THE JBBA

PEER REVIEWED RESEARCH

OPEN ACCESS
ISSN Online: 2516-3957
ISSN Print: 2516-3949
https://doi.org/10.31585/jbba-3-1-(5)2020

The Need for Cyber Resilient Enterprise Distributed Ledger Risk Management Framework

Robert E. Campbell, Sr.
Capitol Technology University, USA

Correspondence: rc@medcybersecurity.com
Received: 24 February 2020 **Accepted**: 02 March 2020 **Published**: 16 March 2020

Abstract

Critical infrastructure sectors are increasingly adopting enterprise distributed ledgers (DLs) to host long-term assets, systems, and information that is considered vital to an organization's ability to operate without clear or public plans and strategies to migrate safely and timely to post-quantum cryptography (PQC). A quantum computer (QC) compromised DL would allow eavesdropping, unauthorized client authentication, signed malware, cloak-in encrypted session, a man-in-the-middle attack (MITM), forged documents, and emails. These attacks can lead to disruption of service, damage of reputation and trust, injury to human life, and the loss of intellectual property, assets, regulated data, and global economic security. In 2018, Gartner revealed that a QC is a digital disruption that organizations may not be ready and prepared for, and CIOs may not see it coming.[1] On September 18, 2019, IBM announced that the largest universal QC for commercial use would be available in October 2019.[2] On October 23, 2019, Google officially announced "Quantum Supremacy," "by performing a calculation in 200 seconds that would take a classical supercomputer approximately 10,000 years."[3] DL cyber resilience requires "reasonable" measures, policies, procedures, strategies, and risk management before large-scale deployment. Cyber resilience implementations must be a critical component during the design and building phase, or during the initialization phase. The most significant existing attack vector for enterprise DLs is the public key infrastructure (PKI), which is fundamental in securing the Internet and enterprise DLs and is a core component of authentication, data confidentiality, and data and system integrity [1] [2]. Effectively implementing and managing a quantum-resistant PKI solution requires adherence to PKI standards, industry requirements, potential government mandates, certificate management policies, training personnel, and data recovery policies that currently do not exist. This research discusses security risks in enterprise DL PKI, areas that can be compromised, and provides an idea of what should be in a PKI DL Risk Management Framework plan.

Keywords: *cyber resilience, PKI, quantum computing, distributed ledger, cyberattack, risk management framework, hyperledger fabric*

[1] Gartner Reveals Seven Digital Disruptions CIOs May Not See Coming: https://www.gartner.com/en/newsroom/press-releases/2018-10-17-gartner-reveals-seven-digital-disruptions-cios-may-not-see-coming

[2] IBM's new 53-qubit quantum computer is the most powerful machine you can use: https://www.technologyreview.com/f/614346/ibms-new-53-qubit-quantum-computer-is-the-most-powerful-machine-you-can-use/

[3] Quantum Supremacy Using a Programmable Superconducting Processor: https://ai.googleblog.com/2019/10/quantum-supremacy-using-programmable.html

Despite the vast opportunities distributed ledger technologies (DLT) offer, they suffer from challenges and limitations such as security and privacy, compliance, and governance issues that have not yet been thoroughly explored and addressed. There are many threats and numerous attack vectors, such as phishing, malware, implementation, and technology. While there are some studies on the security and privacy issues of DLT, they lack a systematic examination of the security of these systems at the fundamental level of digital signatures and public key infrastructure (PKI) vulnerabilities. Vulnerabilities and weaknesses lead to the execution of various security threats to the standard functionality of the distributed ledger (DL) platforms. The rapid development and progress of quantum computing technology are not considerations that CEOs and CIOs are correctly figuring in as a risk factor. Quantum computing poses global security concerns because the technology will be able to hack into and disrupt nearly all current information technologies. In this paper, the author explores the attack surfaces in the open-source-permissioned blockchain project Hyperledger Fabric and its potential exploits through social engineering, malware, and cryptographic tactics. The attacks considered are insider threats, certificate authority (CA) attacks, and private-key attacks from quantum computers (QCs). The author will examine single points of failure in Hyperledger Fabric's membership service provider (MSP), or PKI, which proves to be a centralizing aspect of a decentralized system and a significant weakness of the permissioned blockchain network. Also, the author presents a cyber-resilient framework as possible use in a hybrid post-quantum-resistant enterprise PKI. Cyber resiliency is a feature that must be in systems of the future, which, when implemented, will enable the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, and/or attacks. Both the global security risks and the economic benefits necessitate building in cyber resilience.

Digital Currency and Blockchains under Attack

In 2018 alone, $1 billion in cryptocurrency was hacked from exchanges,[4] approximately $2.7 million stolen per day, or $1,860 each minute. Upbit is the seventh major crypto exchange hack of 2019 so far.[5] Upbit is the largest victim of hacking to date, after losing $49 million at 9:00 UTC on November 26, 2019. The exchange stated that an "abnormal transaction" resulted in a 342,000 ether loss in a few minutes. Some of the most notable attacks occurred in June 2011, when a hacker was able to exfiltrate Mt. Gox's auditor's credentials and transferred 2,609 bitcoins (BTCs) to an address for which Mt. Gox had no keys. The second attack occurred in 2014, resulting in 750,000 BTCs ($350 million) stolen from the exchange, and Mt. Gox halted operations and filed for bankruptcy. The Bitfloor bitcoin exchange was hacked in 2012 when hackers were able to retrieve unencrypted private keys that were kept online for backups. The amount stolen was 24,000 BTCs. Poloniex was hacked in 2014 and only stated it "has lost 12.3% of its total bitcoin supply in an attack." The exchange also explained that "the hacker found a flaw in his site's code that processes withdrawals, and made multiple simultaneous withdrawals," and the system did not respond to this error. The major problem was a coding error, and "the auditing and security features were not explicitly looking for negative balances."[6] On January 4, 2015, Bitstamp announced that an anonymous hacker hacked it, and 19,000 BTCs (worth $5 million) were lost. In 2016, Bitfinex breached and claimed 120,000 BTCs (worth $72 million) hacked. The attackers exploited a vulnerability in the multi-sig wallet architecture of Bitfinex and BitGo.[7] On May 7, 2019, Binance was hacked, losing more than 7,000 BTCs ($40 million). Binance announced that they discovered a large-scale security breach on May 7, 2019. The attackers were able to obtain user Application Orograming Interface (API) keys and 2FA codes. The attackers used techniques such as phishing, viruses, and other attacks, and the hackers were able to withdraw 7,000 BTCs from this one transaction.

Distributed Ledger Growth in Critical Infrastructure

Recent forecasts indicate that global blockchain technology revenues will experience rapid growth in the coming years, with the market expected to rise to over $60 billion worldwide in size by 2024. The financial sector is currently the largest investor in blockchain, with over 60% of the technology's market value concentrated in this field.[8] However, global enterprises are increasingly adopting DLT and are hosting critical assets and critical infrastructure in a hostile, organized, sophisticated, and well-resourced cyber threat environment. As an example, the Energy Web Foundation (EWF) is a global organization that uses

[4] How Hackers Stole $1B From Cryptocurrency Exchanges In 2018:
https://www.forbes.com/sites/daveywinder/2018/12/31/how-hackers-stole-1b-from-cryptocurrency-exchanges-in-2018/#7066025e4d87

[5] Upbit Is the Seventh Major Crypto Exchange Hack of 2019:
https://www.coindesk.com/upbit-is-the-sixth-major-crypto-exchange-hack-of-2019

[6] Yet another exchange hacked: Poloniex loses around $50,000 in bitcoin:
https://arstechnica.com/information-technology/2014/03/yet-another-exchange-hacked-poloniex-loses-around-50000-in-bitcoin/

[7] The Binance Hack:
https://medium.com/coinmonks/the-attack-on-binance-eba46700eef6

[8] Blockchain Market Shares, Market Strategies, and Market Forecasts, 2018–2024:
https://www.ibm.com/downloads/cas/PPRR983X

blockchain technology in the energy sector, with offices in Switzerland, Germany, and the United States. EWF launched the Energy Web Chain, in June 2019, and advertised "the world's first public, open-source, enterprise-grade blockchain tailored to the energy sector."[9] On December 12, 2019, the U.S. President's National Infrastructure Advisory Council published draft findings on the urgent cyber risks in the most critical and highly targeted private infrastructures and called for bold action.[10] The report indicated that escalating cyber risks to critical infrastructures present an existential threat to the continuity of government, economic stability, social order, and national security. Global governments and enterprises adopting DL are on the front lines of a cyberwar; they are ill-equipped to win against organized cybercriminals and nation-states intent on hacking, robbing, disrupting or destroying critical assets.

DLT Complexity

There are more than 30 known DL attack vectors in the categories of network, wallet, mining, double spending, and smart contracts and these attack can be phishing and social engineering, DNS hijacking, exchange hacks, 51% attacks, software flaws, and other types that can be malware and crypotjacking, and other traditional attacks that affect systems that connect to a blockchain [3]. The zero-day vulnerabilities cannot be quantified but must be considered as potential vulnerabilities that will be discovered and exploited. DLT consist of the integration of networked cryptography, fault-tolerance, and distributed consensus. Each of these topics is complicated, intricate and has many known vulnerabilities and weaknesses that are not well-understood by those who lack the technical background in these topics. Also, as with any complicated technology, there are always zero-day vulnerabilities yet to be discovered and made public. The combined technologies used to form DLT dramatically increase the vulnerabilities, threats, and weaknesses. This complexity, along with the intricacies of its ecosystem (wallets, exchanges, sidechains, mining pools, enterprise consortiums), requires a formal and logical framework to address issues systematically and mitigate them to make DLT resilient.

The Quantum Computer Threat

Google's "quantum supremacy" announcement means that QCs can process and solve massive computational problems that exceed the capabilities of current supercomputers and threatens DL cryptography. Complex mathematical problems are the foundation in which much of today's cryptography is based, including PKI and DL. DLT and PKI use asymmetric digital signature schemes for private and public-key generation, signing, verification of digital signatures, and QCs break and all of these functions. This public-key cryptography is in email, web browsing, encrypted storage, banking, virtual private networks, communications, critical infrastructures, and much of the Internet [2]. It would be exceptionally naive to think that covert research and development in "quantum supremacy" is not among the highest priorities of organized groups and nation-states around the planet. Further, it would follow that classified programs seek to protect actual capabilities, or there would not be a need for secrecy. Also, a QC attack could be difficult to detect because the attacker would derive the private key from the available public key, and with the private key, a hacker will have free and absolute access [4].

Impact of Compromised PKI Private Keys

PKI is the backbone of today's enterprise blockchain, DL, network, and internet security. Figure 1 is a depiction of Hyperledger Fabric's Managed Service Provider (MSP) services, which is essentially an abstraction of PKI for enterprise blockchains. Cyber resilience is methods and procedures that aid in preventing adversarial access to systems housing critical data while ensuring the integrity of data, despite the presence of the adversary on the network and being resilient to the adversary's efforts to manipulate data. DL must assume the existence of adversaries in the network and be capable of nullifying adversarial strategies by harnessing the computational capabilities of the honest nodes, and the information exchanged is resilient to manipulation and destruction [5].

Network DL private keys are the credentials and the means of authorizing transactions, which, if compromised, will make all assets controlled or secured by the keys freely available to an adversary. The private keys enable and allow the attacker(s) to capture information, passwords, compromise CAs, certificate forgeries, obtain other private keys, derive other private keys, hijack private keys, and forge validations. The attacks and risks associated with these malicious acts allow forged documents and emails, signed malware, unauthorized clients, eavesdropping, and man-in-the-middle (MITM) attacks. The impact of these activities can result in the loss of personally identifiable information (PII), protected health information (PHI), intellectual property (IP), reputation, assets, crippled operations, and human life.

Each MSP is in a folder with various subfolders containing the administrator certificate(s), root CA certificates, the node's private key, the node's X.509 certificate, and other optional inclusions. An X.509 PKI infrastructure is a security

[9] The Energy Web is unleashing blockchain's potential in the energy sector: https://www.energyweb.org/

[10] NIAC TRANSFORMING THE U.S. CYBER THREAT PARTNERSHIP DRAFT REPORT: https://www.cisa.gov/publication/niac-transforming-us-cyber-threat-partnership-draft-report

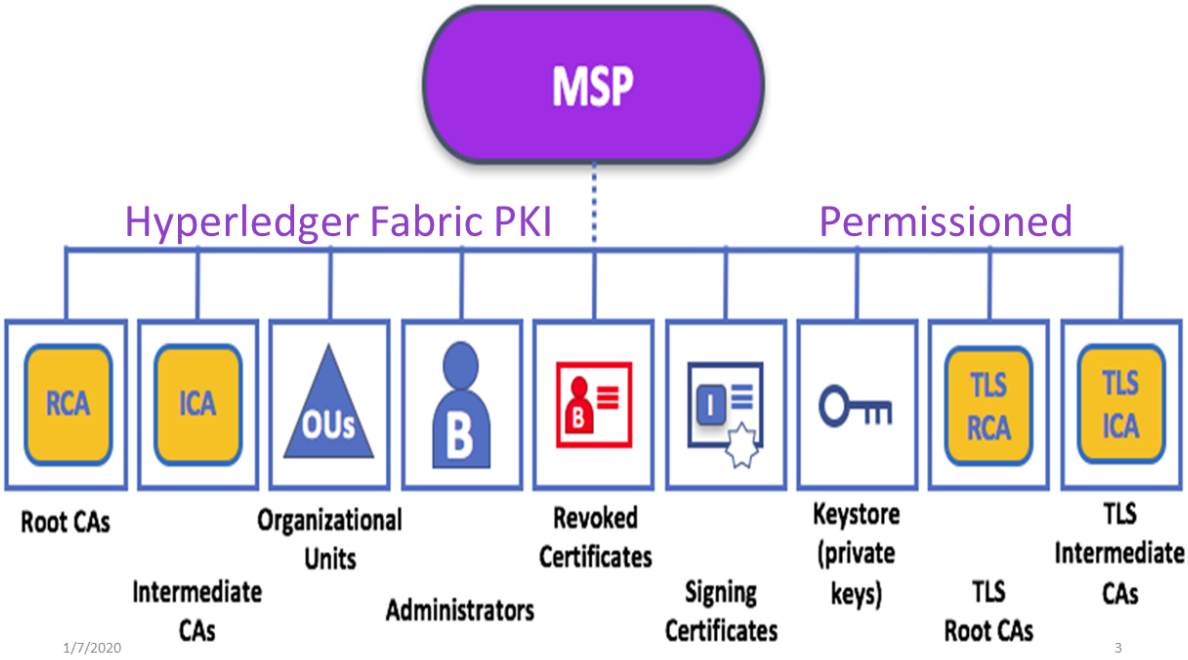

Figure 1. MSP Architecture. Source: Hyperledger Fabric.

architecture or format used in intranets, networks, and the Internet. Its cryptographic mechanisms support functions such as email, server authentication, signature generation, and validation. Specifications such as the secure multipurpose internet mail extensions (S/MIME) and transport layer security (TLS) also rely on this standard. The MSP is used to link identities, public-keys, and CAs; it acts as the primary trusted authority and uses digital signature algorithms to sign certificates of trust. Key security considerations include the ability of untrusted or unauthorized persons to participate in the network and the strength of the bit security of the encryption protocols [2]. Administrative duties include providing access and permissions for the entire blockchain network and are thus a single point of centralization. Each participant on the network is assigned a digital certificate that assures they are whom they say they are and defines the levels of access and permissions. These administrators set the permissions along with a digital certificate; each participant is assigned what Fabric labels a digital signature or the private key half of a public-/private-key pair. These keys sign off on transactions and endorsements to ensure and retain the integrity of the blockchain [6].

In the case of an insider threat such as a rogue administrator, the holder of the administrator certificate(s) is not to be trusted and has free rein over the blockchain. Administrative controls such as adding or revoking access, adding identities to the Certificate Revocation List (CRL), MSP validation of CAs, and manipulating the access a given identity has to the blockchain network are all managed solely by the administrator. Digital certificates and identities are crucial to the operation of the MSP. Cryptogen, a utility for generating Hyperledger Fabric key material, provides a means of preconfiguring a network for testing, and produces all private keys in one centralized location, and it is then up to the user to adequately and safely copy them to appropriate hosts and containers. Allowing new users to decide key management best practices and the lack of standard procedures can easily lead to private-key leakage attacks. Private-key leakage is possible because each participant can choose to store and protect their private key in any way the member determines; there need to be key management best practices for all members [6].

An outside attacker obtaining private key(s) could lead to any number of attacks. As private-key leakage attacks provide potential unlimited access to the blockchain and open the possibility for any number of secondary attacks, they are one of the greatest threats to the MSP. The leakage of private keys or a successful quantum computing attack could further lead to more severe attacks, such as MITM attacks, replay attacks, message tampering attacks, and identity leakage attacks [6]. Figure 2 illustrates the weaknesses, threats, and risks of a compromised MSP or PKI in enterprise blockchains. A further shortcoming of CAs in Hyperledger Fabric is in the way it is implemented in the MSP. The MSP requires at least one root CA and can support as many root and intermediate CAs as desired. If the root CA certificate or implementation were attacked, all certificates leading back to the root certificate are compromised. Successful attacks on the MSP, which controls the membership of the blockchain runs on, would be detrimental to the security of the entire enterprise, resulting in falsified identities and more.

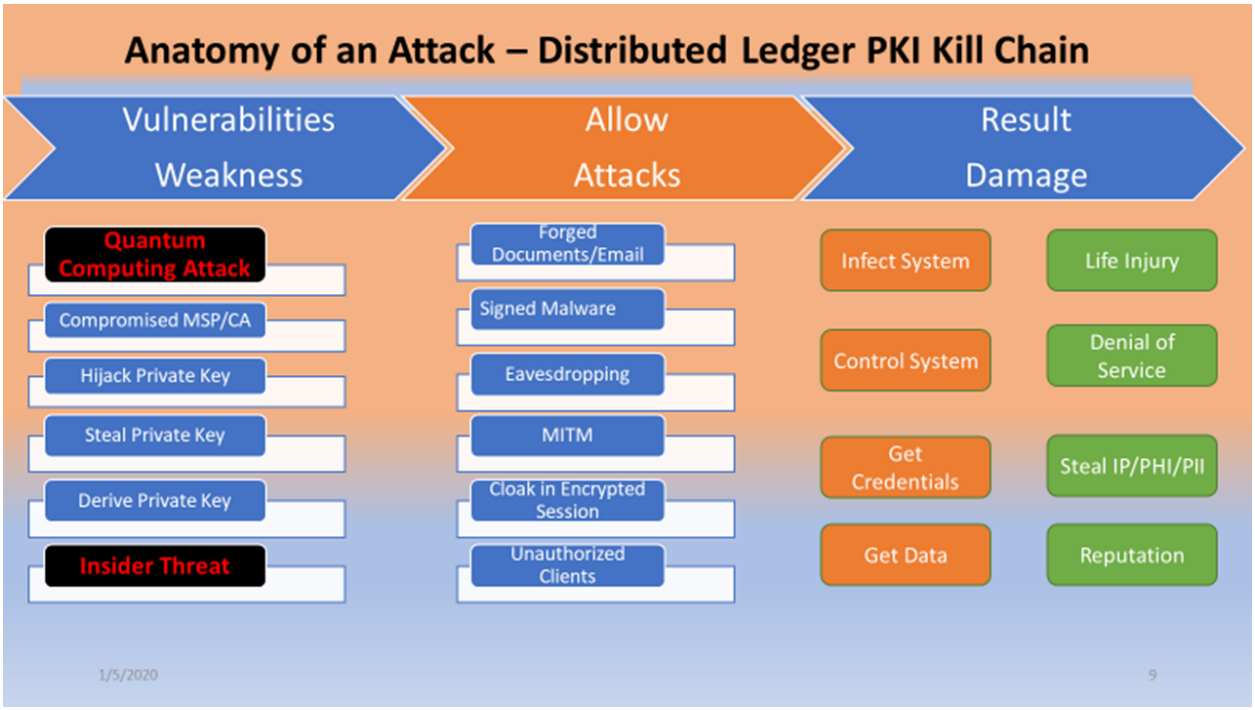

Figure 2. Distributed Ledger Kill Chain.

Anatomy of a Critical Infrastructure Attack Scenario Using Hyperledger Fabric

The following is a hypothetical critical infrastructure attack scenario on an energy plant X using enterprise blockchains such as Hyperledger Fabric and the newly discovered Russian-linked malware, which infects safety instrumented systems (SIS), called Triton. The SIS are automated safety defense systems for industrial facilities, responsible for stopping plant operations in the event of an emergency and are designed to prevent equipment failure and catastrophic incidents such as explosions or fire. FireEye has linked Triton to the Russian state-sponsored hackers.[11]

Quantum Computing Attack Scenario

The hackers are equipped with QCs capable of cracking today's standard PKI cryptography started by researching and gathering information about energy plant X. They looked for network ranges, IP addresses, and domain names. Furthermore, the hackers also searched for email addresses of key players in the organization, such as CFOs, IT professionals, and CTOs. After getting access to the network, the hackers proceeded to infiltrate the organization's network. Once the private keys were derived or obtained, the hackers accessed the entire network and went through the system silently. The attackers, armed with private keys, quickly gained remote access to an SIS engineering workstation and deployed the Triton attack framework. Immediately they started to reprogram the SIS controllers as the infection entered the SIS workstation and system via remote access. Also, the malware compromised the target system's logic controllers, exploiting "zero-day" vulnerabilities and software weaknesses that have not been identified by security experts.

The attackers reprogrammed the SIS to allow an unsafe condition while using the distributed control system (DCS), which allows attackers the ability to monitor and control an industrial process remotely and to cause fires and explosions. The result is that the attackers manipulated the process into an unsafe state from the DCS while preventing the SIS from functioning appropriately and giving false feedback to panel safety controls until it is too late to react. The attackers were able to exploit the weaknesses, vulnerabilities, and risks contained in the current enterprise architecture PKI technology and caused explosions and fires that destroyed the plant and caused the release of lethal gas and radioactive clouds causing massive injuries and loss of human life.

During the incident, none of the SIS controllers entered a visible failed safe state, which provided false safety readings and allowed the industrial process to continue under unsafe and dangerous conditions. The false readings prevented any investigation that would have alerted authorities and initiated an investigation. The attackers employed multiple techniques to conceal their activities and to deter digital forensic investigation of their tools and activities. They renamed the most typical and useful files to make them look legitimate like

[11] TRITON Attribution: Russian Government-Owned Lab Most Likely Built Custom Intrusion Tools for TRITON Attackers: https://www.fireeye.com/blog/threat-research/2018/10/triton-attribution-russian-government-owned-lab-most-likely-built-tools.html

Microsoft update files or a legitimate Schneider Electric application; they also used hacker tools to mimic legitimate administrator activities.[12] The attackers were able to derive the private keys of critical personnel, including safety monitors, and took total control of energy plant X. They gained complete control of SIS and caused dangerous processes to go unnoticed by sending false data to the safety control panels. The panels showed normal readings when the actual condition was increasingly hazardous. This control of the SIS and the extreme safety condition continued until it was too late, and it caused many explosions and the destruction of the plant and release of lethal and toxic clouds.

Urgent Need for Risk Management Framework for Distributed Ledger Systems

There is a pressing need to strengthen further the DL information systems, component products, and adopted services in critical infrastructures and enterprise sectors. It is essential that those systems, products, and services are sufficiently trustworthy throughout the system development life cycle and can provide the necessary resilience to support the economic and security interests of the enterprise. Cyber resiliency can be for system elements, systems, missions or business functions, and the system-of-systems which support those functions, organizations, sectors, or transnational missions/business functions. Nation-states and other well-resourced adversaries have intensified their efforts to infiltrate and gain control of enterprise networks and critical infrastructures, such as financial services and energy and if successful, these could impact the continuity of government, public safety, economic stability, and national security. Global enterprises are on the front lines of a cyberwar; they are ill-equipped to fully understand, thwart, or counter against nation-states' intent upon disrupting and destroying critical infrastructure. Cyber resilient DL systems require developing an integrated approach to building trustworthy systems. The author has modified SP 800-37 Rev. 2 guidelines and recommended steps to help build a more defensible information technology infrastructure, including the component products, systems, and services [7]. Systems security engineers must apply the necessary security measures that assure the system can withstand cyber faults, failures, and attacks.

Mitigating Cyberattacks on Permissioned DLTs

While no known technology, method, or procedure can categorically prevent cyberattacks, some steps and procedures can be put in place to mitigate attacks. The architecture, deployment, and operation impact the network's cybersecurity risks and determine the controls that are best able to reduce those risks. Mitigating considerations include the number and types of participants in the system; unauthorized persons to access the network; the design and sturdiness of the consensus validation rules and processes; the strength of the encryption protocols and the sensitivity of the data or transactions recorded in the ledger; and the ability to correct fraudulent, malicious, or erroneous files or data. At a high level, Figure 3 represents cybersecurity principles and controls of best practices that can be implemented on compromised CA, MSP, public keys, or private keys. These principles and controls include access controls, threat modeling, systems, and procedures to detect actual and attempted attacks or intrusions and risk management practices. The most important contribution this modified framework offers is the ability to adapt, survive, and continue operations with minimum disruption and loss. This framework can be used in building, deploying, and operating DL systems and outlines logical step-by-step procedures needed for cyber resiliency.

Resources Needed for Incident Response

Cyber resilient DL systems must have a business continuity planning (BCP) that delineates the organization's use of strategies, procedures, technical measures, and plans necessary for the recovery of lost data, operations, and systems in the event of a business disruption. The BCP includes a management plan, data backup plan, disaster recovery plan, and an emergency mode operation plan. The plans must consist of roles, responsibilities, and communication strategies in the event of a compromise or disaster, including notification of relevant external partners. Data backup plan is required to establish necessary procedures to ensure the maintenance and retrieval of exact copies of stored regulated data. The disaster recovery plan creates procedures and processes that will assist the restoration of any lost data in case of disaster, system failure, or cyberattacks. This plan is crucial, especially in the case of a cyberattack that may disrupt access to such data for an extended period. This will also require creating an inventory of all the sensitive data and systems that will be necessary for the restoration of an enterprise's activities. The emergency mode operation plan is used to ensure the continuity of an enterprise's operations while protecting critical assets and regulated data. This operation plan assists an organization in resuming its normal operations in the event of a disaster, emergency, system failure, or cyberattack. The plans should be tested and revised as necessary to ensure that the procedures put in place are effective. The main goal should be periodic testing of written contingency plans to identify weaknesses and making necessary revisions on the documentation. Figure 3 outlines the primary phase in the Distributed Ledger Risk Management Framework.

The Distributed Ledger Risk Management Framework starts with Step 1, analyzing the organizational architecture documents and reference materials external to the enterprise. This step is in the context of determining the criticality of the

[12] SAS 2019: Triton ICS Malware Hits A Second Victim: https://threatpost.com/triton-ics-malware-second-victim/143658/

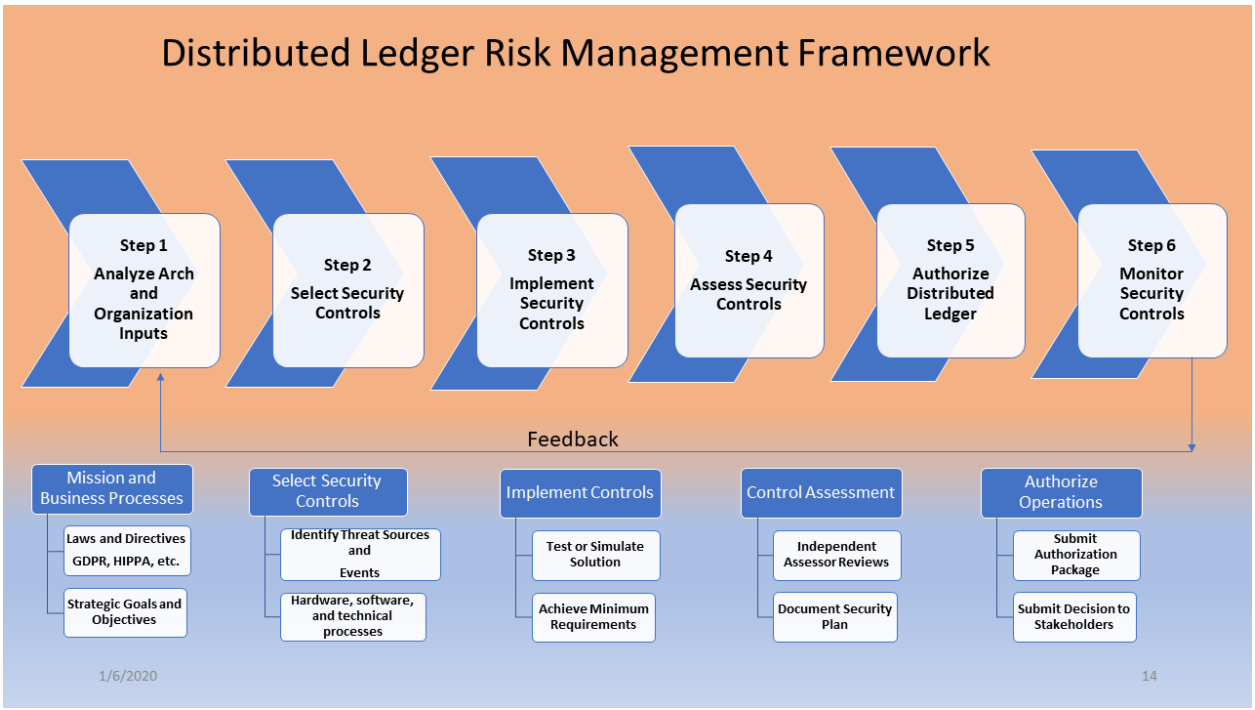

Figure 3. Distributed Ledger Risk Management Framework.

information and system according to potential worst-case, adverse impact on the organization, mission/business functions, and the system. These documents include policy and procedures, data regulating requirements, and laws for protected data such as the General Data Protection Regulation (GDPR) Health Insurance Portability and Accountability Act (HIPAA), Financial Industry Regulatory Authority (FINRA). In this phase, the business processes, objectives, and goals must align with the overall platform design and performance. Selecting security controls in Step 2 is based upon the output of Step 1, which builds the baseline using categorization. Step 2 specifies a minimum baseline of security controls for countermeasures prescribed for the system designed to ensure the integrity, confidentiality, and availability of its information and to meet a set of defined requirements. Step 3 implements security controls within the enterprise architecture and systems using solid system security engineering practices. Step 4 determines security effectiveness—assessing whether the controls are implemented correctly, operating as intended, and meeting the security requirements for the system and environment of operation. Step 5 involves a documented independent assessment of security controls, and this information is promulgated to all stakeholders to ensure everyone understands the configuration changes and its potential impact on operations and business. The authorizing official (AO) examines the output of the security controls evaluation to determine whether or not the risk is acceptable. Step 6 monitors security controls for effectiveness and includes a communication or feedback loop that goes back to Step 1. Continually monitoring the controls applied for the system and its ecosystem of operation for changes, indications of attack, and so on may affect regulation and reassess control effectiveness.

Cyber Resilient Distributed Ledger Systems and NIST Post-quantum Project

Google's surprise announcement of quantum supremacy is a warning to all that quantum computing advances are not predictable. Cyber resiliency requires the ability to react quickly to cryptographic threats by implementing alternative methods of encryption. Specifically, it requires the ability to respond to incidents, has an inventory of all certification and cryptographic keys from all issuing authorities, and is capable of quickly migrating the PKI to new post-quantum resistant PKI algorithms. National Institute of Standards and Technology (NIST) is in the process of choosing one or more public-key cryptographic algorithms through a public competition-like process. The latest public-key cryptography standards will specify one or more additional digital signature and public-key encryption algorithms. These algorithms will likely be capable of protecting sensitive information well into the foreseeable future, including after the advent of QCs. NIST has down-selected a group of potential cryptographic algorithms—down to a bracket of 26. These algorithms are the ones that NIST mathematicians and computer scientists consider to be the strongest candidates. The 9 second round candidates for digital signatures are CRYSTALS-DILITHIUM, FALCON, GeMSS, LUOV, MQDSS, Picnic, qTESLA, Rainbow, and SPHINCS+[13]. While NIST does not expect to formalize new post-quantum cryptography (PQC)

[13] PQC Standardization Process: Second Round Candidate Announcement: https://csrc.nist.gov/news/2019/pqc-standardization-process-2nd-round-candidates

standards until the 2022–2024 time frame,[14] the enterprises cannot afford to wait. The time is now to begin independent testing and evaluation of the most promising NIST candidate algorithms toward migration and replacement. The path to a successful migration is lengthy and complicated.

Recommendations

It is of note that this research does not specify any of the NIST second-round candidate algorithms will be a straightforward "drop-in replacement"; it may need additional NIST rounds and years of follow-on research, analysis, and testing for a suitable "drop-in replacement" to be identified or developed. Therefore, the author believes that now is the time to test possible near-term "Hybrid Quantum Resistant Classical Public Key Infrastructure," a solution with an aim of seeking reductions in public-key size as one of the most significant parameters. It is the public key that is exposed and used the most in today's PKI systems, and it is possible to modify the X.509 certificate standard to accommodate new PQC algorithms, which would only provide the public key that would be much more resistant to implementation and quantum computing attacks.

Additional research is needed on approaches to introducing new PQC algorithms (e.g., hybrids) within live systems that must remain interoperable with other systems during the period of industry migration. This includes such areas as penetration testing, formal testing, formal modeling, automated tools, and approaching transition in complex infrastructures. There is a critical need for research to understand and quantify the implications of replacing today's public cryptography algorithms.

Conclusion

Google's surprise announcement of quantum supremacy is a notice to all that quantum computing advances cannot be perfectly projected. Quantum computing attacks can lead to disruption of service, damage of reputation and trust, injury to human life, and the loss of intellectual property, assets, regulated data, and global economic security. PQC-safe algorithms generally have higher computation, memory, storage, and communication requirements; research and prototyping are needed to understand performance, security, and implementation. In this paper, the author explored the attack surfaces in open-source permissioned blockchain project Hyperledger Fabric and its potential exploits through social engineering, malware, and cryptographic tactics. Despite the vast opportunities DLT offer, they suffer from challenges and limitations such as security and privacy, compliance and governance issues.

The author examined single points of failure in Hyperledger Fabric's MSP, or PKI, which prove to be a centralizing aspect of a decentralized system and a significant weakness of the permissioned blockchain network. Further research is required on policy, process, and people. Global enterprises are increasingly adopting DLT and are hosting critical assets and infrastructure in a hostile, organized, sophisticated, and well-resourced cyber threat environment. As an example, EWF is a global organization that uses open-source blockchain technology in the energy sector without clear or public plans and strategies to migrate safely and timely to PQC. There is a pressing need to further strengthen the critical infrastructures and enterprise sectors and adopted DL information systems, component products, and services. It is essential that those systems, products, and services are sufficiently trustworthy throughout the system development life cycle and can provide the necessary resilience to support the economic and security interests of the enterprise.

Competing Interests:
None declared.

Ethical approval:
Not applicable.

Author's contribution:
Robert E. Campbell, Sr. designed and coordinated this research and prepared the manuscript in entirety.

Funding:
None declared.

Acknowledgements:
Robert E. Campbell, Sr. would like to thank Dr. Ian McAndrew, Dean of Doctoral Programs.

References

[1] R. Campbell, "Evaluation of Post-Quantum Distributed Ledger Cryptography," 2019. [Online]. Available: https://jbba.scholasticahq.com/article/7679-evaluation-of-post-quantum-distributed-ledger-cryptography. [Accessed 21 9 2019].

[2] R. Campbell, "Transitioning to a Hyperledger Fabric Quantum-Resistant Classical Hybrid Public Key Infrastructure," 31 July 2019. [Online]. Available: https://jbba.scholasticahq.com/article/9902-transitioning-to-a-hyperledger-fabric-quantum-resistant-classical-hybrid-public-key-infrastructure. [Accessed 21 September 2019].

[3] H. Chen, M. Pendleton, L. Njilla and S. Xu, "A Survey on Ethereum Systems Security" 13 August 2019. [Online]. Available: https://arxiv.org/pdf/1908.04507. [Accessed 7 1 2020].

[4] A. Majot and R. V. Yampolskiy, "Global catastrophic risk and security implications of quantum computers," Futures, vol. 72, no., pp. 17–26, 2015.

[14] Post-Quantum Cryptography: Workshops and Timeline: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Workshops-and-Timeline

[5] S. Bagheri and G. Ridley, "Organisational cyber resilience: research opportunities," 2017. [Online]. Available: https://eprints.utas.edu.au/25820. [Accessed 7 9 2019].

[6] A. Davenport, X. Liang, and S. Shetty, "Attack Surface Analysis of Permissioned Blockchain Platforms," September 2018. [Online]. Available: https://par.nsf.gov/servlets/purl/10083311. [Accessed 8 1 2020].

[7] J. T. Force, "Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy," December 2018. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final. [Accessed 8 1 2020].

[8] V. Lyubashevsky, T. Giineysu, T. Poppelmann, and D. Stehlé, "Post-Quantum Cryptography - Round 2 Submissions," 30 March 2019. [Online]. Available: https://csrc.nist.gov/projects/post-quantum-cryptography/round-2-submissions. [Accessed 14 January 2020].