accompanying automation tools for security monitoring (e.g., Security Content Automation Protocol- SCAP: NIST SP 800-126) which can be adopted to help manage cyber risk.

Practitioners must carefully consider the laws of each jurisdiction before locating in or interacting with residents in those states/countries. They should also consider these requirements in the context of service providers that they may utilize when operating their business.
IV. CONCLUSION

Public blockchains have incredible potential to revolutionize business models and industries by enabling the internet of value to reduce costs for consumers and increasing transparency to ensure integrity within our economic, social, and environmental systems. In order to enable this future, practitioners and policymakers must continue collaboration to foster and develop best practices for cybersecurity within the crypto ecosystem. The guidelines set forth in this document aim to advance a dialogue around the cyber risks in the token economy and to encourage policymakers and practitioners to design standards for technical and business solutions to mitigate these risks.

Blockchain holds a unique position with regard to cyber risk and security. In many ways, blockchain can mitigate key cybersecurity risks inherent in the current internet structure by design using encryption and distributed computing models, while in other circumstances, the value of the assets hosted on blockchains make them a key target for malicious actors. Although it is beyond the scope of this report, it should be noted that cybersecurity extends beyond blockchain platforms to the devices that transact with them. The security models for e-commerce that rely on continuous observation and logging of data will not translate to the decentralized platforms of blockchain. To address this shortcoming, cybersecurity practitioners should consider leveraging blockchain implementations to capture the evidence of cybersecurity controls along with other transaction data to substantially increase the cybersecurity posture of any system and provide additional proof of compliance, at the transactional level, with applicable regulatory regimes.

The risk considerations and guidelines outlined in this chapter cannot be contemplated as afterthoughts to innovation. Effective cyber risk management and cybersecurity practices should be integrated into business models to ensure the security and longevity of blockchain technology to realize transformative, positive impacts to our economic, social, and environmental systems.
UNDERSTANDING DIGITAL TOKENS:
Considerations and Guidelines for Advancing Cybersecurity in the Token Economy