Blockchain/Distributed Ledger Technology (DLT) Risk and Security Considerations

cloud security alliance®

The permanent and official location for Cloud Security Alliance Blockchain/DLT Working Group is https://cloudsecurityalliance.org/working-groups/blockchain/

Acknowledgments

Lead Author

Frederick Wamala, Ph.D.

Peer Reviewers

Kurt Seifried
Terri Jackson
Goni Sarakinov
Anis Hammami

CSA Global Staff

Hillary Baron

Editor

Larry Hughes

Special Thanks

Bowen Close

Table of Contents

Executive Summary

The Cloud Security Alliance (CSA) seeks to help create and maintain a trusted cloud ecosystem that provides business and government an opportunity to exploit the normal potential benefits of cloud computing, such as reduced capital expenses, agility, redundancy, high availability, and resiliency.[1] Secure cloud platforms enable organizations to transform their operations faster, save money due to reduced capital expenses, make markets, discover and match pricing, and maximizing the returns to their stakeholders. However, CSA's research indicates that, "The improved value offered by cloud computing advances have also created new security vulnerabilities."[2]

Cloud Service Providers (CSPs) use shared responsibility models or matrices to address security threats in the cloud. The models that draw upon guidance, such as NIST SP 500-292[3] and PCI DSS Cloud Computing Guidelines,[4] split cloud security responsibility between the CSPs and Cloud Service Customers (CSCs). The models differ across cloud services and deployment models. Typically, the CSPs secure the virtualization layer, physical hosts, network, and datacenters whilst CSCs manage their data, application logic/code, identity and access, and platform and resource configuration.

The CSA's Blockchain/Distributed Ledger Technology (DLT) Working Group (WG) investigates blockchain technology's potential role in cloud security. Some blockchain technologies use X.509 certificates to create encapsulated digital identities that could control permissions over resources and access to data in the cloud. In addition, blockchain's immutability property ensures that data blocks have not been altered thus reducing fraud, data manipulation and data destruction risks.

The rising frequency of Distributed Ledger Technology (DLT) platform hacks, exploits and scams imperils confidence in blockchain technology's ability to serve as the foundation for cloud security. DLT platforms are attractive to advanced Threat Actors, such as nation state sponsored groups, criminal organizations, etc., because blockchain networks host large codebases, many networked nodes, and valuable data flows.[5] There is no shortage of guidance on how to design, configure and deploy Hyperledger Fabric (hereafter "Fabric"). Fewer documents take a systematic approach to Fabric security that recognizes that durable security always starts with requirements. For example, configuration-led Fabric guidance rarely explains *why* high assurance security controls are needed to obtain Authorization to Operate blockchain solutions in critical sectors. That is what we do here. We offer a Reference Security Architecture to guide your thinking around the *why*, *what*, and *how* aspects of Fabric security. We highlight the steps that you should consider when designing blockchain solutions that must operate within critical sectors. This whitepaper will benefit business leaders, security architects, and anyone else with responsibility for, or an interest in, deploying secure Fabric solutions.

---

1 Mogull, R., et al., *Security Guidance for Critical Areas of Focus in Cloud Computing v4.0*. 2017, Cloud Security Alliance (CSA): Seattle, Washington, United States. p. 1-152.

2 Bhat, S., et al., *Top Threats to Cloud Computing: Egregious Eleven Deep Dive*. 2020, Cloud Security Alliance (CSA): Seattle, Washington, United States. p. 1-30.

3 Liu, F., et al., *NIST Special Publication 500-292 NIST Cloud Computing Reference Architecture*. 2011, National Institute of Standards and Technology (NIST) Gaithersburg, Maryland, United States.

4 PCI-SSC, *Information Supplement: PCI SSC Cloud Computing Guidelines*. 2018, Cloud Special Interest Group - PCI Security Standards Council (PCI SSC): Wakefield, MA, United States.

5 Hyperledger, *An Introduction to Hyperledger*. 2018b, The Linux Foundation®: San Francisco, California, USA.

1. Introduction

1.1 Overview

Blockchain technology has the potential to transform critical sectors.[6] The Hyperledger project explains that "[w]ith blockchains, many existing business processes in many industries can be streamlined to save time, save money, and reduce risk. And many entirely new processes – perhaps even whole new industries – can be invented."[7] For instance, business blockchains enable the tracking and trading of stocks and bonds with reduced risk and time, and increased transparency.[8] Similarly, the Depository Trust & Clearing Corporation (DTCC) has embraced the use of DLT across a range of processing to further lower risk and costs for the financial services industry.[9] Furthermore, Fnality International argues that Financial Market Infrastructure (FMI) based on DLT, aka distributed Financial Market Infrastructure (dFMI), could address issues of operational resilience, transparent risk management and inefficient processes.[10] Hence, these insights offer a method that can help to deploy DLT solutions that are secure, cost-effective, and meet regulatory and compliance requirements of enterprises.

1.2 DLT Security Incidents

The World Economic Forum (WEF) observes that growing institutional and regulatory comfort with blockchain technology has seen many DLT projects move from Proof-of-Concept (PoC) to live production.[11] However, security incidents, mostly in crypto public markets, have raised corporate and government concern that DLT solutions increase exposure to financial, reputational, customer and business disruption risks. For instance, the CSA DLT-Security Incidents list[12] chronicles attacks, such as the theft of $722M in Bitcoin from the Bitclub Network, the theft of $40M from the Binance Cryptocurrency Exchange and the theft of 5% of the total assets held by Crypto Exchange EXMO.[13,14,15]

---

6 HMT, *Cryptoassets Taskforce: Final Report*. 2018, HM Treasury, Financial Conduct Authority (FCA) and Bank of England: London, UK. p. 58.

7 Hyperledger, 2018b.

8 Hyperledger, *The Hyperledger Vision: Blockchain 101, Introducing Hyperledger, Industry Use Cases*. 2018a, The Linux Foundation®: San Francisco, California, USA.

9 DTCC, *Embracing Disruption – Tapping the Potential of Distributed Ledgers to Improve the Post-Trade Landscape*. 2016, Depository Trust & Clearing Corporation (DTCC): New York, United States.

10 Fnality, *The Fnality Narrative Q3 2020*. 2020, Fnality International: London, UK.

11 WEF, *Digital Assets, Distributed Ledger Technology and the Future of Capital Markets in Insight Report*. 2021, World Economic Forum: Geneva, Switzerland.

12 DLT-Security-Framework/DLT-Security-Incidents: https://github.com/cloudsecurityalliance/DLT-Security-Framework/blob/master/DLT-Security-Incidents.csv#L676

13 United States vs. Matthew Brent Goettsche et.al., 19-CR-877-CCC: https://www.justice.gov/usao-nj/bitclub

14 DLT-Security-Framework/DLT-Security-Incidents: https://github.com/cloudsecurityalliance/DLT-Security-Framework/blob/master/DLT-Security-Incidents.csv#L676

15 Hackers steal 5% of the total assets held by the EXMO Crypto Exchange: https://www.coindesk.com/crypto-exchange-exmo-says-hackers-have-stolen-5-of-total-assets

Indeed, the CSA Blockchain/DLT WG has issued Crypto-Asset Exchange Security Guidelines.[16] Additionally, the CSA is creating a Top 10 DLT attacks paper. You should also pay close attention to the https://rekt.news leaderboard. Rekt News is an anonymous platform that allows whistleblowers and decentralized finance (DeFi) enthusiasts to share information on major cryptocurrency and DeFi hacks and exploits.[17] We should stress that it is easier to obtain information about attacks on public blockchains than on private blockchains.

1.2.1 Blockchain/DLT and Critical Sector Ransomware Attacks

As we will discuss in Section 3.1.1 – Concerns of Financial Regulators, governments are alarmed by the use of pseudo-anonymity and privacy features of permissionless blockchain networks, such as Bitcoin and Monero, to facilitate ransomware attacks against critical sectors including energy, food,[18] healthcare,[19] and more. For instance, on September 21, 2021, the US Department of the Treasury sanctioned cryptocurrency exchange SUEX for its alleged part in facilitating financial transactions for ransomware actors. Treasury alleges that over 40% of SUEX's known transaction history is associated with illicit actors.[20]

It is valuable for your organization to plot the DLT attacks on the MITRE ATT&CK® framework, a globally accessible knowledge base of adversary tactics and techniques based on real-world observations.[21] For example, the Credential Access (TA0006) Enterprise Tactic is popular in cryptocurrency heists since gaining access to a private Key offers full access to all digital assets controlled by that key.[22] Ironically, the FBI salvaged $2.3M of the Colonial Pipeline ransom with the tactic of accessing the private key for Darkside's Bitcoin address.[23]

1.3 Blockchain Technology Layers

Understanding blockchain technology and how it interacts with regulated sectors will be critical to securing your critical business services. Blockchain technology is surrounded by misconceptions[24] because most literature addresses the concerns of technical stakeholders, particularly software engineers.

16 CSA Crypto-Asset Exchange Security Guidelines: https://cloudsecurityalliance.org/artifacts/csa-crypto-asset-exchange-security-guidelines-abstract/

17 The Rekt News leaderboard ranks cryptocurrency and DeFi hacks and exploits: https://rekt.news/leaderboard/

18 JBS Paid $11 Million Ransom: https://www.wsj.com/articles/jbs-paid-11-million-to-resolve-ransomware-attack-11623280781

19 Hospitals attacked: https://www.wsj.com/articles/the-ruthless-cyber-gang-behind-the-hospital-ransomware-crisis-11623340215

20 Treasury is designating SUEX pursuant to Executive Order 13694, as amended, for providing material support to the threat posed by criminal ransomware actors: https://home.treasury.gov/news/press-releases/jy0364

21 MITRE ATT&CK® framework- Enterprise tactics: https://attack.mitre.org/tactics/enterprise/

22 Yaga, D., et al., *Blockchain Technology Overview*. 2018, National Institute of Standards and Technology (NIST) Interagency or Internal Report (IR) 8202: Gaithersburg, Maryland, United States.

23 Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside: https://www.justice.gov/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside

24 Yaga, D., et al., 2018.

Chris Hammerschmidt's three layer model is a useful tool for visualizing blockchain technology security risks.[25] The top conceptual layer provides a high-level view of blockchain i.e., settings and the solution it offers. Next, the component interaction layer deals with how the components of blockchain's core technologies, e.g., cryptography, distributed systems, and databases interact to contribute to the system as a whole. Lastly, the technology layer explores how the core technologies work and whether they perform their roles adequately.

Most Fabric security advice focuses on the conceptual and technology layers. Unfortunately, rapid technology and changes in the threat environment routinely invalidate such advice. Consequently, in this paper, you will learn about the three layers and their interaction with on-premises and cloud IT environments of organizations in critical sectors.

1.4 Purpose of the Document

The CSA Blockchain/DLT Working Group has developed this paper to encourage industry to take a holistic view of blockchain/DLT network security. As noted earlier, there is no shortage of guidance on how to design, configure and deploy Fabric solutions. This whitepaper provides insights into how the three layers of blockchain technology interact with enterprise security services to deliver specific security outcomes. Our holistic approach does not shy away from the hard work of operating production blockchain networks within computer networks constrained by critical sector requirements, for example, security accreditation and PCI DSS segmentation. Our recommendations for Fabric can be applied to other permissioned blockchains.

1.5 Scope

As discussed in the Executive Summary, this whitepaper addresses the why, what, and how aspects of Fabric security. Section 3 uses the concept of Business Drivers for Security to show how one could explain *why* securing a DLT/blockchain solution is important to an organization. We address both the value of security controls in terms of controlling an organization's exposure to operational risk but also how the security measures could enable you to exploit business opportunities. Sections 4, 5, 6 and 7 address the *who* and *what* aspects of the DLT/blockchain security. Section 4 offers an overview of a sample Hyperledger solution that identifies the users, external systems, inputs and outputs, and external devices that you would want to protect. We use the STRIDE Threat Model to analyze typical Fabric security threats and compromise methods.[26] Readers could replace the STRIDE Model with other threat modeling techniques, such as Process for Attack Simulation and Threat Analysis (PASTA[27]) and Persona non Grata. In addition, we identify the Logical Security Services that could be utilized to secure Fabric blockchain networks against the identified security risks. We

25 Blockchain layers: https://medium.com/@chrshmmmr/how-much-blockchain-do-you-need-to-know-a-short-analysis-7373853c3043

26 Developed by Praerit Garg and Loren Kohnfelder at Microsoft, STRIDE is a model for identifying computer security threats. STRIDE is a mnemonic for security threats in six categories. The threats are Spoofing, Tampering, Repudiation, Information disclosure (privacy breach or data leak), Denial of service and Elevation of privilege.

27 The Process for Attack Simulation and Threat Analysis (PASTA) is a threat model that combines an attacker's perspective of a business with risk and impact analysis to create a picture of the threats to products and applications and their vulnerability to attack. The threat model informs decisions about risk and priorities for fixes. Source: https://www.cynance.co/pasta-threat-modelling/

map the Logical Security Services[28] to elements of Fabric, such as the Membership Service Provider (MSP), peer, etc. Lastly, Sections 7 and 8 provide examples of *how* you might want to implement the security mitigations required to address the *why* and *what* aspects of DLT security identified above. Specifically, Section 7 presents a risk mitigation approach, and Section 8 proposes a Reference Security Architecture. The Reference Security Architecture is a template that security architects could consider during the design of Fabric solutions in critical sectors. We apply network security principles from frameworks, such as *ITU-T Recommendation X.805: Security architecture for systems providing end-to-end communications* (ITU-T X.805)[29] and the Walled Garden Pattern., to a Hybrid Cloud Model and the IBM Blockchain Reference Architecture.[30]

1.6 Audience

We expect that this paper will be read by individuals who wish to understand, at a high-level, the security and risk considerations for Fabric. We present knowledge from domains ranging from business analysis, requirements engineering, risk assessment to network security because all these areas affect blockchain/DLT network security. Hence, we offer information that can help:

- Business and government leaders to understand the true risk balance of using blockchain and the resultant security, financial, regulatory, reputational, business and consumer risks.
- Chief Information Security Officers, Enterprise Security Architects, etc., to assess the risk of introducing DLT components into a corporate network whilst maintaining compliance.
- Regulators and internal risk managers to evaluate the potential risks associated with financial crime, consumer exposure, espionage, and so forth, and to devise appropriate policies in response.
- Individuals to gain high-level knowledge about blockchain security and thus reduce their exposure to fraudulent activity and unsuitable products.

Sections of this whitepaper would appeal to different audiences. For instance, business leaders and CxO Executives are likely to focus on the *why*, *who* and *what* aspects of the paper because they address Business Drivers for Security, who will use it and security threats. Security architects should understand the business context within which secure Fabric solutions must be designed, built and operated. Hence, security architects should understand the whole paper i.e., *why*, *who*, *what* and *how* aspects. The security architect should understand all these areas because the Architect's view encompasses the overall concept by which the business requirements of the enterprise may be met.[31] We should stress that this paper is not intended to serve as a blockchain technical guide. However, it offers a good amount of technical detail.

28 ISO 7498-2:1989 defines a security service as a capability for safeguarding the security of information in an Open Systems Interconnection (OSI) network architecture context. The Sherwood Applied Business Security Architecture (SABSA) extends the definition to cover any enterprise architectural context. A security service is specified independently of the technical (physical) mechanisms that are to deliver them e.g., encryption is the technical (physical) mechanism for delivering Confidentiality Services.

29 ITU, *ITU-T Recommendation X.805: Security architecture for systems providing end-to-end communications, in Series X: Data Networks and Open System Communications - Security.* 2003, International Telecommunication Union (ITU): Geneva, Switzerland.

30 IBM Blockchain Architecture: https://www.ibm.com/cloud/architecture/architectures/blockchainArchitecture/reference-architecture

31 W100 - SABSA Whitepaper: https://sabsa.org/white-paper-requests/

2. Blockchain Technology Basics

Understanding the main concepts that we use is vital to addressing blockchain technology misconceptions. Thus, we define the main concepts here. The Glossary has mode definitions.

2.1 Distributed Ledger and DLT defined

A distributed ledger is a tamper-evident and tamper-resistant multi-party database that is usually implemented in a distributed fashion (i.e., without a central repository) and usually without a central trusted authority.[32,33] The ledgers process transactions in cryptographically linked blocks (records) according to the ordering of the blocks in the blockchain. Distributed Ledger Technology (DLT) nodes agree upon and record transactions within a shared ledger such that, under normal operation of the blockchain network, no transaction can be edited or deleted once published.[34] Distribution of control amongst entities, rather than reliance on a Trusted Third Party (TTP), saves time and cuts costs across several sectors.[35] For example, in Capital Markets, DLT solutions could address inefficiencies by minimizing the need for reconciliation and manual data verification.[36] Similarly, blockchain security design features could support safe, efficient, and cost-effective transfer of information across different government and military network security domains, for instance, between classified and unclassified military networks.[37,38]

2.2 Permissioned versus Permissionless Blockchain Networks

Permissioned network participants are known to one another, have an intrinsic interest in participating in the consensus making process and seek to share data with a greater degree of security.[39] Permissioned blockchains can limit participation to specific people or organizations. Conversely, permissionless blockchains allow anyone to read and write to the blockchain without authorization.[40] Thus, permissioned blockchains are more able to address the cloud security threats[41,42] that could exploit the pseudo-anonymity of permissionless account provisioning that does not mandate identification and authorization.[43]

32 Hyperledger, 2018a.
33 Yaga, D., et al., 2018.
34 Yaga, D., et al., 2018.
35 Khemissa, S. and M. Roza, *Documentation of Relevant Distributed Ledger Technology and Blockchain Use Cases v2*. 2019, Cloud Security Alliance (CSA): Seattle, Washington, United States. p. 17.
36 WEF, 2021.
37 Olson, T., *Blockchain as a cross-domain security solution*. 2018a, IBM: Somers, New York, USA.
38 Olson, T., *Securing your cross-domain file transfers with blockchain*. 2018b, IBM: Somers, New York, USA.
39 Hyperledger, 2018a.
40 Yaga, D., et al., 2018.
41 Bhat, S., et al., 2020.
42 Brook, J.-M.C., et al., *Top Threats to Cloud Computing: The Egregious 11*. 2019, Cloud Security Alliance (CSA): Seattle, Washington, United States. p. 1-41.
43 Yaga, D., et al., 2018.

2.3 Hyping Blockchain Business and Security Properties

The National Institute of Standards and Technology (NIST) explains that blockchain technology has not been immune from the overhype, overuse, misconceptions, and the fear of missing out that characterize most nascent technologies.[44] For example, the World Economic Forum notes that, "Capital markets are not necessarily moving inexorably towards a global, fully digitized, DLT-based utopia as many predicted."[45] Unsurprisingly, as with other innovative technologies, such as Public Key Infrastructure (PKI),[46] Internet of Things (IoT),[47] Identity and Access Management (IAM),[48] and so forth, blockchain has earned a Gartner Hype Cycle entry.[49]

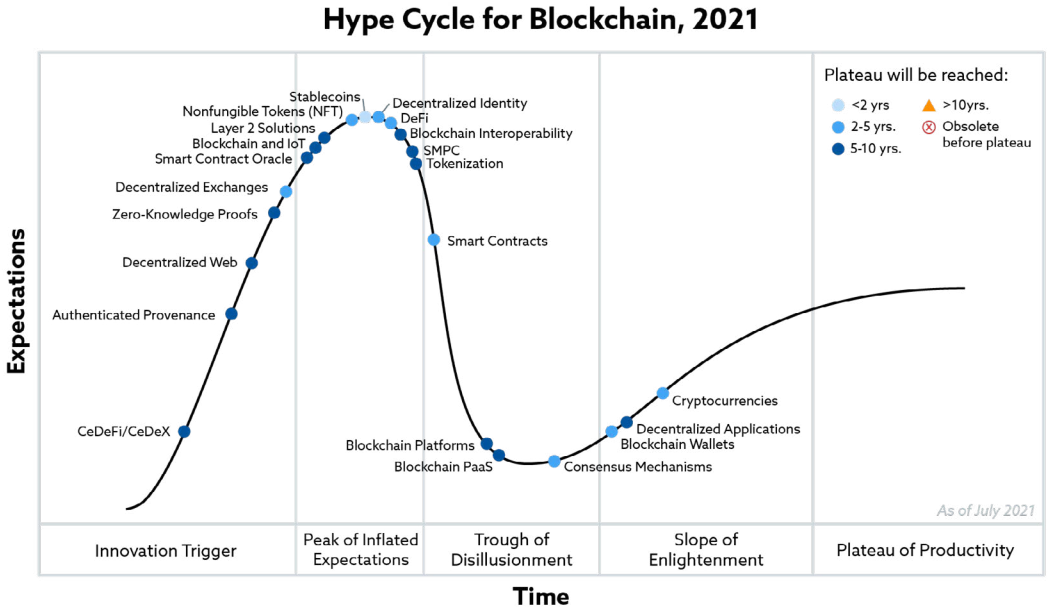

Figure 1 – Gartner's Hype Cycle for Blockchain Business, 2019

Blockchain business hype extends to the technology's security properties, such as immutability, tamper-evidence, and tamper-resistance. NIST notes that, "[t]here are countless news articles and videos describing the 'magic' of blockchain technology."[50] Replicating the hype around PKI, which was once regarded as a kind of "magic security dust" that cures all software security ills, blockchain technology is often treated as a "silver bullet."[51] Yet, Fabric services, such as Membership Service Provider (MSP) rely upon a hierarchical PKI model i.e., PKIX[52]. Section 8.4.1.2 discusses compliance defects in Public-Key Cryptography (PKC).[53]

44 Yaga, D., et al., 2018.

45 WEF, 2021.

46 Gartner PKI Hype Cycle: https://www.gartner.com/en/documents/349524/examining-the-pki-hype-cycle

47 Gartner IoT Hype Cycle: https://www.gartner.com/en/documents/3987602/hype-cycle-for-the-internet-of-things-2020

48 IAM Hype Cycle: https://www.gartner.com/en/documents/3987655/hype-cycle-for-identity-and-access-management-technologi

49 According to Gartner, virtually all "new" technologies go through an observable hype cycle. The phases of Gartner Hype Cycle are Innovation Trigger, Peak of Inflated Expectations, Trough of Disillusionment, Slope of Enlightenment and Plateau of Productivity. More information about the Hype Cycle for Blockchain business is available at https://blogs.gartner.com/avivah-litan/2021/07/14/hype-cycle-for-blockchain-2021-more-action-than-hype/

50 Yaga, D., et al., 2018.

51 Yaga, D., et al., 2018.

52 Hyperledger Fabric – Identity: https://hyperledger-fabric.readthedocs.io/en/release-2.2/identity/identity.html

53 Davis, D., *Compliance defects in Public Key Cryptography.* 1996, Cambridge, Massachusetts: MIT.

2.4 Hyperledger Greenhouse Structure and Fabric

The Hyperledger Architecture Working Group (WG) has developed a generalized reference architecture for permissioned blockchain networks. The Hyperledger Design Philosophy requires that all projects are modular, highly secure, interoperable, cryptocurrency-agnostic, and complete with Application Programming Interfaces (APIs).[54] As illustrated below, the Hyperledger Greenhouse Structure is a governing arrangement for incubating blockchain ideas.

Figure 2 – The Hyperledger Greenhouse Structure.

Our focus is on the "Highly Secure" aspect of the Hyperledger Design Philosophy because, "[s]ecurity and robustness are the keys to enable enterprise-class blockchains to evolve, and provide the critical infrastructure for next-generation business networks."[55]

2.4.1 Fabric

Initiated by Digital Asset and IBM, Fabric transitioned from the "Incubation" stage to the "Active" stage within the Hyperledger Project in March 2017. According to IBM, Fabric "offers a unique approach to consensus that enables performance at scale while also preserving the data privacy enterprises demand."[56] Fabric is a permissioned blockchain network.

54 Hyperledger, 2018b.
55 Hyperledger, 2018b.
56 Hyperledger Fabric: flexible blockchain framework: https://www.ibm.com/blockchain/hyperledger

3. Fabric Security and Risk Context

Several DLT projects are transitioning from PoC to production. For example, the World Economic Forum notes that, as of April 2021, DLT-enabled use cases, such as corporate bond issuances, private fund administration and distribution, securitization of blockchain originated loans, and private equity tokens issued on blockchain were live in production.[57]

To obtain Authorization to Operate (ATO) in critical sectors and achieve scale, DLT solutions must address technical risks and the concerns of business leaders. Thus, we use the business-focused and risk-based Sherwood Applied Business Security Architecture (SABSA) Architectural Framework to depict the business context in which a secure Fabric solution must be designed, built, and operated.

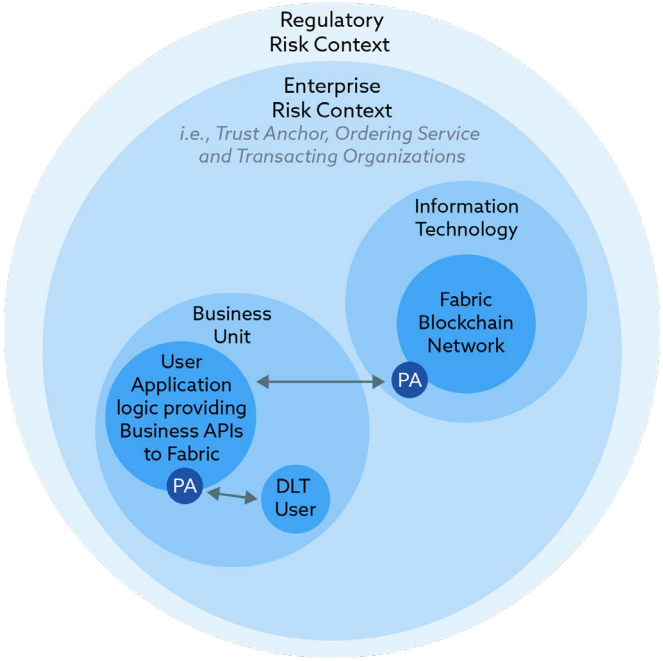

Figure 3 – Fabric Security and Risk Context.

As depicted above, applications rely upon Information Technology (IT) because blockchain takes existing, proven computer science and cryptography concepts and melds them together into a single solution.[58] In SABSA, a Policy Authority (PA) is an entity that owns a security domain and defines security and risk management policy within the domain. PAs dictate the rationale (why) for Fabric security. Thus, IT and business units are PAs for Fabric.

57 WEF, 2021.

58 Yaga, D., et al., 2018.

3.1 Regulatory Risk Context for Fabric

Critical infrastructure sectors are regulated because they host "key systems, services and functions whose disruption or destruction would have a debilitating impact on public health and safety, commerce, and national security, or any combination of these."[59] Fabric is used in critical sectors, such as government, healthcare, finance, etc.[60]

Typically, critical sectors enforce a fortress mentality to foil external attackers. For instance, national security systems implement stringent safeguards to stop lower classification domains from corrupting data in higher classification domains.[61] Yet by design, blockchain networks do not obey perimeter security controls because peer nodes are located throughout the business network, including within a competing organization's security environment and domain.[62] Therefore, to obtain ATO permission in critical sectors, blockchain must address the concerns of regulators and accreditors.[63] Let us consider the concerns of financial and energy regulators.

3.1.1 Concerns of Financial Regulators

Financial regulators are concerned about the misuse of blockchain-based services, notably cryptocurrencies. The European Central Bank (ECB) and the US Department of the Treasury have, for several years, condemned the use of cryptocurrencies for illicit financing and money laundering.[64] Announcing sanctions against SUEX for allegedly laundering cyber ransoms, the US Department of the Treasury stated that, "While most virtual currency activity is licit, virtual currencies can be used for illicit activity through peer-to-peer exchangers, mixers, and exchanges. This includes the facilitation of sanctions evasion, ransomware schemes, and other cybercrimes. Some virtual currency exchanges are exploited by malicious actors, but others, as is the case with SUEX, facilitate illicit activities for their own illicit gains."[65]

Similarly, the FinHub portal of the U.S. Securities and Exchange Commission (SEC) notes that, "In recent years, the SEC has encountered a number of issues relating to the blockchain and distributed ledger technology."[66] The SEC has taken enforcement actions against several organizations with a focus on unregistered initial coin offering of digital tokens (ICO).[67]

---

59 Wamala, F., *ITU National Cybersecurity Strategy Guide*. 2011, Geneva, Switzerland: International Telecommunication Union (ITU).

60 Hyperledger use cases: https://www.hyperledger.org/learn/case-studies

61 The Biba Integrity Model was designed to ensure that a subject cannot corrupt data in a level ranked higher than the subject's and to restrict corruption of data at a lower level than the subject's. https://www.sciencedirect.com/topics/computer-science/biba-model

62 Olson, T., 2018a.

63 ATO is a decision of a Designated Authorizing official: https://csrc.nist.gov/glossary/term/authorization_to_operate

64 US Treasury Secretary, Dr. Janet Yellen, said at her confirmation hearing before the US Senate Finance Committee on 01/19/2021 that, "Cryptocurrencies are a particular concern. I think many are used – at least in a transaction sense – mainly for illicit financing. And I think we really need to examine ways in which we can curtail their use and make sure that money laundering doesn't occur through those channels." Source: https://markets.businessinsider.com/currencies/news/bitcoin-price-cryptocurrency-should-be-curtailed-terrorism-concerns-yellen-2021-1-1029985692

65 Treasury Takes Robust Actions to Counter Ransomware: https://home.treasury.gov/news/press-releases/jy0364

66 Access the SEC's FinHub portal is at this URL: https://www.sec.gov/finhub

67 SEC orders Block.one to pay $24 Million Penalty for Unregistered ICO: https://www.sec.gov/news/press-release/2019-202

Regulators are also grappling with concepts, such as Decentralized finance (DeFi) and Non-Fungible Tokens (NFT). Furthermore, the mainstream adoption of cryptocurrencies, for instance bitcoin and Monero, and private digital money, such as Facebook's Diem could be highly problematic to central banks if the currencies were to suffer a systemic crisis.[68] To address this, in the United States, SEC. 80603 - Information Reporting for Brokers and Digital Assets of *The H.R. 3684 - The Infrastructure Investment and Jobs Act* brings cryptocurrencies more fully under the financial regulatory umbrella by clarifying reporting requirements for digital assets.[69]

3.1.2 Concerns of Energy Regulators

Blockchain has the potential to re-shape how energy is produced, bought, and sold.[70] For example, in 2018, Centrica, the owner of British Gas, and LO3 Energy[71] deployed blockchain technology as part of a Local Energy Market (LEM) trial.[72] Its smart metering supported blockchain applications, such as smart contracts, switching, settlement, and smart grids over the Internet of Things (IoT). The trial involved multi-party peer-to-peer trading across 200 business and residential participants using LO3's Exergy platform.

Regulators are concerned about disruptive or destructive events due to the energy sector's links to public health and safety, and national security. Yet, concerns about the disruption of the supply of energy to consumers have led some regulators to impose hosting restrictions on smart metering systems.[73] The requirements limit the use of systems, such as public cloud services whose pricing model assumes the ability to configure and operate platforms from anywhere.

3.2 Enterprise Risk Context for Fabric

Business blockchain networks must comply with regulatory requirements, such as data residency, anti-money laundering (AML) rules, and data privacy rules. Because regulation varies across jurisdictions, innovative DLT projects would require substantial financial and time commitment from business leaders to promote the idea to consortium members, regulators, and others with decision making powers. Business leadership will only commit to a project long-term if they have clarity around the business opportunity and risk of adoption. Therefore, blockchain network actors should consider using business approaches, such as the SABSA PESTELIM Analysis Framework,[74] American

68 Mark Carney, former Bank of England governor, warns of Crypto, stablecoins and NFTs risk and 'Uberisation' of money: https://www.fnlondon.com/articles/crypto-stablecoins-and-nfts-risk-uberisation-of-money-warns-mark-carney-20210629

69 H.R. 3684 - The Infrastructure Investment and Jobs Act: https://www.congress.gov/bill/117th-congress/house-bill/3684/text

70 Decentralized energy trading: https://theswitch.co.uk/energy/guides/technology/blockchain-energy

71 LO3 Energy's technology platform, Pando, pools local distributed energy resources: https://lo3energy.com/

72 Centrica and LO3 Energy blockchain technology Local Energy Market (LEM) trial: https://www.centrica.com/news/centrica-and-lo3-energy-deploy-blockchain-technology-part-local-energy-market-trial-cornwall

73 Part F, 8.15(c) of the Smart requires that Licensee, "ensure that all sites and systems that the Licensee relies upon to detect and prevent events that: (i) appear to be anomalous; and (ii) may have the potential to impact on the Supply of Energy to Energy Consumers, are configured, operated, and maintained within the United Kingdom." https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/484712/Annex_D_-_DCC_Licence_-_Consolidated_-_December_2015_-_Conclusions_and_L___.pdf

74 Political (P), Economic (E), Social (S), Technological (T), Environmental (E), Legislative (L), Industry (I) and Military (M).

Express' seven business risk areas,[75] and so forth to explain the adoption risk. This paper uses SABSA to model the risk context for a secure Fabric solution.[76] Other approaches could be used.

3.2.1 Business Drivers for Security

We use SABSA to model the risk context for a secure Fabric solution because it offers the capability to abstract business risk into Business Drivers for Security. Business Drivers for Security present the rationale (*the why*) for using a specific Fabric solution by linking it back to the business requirements. The Drivers focus on the things (*the what*) that really matter to an enterprise and, thus, must be protected, including business reputation and regulatory compliance. Table 1 below shows how to abstract the business requirements for financial services firm X into Business Drivers for Security. Whilst the list is widely applicable to regulated organizations, it is an example and not a prescriptive list of Business Drivers for Security.

Driver Number	Business Drivers
BD1	Protecting Firm X against cybersecurity incidents and other blockchain network attacks that could have a significant adverse impact on the firm's reputation. Could impact the firm's ability to continue to provide adequate services to its customers, or result in serious financial consequences to the wider financial sector or other firms.[77]
BD2	Protecting Firm X against cybersecurity incidents and other blockchain network attacks that could lead to the firm failing to satisfy one or more reporting requirements for regulatory and internal risk compliance. Could damage the firm's reputation for legal and regulatory compliance.
BD3	Ensuring that blockchain network assets are categorized and handled in accordance with the relevant Classification Scheme.
BD4	Ensuring that all users of the blockchain network are fully identified, authenticated, authorized, and their transactions fully auditable.
BD5	Preventing attacks against the blockchain network that could lead to losses through actual or attempted financial fraud and detecting attempted financial fraud.
BD6	Maintaining the privacy of personal data, and confidentiality of business information, that is stored, processed, or transmitted by Firm X's blockchain network/DLT platforms or its operators.

75 American Express: Seven Business Risks Every Business Should Plan For: https://www.americanexpress.com/en-us/business/trends-and-insights/articles/7-business-risks-every-business-should-plan-for/

76 TOGAF® and SABSA®, *TOGAF® and SABSA® Integration: How SABSA and TOGAF complement each other to create better architectures*. 2011, The Open Group and the SABSA Institute: San Francisco, CA and London, UK. p. 1-58.

77 BD1 is based on General Notification Requirement 2.1 in the Notifications Instrument 2014 – UK PRA Rulebook: https://www.prarulebook.co.uk/rulebook/Media/Get/805c0cfd-69d8-4c13-bbe8-fb1c2b64ffad/PRA_2014_20/pdf

Driver Number	Business Drivers
BD7	Ensuring that only blockchain network/DLT system users are granted authorization to access Firm X's blockchain data, in accordance with sound security principles like need-to-know and least privilege.
BD8	Implementing measures, proportionate to security risk, to protect data-in-transit, data-in-use and data-at-rest.

Table 1 – Business Drivers for Security.

Table 1 shows how blockchain/DLT risk and security considerations can constrain architectural options. For example, BD4 strongly encourages a permissioned blockchain because the pseudo-anonymity of permissionless networks can allow account creation without any identification or authorization. Although not the norm, permissionless blockchains can have Know Your Customer / Anti-Money Laundering (KYC/AML), and parties might agree to communicate with only certain other parties. BD6 would, typically, imply a permissioned and private blockchain, "[s]ince public blockchains can risk compromising a participant's privacy and confidentiality."[78] However, encryption and other advanced technologies like Zero Knowledge Proofs can protect private data stored on public blockchains.

3.2.2 Business Attribute Profile

The SABSA Business Attribute Profile (BAP) is a crucial requirements engineering technique because it links Business Drivers for Security and Business Attributes.[79] Business Attributes are abstractions of real business requirements for the Fabric solution. Business Attributes express which assets the business would like to protect, and the expected security outcomes, say customer privacy. Table 2 below combines Table 1 and Business Attributes As with Table 1, Table 2 is an example and not a prescriptive list of Business Drivers for Security.

78 Hyperledger, 2018b.

79 The SABSA Business Attributes Taxonomy eliminates the need for splitting requirements into Functional and Non-Functional categories. The Taxonomy is grouped into User, Management, Operational, Risk Management, Legal and Regulatory, Technical Strategy and Business Strategy Attributes. The "Risk Management Attributes" group of attributes mostly relate to the traditional 'security requirements' for protecting the business. The SABSA Business Attributes categories and definitions of individual Attributes can be obtained here: https://onlinelibrary.wiley.com/doi/pdf/10.1002/9780470476017.app1

Driver Number	Business Drivers	Attribute(s)
BD1	Protecting Firm X against cybersecurity incidents and other blockchain network attacks that could have a significant adverse impact on the firm's reputation. Could impact the firm's ability to continue to provide adequate services to its customers, or result in serious financial consequences to the wider financial sector or other firms.[80]	Available Competent Confident Protected Reputable
BD2	Protecting Firm X against cybersecurity incidents and other blockchain network attacks that could lead to the firm failing to satisfy one or more reporting requirements for regulatory and internal risk compliance. Could damage the firm's reputation for legal and regulatory compliance.	Available Compliant Regulated Reputable
BD3	Ensuring that blockchain network assets are categorized and handled in accordance with the relevant Classification Scheme.	Authorized Classified Confidential
BD4	Ensuring that all users of the blockchain network are fully identified, authenticated, authorized, and their transactions fully auditable.	Access-Controlled Auditable Authenticated Authorized Identified
BD5	Preventing attacks against the blockchain network that could lead to losses through actual or attempted financial fraud and detecting attempted financial fraud.	Detectable Risk-managed Trustworthy
BD6	Maintaining the privacy of personal data, and confidentiality of business information, that is stored, processed, or transmitted by Firm X's blockchain network/DLT platforms or its operators.	Confidential Private Protected

80 BD1 is based on General Notification Requirement 2.1 in the Notifications Instrument 2014 – UK PRA Rulebook: https://www.prarulebook.co.uk/rulebook/Media/Get/805c0cfd-69d8-4c13-bbe8-fb1c2b64ffad/PRA_2014_20/pdf

Driver Number	Business Drivers	Attribute(s)
BD7	Ensuring that only blockchain network/DLT system users are granted authorization to access Firm X's blockchain data, in accordance with sound security principles like need-to-know and least privilege.	Authorized Duty Segregated
BD8	Implementing measures, proportionate to security risk, to protect data-in-transit, data-in-use and data-at-rest.	Authenticated Confidential Integrity-Assured Non-Repudiable Private Protected

Table 2 – Business Attribute Profile (BAP).

Definitions of Business Attributes can be aligned with internal or industry best practices to maintain focus on an enterprise's expected security outcomes. For example, the "Access-Controlled" Attribute aligns with the definition of Access Control in NIST SP 800-53 Revision 5.[81] Similarly, A.8.2.1 – ISO/IEC 27001 offers a good definition for the "Classified" attribute.

81 NIST, *NIST SP 800-30 Rev. 1 - Guide for Conducting Risk Assessments*. 2012, National Institute of Standards and Technology (NIST) Gaithersburg, Maryland, USA.

4. Fabric Solution Overview

Before committing to an architecture and writing code, we recommend that you develop an understanding of the full scope of the Fabric solution. Therefore, this Section deals with the who aspects of the Fabric solution. From a SABSA perspective, *who* deals with the organizational aspects of business security. A System Context Diagram can help plot the *who* aspects.

4.1 System Context Diagram

We recommend using a formal Architectural Framework, such as TOGAF® to develop your Fabric System Context diagram. The diagram should represent the entire system (think: ecosystem) as a single object or process. The diagram should also identify and describe all the information and control flows that cross the system boundary. Skipping this step could lead to an incomplete solution. We derived most elements below from the Hyperledger Fabric Glossary.[82]

Figure 4 – Fabric System Context Diagram.

82 Hyperledger Fabric Glossary: https://fabric-docs-test.readthedocs.io/en/latest/glossary/

The elements include Fabric entities, participants, network entities, member management, and so forth as you can see. Additionally, the diagram covers enterprise services, such as security services and data storing services. The actual entities will depend on your use case.

4.2 Fabric Key Users and Interfaces

The elements in the System Context Diagram must be described to ensure that the blockchain team, business leaders and technology teams (e.g., Enterprise Architecture) have a shared view of risk and opportunity. Below is an example of how to describe elements by type and role.

Type	User/System	Notes
User / Participant	Solution User	End users initiate transactions on a chain network through solutions provider applications. End users are agnostic about the details of chain networks.
User / Participant	Solution Provider	Acting in a Chain Transactor[83] role, a Solution Provider is an organization that develops mobile and/or browser-based applications for end (solution) users to access chain networks. Some Solution Providers may also be Network Owners.
User / Participant	Network Proprietor	Acting in Chain Transactor and Chain Validator[84] roles on the chain network, the Proprietor sets up and defines the purpose of a chain network.
User / Participant	Network Owner	Owners can validate transactions on a chain network. The proprietor (who then becomes an owner) invites partners to co-own the network by assigning them Validating Nodes. Owners can act in Chain Transactor and Chain Validator roles.
User / Participant	Network Member	Members are able to add users to the network but cannot validate transactions. Members act in Chain Transactor and Chain Member[85] roles.
User / Participant	Network Users	Unlike network owners and members, Network Users (also known as Solution Users) do not own nodes but act in a Chain Transactor role through an entry point offered by a member or an owner node.

83 Chain Transactors are entities that have permission to create transactions and query network data.

84 Chain Validators are entities that own a stake of a chain network. Each Chain Validator has a voice in deciding whether a transaction is valid, therefore chain validators can interrogate all transactions sent to their chain.

85 Chain Members are entities that do not participate in the validation process of a blockchain network but help to maintain the integrity of a network. Unlike Chain transactors, Chain Members maintain a local copy of the ledger.

Type	User/System	Notes
User / Participant	Network Auditors	Acting in the Chain Auditor[86] role, Network Auditors are individuals or organizations with the permission to interrogate transactions.
System / Network Management	Member Management	Because Fabric is a permissioned network, blockchain participants must be registered. Find more information about this element in *Section 8 – Fabric Reference Security Architecture*.
System / Network Entity	Application Backend	The Backend supports applications (mobile/web) by managing users and registering them with the membership service. Find more details in *Section 8 – Fabric Reference Security Architecture*.
System / Network Entity	Non-Validating Node (Peer)	This node is owned by the Solution Provider or Network Auditor. Find more details in *Section 8 – Fabric Reference Security Architecture*.
System / Network Entity	Validating Node (Peer)	This node is owned by Network Proprietor / Solution Provider (if they belong to the same entity). Find more details in *Section 8 – Fabric Reference Security Architecture*.
System / Network Entity	Membership Service	A Membership Service is a component that defines the rules that govern the valid identities for their organization. Find more details in *Section 8 – Fabric Reference Security Architecture*.
System	Cryptography Services	Fabric uses cryptographic primitives, such as cryptographic hash functions, digital signatures, asymmetric-key cryptography. Find more information about this element in Section 8 – Fabric Reference Security Architecture.
System / Hyperledger Fabric Entities	Chaincode / Smart Contract	A Chaincode handles business logic agreeable to members of the network. Find more details about this element in *Section 8 – Fabric Reference Security Architecture*.
System / Hyperledger Fabric Entities	Ledger	A ledger stores information about business objects. Find more details in *Section 8 – Fabric Reference Security Architecture*.

86 Chain Auditors are entities with the permission to interrogate transactions.

Type	User/System	Notes
System / Hyperledger Fabric Entities	Node	Nodes are the communication entities of the blockchain. Find more details in *Section 8 – Fabric Reference Security Architecture*.
System	Enterprise Security Services	Chain networks interact with security services that protect the network. Find more details in *Section 8 – Fabric Reference Security Architecture*.
System	Enterprise Resource Planning (ERP) Systems	ERPs are critical systems of record (SoR) that run core business processes, such as accounting, procurement, supply chain operations, etc., that create and maintain customer data in enterprise data stores and blockchain ledgers. Find more information about this element in *Section 8 – Fabric Reference Security Architecture*.
System	Enterprise Data Stores	It should be possible to extract blockchain ledger data for further analysis by the enterprise data store. Find more details in *Section 8 – Fabric Reference Security Architecture*.

Table 3 – Key Users and Interfaces.

5. Fabric Threat Assessment

National security concerns have highlighted the need to identify the threat sources, analyze, and estimate the impact of the technical security risks applicable to blockchain networks. According to The Wall Street Journal, senior US Government officials regard ransomware, "as an urgent national-security threat."[87] As noted earlier, ransomware attacks have exploited the pseudo-anonymity of permissionless blockchain networks, such as Bitcoin. In May 2021, the US government issued a cybersecurity Executive Order just after a ransomware attack on Colonial Pipeline paralyzed the company's operations and caused fuel shortage on the East Coast.[88] Hence, cryptocurrency's role in ransomware payments has shone an undesirable spotlight on blockchain technology. Ironically, if designed properly, DLT platforms could eliminate, or reduce, central points of failure and, thus, improve the resilience of critical infrastructure against attacks.

5.1 Technical Risk Assessment Approach

Some of the Fabric risk assessments that we have seen regard hackers and criminal groups as the most potent Fabric threat actors. This view is incomplete for two reasons. First, given the increased use of Fabric in critical sectors including government,[89] healthcare,[90] finance,[91] and so on, accreditors would require blockchain networks to have security controls that can deter, detect, resist, and defend against the most advanced threats. State-sponsored groups are the most powerful threat actors due to their ability to launch complex attacks and influence other actors. Second, the Colonial Pipeline attack showed that adversaries can attack blockchain networks that deliver or support critical services either directly or indirectly, for fear of attribution and retribution, to achieve national security or societal disorder objectives. Therefore, our approach combines aspects of NIST SP 800-30 Rev. 1,[92] the UK technical risk assessment approach[93] and the STRIDE Model[94] to depict the full complexity of the blockchain threat landscape. In common with the UK approach, NIST SP 800-30 recognizes the concept of a Threat Source.

87 FBI gets Ransom Money Back: https://www.wsj.com/articles/how-the-fbi-got-colonial-pipelines-ransom-money-back-11623403981

88 Executive Order on Improving the Nation's Cybersecurity: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

89 Dubai's Digital Silk Road uses Hyperledger Fabric: https://www.hyperledger.org/learn/publications/avanza-case-study

90 Pharmaceutical Supply Chain: https://www.hyperledger.org/learn/publications/ledgerdomain-case-study

91 Mindtree revolutionized loyalty platforms with Fabric: https://www.hyperledger.org/learn/case-studies/mindtree-case-study

92 NIST, 2012.

93 HMG Information Assurance (IA) Standard Number 1 & 2 was produced to be consistent with and to support the application of the ISO/IEC 27000 series, as good practice for the risk management of information systems. Whilst no longer mandated, when used properly, it remains a valuable method for assessing and managing risk under the UK Government Security Classifications Policy: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/286667/FAQ2_-_Managing_Information_Risk_at_OFFICIAL_v2_-_March_2014.pdf

94 Brook, J.-M.C., et al., 2019.

5.2 Threat Sources

Intel's Threat Agent Risk Assessment (TARA)[95] provides a Threat Agent Library[96] and a Methods and Objectives Library that is used in threat assessments.[97] Given that DLT-enabled ransomware attacks are impacting critical sectors such as public health and safety[98] and posing an urgent national security threat, we split the TARA list into Threat Sources and Threat Agents to offer a wider set of credible threat scenarios. We regard a Threat Source as an entity that desires to breach an information or physical asset's security controls[99] to achieve objectives, such as espionage, financial gain, intellectual property, and theft. Similarly, NIST describes Adversarial Threat Sources as, "[i]ndividuals, groups, organizations, or states that seek to exploit the organization's dependence on cyber resources."[100] Threat Sources include persons with legitimate access that may accidentally compromise confidentiality, integrity, and availability.

5.2.1 Threat Source Capability and Priority Assessment

Risk analysts require a mechanism for assessing potential Threat Sources from Capability and Priority perspectives. We used Table D-3 in NIST SP 800-30 Rev. 1 to generate Capability and Tables D-4 and D-5 from the same document to generate Priority assessment scales. Capability assesses the potential of the Threat Source to exploit vulnerabilities and breach the security of a Fabric network. Priority or motivation measures both the adversary's intent (Table D-4) and the targeting (Table D-5) of a specific blockchain network. Table 4 below shows how to combine Capability and Priority to estimate the Threat Level associated with a Threat Source. Risk analysts should feel free to use other appropriate Threat Assessment terminology.

95 Originally developed by Intel Corporation, TARA is a threat-based methodology to help identify, assess, prioritize, and control cybersecurity risks: https://cio-wiki.org/wiki/Threat_Agent_Risk_Assessment_(TARA)

96 The agents identified in the TARA paper are competitor, data miner, radical activist, cyber vandal, sensationalist, civil activist, terrorist, anarchist, irrational individual, government cyber warrior, organized criminal, corrupt government official, legal adversary, internal spy, government spy, thief, vendor, reckless employee, untrained employee, information partner and disgruntled employee.

97 Shostack, A., *Threat Modeling: Designing for Security*. 2014, Boulevard, Indianapolis, Indiana, USA: John Wiley & Sons, Inc.

98 Irish health service hit by 'very sophisticated' ransomware attack: https://www.reuters.com/technology/irish-health-service-hit-by-ransomware-attack-vaccine-rollout-unaffected-2021-05-14/

99 Wamala, F., 2011.

100 NIST, 2012.

		Capability Level				
		0 Very Low	2 Low	5 Moderate	8 High	10 Very High
Priority	0 Very Low	Negligible	Negligible	Low	Low	Moderate
	2 Low	Negligible	Negligible	Low	Moderate	Substantial
	5 Moderate	Negligible	Low	Moderate	Substantial	Severe
	8 High	Low	Low	Moderate	Severe	Severe
	10 Very High	Low	Moderate	Substantial	Severe	Critical

Table 4 – Threat Level Assessment Scale.

5.2.2 Threat Source Types

As noted in *Section 5.1 – Technical Risk Assessment Approach*, critical sectors increasingly use Fabric solutions. The relevant Threat Sources for Fabric are nation-state sponsored groups, criminal organizations, terrorist organizations, media and investigative journalists, activist and protest groups, hacktivist and cyber protest groups, and security researchers. We should note that threats from nation-state sponsored groups are difficult to address due to jurisdictional uncertainty, attribution issues, and the risk of escalation of force between countries. Similarly, criminal organizations are challenging to address, especially if they are acting as proxies for states where governments tolerate their activities. For example, despite the displeasure of the US government, a few countries continue to harbor criminal networks that launch ransomware attacks worldwide.

5.2.2.1 Modeling Fabric Threat Sources

In the table below we show how one could model the Fabric Threat Sources. Using *Table 4 – Threat Level Assessment Scale*, we focus on the Threat Sources that can launch major attacks on Fabric networks: nation-state sponsored groups and criminal organizations.

Source Name	Description	Property	Capability	Priority	Threat Level
Nation-State Sponsored Groups	Fabric blockchain networks are targets for highly capable Nation-State Sponsored Groups seeking to undermine, severely impede, or destroy critical infrastructure sectors for an intelligence advantage.[101] For instance, entry DLTI-2020-01-08-1 on the CSA DLT Security Incidents is for a data theft attack by the Lazarus Group Advanced Persistent Threat (APT) which is linked to the North Korean government.[102]	C	10	5	Severe
		I	10	10	Critical
		A	10	10	Critical
Criminal Organizations	Criminal organizations attack Fabric blockchain networks primarily for financial gain. criminal organizations may use blockchain networks to access personal data to perpetrate fraud, extort companies, steal private keys, and thus take over digital assets. Most recently, criminal organizations such as DarkSide have used digital wallets of DLT platforms, such as Bitcoin, to transfer ransom payments.[103]	C	8	10	Severe
		I	8	10	Severe
		A	5	10	Substantial

Table 5 – Sample Blockchain Network Threat Sources.

5.2.2.2 Nation-State Sponsored Groups

As depicted in Table 5, we assign nation-state sponsored groups a Very High (10) capability score to attack a Fabric blockchain's confidentiality, integrity, and availability because the Groups have the resources to execute sophisticated attacks including cryptographic ones that could undermine the security of Fabric solutions. The Groups only have a Moderate (5) score for confidentiality, because typically, blockchains record transactions are in a shared ledger within a community.[104] However, permissioned blockchain networks may or may not reveal blockchain data publicly, and private transactions deliver data only to selected nodes. The Groups have Very High (10) scores for integrity and availability as states can dedicate resources to execute the most sophisticated attacks.

101 Microsoft sounded an alarm about state-sSponsored cybersecurity threats after a Russian government-backed attack that exploited flaws in SolarWinds: https://www.investors.com/news/technology/microsoft-stock-ces-2021-keynote-cybersecurity-threats/

102 Lazarus Group is a threat group that has been attributed to the North Korean government: https://attack.mitre.org/groups/G0032/

103 The US Cybersecurity and Infrastructure Security Agency (CISA)'s Alert (AA21-131A) provides good information on DarkSide and best practices for preventing business disruption from ransomware attacks: https://us-cert.cisa.gov/ncas/alerts/aa21-131a

104 Yaga, D., et al., 2018.

5.2.2.3 Criminal Organizations

As depicted in Table 5, we assign criminal organizations a High (8) capability score to attack a Fabric's confidentiality and availability. In addition to the ability to execute complex attacks, the organizations can bribe, coerce, and blackmail targets as shown by ransomware attacks against Colonial Pipeline, JBS, AXA,[105] and Toshiba.[106] The organizations have only a Moderate (5) Capability to imperil a Fabric network's availability because, by design, blockchains are distributed, heterogeneous and can be composed of geographically diverse nodes.[107] We assign such organizations Very High (10) priority scores for attacking the confidentiality, integrity, and availability of a Fabric blockchain for financial gain.

5.3 Threat Actors

A Threat Actor is an entity that actually performs the attack, or in the case of accidents, will exploit the accident.[108] The worst-case motivation of a Threat Source should be assumed if the attack is influenced by another party. For example, the FBI seized 63.7 bitcoins (about $2.3 million), as part of the ransom payment to DarkSide by Colonial Pipeline, by gaining access to a private key for a Bitcoin address. Whilst not disclosing methods and techniques, the FBI possibly gained access to the private key for DarkSide's Bitcoin address by influencing the threat actors.[109] From a security (rather than moral or legal) perspective, the private key to DarkSide's bitcoin wallet was meant to remain secret. Yet, the FBI had ample leverage to obtain disclosure of the private key. An entity can be both a Threat Source and a Threat Actor.

5.3.1 Threat Actor Capability and Priority

As depicted in Table 4, threat actor capability ranges from Very Low (0) to Very High (10). Similarly, priority or motivation ranges from Very Low (0) to Very High (10). As noted above, for Fabric deployed in critical sectors, we assume that some of the potential threat actors would require a security clearance, which typically serves to deter some of the attacks. We should note that Ransomware-as-a-Service (RaaS) offerings can rapidly change threat actor capability estimates. Hence, some states oppose ransomware payments because threat actors use the funds to develop even more sophisticated variants of cyber-attacks.

105 Ransomware Attack Reported at Insurance Giant AXA: https://www.cpomagazine.com/cyber-security/ransomware-attack-reported-at-insurance-giant-axa-one-week-after-it-changes-cyber-insurance-policies-in-france/

106 Toshiba unit hacked by DarkSide: https://www.reuters.com/business/autos-transportation/toshibas-european-business-hit-by-cyberattack-source-2021-05-14/

107 Yaga, D., et al., 2018.

108 Wamala, F., *2011.*

109 Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside: https://www.justice.gov/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside

5.3.2 Threat Actor Types/Categories

The Threat Actor types in this paper are similar to those presented in *Table D-2: Taxonomy of Threat Sources* of NIST SP 800-30 Rev.1.[110] Adversarial sub-categories are individual (outsider, insider, trusted insider, and privileged insider), group (ad-hoc and established), organization (competitor, supplier, partner, and customer) and nation-state. User and privileged user/administrator are in the Accidental sub-category. In Table 6 below are the typical Threat Actor Types for UK national infrastructure sectors, such as the Government sector. Other categories are equally valid.

Threat Actor Type/ Category	Description
System and Service Users	Entities, such as Transacting Organizations, Ordering Services, etc., that have authorized logical access to a blockchain network and any services it provides. The group could include privileged users, ordinary users, service consumers, and shared service subscribers.
Direct Connections	The group would have business or network connections to facilitate the exchange of information, or the provisioning and managing of the services delivered by the blockchain network. The Threat Actors could include information exchange partners and service providers.
Indirect Connections	This group of Threat Actors represents entities that are not connected to the blockchain network domain for business purposes. Indirectly connected parties, such as cyber attackers, would have connections to partners directly connected to the blockchain network for business purposes, or to those that share services and infrastructure with the blockchain network participants.
Supply Chain	This is a group of threat actors that have access to hardware, software, and services, such as Domain Name System (DNS) before the blockchain network is commissioned, or those that are responsible for the implementation, configuration, or management of the blockchain network components, such as wallets. It includes suppliers and handlers of blockchain hardware and software.
Physical Present	This group of threat actors represents entities that could attack the blockchain network by being in the physical locality, either through authorized or unauthorized access or in the general physical proximity. This group could include privileged users, ordinary users, and bystanders.

Table 6 – Sample Blockchain Network Threat Actor Types.

110 NIST, 2012.

The Threat Actor Types in the table above are illustrative only. Therefore, Blockchain Network Proprietors and Network Owners should feel free to use the Threat Actor Types provided by internal risk teams, regulators, and national security agencies if the list above is not suitable.

5.3.3 Threat Actor Metrics

The table below depicts how to summarize the threat that a Privileged User Threat Actor could pose to the Runtime Security Domain of the Reference Security Architecture (Figure 6). Using the Sub-Quantitative Values 0-10 in Table 4, we depict the Threat Actor's native Capability and Priority to attack the domain, and the Enhanced Capacity and Priority due to the influence of Threat Sources.

Domain	Example: Blockchain Runtime Security Domain										
Threat Actor Group Name	Security Clearance	Property	Native Capability	Native Priority	Native Threat Level	Dominant Influencing Threat Source	Enhanced Capability	Enhanced Priority	Enhanced Threat Level	Final Threat Level
Privileged User	Security Clearance Level	C	8	2	Moderate	Media and Investigative Journalists	10	8	Severe	Severe
		I	8	5	Substantial	Nation-State Sponsored Groups	10	10	Critical	Critical
		A	5	5	Moderate	Hacktivist and Cyber Protest Groups	10	8	Severe	Severe
		Accidental Compromise								Moderate

Table 7 – Privileged Threat Actor Metrics.

5.3.4 Security Clearance

Section 3 – Fabric Security and Risk Context stressed the importance of understanding the business context in which a secure DLT solution must be designed, built, and operated. Therefore, security clearance is part of Table 7 above because security vetting is a typical requirement for staff and contractors that deliver infrastructure in critical sectors. For example, according to Tim Olson, "a Hyperledger Fabric (HLF) blockchain network hosted on a high assurance platform is well suited for secure information exchanges across network security domains — for example, exchanging unclassified information between a classified and unclassified network."[111] Staff supporting such a solution would undergo security vetting to obtain and maintain the requisite security clearances. Most countries require deeper security vetting to access SECRET and above classifications. For example, the United Kingdom requires that Privileged Users accessing assets that are classified as SECRET or TOP SECRET require a national security clearance, such as Security Check (SC) and Developed Vetting (DV).[112]

111 Olson, T., *2018b.*

112 UK National security vetting: clearance levels: https://www.gov.uk/government/publications/united-kingdom-security-vetting-clearance-levels/national-security-vetting-clearance-levels#security-check-sc

6. Risk Assessment

The NIST Cybersecurity Framework cautions against taking a one-size-fits-all approach to managing cybersecurity risk for critical infrastructure because every organization has unique risks: different threats, different vulnerabilities, different risk tolerances.[113] Similarly, NISTIR 8202 counsels that, "The use of blockchain technology does not remove inherent cybersecurity risks that require thoughtful and proactive risk management."[114] Hence, before choosing a technical solution, we must use risk assessment to identify, assess, manage, and report the threats that are most consequential to the secure operation of a Fabric blockchain network. As depicted in the table below, the risk level can be evaluated by combining the assessed threat level and the business impact level.

		Threat Level					
		Negligible	Low	Moderate	Substantial	Severe	Critical
Business Impact Level (BIL)	BIL0	Very Low	Very Low	Very Low	Very Low	Very Low	Very Low
	BIL1	Very Low	Very Low	Very Low	Low	Low	Low
	BIL2	Very Low	Low	Low	Medium	Medium	Medium
	BIL3	Very Low	Low	Medium	Medium	Medium-High	Medium-High
	BIL4	Low	Medium	Medium	Medium-High	High	High
	BIL5	Medium	Medium	Medium-High	High	High	Very High
	BIL6	Medium	Medium	Medium-High	High	Very High	Very High

Table 8 – Risk Levels.

6.1 Compromise Methods

Fabric blockchain networks and participating organizations require protection from cyber threats that will only increase as Threat Actors and influencing Threat Sources, "develop more knowledge about blockchain networks and their vulnerabilities."[115] Several models can be used to model blockchain security risks. For instance, the Asset-Based Cryptocurrency-focused threat modeling framework

113 Barrett, M.P., *Framework for Improving Critical Infrastructure Cybersecurity*. 2018, National Institute of Standards and Technology (NIST): Gaithersburg, Maryland, USA.

114 Yaga, D., et al., 2018.

115 Yaga, D., et al., 2018.

uses collusion matrices to identify security risks.[116] We use the STRIDE Threat Model for two reasons. Firstly, using STRIDE to analyze compromise methods maintains consistency with other CSA documents.[117] Secondly, the Model enables us to consider a broad range of methods that a Threat Actor may use to exploit Fabric vulnerabilities.

Threat	Property Violated	Threat Definition
Spoofing	Authentication	A malicious entity pretends to be or impersonates a legitimate Solution User.
Tampering	Integrity	Modification or corruption of data on a Fabric blockchain network, for example altering a message during transmission, inserting invalid or repeated events, etc.
Repudiation	Non-Repudiation	A Solution User, Network User, Network Member, etc., denying having sent a message.
Information Disclosure	Confidentiality	The deliberate or accidental exposure of confidential transaction (i.e., a transaction with its payload cryptographically hidden) or confidential Chaincode transaction (i.e., a transaction with encrypted payload) to stakeholders or validators that are not authorized to interrogate its content or decrypt it.
Denial of Service	Availability	Malicious or accidental actions that absorb Fabric blockchain network resources making it difficult or impossible to provide normal service. For instance, according to NIST, "Denial of service attacks can be conducted on the blockchain platform or on the smart contract implemented on the platform."[118]
Elevation of Privileges	Authorization	Fabric Network Users, Network Members, etc., elevating their access privileges to do something they are not authorized to do.

Table 9 – Potential Threats against a Fabric Blockchain Network.

In Table above, we adjust STRIDE threat definitions to reflect Fabric blockchain's attributes.[119]

116 Almashaqbeh, G., A. Bishop, and J. Cappos. *ABC: A Cryptocurrency-Focused Threat Modeling Framework,* in IEEE INFOCOM 2019 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), 29 April-2 May 2019. 2019. Paris, France: IEEE.

117 Brook, J.-M.C., et al., *2019.*

118 Yaga, D., et al., 2018.

119 Shostack, A., 2014.

6.1.1 Example – Privileged User Compromise Methods

We present the compromise method in broad terms, such as Changes Configuration. In practice, the Changes Configuration compromise method could encompass several types of attack. The risk analyst or security architect would require detailed information about the Fabric network architecture, services and security controls deployed to specify the actual attack in the technical risk assessment. For example, the Changes Configuration compromise method could cover specific attacks on the configuration of assets, such as nodes, network infrastructure, application platform, etc. Below are some of the compromise methods that a Privileged User Threat Actor may use to impact the confidentiality, integrity, and availability of Runtime assets.

Domain	Example: Fabric Trust Anchor Runtime/Applications Domain
Threat Actor Group	Privileged User e.g., Chain Member Role[64]
Influencing Threat Sources	**Confidentiality [C]** – Media and Investigative Journalists **Integrity [I]** – Nation-State Sponsored Groups **Availability [A]** – Hacktivist and Cyper Protest Groups

Property	Score	Compromise Method	Threat Level	Risk Level
C	3	Accidentally Releases information from the Trust Anchor Runtime/ Applications Domain compromising the confidentiality of Business User data.	Moderate	Medium
I	5	Accidentally Disrupts the Trust Anchor Runtime/ Applications Domain compromising its integrity leading to attacks, such as the repudiation of transactions.	Moderate	Medium-High
A	5	Accidentally Disrupts in the Trust Anchor Runtime/ Applications Domain causing a denial of service.	Moderate	Medium-High
C	3	Deliberately Discloses information from the Trust Anchor Runtime/ Applications Domain.	Substantial	Medium
I	5	Deliberately Tampers the Trust Anchor Runtime/ Applications Domain compromising its integrity leading to attacks, such as the repudiation of transactions.	Severe	High
A	5	Deliberately causes a Denial of Service the Trust Anchor Runtime/ Applications Domain.	Moderate	Medium
C	3	Changes the Configuration of the Trust Anchor Runtime/ Applications Domain compromising its confidentiality and leading to information disclosure.	Substantial	Medium
I	5	Changes the Configuration of the Trust Anchor Runtime/ Applications Domain compromising its integrity and attacks, such as the repudiation of transactions.	Severe	High
A	5	Changes the Configuration of the Trust Anchor Runtime/ Applications Domain compromising its availability and causing a business disruption as a Denial of Service.	Moderate	Medium-High

Table 10 – Privileged User Risk Assessment.

The example above assumes that Privileged Users have limited capacity to impact the availability of a blockchain network due to the trust, security, and reliability benefits that a distributed ledger has over ledgers with centralized ownership. In addition, the Privileged User is assigned relatively low integrity scores because, unlike the centrally owned ledgers that might be incomplete, a blockchain network ensures that all transactions are valid and confirms completeness by holding all accepted transactions within its ledger.

7. Risk Mitigation

NIST SP 800-30 Rev. 1 describes risk mitigation as a process of prioritizing, evaluating, and implementing the appropriate risk-reducing controls/countermeasures recommended from the risk management process.[120] Risk mitigation is a subset of risk response: accepting, avoiding, mitigating, sharing, or transferring risk. Since Fabric is an extensible blockchain platform that could be tailored to different use cases and trust models, the Logical Security Services and Reference Security Architecture support a security outcome-based risk mitigation approach.

7.1 Risk Mitigation Approach

Sections 3-5 aim to demonstrate how to develop a Fabric blockchain network that can obtain ATO in critical sectors. *Section 3 – Fabric Security and Risk Context* depicts the business context in which a secure Fabric solution must be designed, built, and operated. Ignoring the business context, particularly, the concerns of regulators could lead to the denial of ATO and/or limit the scale of the blockchain. Furthermore, before diving into coding and/or configuration, we showed how one could align the Fabric solution with the mission/business requirements and risk tolerance of the organization. Sections 3-5 support the SABSA Two-Way Traceability approach that offers both a completeness check and justifies expenditure of Fabric blockchain security measures. Therefore, the Logical Security Services, and their related Security Mechanisms, flow directly from the preceding sections.

7.2 Logical Security Services

ISO 7498-2[121] describes a security mechanism as a type of technology or process that can deliver a security service.[122] In turn, a security service is a capability for safeguarding the security of information in an Open Systems Interconnection (OSI) network architecture context. SABSA has extended the definition to include any enterprise architectural context. Whilst a security service is a logical building block, a security mechanism is a physical equivalent. For example, encryption is a Security Mechanism for delivering confidentiality, which is a logical security service. Logical Security Services act on information whilst security mechanisms act on data.

7.2.1 Logical Security Services, Fabric and Enterprise Security Mechanisms

Below is a Logical Domain Model populated with Logical Security Services. Based on a SABSA at Work™ paper,[123] it shows the Security Mechanisms that deliver the Logical Security Services. For instance, the Fabric Certificate Authority (CA) delivers the Confidentiality Service. The Model is version and product agnostic and could be applied to other permissioned blockchain networks.

120 NIST, 2012.

121 ISO 7498-2:1989 – Information processing systems — Open Systems Interconnection — Basic Reference Model — Part 2: Security Architecture. A copy can be purchased at: https://www.iso.org/standard/14256.html

122 SABSA® and TOGAF®, *TSI R100 - Security Services Catalogue.* 2018, Security Services Project Working Group, Jointly Sponsored by The SABSA Institute and The Open Group: London, UK and San Francisco, CA. p. 1-36.

123 Laurie, R., *SW101 – SABSA Applied to Top-Secret Classified Information, in SABSA at Work™.* 2018, The SABSA Institute C.I.C: East Sussex, UK. p. 13.

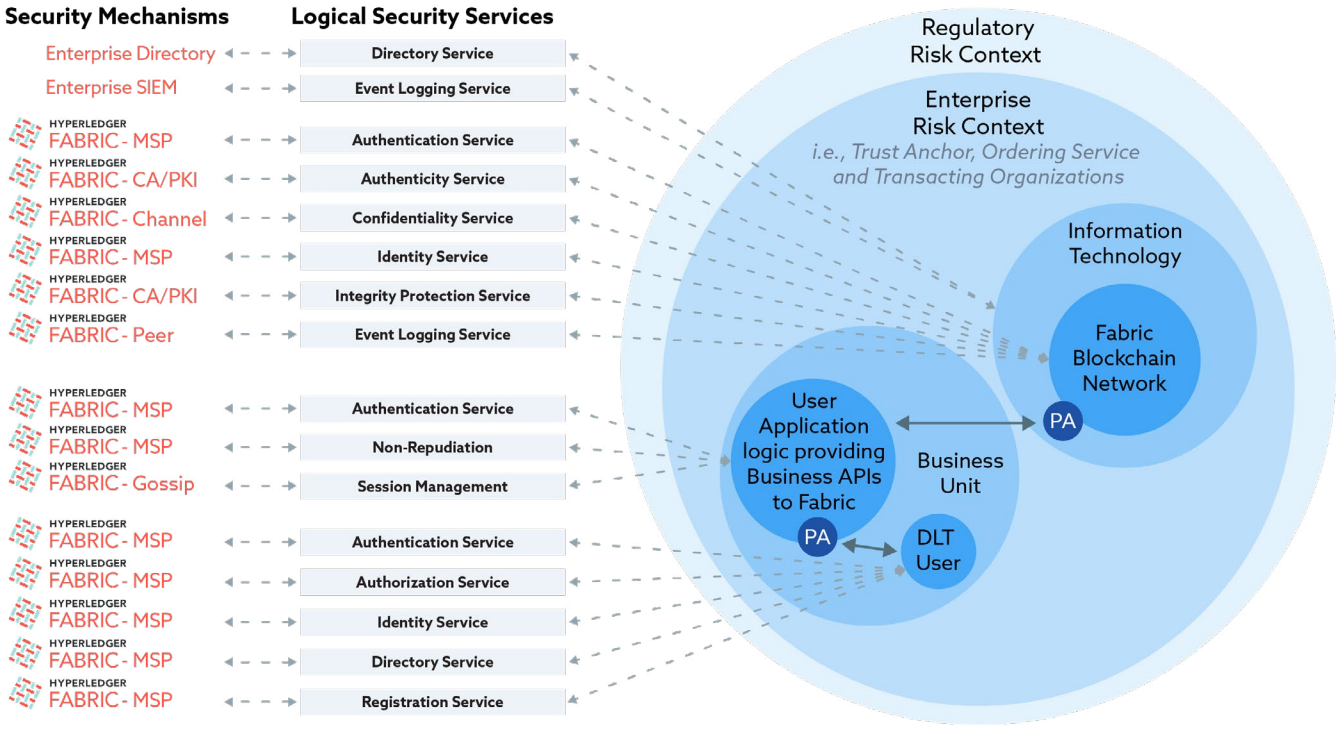

Figure 5 – SABSA Logical Domain Model Populated with Logical Security Services and Fabric and Enterprise Security Mechanisms.

7.2.2 Overview of Logical Security Services

Most of the Fabric Logical Security Services we depict in Figure 5 are either based on cryptography or reliant upon it. These include the *Confidentiality Service, Authenticity Service, Integrity Protection Service, Identity Service* and *Authorization Service*. In terms of the *Identity Service*, we see later that the Membership Service Provider (MSP) in Fabric uses X.509 certificates as identities. In addition, whilst not a cryptographic service, *Event Logging* benefits from cryptography-enabled integrity-protection and non-repudiation services. Unfortunately, as we will discuss in *Section 8.4.1 – Cryptography Services*, cryptography is one of the most widely misunderstood topics in security. Indeed, it is common to focus on the security benefits of cryptographic mechanisms rather than the trade-offs or challenges, such as key management, cost, performance, and non-compliance with privacy laws due to the immutability property.[124]

124 The Enhanced Distributed Ledger Technology project has designed and implemented a new form of distributed ledger technology (DLT), known as a data block matrix, which provides the integrity assurance of blockchain but allows for controlled revision or deletion of data: https://csrc.nist.gov/projects/enhanced-distributed-ledger-technology

8. Fabric Reference Security Architecture

You will only gain a full return on investment from Fabric if the solution interacts securely with other networked devices and systems. Therefore, we provide a Reference Security Architecture to serve as a template that security architects could consider during the design of Fabric solutions in critical infrastructure sectors. The pattern shows how to embed a Fabric blockchain solution within a corporate computer network constrained by requirements, such as PCI DSS network segmentation or security accreditation requirements for national security systems. The Reference Security Architecture covers the Physical, Component and Management Architecture layers of the SABSA Matrix.[125] Therefore, we suggest possible on-premises and cloud locations for the Security Mechanisms that are depicted in Figure 5 above.

8.1 Blockchain Reference Architecture

Several individuals and organizations have proposed general blockchain and Fabric-specific reference architectural diagrams. Whilst some of these diagrams go beyond the conceptual layer to describe security controls, they are predominantly connectivity-oriented rather than security-oriented architectures. Connection-oriented diagrams result in a flat network architecture that does not meet network segmentation requirements for critical infrastructure systems. Hence, network segmentation is a core network protection strategy in this document.

8.2 Network Security and DLT Networks

We adopt the network security approach outlined in ITU-T X.805.[126] The Recommendation defines a network security architecture that applies to Fabric because end-to-end security is a concern for DLT Networks. The ITU-T X.805 security architecture addresses security concerns for the management, control, and use of network infrastructure, services, and applications. It identifies eight security dimensions to address a particular aspect of network security. The dimensions, which align with *Section 3.2.2 – Business Attribute Profile*, are access control, authentication, non-repudiation, data confidentiality, communication security, data integrity, availability, and privacy. Cryptography is a foundational control because it delivers the security dimensions. The security dimensions protect security planes (i.e., management, control, and end-user) which address specific security needs related to network management activities.[127]

125 SABSA® and TOGAF®, 2018.

126 ITU, 2003.

127 ITU, *ITU-T Recommendation X.1205: Overview of Cybersecurity, in Series X: Data Networks, and Open System Communications and Security.* 2008, International Telecommunication Union (ITU): Geneva, Switzerland.

8.3 End-to-End Fabric Reference Security Architecture

We apply network security principles to a Hybrid Cloud Model and use elements of the IBM blockchain reference architecture.

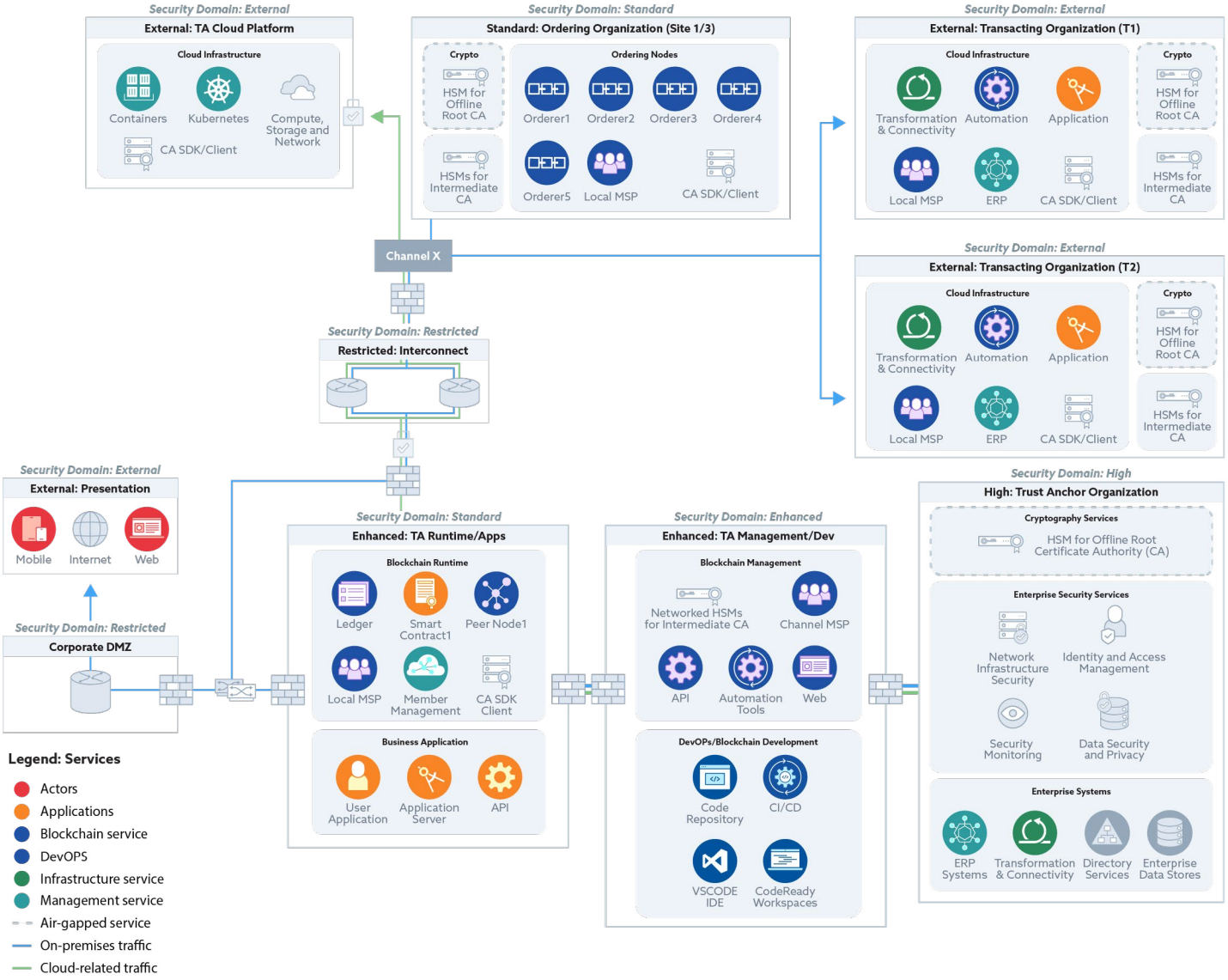

Figure 6 – End-to-End Fabric Reference Security Architecture.

8.3.1 Overview of Reference Security Architecture Components

The Reference Security Architecture diagram above combines the blockchain-oriented and solution-oriented views of the IBM blockchain reference architecture with enterprise security components. We should stress that we use several elements of the IBM blockchain reference architecture because the information is readily available on the Internet.[128] Please note that we

128 To obtain information about the IBM Blockchain reference architecture, follow this link please: https://www.ibm.com/cloud/architecture/architectures/blockchainArchitecture/reference-architecture

are neither endorsing the IBM Blockchain Platform nor discounting other Blockchain-as-a-Service (BaaS) solutions. Indeed, we reference BaaS solutions from companies, such as Amazon, Microsoft, Oracle, SalesForce, and Alibaba. As noted earlier, IBM and Digital Asset are the original contributors of Fabric. Therefore, the IBM blockchain reference architecture offers valuable building blocks for a Fabric Reference Security Architecture. Figure 6 above identifies three types of organizations that form a Fabric blockchain network: Trust Anchor, Ordering Service and Transacting Organizations. We discuss their respective roles.

8.3.2 Assumptions of the Reference Security Architecture

Critical sector stakeholders, such as security accreditors, network auditors, and regulators, require reasonable assurance that the use of blockchain technology would not lead to attacks that could impact national security, public health and safety, commerce, or any combination of these.[129] Hence, our proposed Reference Security Architecture assumes that, to obtain ATO permission for critical sector live operation, DLT solutions shall:

1. Address security risks across the entirety of the blockchain network lifecycle i.e., design, development, acceptance, use, decommissioning and disposal.
2. Have adequate security controls to deter, detect, resist, or defend against advanced threats including attacks by Threat Actors influenced by Nation-State Sponsored Groups.
3. Use a data classification scheme to indicate the security controls that are required to protect valuable, sensitive, and business critical information on the chain.
4. Comply with regulatory requirements around the use of Public Cloud Services to operate services that have the potential to materially impact critical sectors, such as energy.
5. Apply security domains/zones to separate data and assets based on their sensitivity.
6. Use security patterns, such as NIST SP 800-46 Rev. 2 and the Walled Garden[130] to enable peer nodes located on the on-premises network to securely communicate with nodes physically located in less trusted domains, such as the cloud and competitors' networks.
7. Adopt the hybrid cloud model as it offers enterprises the ability to retain control over critical SoR whilst using public cloud for non-mission-critical workloads.
8. Defend against network attacks by air-gapping Root of Trust (RoT) systems, such as Hardware Security Modules (HSMs) that host the Root Certification Authority (CA).
9. At a minimum, use hardware cryptographic modules that comply with industry best practice, such as FIPS 140-2 or FIPS 140-3 and PCI PIN Transaction Security (PTS) HSM for digital signature key generation, and CA digital Signature key storage and certificate Signing.
10. Ensure that Boundary or Perimeter Protection devices, such as firewalls, IDS, and IPS, meet international assurance requirements, such as Common Criteria.

The Security Architectural Pattern above is security countermeasure agnostic. Thus, to deliver the security outcomes expected by the Business Attributes (Section 3.2.2), the actual security controls deployed may originate from entities, such as the CSA, NIST, ISO/IEC, or MITRE.[131]

129 Wamala, F., *2011.*

130 Architectural Pattern No. 2 – Walled Gardens for Remote Access was published by CESG, the forerunner for the UK National Cyber Security Centre (NCSC), in March 2011. The NCSC notes that it, "Still provides a sensible and logical approach to connecting trusted networks to less trusted ones in a classic on-premises setup": https://www.ncsc.gov.uk/blog-post/ncsc-it-networking-cloud

131 MITRE D3FEND™ is a knowledge graph of cybersecurity countermeasures: https://d3fend.mitre.org/

8.3.2.1 High Assurance Cross-Domain Guards

Physical or logical means, such as firewalls, routers, and access control lists, can be utilized to enforce network segmentation. In Figure 6 above, firewalls represent High Assurance cross-domain guards that connect domains for assured information sharing.[132,133] National security systems use cross-domain guards to prevent the spillage of information to lower classification domains. Tim Olson, a contributor to IBM's Blockchain Blog, argues that a blockchain-based cross-domain solution is likely to address the risk of cross-domain information transfer more effectively, cheaply and with less complexity than traditional, special-purpose cross-domain guard.[134] He adds that, "In a blockchain network, the role of cross-domain guard would be performed by a blockchain network peer installed on a high assurance platform, referred to as a High Security Business Node (HSBN)."[135] Thus, the guards mitigate cross-domain information transfer risks and support security accreditation.

8.3.3 Network Segmentation in Reference Security Architecture

Business Driver 3 (BD3) defines a business requirement to categorize and handle blockchain network assets in accordance with the relevant Classification Scheme. As outlined in Assumption 5, we use network segmentation to enforce the separation between blockchain network components handling data of different security classifications or levels of trust.[136] Network segmentation is a compliance requirement in many critical sectors. For instance, in financial services, isolating the cardholder data environment from the remainder of an entity's network can help to reduce the scope of the PCI DSS assessment. Indeed, segmentation is a critical defense against network attacks, such as the MITRE ATT&CK® Framework Lateral Movement adversary tactic (TA0008).[137] We use five domains to show how blockchain services could be separated into different domain levels of trust: High Security, Enhanced Security, Standard Security, Restricted Security, and External Security.

8.4 High Security Domain

The High Security Domain should host systems with the highest protection requirements, including networks handling the most sensitive information and critical SoR. Stringent controls are required because the compromise of systems hosted within the domain could have business impacts so grave as to threaten the viability of the organization. Hence, the sensitivity of the information hosted in this domain justifies the use of a holistic set of security measures to defend against highly capable threat actors, such as Nation State-Sponsored Groups.

132 Olson, T., *2018b.*

133 Olson, T., *Mapping cross-domain security requirements to blockchain.* 2018c, IBM: Somers, New York, USA.

134 We would like to thank Tim Olson for sparing time to help us to validate our ideas around the importance of enforcing security domains in business blockchain networks. Tim is a Distinguished Certified IT Architect at IBM. He is contributor the IBM Blockchain Blog: https://www.ibm.com/blogs/blockchain/author/tim-olson/

135 Olson, T., *2018a.*

136 Wamala, F., *2011.*

137 Techniques that adversaries use to enter and control remote systems on a network: https://attack.mitre.org/tactics/TA0008/

8.4.1 Cryptography Services

NIST Special Publication 800-57, Revision 5 describes the compromise of cryptographic primitives as the unauthorized disclosure, modification, substitution or use of sensitive key information (e.g., a secret key, private key, or secret metadata).[138] Cryptography is critical to a blockchain network's functionality and security. Functionally, a "blockchain" is created when each block is cryptographically linked to the previous one (making it tamper evident) after validation and undergoing a consensus decision. In terms of security, in Section 8.3.1 we noted that cryptography is a foundational security control for Fabric because it delivers the eight ITU-T X.805 security dimensions. The diagram below presents the dimensions in a tabular form.

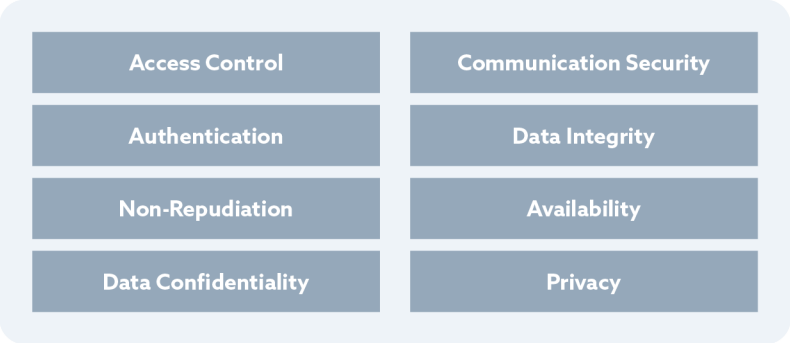

Figure 7 – Eight Security Dimensions.

Indeed, cryptography addresses most of the threats to Fabric that we outlined in *Section 6.1 – Compromise Methods*. Cryptographic primitives are reliant upon the personnel, physical, procedural, and technical controls in the High Security Domain.

8.4.1.1 Cryptography-based Blockchain Network Services

Fabric uses cryptographic primitives, such as asymmetric-key cryptography, hash functions, and digital signatures. According to *NISTIR 8202 – Blockchain Technology Overview*, the cryptography-based blockchain network services include:[139]

- Private keys that are used to *digitally sign transactions*.
- Public keys that are used to *derive addresses*.
- Public keys that are used to *verify signatures* generated with private keys.
- The ability to verify that the user transferring value to another user is in possession of the private key capable of signing the transaction.

Cryptographic hash functions perform several critical tasks within a blockchain network. These include address derivation, creation of unique identifiers, security of the block data and securing the block data. Indeed, some blockchain networks only use the cryptographic hash functionality.

138 Barker, E., *NIST SP 800-57, Part 1, REV. 5 - Recommendation for Key Management Part 1 – General*. 2020, National Institute of Standards and Technology (NIST) Gaithersburg, Maryland, USA.

139 Yaga, D., et al., 2018.

8.4.1.2 Public-key cryptography (PKC)'s Compliance Defect

PKC is preferred to symmetric key cryptography in interactions between strangers because symmetric key cryptography requires a secure out-band channel to exchange the secret key before secure communication occurs. Whitfield Diffie and Martin E. Hellman note in New Directions in Cryptography that, "A large number of users *n* results in an even larger number, $(n^2-n)/2$ potential pairs who may wish to communicate privately from all others."[140] Regrettably, PKC has security weaknesses. Don Davis argues that PKC is popular in real-time transactions even between strangers, as it "[h]as low infrastructural overhead because public-key users bear a substantial but hidden administrative burden."[141] As a public-key security system, PKIX) "[t]rusts its users to validate each other's public keys rigorously and manage their own private keys securely. Both tasks are hard to do well, but public-key security systems lack a centralized infrastructure for enforcing users' discipline."[142] As discussed below, the defect can be mitigated using personnel, physical, procedural, and technical security controls.

8.4.1.3 Public-Key Infrastructure (PKI)

Permissioned blockchains may strengthen the security of asymmetric-key cryptography by using a PKI to issue credentials rather than expecting each blockchain user to manage their own key pairs.[143] Key management is crucial to the security of Fabric because once a threat actor gains control of the private key, they can transfer digital assets, such as monetary funds, to another account, often with no way of undoing the transaction. Crypto-Asset Exchange hacks[144] and the FBI's counterattack on DarkSide[145] exemplify the difficulty that blockchain users encounter in keeping their private keys secure. Let us consider production PKI options.

8.4.1.3.1 Fabric Certificate Authority (CA) Server

The default Fabric Membership Service Provider (MSP) uses the hierarchical PKIX to generate the digital certificates it uses as identities. Fabric provides a built-in Certificate Authority (CA)[146] component to create CAs for blockchain networks. The Fabric CA provides features, such as registration of identities or connection to directories as the user registry; issuance of Enrollment Certificates (ECerts), and certificate renewal and revocation. The diagram below illustrates how the Fabric CA server fits within the overall Fabric architecture.

140 Diffie, W. and M. Hellman, *New Directions in Cryptography.* IEEE Transactions on Information Theory, 1976. IT-22(6): p. 644-654.

141 Davis, D., 1996.

142 Davis, D., *1996.*

143 Yaga, D., et al., 2018.

144 A 'Blockchain Bandit' Is Guessing Private Keys: https://www.wired.com/story/blockchain-bandit-ethereum-weak-private-keys/

145 The FBI didn't hack Bitcoin — but it won't say how it got DarkSide's private key: https://protos.com/fbi-didnt-hack-bitcoin-but-it-wont-say-how-it-got-darksides-private-key/

146 Obtain the Fabric CA User's Guide here: https://hyperledger-fabric-ca.readthedocs.io/en/latest/users-guide.html#table-of-contents

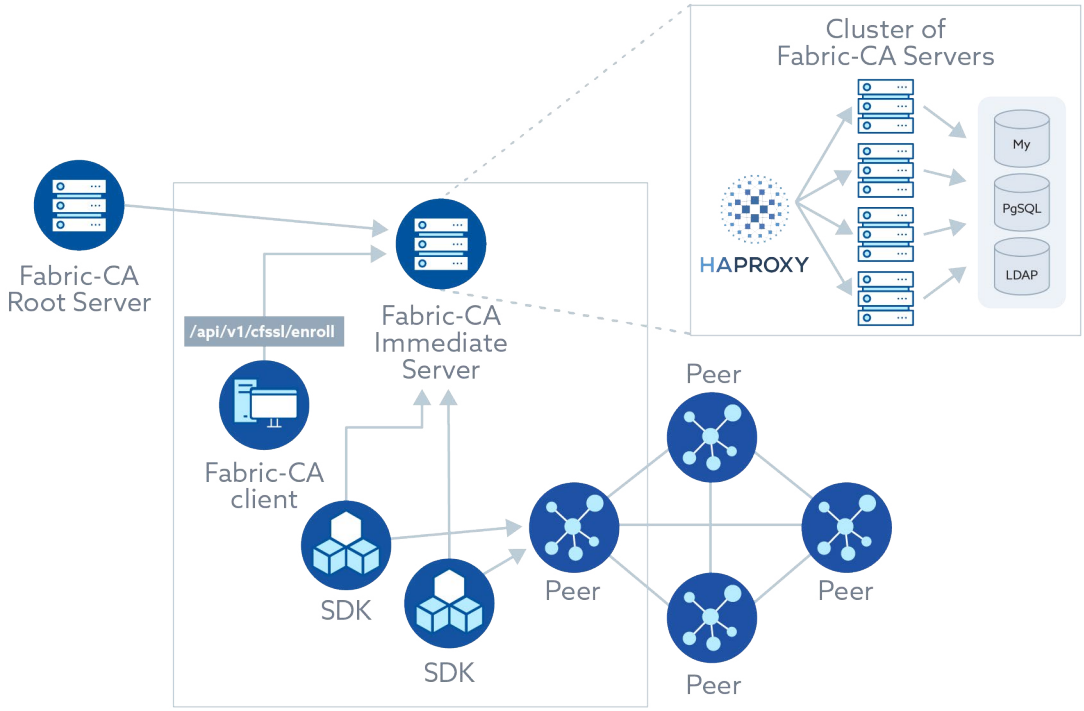

Figure 8 – Fabric CA server.

As depicted above, the Fabric CA server can be accessed either via the Fabric CA client or one of the Fabric SDKs. We discuss Fabric CA access in the Enhanced and Standard domains.

8.4.1.3.2 Use of Public/Commercial PKI Services in Production

The Fabric CA is a private root CA provider that can manage digital identities of Fabric participants that have the form of X.509 certificates. However, Hyperledger documentation states that, "Because Fabric CA is a custom CA targeting the Root CA needs of Fabric, it is inherently not capable of providing SSL certificates for general/automatic use in browsers."[147] Therefore, we agree with the Hyperledger project that production Fabric environments should use a trusted enterprise/commercial root or intermediate CA to provide services, such as user enrollment, transaction protection, and issuance of TLS certificates that secure connections.

8.4.1.4 Security recommendation for a Production Root CA

PKI must meet compliance requirements to support systems/networks in critical sectors. For example, PCI DSS Requirement 4.1 states that, "Only trusted keys and certificates are accepted."[148] As the trust anchor, the Root CA signs and issues certificates for all intermediate or issuing CAs. Therefore, we recommend that organizations should:

147 Hyperledger Fabric – Identity: https://hyperledger-fabric.readthedocs.io/it/latest/identity/identity.html
148 PCI DSS Version 3.2.1, May 2018: https://www.pcisecuritystandards.org/document_library

- Operate an air-gapped and offline Root CA with activities, such as Authority Revocation List (ARL) issuance performed via an occasional reactivation of the Root CA HSM.
- Adopt Certificate Policies and Certification Practices Statements that comply with guidance, such as RFC 3279,[149] RFC 3647,[150] RFC 5280,[151] RFC 5480,[152] and RFC 5759.[153]
- Use HSMs to build secure foundations for cryptographic operations, such as digital signature key generation, CA digital signature key storage and certificate signing, transaction signing and cryptographic key lifecycle management.
- Ensure that HSMs, to which cryptographic operations performed by Fabric nodes[154] are delegated, are at least FIPS 140-2 or FIPS 140-3 Level 3 certified and PCI validated for commercial entities. Typically, the HSMs for national security systems/networks are at least FIPS 140-2 or FIPS 140-3 Level 4, or Common Criteria EAL 4+.
- Ensure that, in accordance with RFC 3647, all CAs are subject to regular compliance audits under the auspices of schemes, such as the WebTrust Seal program[155] or tScheme.[156]
- Adopt secure key lifecycle practice to reduce the risk of unauthorized disclosure, modification, substitution, or use of sensitive data, such as secret keys and private keys.
- Follow guidance in good practice documents, such as in NIST Special Publications like SP 800-57 (Parts 1-3), SP 800-52, and 800-130. Financial service firms should comply with cryptography guidance in standards, such as ISO 9564-1, 11568-1, 11568-2 and 11568-4.
- Use formal Cryptography Architectural Principles to guide security and solution architects during the specification of solution architecture. The principles include Key Lifecycle Security, Key Ownership, Key Purpose, Key Usage,[157] Cryptoperiods, and Key Hierarchy.
- Replace algorithms and key lengths considered to be insecure.

Overall, organizations should pursue a risk-based approach to cryptography to ensure that the controls are proportionate to the risk, legitimate, and meet the Business Drivers for Security and security outcomes, outlined in Section 3.2.2 – Business Attribute Profile.

149 RFC 3279 – Algorithms and Identifiers for the Internet X.509 PKI Certificate and Certificate Revocation List (CRL) Profile.

150 RFC 3647 – Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.

151 RFC 5280 – Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.

152 RFC 5480 – Elliptic Curve Cryptography Subject Public Key Information.

153 RFC 5759 – Suite B Certificate and Certificate Revocation List (CRL) Profile.

154 Refer to Hyperledger documentation on how to delegate the cryptographic operations performed by Fabric nodes to an HSM: https://hyperledger-fabric.readthedocs.io/en/release-2.2/hsm.html?highlight=Hardware%20Security%20Module%20(HSM)

155 WebTrust: https://www.cpacanada.ca/en/business-and-accounting-resources/audit-and-assurance/overview-of-webtrust-services

156 tScheme is a UK body that assesses Trust Service Providers (TSPs) including PKI: https://www.tscheme.org/about-us

157 Refer to Section 5 General Key-Management Guidance of *NIST SP 800-57 Part 1 Rev. 5 Recommendation for Key Management: Part 1 – General*: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r5.pdf

8.4.1.5 Quantum Computer Readiness

Network Owners and Network Proprietors should prepare blockchain networks for the potential arrival of quantum computers. A future large-scale quantum computer could break current "conventional" PKCs that are based on difficult or intractable mathematical problems.[158,159,160,161] Additionally, a quantum computer could weaken the security strengths in quantum bits of symmetric-key cryptography. The challenges to PKC and secret-key cryptography are Shor's Algorithm and Grover's Algorithm.

8.4.1.5.1 Shor's Algorithm

Shor's Algorithm is an integer factorization algorithm formulated by Peter Shor in 1994.[162] If a quantum computer with enough qubits could operate without errors, Shor's algorithm could be used to break "conventional" public-key cryptosystems that are based on integer factorization, such as RSA and discrete log problems, using elliptic curves. Therefore, Shor's Algorithm would allow resourced Threat Actors to decrypt data that has been encrypted in the past and to forge digital signatures in the future. Given that the quantum computer easily solves RSA and Diffie-Hellman problems, it would obliterate the security of Fabric blockchain networks because most X.509 digital certificates that the MSP uses for trusted identities rely on these protocols. Additionally, the quantum computer would crush confidence in PKC-based blockchain operations, such as digital signing of transactions using private keys, address derivation with public keys, and use of public keys to verify signatures generated with private keys. The CSA's "*Blockchain in the Quantum Era*" paper covers potential impacts on Fabric.[163]

8.4.1.5.2 Grover's Algorithm

Grover's Algorithm enables a quantum computer to find a value that has a certain property much faster than is possible on a classical computer.[164] As a result, Grover's Algorithm halves the security strength in bits for symmetrically keyed encryption algorithms, such as Advanced Encryption Standard (AES). Current understanding is that secret-key security is maintained by doubling the key size and restoring the original work factor. For example, using 256-bit keys (instead of 128-bit) for the AES block cipher is assumed to protect against future conventional or quantum computers.

158 ASC.X9, *ASC X9 IR 01-2019: Informative Report - Quantum Computing Risks To The Financial Services Industry*. 2019, ASC X9 Quantum Computing Risk Study Group: Annapolis, MD, USA. p. 1-50.

159 ETSI, *DTR/CYBER-QSC-0013 - CYBER: Migration strategies and recommendations to Quantum Safe schemes*, in ETSI TR 103 619 V1.1.1. 2020, European Telecommunications Standards Institute (ETSI): Sophia Antipolis Cedex, France.

160 NCSC, *Preparing for Quantum-Safe Cryptography*. 2020, National Cyber Security Centre (NCSC): London, UK.

161 Chen, L., et al., *NISTIR 8105 - Report on Post-Quantum Cryptography*. 2016, National Institute of Standards and Technology (NIST) Gaithersburg, Maryland, USA.

162 ASC.X9, 2019.

163 Huttner, B., *Blockchains in the Quantum Era.* 2021, Cloud Security Alliance (CSA): Seattle, Washington, United States. p. 16.

164 ASC.X9, *2019.*

8.4.1.5.3 Quantum-Safe Cryptography

As of this writing, NIST's work to develop quantum-safe Key-Establishment Mechanism (KEM)/ Public Key Encryption (PKE) and Digital Signature algorithms is in the third round. The 3rd Round Finalist KEMs/PKEs are Kyber (MLWE lattice), Saber (MLWR lattice), NTRU (NTRU lattice) and Classic McEliece (GoppaCodes). The alternate KEMs/PKEs are FrodoKEM, NTRUprime, SIKE, BIKE and HQC. The 3rd Round Finalist Signatures are Dilithium (MLWE Fiat-Shamir), Falcon (NTRU Hash-and-Sign) and Rainbow (UOV Multivariate). The alternate Signatures for the NIST PQC Programme are SPHINCS+, Picnic and GeMSS. The NIST PQC Programme is expected to issue standards between 2023 to 2025.[165]

8.4.2 Enterprise Security Services

Organizations or individuals in a permissioned blockchain consortium must protect mission-critical data and workloads within its own environment from threats and vulnerabilities resulting from interaction with and/or reliance on blockchain networks. The services below provide a strong foundation for protecting enterprise devices, applications, networks, data, and users.

8.4.2.1 Network Infrastructure Security

The High Security Domain typically hosts assets for the management plane. According to ITU-T X.805, the management plane of the infrastructure layer is concerned with securing the operations, administration, maintenance, and provisioning of the individual network elements, communication links, and server platforms that comprise the network.[166] The security controls for the Domain could include:

- A network architecture with dedicated switches; in-line firewalls at the boundary of the network; all traffic via physical firewall interfaces, etc.
- Secure connectivity, e.g., allowing only minimal traffic; specific source/destination/port; limiting bi-directional firewall rules; restricting IP address ranges; explicit deny policies, etc.
- Secure privileged access / system management, e.g., a dedicated management platform.
- Secure user access, e.g., single point of user entry into the network; no console access, etc.

The network security controls that you deploy will depend on the expected security outcomes (discussed in *Section 3.2.2*) and the results of the Threat Assessment. Additionally, the cloud computing platforms could offer synergy, because CSPs offer very secure networks due to not trusting users. Due to low trust, CSPs enforce stringent authentication, authorization and accounting controls to segment customer environments which improves security for all users.

165 NIST Post-Quantum Cryptography (PQC) Standardization: https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization.

166 ITU, 2003.

8.4.2.2 Identity and Access Management (IAM)

As a permissioned blockchain network, Fabric must be built on strong identity and access management (IAM). Indeed, Business Driver 4 discussed in Section 3 requires that, "[a]ll users of the blockchain network are fully identified, authenticated, authorized and their transactions fully auditable." X.509 digital certificates are used to associate Fabric network components, such as applications and peer, ordering and certificate authority nodes with a specific role within a specific organization. Figure 6 shows that each network organization obtains verifiable identities from its own PKI service. However, in practice, organizations routinely share or subscribe to the same PKI service.

8.4.2.2.1 IAM Security Recommendations

ITU-T 8.05 addresses IAM through the access control security plane and the end-user security plane respectively. The access control dimension would use IAM to help ensure that only authorized users or components are allowed access to Fabric network elements, stored information, information flows, services, and applications. The end-user security plane would enable Fabric to secure the actual end-user data flows. The actual IAM controls applied will depend on the threat landscape. Overall, it is good security practice to ensure that:

- Enterprise authentication services, such as Active Directory domain controllers, are located within the High Security Domain to be used by High, Enhanced and Standard networks.
- Systems within the network should not rely on authentication services hosted on systems that reside outside the network, as it could be challenging to gain assurance about the IAM credentials. This decision should be risk-based since private-key security issues and Know Your Customer laws have engendered private key escrow services.
- Identity stores are protected against unauthorized access and modification.
- In line with Business Driver 7 (BD7 discussed in Section 3), IAM should ensure that Fabric users are only granted authorized access in accordance with good security principles, such as need-to-know and least privilege.

8.4.2.3 Data Security and Privacy

Data security and privacy controls aim to prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information. We defined privacy and data security requirements in Section 3, i.e., BD6 and BD8 respectively. ITU-T X.805 considers data security issues within the data confidentiality,[167] data integrity,[168] and privacy[169] security dimensions. Blockchain dataflows expand the enterprise attack surface and the compliance scope for data, because peer nodes in a network could be physically located on-premises, at a competing organization, or in a cloud environment.

167 The data confidentiality security dimension protects data from unauthorized disclosure. Data confidentiality ensures that the data cannot be understood by unauthorized entities. Encryption, access control lists, and file permissions are typical controls.

168 The data integrity security dimension ensures the correctness or accuracy of data. The data is protected against unauthorized modification, deletion, creation, and replication, and provides indicators of these unauthorized activities.

169 The privacy security dimension provides for the protection of information that might be derived from the observation of network activities. Examples include websites a user visited, their geographic locations, and the IP addresses and DNS names of their devices.

8.4.2.3.1 Data Security and Privacy Recommendations

The data security and privacy requirements are guided by the security, compliance, and regulatory needs of the business. The following controls are useful:

- In accordance with Business Driver 3 (BD3) in Section 3, clearly classify data as personal, sensitive, or both, and apply the security controls mandated by the relevant classification level.
- Ensure that encrypted sensitive data is processed within high security networks.
- Use Fabric's channels to support data privacy requirements of specified jurisdictions.
- Restrict data replication to only permissioned parties, to support privacy and confidentiality.
- Users should have the ability to encrypt data stored on the Fabric blockchain network.
- Offer users the capacity to manage their private keys securely, including seamless integrations with private-key escrow or custody services.

8.4.2.4 Security Monitoring

According to Center for Internet Security (CIS) Controls Version 8, monitoring is a critical component of security operations,[170] such as *Control 12 – Network Infrastructure Management*, *Control 13 – Network Monitoring and Defense*, and *Control 08 - Audit Log Management*.

A Fabric blockchain could use the CIS controls to identify and detect security vulnerabilities, and protect against, respond to, and recover from attacks.

8.4.2.4.1 Security Monitoring Recommendations

As noted above, Fabric solutions in critical sectors must be able to detect the most advanced threats including attacks by Threat Actors that are capable of evading monitoring defenses.[171] A SIEM solution delivers the logical Event Logging Service shown in Figure 5.

Tomasz Klim observes that, "[d]evelopers often make the mistake of trying to implement Hyperledger Fabric security themselves. They focus on its functional security while leaving basics, such as network or firewalling open to potential attacks."[172] Thus, security monitoring should identify:

- Misconfigurations e.g., internal services exposed outside the Hyperledger server node.
- Use of default ports.
- Excessively permissive firewall rules.
- Insecure, or unpatched Hyperledger application stack components, such as Fabric's main component\ Apache Kafka, Apache ZooKeeper, and Apache CouchDB.

In addition, Fabric integrates with the ELK (Elasticsearch, Logstash, and Kibana) stack, and the logcheck and logwatch utilities. The ELK Stack offers the ability to aggregate logs from a variety of

170 Obtain a copy of CIS Controls Version 8 at: https://www.cisecurity.org/controls/v8/

171 Defense Evasion (TA0005) MITRE ATT&CK® Enterprise tactic consists of techniques that adversaries use to avoid detection throughout their compromise: https://attack.mitre.org/tactics/TA0005/

172 Klim, T., *A practical guide to Hyperledger Fabric security*. 2020, Espeo Blockchain: Poznań, Poland.

systems and applications, analyze them, and create visualizations for application and infrastructure monitoring, faster troubleshooting, and security analytics.[173] Public cloud providers, such as AWS, Azure,[174] Google Cloud Platform,[175] provide ELK Stack managed services. Software-Defined Perimeter (SDP)/Zero Trust Network Access (ZTNA) could be a solution to some of these classic IT flaws. However, the viewpoint of security accreditors must be obtained.

8.4.3 Enterprise Systems

A Fabric blockchain network enables organizations and individuals that do not trust each other to share discrete sets of information, and track assets immediately and transparently, by using a shared immutable ledger. However, blockchain networks should only store transactions that are shared with other organizations. Therefore, blockchains must interact securely with enterprise SoR or source systems of record (SSoR) because such systems are authoritative data sources for the most sensitive information. Given that the compromise of a SoR could have devastating financial, reputational, regulatory, customer and business impacts on the enterprise, we position the systems in the Trust Anchor Organization's High Security Domain.

8.4.3.1 Enterprise Resource Planning (ERP) System

ERPs, such as SAP, Oracle E-Business Suite, Microsoft Dynamics, Salesforce, and IBM CICS, create and maintain some of the most critical business and customer data that ends up in enterprise data stores and blockchain ledgers. Integrating the ERPs with blockchain offers several benefits. For example, smart contracts can increase the transparency and auditability of business records. In addition, ERP and Fabric integration bolsters security and reduces exposure to audit or accounting risk, since under normal operation of the blockchain network, no transaction can be changed once published.[176]

ERP and Fabric integration must be secure to avert the risk of disruptive attacks. Provided that the private key is managed securely, the associated public key could be used to verify transactions at any time. ERPs may interact with Fabric blockchain directly using an SDK or indirectly using an API or integration technology.

8.4.3.2 Transformation and Connectivity

The IBM Blockchain reference architecture states that organizations should use connector and transformation integration technologies to connect blockchain to ERP systems and data stores. Integration technologies are popular because they simplify the integration of blockchain transaction data with enterprise data stores. Additionally, integration technologies can synchronize ERP systems with blockchains in near real-time. Examples of transformation and connection technologies include IBM App Connect, IBM InfoSphere DataStage, Mulesoft, RedHat Fuse, and WS02.

173 The ELK stack works with the Amazon Elasticsearch Service: https://aws.amazon.com/elasticsearch-service/the-elk-stack/

174 Elastic on Azure: https://azure.microsoft.com/en-gb/overview/linux-on-azure/elastic/

175 Elastic on Google Cloud Platform: https://console.cloud.google.com/marketplace/product/endpoints/elasticsearch-service.gcpmarketplace.elastic.co?utm_source=elasticpartnerpage&utm_campaign=ctabutton

176 Yaga, D., et al., *2018.*

Given their integration with systems that host the most mission-critical data, we recommend that the connectors and integration technologies be covered by the strong security controls in the High Security Domain.

8.4.3.3 Directory Services

Directories should benefit from the security controls of the High Security Domain because they play a critical role in securing network resources in an interconnected environment. Directories centralize enterprise access controls by storing information about people, hardware, applications, and data about network users. Additionally, directories enable the assignment of roles and the management of access credentials for user accounts, including administrator and service accounts. *Section 4.1 – System Context Diagram* describes the Member Management function that registers blockchain participants in a directory. Directories support the enrollment of Fabric users and the mapping of blockchain-specific roles, such as Chain Member, to organizational roles. The Fabric CA server can be configured to connect to a Lightweight Directory Access Protocol (LDAP) server,[177] either to authenticate an identity prior to enrollment, or to retrieve an identity's attribute values used for authorization. Blockchain networks utilize existing directory services to connect to commercial CAs.

For example, the Azure Blockchain Workbench associates blockchain identities with Azure Active Directory.[178] Private keys can be stored in Azure Key Vault. Similarly, a Fabric network on Amazon Managed Blockchain uses directories for user enrollment.[179] AWS Key Management Service (KMS) secures Fabric entities.[180]

8.4.3.4 Enterprise Data Store

We stated in *Section 8.4.1.3.1 – Data Security and Privacy Recommendations* that encrypted sensitive data should be processed within high security networks. This is because personnel, physical, procedural, and technical security controls offer the enterprise's mission-critical data the best protection against MITRE ATT&CK® Tactic TA0010: Exfiltration.

Typically, a firm's most valuable data is stored in Relational and NoSQL enterprise data stores such as Oracle Database, Microsoft SQL Server, MySQL, IBM Db2, Amazon DynamoDB, Azure Cosmos DB, Redis, and Neo4J.

According to the IBM blockchain reference architecture, despite their close relationship, blockchains differ from enterprise data stores. Whilst blockchains store transactions that are shared with other organizations, access to enterprise datastores must be restricted to those parties with the appropriate security clearance and need-to-know. Given the criticality of protecting mission-critical information assets, and the relatively slow performance of blockchain, it is advisable to extract and transform ledger data into a data store for subsequent processing.

177 Fabric CA User's Guide: https://hyperledger-fabric-ca.readthedocs.io/en/release-1.4/users-guide.html

178 Azure Blockchain Workbench: https://azure.microsoft.com/en-us/features/blockchain-workbench/

179 Creating a Hyperledger Fabric Blockchain Network Using Amazon Managed Blockchain: https://docs.aws.amazon.com/managed-blockchain/latest/hyperledger-fabric-dev/managed-blockchain-get-started-tutorial.html

180 Encryption at Rest for Hyperledger Fabric on Managed Blockchain https://docs.aws.amazon.com/managed-blockchain/latest/hyperledger-fabric-dev/managed-blockchain-encryption-at-rest.html

8.5 Enhanced Security Domain

The Enhanced Security Domain should host sensitive information related to blockchain management and development activities. This is because, to borrow the language of the UK Prudential Regulation Authority (PRA), the compromise of such information, "[c]ould have a significant adverse impact on the firm's reputation; could impact the firm's ability to continue to provide adequate services to its customers; or could result in serious financial consequences" to the wider financial sector or to other firms.[181] Hence, the sensitivity of blockchain management and development activities justifies heightened protective security measures to defend against determined and highly capable Threat Actors, such as large Criminal Organizations.

8.5.1 Network Security Controls

From a network security perspective, the Enhanced Security Domain is equivalent to the control security plane of the ITU-T X.805 Recommendation. The plane is concerned with the protection of the activities that enable the efficient delivery of information, services, and applications across the network.[182] Naturally, the network security controls deployed in the domain will depend on your threat landscape and the expected security outcomes. You should consider:

- A network architecture that uses either a physical firewall interface or Virtual LANs (VLANs) to manage traffic in and out of the network. However, a physical firewall interface would be preferred.
- Deploying firewall rules that have an explicit deny by default policy.
- Using firewall rules that allow large IP address ranges only if a clear business need exists.
- Using a "jump server" as a single point of entry into the management plane.
- Allowing users to access only the applications or systems they need to perform their job.
- Terminating and inspecting all outbound traffic to the Internet from within the Standard Domain.
- Prohibiting direct access to the Enhanced Security Domain by third parties. However, third parties may be granted access to services within the Standard Domain after going through access control points.

You should work with vendors to develop a deployment pattern for the Domain. SDP/ZTNA, Virtual Private Cloud (VPC) or Virtual Private Network (VPN) could be the solutions.

8.5.2 Trust Anchor – Blockchain Management and Development

The Trust Anchor organization hosts the three key components that are required to provide blockchain services: peer node, ledger, and smart contract. The organization delivers blockchain services to applications through peers that host replicas of the ledger and smart contracts that provide controlled access to it. A Trust Anchor organization serves a security role because it maintains a network policy that determines the access rights of each component to network

181 Consultation Paper | CP29/19 – Operational resilience: Impact tolerances for important business services, December 2019: https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/consultation-paper/2019/cp2919.pdf
182 ITU, 2003.

resources according to their role. Thus, an attack on its management and development activities would affect the network. An entity can serve in both Trust Anchor and Transacting roles.

8.5.2.1 Blockchain Management

Blockchain management focuses on the secure configuration and operation of the components that comprise a Fabric network, such as peer, ordering and certificate authority nodes. The aim is to reduce exposure to security vulnerabilities that result from poor configuration whilst benefiting from the decentralization features of blockchain. Let us consider the tools that administrators could use to configure and manage a Fabric blockchain network.

8.5.2.1.1 Networked HSMs for Intermediate CA

Intermediate CAs issue certificates to network components and maintain certificate status information. According to Hyperledger documentation, the MSP identifies the Root CAs and Intermediate CAs that are accepted for defining the members of a trust domain either by listing the identities of their members, or by identifying which CAs are authorized to issue valid identities for their members. Fabric nodes can delegate cryptographic operations to an HSM to improve protection against key compromise owing to malicious acts, inadvertent errors and/or system failures. The HSMs protect the private keys and handle cryptographic operations, allowing peers and ordering nodes to sign and endorse transactions without exposing their private keys. HSMs can protect the keys that are used to secure the blockchain from initial generation and storage to issuance, use, rotation, revocation, and retirement. Typically, critical sectors, such as finance require a FIPS 140-2 or FIPS 140-3 Level 3 certified, or PCI validated cryptographic boundary. Fabric communicates with HSMs over a PKCS11[183] interface. Within a native Fabric CA, the client routes to an High Availability (HA) Proxy endpoint which load balances traffic to one of the Fabric-CA-Server cluster members. Similarly, most HSMs support automatic and transparent replication of cryptographic key material within a cluster.

8.5.2.1.2 Channel MSP

Hyperledger documentation describes a Fabric Channel as a private "subnet" of communication between two or more specific network members, for the purpose of conducting private and confidential transactions. A Channel MSP should be hosted within the management zone of the Enhanced Security Domain because it defines administrative and participatory rights at the channel level. It defines the relationship between the identities of channel members (which themselves are MSPs) and the enforcement of channel-level policies. Channel MSP includes MSPs of all the organizations on a channel, such as the "peer organizations," which own peers and invoke Chaincodes, and the organizations that own and run the ordering service. Channels offer transaction isolation and the ability to keep data private whilst sharing hashes as transaction evidence on the ledger. Indeed, private data could be shared among "collection" members, or with selected entities on a need-to-know basis. Hence, channels enable network segmentation which supports compliance with multiple jurisdictions and regulatory regimes.

183 The Public-Key Cryptography Standards (PKCS) #11 Standard specifies an application programming interface (API), called "Cryptoki," for devices that hold cryptographic information and perform cryptographic functions: http://docs.oasis-open.org/pkcs11/pkcs11-base/v2.40/os/pkcs11-base-v2.40-os.html#_Toc416959676.

8.5.2.1.3 Application Programming Interface (API)

Fabric complies with the "complete with APIs" principle of the Hyperledger design philosophy.[184] Accordingly, Fabric APIs are the primary mechanism for enabling external clients and applications to interface quickly and easily with the Fabric blockchain network. For instance, the IBM Blockchain Platform uses a web API to enable network administrators to programmatically manage their organization's network components and resources, including peers, orders, CAs, organizations, channels, policies, identities, and wallets. Thus, the Enhanced Security Domain offers the security controls required to protect the API infrastructure.

8.5.2.1.4 Automation Tools

As discussed throughout this whitepaper, blockchain networks increasingly support mission-critical business processes in sectors that require high levels of confidentiality, such as financial services and national security. Therefore, automation tools should be the preferred approach for deploying the blockchain network to enable timely delivery and identification of critical software faults. For example, the IBM Blockchain Platform collection for Ansible provides reusable modules and roles that capture the common tasks that are required to define a blockchain network. Ansible's declarative approach reduces errors and streamlines network management. Administrators simply declare the target state for network components and Ansible makes all the changes required to achieve the desired results. Similarly, the Amazon Managed Blockchain supports API automation tools, such as Ansible, Chef, SaltStack, Terraform and Puppet.

8.5.2.1.5 Web Console

Given that a business blockchain network shares information between different organizations, network members acting in roles, such as Chain Member or Chain Transactor, it should be possible to manage the network through APIs accessible via the web. Using appropriate security controls, such as Multi-Factor Authentication (MFA), blockchain administrators should manage the blockchain network lifecycle, including smart contract deployment, over the Web. *Section 8.5.1 – Network Security Controls* notes that a jump server should act as a single point of entry into the Enhanced Domain for all Fabric blockchain solution administration activities.

8.5.2.2 Blockchain Development and DevSecOPs

The "complete with APIs" principle of the Hyperledger Design Philosophy seeks to support the growth of a rich developer ecosystem, and to help blockchain and distributed ledger technologies proliferate across a wide range of industries and use cases.[185] Blockchain development/DevSecOps services allow developers to leverage common tools and languages to shorten the systems deployment cycle for blockchain business applications. Therefore, consider hosting blockchain development/DevSecOps services in the Enhanced Security Domain to balance security and the need to rapidly test interactions with external clients and applications via APIs.

184 Hyperledger, 2018b.
185 Hyperledger, 2018b.

8.5.2.2.1 Blockchain Development

By design, Fabric is a foundation for developing applications or solutions with a modular architecture. For example, Fabric components, such as consensus and membership services, can be customized to satisfy a broad range of industry use cases. Earlier on, we noted the growing adoption of Fabric solutions within critical sectors.

Additionally, the massive attack on Kaseya VSA users[186] highlights the popularity of the Compromise Software Supply Chain sub-technique (T1195.002) of the Supply Chain Compromise technique[187] in MITRE ATT&CK® Framework. Hence, blockchain developer tools should be hosted within the Enhanced Security Domain to protect against attacks, such as manipulation of the application source code and manipulation of software update/distribution mechanisms. Let us consider two examples.

8.5.2.2.1.1 Visual Studio Code IDE

Visual Studio could benefit from the security controls in Enhanced Domain because it provides the tools required from initial design to final deployment. It is an integrated development environment (IDE) used to code, debug, test, and deploy to any platform. Features include local development with many common emulators, test access in Solution Explorer, Git experience to create and clone repos, and Kubernetes support. Visual Studio Code IDE supports application and smart contract development. For example, the IBM Blockchain Platform uses the Microsoft Visual Studio Code plugin to accelerate application and smart contract development. Blockchain developers could create local test networks and connect to the remote Fabric network.

8.5.2.2.1.2 Red Hat® CodeReady Workspaces

Red Hat® CodeReady Workspaces is a developer tool that supports cloud-native development using Kubernetes and containers. It provides a consistent, preconfigured development environment for developers to code, build, and test in containers running on Red Hat OpenShift®. Red Hat® CodeReady Workspaces offers a Red Hat OpenShift® development team access to the full Visual Studio Code blockchain IDE via a shared development server. Developers can collaborate on application and smart contract development by using recipes, stacks, and workspaces. RedHat® CodeReady Workspaces features include an in-browser IDE with support for Visual Studio Code extensions and an administrative dashboard.

8.5.2.2.2 DevSecOPs

DevOps brings together software development (Dev), security (Sec) and IT operations (Ops) practices. DevSecOps primarily seeks to shorten the systems development lifecycle (SDLC) and support continuous delivery whilst delivering high quality and secure software products. DevSecOps frameworks offer members the capacity to develop and maintain application code, smart contract source code, and blockchain network component configurations.

186 Kaseya victim struggling with decryption after REvil goes dark: https://www.zdnet.com/article/kaseya-victim-struggling-with-decryption-after-revil-goes-dark/

187 Supply Chain Compromise: Compromise Software Supply Chain: https://attack.mitre.org/techniques/T1195/002/

8.5.2.2.2.1 Continuous Integration and Continuous Delivery (CI/CD)

CI/CD aims to help DevSecOps teams to release better quality software at a faster pace through automation. DevSecOps should integrate security services, such as automated application vulnerability scanning, code signing and key lifecycle management. CI/CD products include GitLab CI/CD, Jenkins, IBM DevOps, Microsoft Azure DevOps, AWS DevOps, etc. For example, the IBM Blockchain Platform uses CI to ensure that whenever a user changes an application, smart contract, or network component definition or configuration, the change is verified and automatically integrated with the code repository. Continuous Delivery (CD) ensures that changes to source repositories are rolled into new versions of applications, smart contracts, and network components. In turn, Continuous Delivery automates the release of applications, smart contracts, and network components to test and production environments.

8.5.2.2.2.2 Code Repository

Code repositories enable blockchain network participants to store and assign versions to smart contract and application code. Code repository products and services include Git, GitHub, GitLab, BitBucket, and Apache Subversion. IBM regards information about network component definition and configuration as infrastructure-as-code (IaC). Therefore, it should be managed as IaC. For example, timely action must be taken to address security vulnerabilities in IaC templates to protect the blockchain network from attack. Blockchain participants exercise different levels of control over code repositories. Typically, blockchain participants control their own application code and peer, certificate, authority and orderer definitions. Blockchain participants may use common code repositories if there is a need to share smart contract and channel policy definitions with other participants. Local repositories store copies of these assets.

8.6 Standard Security Domain

The Standard Security Domain should have adequate security controls to protect the organization's participation in a Fabric blockchain network. Security is vital, especially in interactions with peer nodes that are physically located within a competing organization's security environment and domain.[188] Whilst a blockchain enables a community of users to record transactions in a shared ledger, each participant would have unique security, regulatory, and compliance requirements. The Domain should use the Fabric's features to enforce a "network of networks" that enable members to maintain separate relationships within their networks.

8.6.1 Network Security Controls

From a network security perspective, the Standard Security Domain is equivalent to the End-User Security Plane of the ITU-T X.805 Recommendation.[189] The plane addresses security of access and use of the blockchain network by network members. The End-User Security Plane represents actual end-user data flows. In addition, to the PKI-based verifiable identities that MSPs turn into the members of a blockchain network, you should ensure that:

188 Olson, T., *2018a*.
189 ITU, 2003.

- In accordance with Business Driver 7[190] (BD7 in Section 3), user access is limited to the specific applications or systems they require to perform routine, legitimate business activities.
- Outbound access to untrusted domains, such as the Internet and competitor organizations, is controlled using boundary devices in the Domain, the external services Interconnect, or the DMZ.
- Boundary devices and the external services Interconnect restrict outbound connectivity to third parties to specific destination IP ranges, IP addresses and ports.
- Third parties are not permitted direct access to the Domain. Rather use boundary devices in the Domain, the external services Interconnect, or the DMZ to ensure that only specified third-party applications and systems with legitimate business reasons connect to the Domain.
- Systems within the Standard Security Domain must either rely on authentication services within high security networks in the High and Enhanced domains, or a secure local database.
- In common with other Domains, your expected security outcomes will dictate the controls to use.

8.6.2 Blockchain Runtime

Blockchain runtime deals with the service level requirements which a Fabric system, or parts of the system, must meet. Runtime properties include availability, capacity, performance, and sometimes security. The blockchain runtime environment inherits the security controls in higher security domains. For example, systems within the Standard Security Domain use authentication services hosted within the High and Enhanced Domains. As outlined in *Figure 6 – End-to-End Fabric Reference Security Architecture*, runtime components include the following below.

8.6.2.1 Ledger

According to Hyperledger documentation, a ledger provides a verifiable history of all successful state changes (i.e., valid transactions) and unsuccessful attempts to change state (i.e., invalid transactions), that occurred during the operation of the system.[191] A ledger stores information about business objects, both the current value of the object attributes and the transaction history that resulted in the current values. In Fabric blockchain, a ledger consists of two distinct, though related, parts: a world state, and a blockchain.[192] Ledgers utilize cryptographic mechanisms, such as digital signatures and hash functions, to support tamper-evident and tamper-resistant features. A ledger is only as trusted as the cryptographic mechanisms upon which it relies to manage transactions. Therefore, *Section 8.4.1 – Cryptography Services* is crucial to ledger security. As noted above, business requirements could mandate that private transactions protect against information disclosure by delivering data only to selected nodes.

190 BD7: Ensuring that blockchain network/DLT system users are only granted authorized access in accordance with good security principles, such as Need-to-Know, Least Privilege, etc.

191 Fabric Architecture Origins: https://hyperledger-fabric.readthedocs.io/en/release-1.4/arch-deep-dive.html

192 Fabric Ledger: https://hyperledger-fabric.readthedocs.io/en/release-2.2/ledger/ledger.html

8.6.2.2 Smart Contract / Chaincode

A Chaincode handles business logic agreed to by members of the network, so it may be considered as a "smart contract." According to the Fabric Glossary, Chaincodes fall into three categories: Public, Confidential or Access-Controlled.[193] Public Chaincodes are deployed by public transactions and can be invoked by any member of the network. In contrast, Confidential Chaincodes are deployed by confidential transactions and can only be invoked by validating members of the network i.e., Chain Validators. Lastly, Access-Controlled Chaincodes are deployed by confidential transactions that also embed the tokens of approved invokers. Additionally, the Access Controlled Chaincode invokers are allowed to invoke confidential Chaincodes even though they are not validators.

8.6.2.3 Peer Node

According to Hyperledger documentation, a Peer is a node that commits transactions and maintains the state and a copy of the ledger.[194] Peer nodes host a ledger and multiple Chaincodes. Community peers enable the sharing of a ledger by multiple transacting organizations. In the Reference Security Architecture diagram, we use the formulation "Peer Node1" to indicate that Trust Anchor organizations use multiple Peers to meet the service levels (i.e., runtime requirements) that the Fabric blockchain must meet. As we noted in *Section 4.2 – Fabric Key Users and Interfaces*, Fabric contains the following types of peer nodes:

8.6.2.3.1 Non-Validating Node (Peer)

The Non-Validating Node (Peer) is primarily responsible for constructing transactions and forwarding them to the Validating Nodes. The Peer's main roles is to:

- Manage and maintain user certificates issued by the membership service.
- Construct transactions and forward them to Validating Nodes.
- Keep a local copy of the ledger and allow application owners to query information locally.

Solution Providers or Network Auditor blockchain participants own the Non-Validating Node.

8.6.2.3.2 Validating Node (Peer)

The Validating Node (Peer) is responsible for creating and validating transactions and maintaining the state of Chaincodes. The Peer's main roles are to:

- Manage and maintain user certificates issued by membership service.
- Create transactions.
- Execute and validate transactions with other Validating Nodes on the network.
- Maintain a local copy of ledger.
- Participate in consensus and update of the ledger.

Network Proprietor and Solution Provider (if they belong to the same entity) own the node.

193 Fabric Glossary: https://fabric-docs-test.readthedocs.io/en/latest/glossary/

194 Fabric Architecture Origins: https://hyperledger-fabric.readthedocs.io/en/release-1.4/arch-deep-dive.html

8.6.2.4 Local MSP

We recommended earlier that you should host Channel MSPs within the Enhanced Security Domain because they define administrative and participatory rights at the channel level. Conversely, local MSPs are defined for clients and for nodes, i.e., Peers and Orderers. Given that local MSPs define the permissions for a node, they should be hosted in the blockchain runtime zone of the Standard Domain. Physically and logically, there is only one local MSP per node. A channel MSP is present on the file system of every node in the channel and is synchronized via consensus. Logically, it resides on and is maintained by the channel or the network.

8.6.2.5 Fabric SDK / CA Client

We noted above that the default MSP implementation uses X.509 certificates as identities. CAs issue identities by generating public and private keys which form a keypair that the MSP uses to prove the identity of network components, such as Peers. Therefore, blockchain network components require a secure mechanism for interacting with the CAs. As illustrated in *Figure 7 – Hyperledger Fabric CA server*, interactions with the Fabric CA server could be via either the Fabric CA client or through one of the Fabric SDKs. We have recommended that production Fabric solutions should use HSMs to allow peers and ordering nodes to sign and endorse transactions without exposing their private keys. Fabric blockchain currently interacts with HSMs over a PKCS #11 interface. Fortunately, most commercial HSMs support the use of RSA's PKCS #11 Cryptographic Token Interface to create, store and use cryptographic objects.

8.6.3 Business Applications

Blockchain technology offers the opportunity to re-invent and streamline business processes across various industries to save time, save money, and reduce risk.[195] Hence, new business applications are essential to realizing blockchain's benefits.

For example, in the IBM Blockchain Platform and competitor platforms such as Azure Blockchain Workbench, and Amazon Managed Blockchain, this tier of architecture implements the user application logic that provides the business APIs.

8.6.3.1 User Application

As discussed in *Section 8.4.3 – Enterprise Systems*, the High Security Domain hosts systems that manage the most sensitive business information. User applications bring together enterprise applications and blockchain functionality to provide transformative business logic. Users access blockchain functionality through a blockchain SDK for the relevant programming languages.

For example, Fabric functionality is currently offered via Node.js and Java SDKs. The Linux Foundation plans to support Python, REST, and Go SDKs in a later Fabric release.

195 Hyperledger, 2018b.

8.6.3.2 Application Server

The application server provides the resources, data, services, or programs for an application that uses blockchain resources. According to IBM Blockchain Reference Architecture, different application servers provide varying levels of functionality, ranging from lightweight web serving to comprehensive resource management. Additionally, the programming language chosen can often influence the application server. Potential application server products include Node.js, Quarkus, IBM WebSphere Liberty, Nginx, and Tomcat JBoss (WildFly).

8.6.3.3 Application Programming Interface (API)

A well-defined set of APIs enables customers to access the Fabric infrastructure quickly and easily. For example, applications that provide services through a web API are widely portable because they abstract technical details, such as programming language and application server technology. Representational state transfer (REST) is the preferred architectural style for APIs that use HTTP requests to access and use data because its low bandwidth needs make it more suitable for efficient internet usage. Swagger and gRPC are the other API options.

8.6.4 Ordering Service Organizations

Unlike permissionless blockchains, such as Ethereum and Bitcoin, the Fabric architecture contains a specialized node called an Orderer (it's also known as an "Ordering Node") that is responsible for transaction ordering. The Ordering Service Organization owns the Ordering Nodes that constitute the Ordering Service. The role is distinct from a transacting or trust anchor organization role. In *Figure 6 – End-to-End Fabric Reference Security Architecture*, we logically separated the Trust Anchor and Ordering Service entities to underline the importance of protecting the block formation and distribution process from security attack. The Ordering Service is usually part of the same real-world organization as a Trust Anchor, however. We depict one Ordering Service organization for brevity. Networks define two or more organizations to offer sufficient decentralization of transaction packaging and distribution.

8.6.4.1 Cryptography

We noted above that, typically, the Ordering Service is part of the same real-world organization as a Trust Anchor. Hence, the Ordering Service will use the same cryptography service as the Trust Anchor Organization if it is part of the same entity. *Section 8.4.1 – Cryptography Services* described the security controls that can prevent the unauthorized disclosure, modification, substitution and use of secret keys, private keys, or secret metadata for the Ordering Nodes.

8.6.4.2 Ordering Nodes

In a similar way to miners in permissionless blockchains, Orderers package transactions into blocks for distribution to peers. In turn, peers add the transactions to the ledger. Orderers do not validate the transactions, however. Validation is delegated to Trust Anchors and endorsement policies. According to Hyperledger documentation, "every chaincode has an endorsement policy which specifies the set of peers on a channel that must execute chaincode and endorse the execution

results in order for the transaction to be considered valid."[196] The endorsement policies define the organizations (through their Peers) that must "endorse" (i.e., approve) the execution of a proposal. A configuration of five Ordering Nodes across three distinct physical sites can help to create a resilient ordering service. In Figure 6, we depicted 1 of 3 sites for conciseness. Organizations could use larger configurations to meet resilience requirements. Even if the Ordering Service and Trust Anchor belong to the same real-life organization, there must be security controls to enable the secure distribution of fully formed blocks for inclusion on their Peer's copy of the ledger. In Figure 6, the Interconnected enforces separation and security.

8.6.4.2.1 Raft Protocol versus Apache Kafka

Fabric networks use the Raft consensus protocol to coordinate block formation and distribution by nodes. Raft follows a "leader and follower" model, where a leader node is elected (per channel) and its decisions are replicated by the followers. Apache Kafka is an alternative to Raft. Kafka-based ordering services have been available since Fabric v1.0. In common with the Raft Protocol, Apache Kafka is a crash fault tolerant (CFT) implementation that uses a "leader and follower" node configuration. Kafka utilizes a ZooKeeper ensemble for management purposes. The Hyperledger project cautions that deploying Kafka is complicated and requires high-level expertise. Kafka also has more components to manage than Raft and, thus, more potential areas of security exposure. Furthermore, whilst Kafka versions must be coordinated with the Orderers, Raft embeds all features within the ordering node. Hence, we exclude Kafka-based ordering services, which are deprecated in Fabric v2.x, as, "Many users may find the additional administrative overhead of managing a Kafka cluster intimidating or undesirable."[197]

8.7 Restricted Security Domain

As a permissioned blockchain, the Trust Anchor enforces Business Driver 4 (BD4) in *Section 3.2.1 - Business Drivers for Security* which requires that all users of the blockchain network are fully identified, authenticated, authorized and their transactions fully auditable. For example, Trust Anchors can add or remove publishing nodes from the Fabric blockchain network. The Trust Anchor's actions could be supported by legal contracts in place for the network users.[198] Thus, the Restricted Domain should have controls capable of thwarting threat actors with substantial IT knowledge but neither the capability nor the resources to implement advanced attacks.

8.7.1 Network Security Controls

The Restricted Domain is a subset of the Standard Security Domain because, in common with the latter, it seeks to protect the community of users that comprise a Fabric business blockchain network. Hence, from a network security perspective, the Restricted Security Domain should also be governed by rules of the end-user security plane of the ITU-T X.805 Recommendation.[199] Therefore, we recommend that you ensure:

196 Endorsement policies: https://hyperledger-fabric.readthedocs.io/en/release-2.2/endorsement-policies.html

197 Orderers: https://hyperledger-fabric.readthedocs.io/en/release-2.2/orderer/ordering_service.html?highlight=Raft%20Protocol#raft

198 Yaga, D., et al., *2018.*

199 ITU, 2003.

- As illustrated in Figure 6, the Domain has in-line firewalls to protect the Trust Anchor organization from external networks and components, including Ordering Services (if part of a separate real-life organization), Transacting Organizations, and cloud environments.
- The Domain does not permit direct connectivity from the Internet or external blockchain network participants to services beyond the Trust Anchor's blockchain runtime environment.
- The Blockchain Runtime layer is isolated from external networks using protocol termination. Traffic is stopped on the external interface of the firewalls in the Interconnect or DMZ before a new session is initiated on the internal interface.
- Network ingress and egress traffic goes through physical interfaces of firewalls in the Interconnect.
- Interconnect or DMZ firewalls only permit limited access to the blockchain services required.
- In line with higher security Domains, security outcomes should dictate controls.

8.7.2 Blockchain Interconnect

As illustrated in Figure 6, the Blockchain Interconnect serves as a central connection point for routing traffic to blockchain network participants and external services, such as public cloud environments. The Interconnect offers a means for exposing blockchain runtime services in a secure and consistent manner. Indeed, as explained in *Section 8.7.1 – Network Security Controls* above, the Blockchain Interconnect implements the security measures that prevent blockchain network and component compromise, detects attacks, and mitigates the impact of any successful compromise. The security-enforcing devices in the Interconnect may include:

- Traffic management devices to handle allocated bandwidth, including ones that throttle in the event of Denial of Service (DOS) or Distributed Denial of Service (DDoS) attacks against the blockchain platform or on the smart contract implemented on the platform.[200]
- Firewalls to isolate the blockchain runtime environment from external network connections, and filter traffic by IP address and communication ports.
- Load balancers that perform code node validation by only accepting traffic from predefined source IPs and protocol type.
- VPN gateways could perform security functions, such as user validation, protocol termination, content inspection, and audit logging.
- Network Intrusion Prevention Systems (NIPS) that inspect traffic for threats to confidentiality and integrity, contribute to DOS/DDoS defenses, and prevent unauthorized usage.
- Anti-malware engine to stop viruses, trojans, worms, and other forms of malicious code, including zero-day attacks.

The Trust Anchor organization should own the Blockchain Interconnect because it helps enforce the network policy that determines the access rights of each component to network resources.

200 Yaga, D., et al., 2018.

8.7.3 Corporate Demilitarized Zone (DMZ)

The DMZ (also known as a boundary network) separates a trusted private network from potential attacks originating from untrusted external networks, such as the Internet. The DMZ should only host systems that require direct connectivity to the Internet. Based on requirements, a tiered DMZ architecture may be used for Internet-facing segments. The DMZ may contain devices, such as routers, switches, firewalls, DNS appliances, load balancers, Network Intrusion Prevention Systems (NIPS), proxy servers, and remote access gateways. The devices prevent system and application compromise, detect attacks, and mitigate the impact of any successful compromise. As depicted in Figure 6, user access to blockchain APIs must transit via the DMZ.

8.8 External Security Domain

As a permissioned blockchain network, Fabric blockchain participants could arguably be hosted within the Restricted Domain. Given our focus on the use of blockchain technology in critical sectors, we position blockchain participants in this Domain because external users are typically outside the Accreditation Scope of a national security system or network.[201] We assume that the Threat Actors targeting the Domain would have some IT knowledge and resources to launch opportunistic attacks using free malware. The security measures in this Domain should be adequate to deter Threat Actors that are resourced to attack the blockchain network part time.

8.8.1 Network Security Controls

As depicted in Figure 6, any network access or data exchange to or from external networks should go through the Restricted Security Domain. As such, entities in the External Security Domain should rely on the security provided by access points in the Blockchain Interconnect and corporate DMZ. The Interconnect should support blockchain participants, such as Ordering Service Organizations (if part of a separate real-world organization), Transacting Organizations (if not part of the Trust Anchor organization) and cloud platforms. The DMZ enables external users over web and mobile devices to access blockchain functionality via business APIs.

8.8.2 Trust Anchor – Cloud Platform

Figure 6 – End-to-End Fabric Reference Security Architecture depicts a hybrid cloud deployment model because cloud computing offers potential benefits, such as reduced capital expenses, agility, redundancy, high availability, and resiliency.[202] Typically, regulatory and security accreditation regimes require that SoR hosting mission-critical data are hosted on secure on-premises infrastructure. Therefore, a hybrid cloud deployment model offers the most plausible approach for using blockchain technology in critical sectors.

201 The Glossary defines the concept of an accreditation scope.

202 Mogull, R., et al., 2017.

8.8.2.1 Cloud Infrastructure

The CSA has chronicled the top threats to cloud computing[203,204] over many years. We highlight *Security Issue 3: Lack of Cloud Security Architecture and Strategy* because of its relevance to blockchain technology adoption. The quest for "functionality and speed" often takes precedence over the need to devise and implement a security architecture that could withstand cyberattacks[205] against cloud and blockchain platforms. Additionally, given that blockchain networks and public cloud environments are both shared platforms, organizations should understand and carefully apply the relevant shared security responsibility model. Organizations require a unified Target Operating Model (TOM) for blockchain governance, delivery and assurance activities. Indeed, a TOM is vital for compliance with shared responsibility models.

8.8.2.1.1 Compute, Storage and Network

Cloud computing platforms can deliver cost-effective and resilient compute, storage, and network resources for an organization's blockchain components. Organizations could procure the requisite cloud resources and perform all the necessary security configuration and management tasks as part of an Infrastructure-as-a-Service (IaaS) contract. Alternatively, organizations could take advantage of Blockchain-as-a-Service (BaaS) solutions from companies, such as IBM, Amazon, Microsoft, Oracle, SalesForce, Alibaba, and Baidu. BaaS solutions provide purpose-built tools for specific needs and fully managed blockchain networks.

8.8.2.1.2 Containers

Cloud container platforms package compute, storage, and network resources. Containers provide a virtualization environment with resources, such as operating systems, peers, CAs, ordering nodes, and their dependencies. Containers should be Open Container Initiative (OCI)-compliant.[206] For example, the entire Hyperledger stack could be in a Docker container. Tomasz Klim provides a configuration guide for containerized Fabric components.[207] The guide covers the configuration of a Kafka-based ordering service, which, as we noted above, was deprecated in Fabric v2.x. The components in a container are cloud platform agnostic because they communicate with each through web APIs that are based on REST or gRPC.

8.8.2.1.3 Kubernetes

Kubernetes, also known as K8s, is an open-source system for automating the deployment, scaling, and management of containerized applications. A Kubernetes cluster can ensure that containerized applications, smart contracts, and blockchain network components use compute, network, and storage infrastructure nodes efficiently. The Kubernetes API can be extended to support the management of blockchain components. Common technologies include Red Hat OpenShift Container Platform and Rancher.

203 Bhat, S., et al., 2020.
204 Brook, J.-M.C., et al., *2019.*
205 Brook, J.-M.C., et al., *2019.*
206 The Open Container Initiative: https://opencontainers.org/
207 Hyperledger Fabric security practical guide: https://espeoblockchain.com/blog/a-practical-guide-to-hyperledger-fabric-security#4

8.8.2.2 Fabric SDK / CA Client

The cloud environment must obtain X.509 certificates for the MSP to prove identity of network components. Given that the cloud environment is an extension of the Trust Anchor's environment, certificates could be issued by the intermediate CA as defined in *Section 8.5.2.1.1 – Networked HSMs for Intermediate CA*. The on-premises CA should also integrate with cloud-native certificate services, such as Amazon Certificate Manager (ACM), and Azure Key Vault, Google Cloud Platform Certificate Authority Service, to facilitate automation of the certificate lifecycle management.

8.8.3 Transacting Organization(s)

Transacting organizations are a community of users that consume blockchain services. The organizations own the application components that use blockchain services by querying the shared ledger, submitting new transactions, or listening for notifications. The Trust Anchor Organization owns the ledger and Chaincode. Given that Fabric is a permissioned blockchain network, the applications must use the identity associated with a specific role within an organization to complete an operation. The Fabric MSP uses Organizational Units (OUs) to assign different units specific responsibilities or affiliations. A special kind of OU (i.e., Node OU), can be used to confer a role to an entity, e.g., client, peer, admin, or orderer.

8.8.3.1 Cryptography

We noted throughout this paper that the default MSP implementation in Fabric uses X.509 certificates as identities. MSPs turn verifiable identities into members of a blockchain network. MSP roles can be distinguished by the OU present in the CommonName attribute of the X.509 certificate. The Node OU roles for the MSP could appear in certificates as OU=client for a client role or OU=peer for a peer role. Roles and OU attributes are assigned during the certification issuance process. We recommended that production Fabric solutions use a commercial PKI rather than Fabric CA. Hence, in line with *RFC 5280 – Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*, CAs will verify the suitability of certificate names unless otherwise stated in the Certificate Policy.

8.8.3.2 Local MSP

As outlined in *Section 8.6.2.4 – Local Peer MSP*, local MSPs are only defined on the file system of the node or user to which they apply. Local MSPs of Transacting Organizations allow the entity to authenticate itself in its transactions as a member of a channel e.g., in Chaincode transactions. In addition, the local MSP allows Transacting Organizations to claim ownership of a specific role, such as an organization admin. Every node must have a local MSP defined because it defines who has administrative or participatory rights at that level. Thus, the local MSPs facilitate the authentication of member messages outside the context of a channel and define permissions over a particular node, for example the ability to install Chaincode on a Peer.

8.8.3.3 Transformation and Connectivity

Transformation and connectivity services provide secure connectivity between blockchain and data/applications running on-premises or in cloud environments. For example, in the IBM Blockchain Platform, integration technology, such as message brokers, can act as proxies that present blockchain services to application customers via a business API. In addition, integration technologies can transform blockchain data for use by other enterprise systems.

8.8.3.4 ERP System

As outlined in *Section 8.4.3.1 – Enterprise Resource Planning (ERP) System*, ERPs create and maintain critical business and customer data that ends up in enterprise data stores and blockchain ledgers. ERPs may provide an API that enables business applications to consume blockchain services. Therefore, proportionate security controls must be in place to ensure that the ERP's interactions with the blockchain ledger do not expose mission-critical data.

8.8.3.5 Automation Tools

Section 8.5.2.1.4 – Automation Tools discusses the role automation tools play in the timely delivery of blockchain services and the identification of critical software faults. Transacting Organizations should use automation tools to ensure the secure and timely deployment of blockchain network components. For example, the tools could enable the rapid deployment of business functionality by packaging blockchain technology with applications and databases.

8.8.4 External: Presentation

The presentation layer focuses on enabling users to access blockchain-based functionality without the need for middlemen, which, as we noted above, saves time and cuts costs. Typically, the layer does not interact with blockchain directly. As discussed in *Section 8.6.3.3 – Application Programming Interface (API)*, web APIs abstract technical details from end users.

8.8.4.1 Web Users

Web users access business functionality through APIs using a browser-based interface from popular browsers, such as Google Chrome, Firefox, and Microsoft Edge. According to IBM, web interfaces could use web technologies, such as React Library or Angular framework.

8.8.4.2 Mobile Users

Users utilize mobile-based interfaces from popular operating systems, such as iOS and Android, to access application functionality through business APIs. Unlike browser technologies, services to mobile platforms typically require modification to accommodate a smaller screen size.

8.9 Conclusion

Blockchain technology offers unlimited opportunity to re-invent and streamline business processes across various industries to save time, save money, and reduce risk. However, organizations will only be able to use Fabric's immense potential if blockchain/DLT networks are trusted to interact securely with other networked devices and systems. Fabric is built on a strong security foundation because it relies on cryptography, distributed systems, and databases. Nevertheless, production Fabric solutions must operate within computer networks constrained by critical sector requirements, such as security accreditation and PCI DSS network segmentation. Additionally, public-key cryptography (PKC), a foundational blockchain component, is afflicted with a *compliance defect*: it lacks a centralized mechanism for enforcing the user discipline it relies on to operate securely. If implemented correctly, personnel, physical, procedural, and technical security controls could help to mitigate the compliance defect.

As of this writing, blockchain technology's biggest challenge is the reputational damage caused by the involvement of cryptocurrencies in ransomware payments, and associated money laundering activities. Ransomware attacks have dissipated the once rising institutional and regulatory comfort with blockchain technology. In Section 5, *The Wall Street Journal* quotes US Government officials as describing ransomware, "as an urgent national-security threat." Indeed, strident voices in the cybersecurity community have called for an approach that targets the ransomware criminals' operations: their personnel, infrastructure, and money.[208] The US Department of the Treasury's sanctioning of the SUEX crypto exchange for providing material support to the threat posed by criminal ransomware actors is an example of a tougher response.

In summary, it is clear that the rules that apply to Fabric PoCs are inadequate for live production in critical sectors. Hence, we have offered an example of a holistic approach that Fabric solution owners could use to demonstrate to stakeholders, such as regulators, that DLT risks have been adequately identified and managed and that the technical solutions are secure and meet regulatory and compliance needs of the business. We feel that the business-focused and risk-based approach described in this paper offers a sound basis for durable Fabric security.

208 America Is Being Held for Ransom. It Needs to Fight Back. https://www.nytimes.com/2021/09/20/opinion/ransomware-biden-russia.html

9. Glossary

To understand this paper, the following definitions apply.

Term	Definition
Accreditation Scope	An accreditation scope distinguishes information resources that must undergo a formal assessment from related or interconnected assets. Typically, the accreditation scope covers: (a) physical and logical assets external to and/or outside the control of an organization; (b) physical and logical assets controlled or contracted by the organization but outside the direct management and control of a secure project; (c) the physical and logical assets under the full management and control of a secure project, such as internal networks including production, disaster recovery, etc.
Authenticity	The property of being genuine and being able to be verified and trusted, confidence in the validity of a transmission, a message, or message originator. Source: https://csrc.nist.gov/glossary/term/authenticity
Blockchain	A distributed ledger with confirmed blocks organized in an append-only, sequential chain using cryptographic links. **Note 1:** Blockchains are designed to be tamper resistant and to create final, definitive, and immutable ledger records. Source: *ISO 22739:2020 - Blockchain and distributed ledger technologies — Vocabulary.*
Consensus	Agreement among DLT nodes that 1) a transaction is validated and 2) that the distributed ledger contains a consistent set and ordering of validated transactions. **Note 1:** Consensus does not necessarily mean that all DLT nodes agree. **Note 2:** The details regarding consensus differ among DLT designs and this is a distinguishing characteristic between one design and another. Source: *ISO 22739:2020 - Blockchain and distributed ledger technologies — Vocabulary.*
Cryptoasset or crypto-asset	Broadly, a cryptoasset is a cryptographically-secured digital representation of value or contractual rights that uses some type of Distributed Ledger Technology (DLT) and can be transferred, stored, or traded electronically. Source: https://www.gov.uk/government/publications/cryptoassets-taskforce

Term	Definition
Cryptocurrency	Crypto-asset designed to work as a medium of value exchange. **Note 1:** Cryptocurrency involves the use of decentralized control and cryptography to secure transactions, control the creation of additional assets, and verify the transfer of assets. Source: *ISO 22739:2020 - Blockchain and distributed ledger technologies — Vocabulary.*
Decentralized System	Distributed system wherein control is distributed among the persons or organizations participating in the operation of the system **Note 1:** In a decentralized system, the distribution of control among persons or organizations participating in the system is determined by the system's design. Source: *ISO 22739:2020 - Blockchain and distributed ledger technologies — Vocabulary.*
Digital Asset	A digital representation of value which can be used for payment or investment purposes. This does not include digital representations of fiat currencies. Source: https://www.fsb.org/wp-content/uploads/P131020-3.pdf
Distributed Ledger	A ledger that is shared across a set of DLT nodes and synchronized between the DLT nodes using a consensus mechanism. **Note 1:** A distributed ledger is designed to be tamper resistant, append-only, and immutable containing confirmed and validated transactions. Source: *ISO 22739:2020 - Blockchain and distributed ledger technologies — Vocabulary.*
Distributed Ledger Technology (DLT)	A technology that enables the operation and use of distributed ledgers. Source: *ISO 22739:2020 - Blockchain and distributed ledger technologies — Vocabulary.*
DLT Network	A network of DLT nodes which make up a DLT system. Source: *ISO 22739:2020 - Blockchain and distributed ledger technologies — Vocabulary.*
DLT Node	Is a <distributed ledger technology> device or process that participates in a network and stores a complete or partial replica of the ledger records. Source: *ISO 22739:2020 - Blockchain and distributed ledger technologies — Vocabulary.*

Term	Definition
DLT Platform	A set of processing, storage and communication entities which together provide the capabilities of the DLT system on each DLT node. Source: *ISO 22739:2020 - Blockchain and distributed ledger technologies — Vocabulary.*
DLT System	A system that implements a distributed ledger. Source: *ISO 22739:2020 - Blockchain and distributed ledger technologies — Vocabulary.*
DLT User	An entity that uses services provided by a DLT system. **Note 1:** An entity is an item inside or outside an information and communication technology system, such as a person, an organization, a device, a subsystem, or a group of such items that has recognizably distinct existence. Source: *ISO 22739:2020 - Blockchain and distributed ledger technologies — Vocabulary.*
Genesis Block	First block in a blockchain. **Note 1:** A genesis block has no previous block and serves to initialize the blockchain. Source: *ISO 22739:2020 - Blockchain and distributed ledger technologies — Vocabulary.*
Global stablecoin (GSC)	A stablecoin with a potential reach and adoption across multiple jurisdictions and the potential to achieve substantial volume. Source: https://www.fsb.org/wp-content/uploads/P131020-3.pdf
Hard Fork	A Change to a DLT platform in which new ledger records or blocks created by the DLT nodes using the new version of the DLT platform are not accepted as valid by DLT nodes using old versions of the DLT platform. **Note 1:** If not adopted by all DLT nodes, a hard fork can result in a ledger split. **Note 2:** In some contexts, the terms “hard fork” and “fork” are sometimes used for a ledger split that results from a hard fork of a DLT platform. Source: *ISO 22739:2020 - Blockchain and distributed ledger technologies — Vocabulary.*

Term	Definition
Immutability	Property wherein ledger records cannot be modified or removed once added to a distributed ledger. **Note 1:** Where appropriate, immutability also presumes keeping intact the order of ledger records and the links between the ledger records. Source: *ISO 22739:2020 - Blockchain and distributed ledger technologies — Vocabulary.*
Majority Attack	A Majority Attack is a blockchain attack where an attacker can gain back the coins from a transaction from the merchant by forking the blockchain and getting the majority of confirmations. Source: https://en.bitcoin.it/wiki/Majority_attack
Time-jacking Attack	Time-jacking is an attack mode against a timestamp's vulnerability. The attacker can change the target node's network time and deceive it into accepting an alternate blockchain by announcing an inaccurate timestamp. A time-jacking attack is mainly aimed at the vulnerability of timestamps in the Bitcoin system. Source: https://link.springer.com/article/10.1007/s12083-020-00905-6
Stablecoin (or coin)	A crypto-asset that aims to maintain a stable value relative to a specified asset, or a pool or basket of assets. Source: https://www.fsb.org/wp-content/uploads/P131020-3.pdf
Stablecoin Arrangement	An arrangement that combines a range of functions (and the related specific activities) to provide an instrument that purports to be used as a means of payment and/or store of value. Source: https://www.fsb.org/wp-content/uploads/P131020-3.pdf
Smart Contract	Computer program stored in a DLT system wherein the outcome of any execution of the program is recorded on the distributed ledger. Source: *ISO 22739:2020 - Blockchain and distributed ledger technologies — Vocabulary.*
Wallet	Application used to generate, manage, store, or use private and public keys. **Note 1:** A wallet can be implemented as a software or hardware module. Source: *ISO 22739:2020 - Blockchain and distributed ledger technologies — Vocabulary.*

10. References

Almashaqbeh, G., A. Bishop, and J. Cappos. *ABC: A Cryptocurrency-Focused Threat Modeling Framework,* in IEEE INFOCOM 2019 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), 29 April-2 May 2019. 2019. Paris, France: IEEE.

ASC.X9, *ASC X9 IR 01-2019: Informative Report - Quantum Computing Risks To The Financial Services Industry.* 2019, ASC X9 Quantum Computing Risk Study Group: Annapolis, MD, USA. p. 1-50.

Barker, E., *NIST SP 800-57, Part 1, REV. 5 - Recommendation for Key Management Part 1 – General*. 2020, National Institute of Standards and Technology (NIST) Gaithersburg, Maryland, USA.

Barrett, M.P., *Framework for Improving Critical Infrastructure Cybersecurity.* 2018, National Institute of Standards and Technology (NIST): Gaithersburg, Maryland, USA.

Bhat, S., et al., *Top Threats to Cloud Computing: Egregious Eleven Deep Dive*. 2020, Cloud Security Alliance (CSA): Seattle, Washington, United States. p. 1-30.

Brook, J.-M.C., et al., *Top Threats to Cloud Computing: The Egregious 11*. 2019, Cloud Security Alliance (CSA): Seattle, Washington, United States. p. 1-41.

Chen, L., et al., *NISTIR 8105 - Report on Post-Quantum Cryptography.* 2016, National Institute of Standards and Technology (NIST) Gaithersburg, Maryland, USA.

Davis, D., *Compliance defects in Public Key Cryptography.* 1996, Cambridge, Massachusetts: MIT.

Diffie, W. and M. Hellman, *New Directions in Cryptography.* IEEE Transactions on Information Theory, 1976. IT-22(6): p. 644-654.

DTCC, *Embracing Disruption – Tapping the Potential of Distributed Ledgers to Improve the Post-Trade Landscape*. 2016, Depository Trust & Clearing Corporation (DTCC): New York, United States.

ETSI, *DTR/CYBER-QSC-0013 - CYBER: Migration strategies and recommendations to Quantum Safe schemes,* in ETSI TR 103 619 V1.1.1. 2020, European Telecommunications Standards Institute (ETSI): Sophia Antipolis Cedex, France.

Fnality, *The Fnality Narrative Q3 2020*. 2020, Fnality International: London, UK.

HMT, *Cryptoassets Taskforce: Final Report.* 2018, HM Treasury, Financial Conduct Authority (FCA) and Bank of England: London, UK. p. 58.

Huttner, B., *Blockchains in the Quantum Era.* 2021, Cloud Security Alliance (CSA): Seattle, Washington, United States. p. 16.

Hyperledger, *The Hyperledger Vision: Blockchain 101*, Introducing Hyperledger, Industry Use Cases. 2018a, The Linux Foundation®: San Francisco, California, USA.

Hyperledger, *An Introduction to Hyperledger.* 2018b, The Linux Foundation®: San Francisco, California, USA.

ITU, ITU-T *Recommendation X.805: Security architecture for systems providing end-to-end communications,* in Series X: Data Networks and Open System Communications - Security. 2003, International Telecommunication Union (ITU): Geneva, Switzerland.

ITU, ITU-T *Recommendation X.1205: Overview of Cybersecurity,* in Series X: Data Networks, and Open System Communications and Security. 2008, International Telecommunication Union (ITU): Geneva, Switzerland.

Khemissa, S. and M. Roza, *Documentation of Relevant Distributed Ledger Technology and Blockchain Use Cases v2.* 2019, Cloud Security Alliance (CSA): Seattle, Washington, United States. p. 17.

Klim, T., *A practical guide to Hyperledger Fabric security.* 2020, Espeo Blockchain: Poznań, Poland.

Laurie, R., *SW101 – SABSA Applied to Top-Secret Classified Information,* in SABSA at Work™. 2018, The SABSA Institute C.I.C: East Sussex, UK. p. 13.

Liu, F., et al., *NIST Special Publication 500-292 NIST Cloud Computing Reference Architecture*. 2011, National Institute of Standards and Technology (NIST) Gaithersburg, Maryland, United States.

Mogull, R., et al., *Security Guidance for Critical Areas of Focus in Cloud Computing v4.0*. 2017, Cloud Security Alliance (CSA): Seattle, Washington, United States. p. 1-152.

NCSC, *Preparing for Quantum-Safe Cryptography.* 2020, National Cyber Security Centre (NCSC): London, UK.

NIST, *NIST SP 800-30 Rev. 1 - Guide for Conducting Risk Assessments.* 2012, National Institute of Standards and Technology (NIST) Gaithersburg, Maryland, USA.

Olson, T., *Blockchain as a cross-domain security solution.* 2018a, IBM: Somers, New York, USA.

Olson, T., *Securing your cross-domain file transfers with blockchain.* 2018b, IBM: Somers, New York, USA.

Olson, T., *Mapping cross-domain security requirements to blockchain*. 2018c, IBM: Somers, New York, USA.

PCI-SSC, *Information Supplement: PCI SSC Cloud Computing Guidelines.* 2018, Cloud Special Interest Group - PCI Security Standards Council (PCI SSC): Wakefield, MA, United States.

SABSA® and TOGAF®, *TSI R100 - Security Services Catalogue.* 2018, Security Services Project Working Group, Jointly Sponsored by The SABSA Institute and The Open Group: London, UK and San Francisco, CA. p. 1-36.

Shostack, A., *Threat Modeling: Designing for Security*. 2014, Boulevard, Indianapolis, Indiana, USA: John Wiley & Sons, Inc.

TOGAF® and SABSA®, *TOGAF® and SABSA® Integration: How SABSA and TOGAF complement each other to create better architectures.* 2011, The Open Group and the SABSA Institute: San Francisco, CA and London, UK. p. 1-58.

Wamala, F., *ITU National Cybersecurity Strategy Guide.* 2011, Geneva, Switzerland: International Telecommunication Union (ITU).

WEF, *Digital Assets, Distributed Ledger Technology and the Future of Capital Markets in Insight Report.* 2021, World Economic Forum: Geneva, Switzerland.

Yaga, D., et al., *Blockchain Technology Overview.* 2018, National Institute of Standards and Technology (NIST) Interagency or Internal Report (IR) 8202: Gaithersburg, Maryland, United States.