OCTOBER 2024

THE SMART CONTRACT PRIMER

An Initial Overview of Smart Contract Implementation within Financial Services & Regulatory Solutions for Risk Management

Foreword

The future of the global digital ecosystem in financial services will be better served with a closer alignment of policymakers and market participants across jurisdictions on the proportionality of regulation that provides appropriate protections and promotes innovation. This Primer provides an introduction to what smart contracts are, how they are being implemented within financial services, and proposes how to apply existing legal and regulatory frameworks to help mitigate the risks of deploying this new digital technology.

Through this Primer, the central role smart contracts play in the future of digital financial services and the importance of role of the standardization of smart contracts has been clearly set out. This Primer also shares an extensive assessment how existing regulatory operational and technology-oriented risk management frameworks and guidance can be implemented to mitigate smart contract risk and how best practices across industry are already applying and adhering to these standards.

Policymakers and regulators can further support the industry's scaling of smart contract use cases by working with industry to support best practices, while also considering how to future proof legal and regulatory regimes for the broader digitization of financial services. Finally, key calls to action have been proposed for all market stakeholders to come together and work towards the coordinated the scaling of smart contracts to help achieve the network effects and benefits for the consumers of financial services.

As discussed throughout this Primer, the standards of existing regulatory frameworks, regulatory requirements, and oversight – together with specific application of smart contract mitigants recommended by GFMA and GDF members in this Primer – can be applied to manage smart contract risk. Together, these help to eliminate the need for special regimes to regulate smart contracts and/or duplicative or disproportionate requirements applicable to smart contracts.

As smart contracts continue to scale across jurisdictions, harmonizing approaches across markets will be a key and critical enabler to a future, globally interoperable DLT-based market with more consistent regulatory perimeters. The recommendations in this Primer aim to ensure that DLT-based innovation is be driven by responsible, regulated financial institutions implementing the appropriate standards expected of capital markets technology.

The members of GFMA and GDF support policymakers globally being guided by "technology-agnostic" regulatory principles and utilizing existing operational and technology risk management frameworks wherever possible in order to best avoid blanket technology-specific approaches which may hamper the evolution of digital financial markets. This will help to both protect market participants and promote responsible innovation, in particular with regard to smart contracts.

Adam Farkas
CEO, GFMA

Lawrence Wintermeyer
Executive Co-Chair, GDF

Contacts & Authors

Contacts

Allison Parent, GFMA
Executive Director
aparent@global.gfma.org

Charles DeSimone, SIFMA
Managing Director,
Deputy Head of Technology,
Operations, and BCP
cdesimone@sifma.org

Laurence Van Der Loo, ASIFMA
Director,
Technology and Operations
lvanderloo@asifma.org

Coen ter Wal, AFME
Director,
Technology and Operations
coen.terwal@afme.eu

Coco Chen, AFME
Associate Director
Technology and Operations
coco.chen@afme.eu

Elise Soucie, GDF
Executive Director
elise@gdf.io

Authors

John Salmon, Hogan Lovells
Partner and Co-Chair of Digital
Assets and Blockchain Practice
john.salmon@hoganlovells.com

Christina Wu, Hogan Lovells
Associate
christina.wu@hoganlovells.com

Alan Cohn, Steptoe
Partner
acohn@steptoe.com

Stephen A. Aschettino, Steptoe
Partner
saschettino@steptoe.com

Ryan Hayden, Steptoe
Of Counsel
rhayden@steptoe.com

I. EXECUTIVE SUMMARY

I. Executive Summary

This smart contract Primer (referred to henceforth as this "Primer") provides an initial overview of what smart contracts are, how they are being implemented within financial services and proposes how to apply existing legal and regulatory frameworks to mitigate risks from utilizing such technology. Developed by the members of Global Financial Markets Association ("GFMA") and Global Digital Finance ("GDF"), this Primer represents the broad perspectives of industry practitioners who are pioneering both research as well as the real-world implementation of distributed ledger technology ("DLT") and smart contracts within business models across the globe.

In May 2023, the GFMA together with Boston Consulting Group (BCG), Clifford Chance, and Cravath, Swaine & Moore LLP, published a seminal report, "The Impact of Distributed Ledger Technology in Global Capital Markets[1]" referred to henceforth as 'The DLT Report', which evaluates the opportunities and risks of DLT and DLT-based securities, and assesses the applicability of existing legal, regulatory, and risk management frameworks. Building upon the findings in this report, as well as the findings from GDF reports and technical programs, GFMA and GDF are partnering to provide this Primer as a next step towards supporting consistent and responsible implementation of smart contracts within capital markets infrastructure. This Primer does not intend to cover all uses of smart contracts, rather, it primarily assesses smart contract usage within the regulated financial services industry to identify best practices as a first step towards global interoperability of DLT and standardization of smart contracts.

Smart Contracts are a Key Concept for the Evolution of the Financial System

Smart contracts are fundamentally software code. The standardization and ledger interoperability of smart contracts will be critical factors in the digitization and evolution of financial services. Crucially, as DLT scaling is already underway across financial services, this Primer also sets out practical examples of best practices within the industry, including how existing regulation for operational and technology risk management can be utilized to mitigate risks. The best practices presented are technology-neutral and supportive of appropriate future-proof regulation.

As regulators globally are forming policy to govern smart contracts as a technical aspect of the ecosystem, it is essential that policymaking works towards appropriate outcomes that mitigate risks, while also encouraging innovation and the updating and improvement or transformation of existing processes where new, enhanced outcomes can be achieved with technology.

This Primer advocates that regulators need not start from scratch when building frameworks for smart contracts. Market participants clearly articulated through the course of the engagement on this Primer that similar to implementing other new technologies through the years (e.g., cloud) there are tried and tested methodologies in place for change management and technology transformation. As with any technology change management program, this Primer acknowledges that there will be some risks unique to smart contracts needing specific mitigations. **It is this Primer's aim, however, to discuss how both traditional technology risks and unique challenges are already being addressed, and can be comprehensively covered through existing regulatory frameworks, to support smart contract and DLT scaling in the financial services ecosystem in a compliant and responsible manner.**

[1] "Impact of Distributed Ledger Technology in Global Capital Markets", GFMA (2023). Available at: https://www.gfma.org/policies-resources/gfma-publishes-report-on-impact-of-dlt-in-global-capital-markets/

I. A. Scope

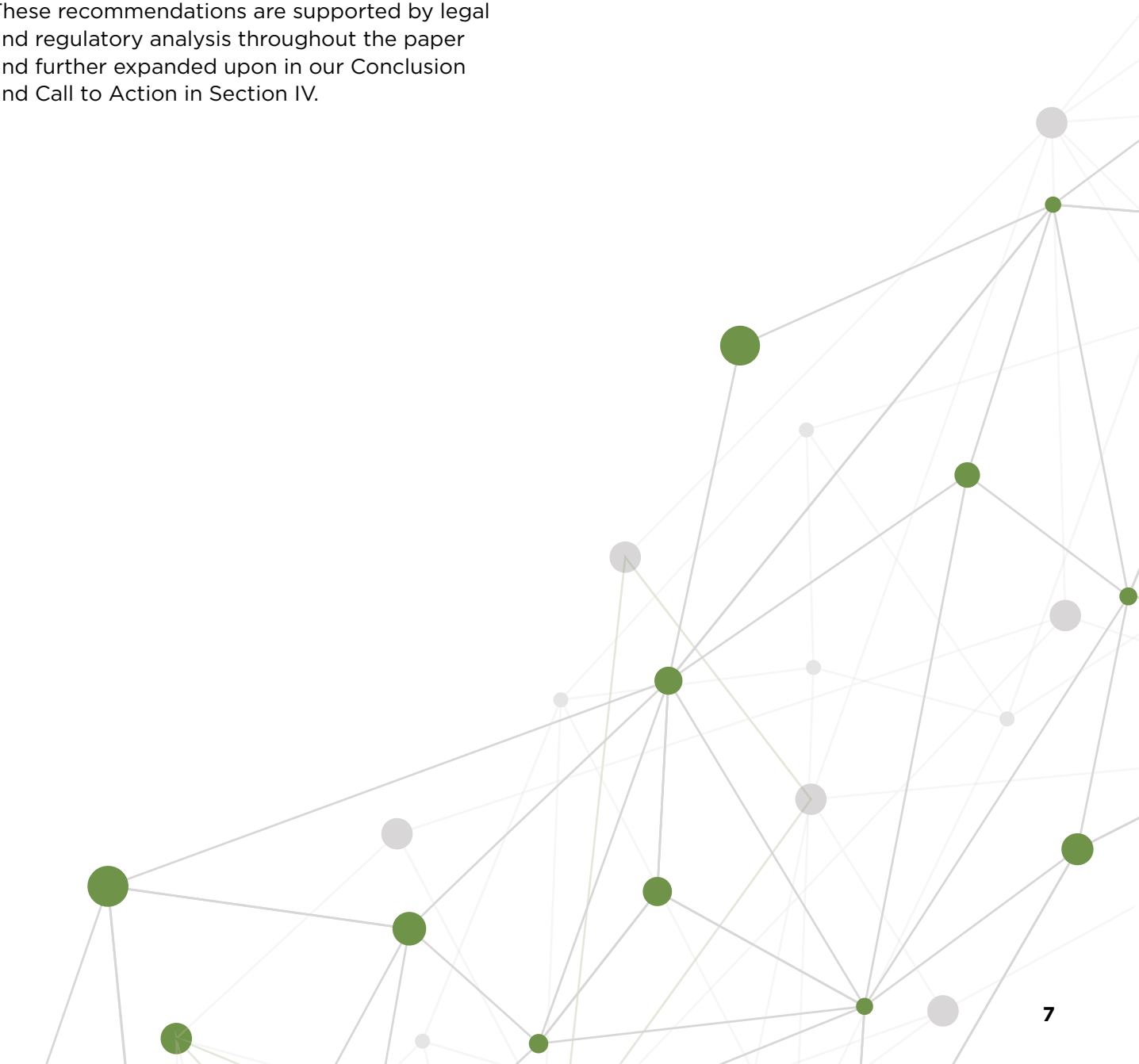
This Primer explores what smart contracts are and the role they play in scaling DLT within regulated financial services. It then proposes next steps for standardization and interoperability of smart contracts, as well as how regulators can utilize existing guidance and frameworks to mitigate risks. This Primer's key recommendations and findings are:

Recommendation #1: Prioritize key drivers of smart contract interoperability through technical standards and develop a template-based approach to smart contract standardization.

Recommendation #2: Support for utilization of existing technology and operational risk frameworks to regulate smart contract implementation.

Recommendation #3: Look to future-proof legal and regulatory regimes by providing clarity and support for responsible innovation, addressing where unique risks arise without creating special new regimes for smart contracts.

These recommendations are supported by legal and regulatory analysis throughout the paper and further expanded upon in our Conclusion and Call to Action in Section IV.



II. SMART CONTRACTS OVERVIEW AND THE CRITICALITY OF INTEROPERABILITY AND STANDARDIZATION

II. Smart Contracts Overview and the Criticality of Interoperability and Standardization

II. A. What is a Smart Contract & Why Does It Matter?

The term "smart contract" is now widely used across industry. Prior to commencing this Primer, the legal teams aimed to conduct a literature review of previous work done on this topic, and where relevant have been noted in the footnotes. Following this review, for the purposes of this Primer, the term "smart contract" is defined as:

software code that is designed to automatically execute upon the occurrence of predefined conditions, deployed within a distributed ledger technology environment, and may be executed within the context of a binding agreement between the counterparties of a transaction.

The role of smart contracts may vary, depending upon the context, and may include (among other things) enabling automation of operational processes, allowing for automated registration of securities ownership, and establishing the mechanisms needed to efficiently and effectively memorialize and effectuate the requisite mutual agreement necessary to arrive at binding contractual terms.

This definition was developed noting that this Primer's context largely refers to financial institutions implementing smart contracts for enhancing existing workflows via the broader transformation and scaling of DLT-based technologies and systems. This includes, for example, DLT-based recordkeeping, tokenization of regulated financial instruments, and DLT-based clearing and settlement, as opposed to its use in various decentralized finance (De-Fi) arrangements.[2] This Primer acknowledges that broader uses and definitions may be implemented and utilized elsewhere and that smart contracts are also widely used in public networks, but puts forward this definition as a foundation for discussions to drive interoperability and standardization, as well as regulatory clarity and legal guidance.[3]

This definition also refers to the use of smart contracts *"within the context of a binding agreement between the counterparties of a transaction"*—it is worth clarifying that smart contracts utilized on internal DLT- or blockchain- based books and records systems of one or more financial institutions (collectively, "Books and Records Smart Contracts") have a fundamentally different risk profile to smart contracts utilized in the context of a legal agreement between counterparties of a transaction. Books and Records Smart Contracts serve the same function, albeit more efficiently, as operational lines of code in traditional books and records systems. As Books and Records Smart Contracts control and mitigate risks, as they are part of internal functionality, **they should be subject to the same regulatory regime that applies to any other books and records system of the financial institution**, the design, adoption, and maintenance of which is subject to the financial institution's internal risk, technology, operational, and security standards as well as the existing supervisory oversight of financial institution's systems by its regulators.

It is also important to delineate the "smart contracts" referred to in this Primer from what may be referred to as "smart legal contracts" (e.g., International Swaps and Derivatives Association ("ISDA"),[4] the Law Commission of England and Wales[5]), which generally refers to legally binding contracts in which some or all of the contractual terms between counterparties

[2] See "Impact of Distributed Ledger Technology in Global Capital Markets", GFMA (2023) for a comprehensive report on the use of DLT in capital markets

[3] Note that this Primer's basic definitions and risk mitigations are applicable to smart contracts and smart contract-based protocols that are developed and deployed on an open-source, permissionless basis or used by firms multilaterally as a form of market utility. However, there are additional considerations beyond the issues discussed in detail within this Primer when financial institutions make use of such smart contracts and protocols, such as (i) who bears regulatory and/or operational execution responsibility for open-source, permissionless smart contracts and protocols, or (ii) intellectual property rights pertaining to smart contract code that have been "released" on an open-source basis (as opposed to intellectual property rights over proprietary code which, in the same way as other forms of software, may be licensed to or owned by the relevant financial entity using or developing such smart contract code).

[4] ISDA, "Legal Guidelines for Smart Derivatives Contracts" (Jan. 2019) Available at: https://www.isda.org/a/MhgME/Legal-Guidelines-for-Smart-Derivatives-Contracts-Introduction.pdf (hereinafter, "ISDA Guidelines").

[5] Law Commission of England and Wales, "Smart legal contracts – Advice to Government" (Nov. 25, 2021). Available at: https://s3-eu-west-2.amazonaws.com/cloud-platform-e218f50a4812967ba1215eaecede923f/uploads/sites/30/2021/11/Smart-legal-contracts-accessible.pdf

are defined in and performed automatically by a computer program. In other words, as explained in ISDA's guidelines:

'when lawyers speak about smart contracts, they may be referring to a "smart legal contract", which envisages a written and legally enforceable contract where certain of the obligations may be represented or written in code. Computer scientists may interpret the term more narrowly as a piece of "smart contract code", which is designed to execute certain tasks if pre-defined conditions are met.[6]*'*

The term "smart contract" is therefore broader than a "smart legal contract" as defined by ISDA, given that a smart contract may also be used to execute internal functions, and therefore does not inherently require the mutual consensus needed for bespoke terms that remain necessary to establish a contractual agreement between two parties. As stated, smart contacts are fundamentally software code. This is in line with industry and international policymaker usage of the term.[7] Accordingly, smart contracts supporting DLT-based recordkeeping, accounting, reporting, and other back-office functions that are centrally administered by a financial entity are to a large extent akin to any other software code used by financial institutions to support traditional books and records systems.

The definition proposed by the Bank of International Settlements ("BIS") ("self-executing applications of programmable platforms that can trigger an action if some pre-specified conditions are met")[8] is consistent with this separation between code and legal contract but, importantly, also points to the underlying characteristic that distinguishes smart contracts from other code and highlights the critical role of smart contracts in a DLT-based financial ecosystem: "programmability."

[6] ISDA Guidelines, at p.6.

[7] For example:
- IOSCO's Policy Recommendations for Crypto and Digital Asset Markets defines smart contracts as "[c]ode deployed in a distributed ledger technology environment that is self-executing and can be used to carry out certain "if/then" type computations. The execution of a smart contract is triggered when that smart contract is "called" by a transaction on the blockchain." Available at: Policy Recommendations for Crypto and Digital Asset Markets
- The FSB's report on The Financial Stability Risks of Decentralised Finance and the High-level Recommendations for the Regulation, Supervision and Oversight of Crypto-Asset Activities and Markets refers to smart contracts as "self-executing code" and "software," respectively. Available at: https://www.fsb.org/uploads/P170723-2.pdf
- The EU Data Act (Regulation (EU) 2023/2854), which came into force on January 11, 2024 and applies from September 12, 2025, defines a smart contact as "a computer program used for the automated execution of an agreement or part thereof, using a sequence of electronic data records and ensuring their integrity and the accuracy of their chronological ordering." (Article 2(39)) (emphasis added). For completeness, it is worth noting that the Data Act aims to enhance the EU's data economy by establishing a harmonized framework on access and use of data, particularly in the context of connected devices services given the expansion of the Internet of Things) – it is not specific to financial services and/or to the use cases discussed in this Primer. However, it is included here for reference as one of the few examples of a legislative definition of "smart contracts". The Data Act imposes (among other things) obligations on vendors of smart contracts which are used to execute data sharing agreements to ensure that smart contracts meet certain requirements, such as the ability for smart contracts to be interrupted and terminated (e.g. to avoid future accidental executions).
- FATF's Updated Guidance on Virtual Assets and Virtual Asset Service Providers (Oct. 2021, at 21, n.14.) states: "In a VA context, a smart contract is a computer program or a protocol that is designed to automatically execute specific actions such as VA transfer between participants without the direct involvement of a third party when certain conditions are met." Available at: https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Updated-Guidance-VA-VASP.pdf.coredownload.inline.pdf
- International Capital Market Association Fintech Glossary defines smart contracts as "An automated mechanism involving two or more parties where digital assets are put in and redistributed at a later date based on some preset formula and triggering event. The contract can run as programmed without any downtime, censorship, fraud or third-party interference…". Available at: https://www.icmagroup.org/fintech-and-digitalisation/fintech-resources/fintech-jargon/
- International Securities Services Association Distributed Ledger Technology (DLT) and Crypto Assets Glossary (Mar. 2022) states: "Self-executing computer code that performs pre-defined tasks based on a pre-defined set of criteria or conditions. Smart contracts cannot be altered once deployed, since only this can guarantee faithful fulfilment of contractual obligations. A smart contract could, for example, be used to instruct a regular interest payment on a bond to be made to registered investors." Available at: https://issanet.org/content/uploads/2022/03/ISSA-DLT-Glossary-March-2022.pdf
- ISDA's 2017 whitepaper primarily emphasizes the distinction between smart contract code and contracts in the "legal" sense (p.4-6, Available at: https://www.isda.org/a/6EKDE/smart-contracts-and-distributed-ledger-a-legal-perspective.pdf). However, ISDA also references a definition by Clack, Bakshi and Braine which may encapsulate both ("A smart contract is an automatable and enforceable agreement. Automatable by computer, although some parts may require human input and control. Enforceable either by legal enforcement of rights and obligations or via tamper-proof execution of computer code." (Clack, C., Bakshi, V. & Braine, L. (2016, revised March 2017). Smart Contract Templates: foundations, design landscape and research directions)). In order to avoid confusion and to remain in alignment with the use of the term in the examples given above, this Primer report mainly refers to smart contracts as smart contract code.

[8] "Blueprint for the future monetary system: improving the old, enabling the new"", Chapter III of BIS Annual Economic Report (2023). Available at: https://www.bis.org/publ/arpdf/ar2023e3.pdf

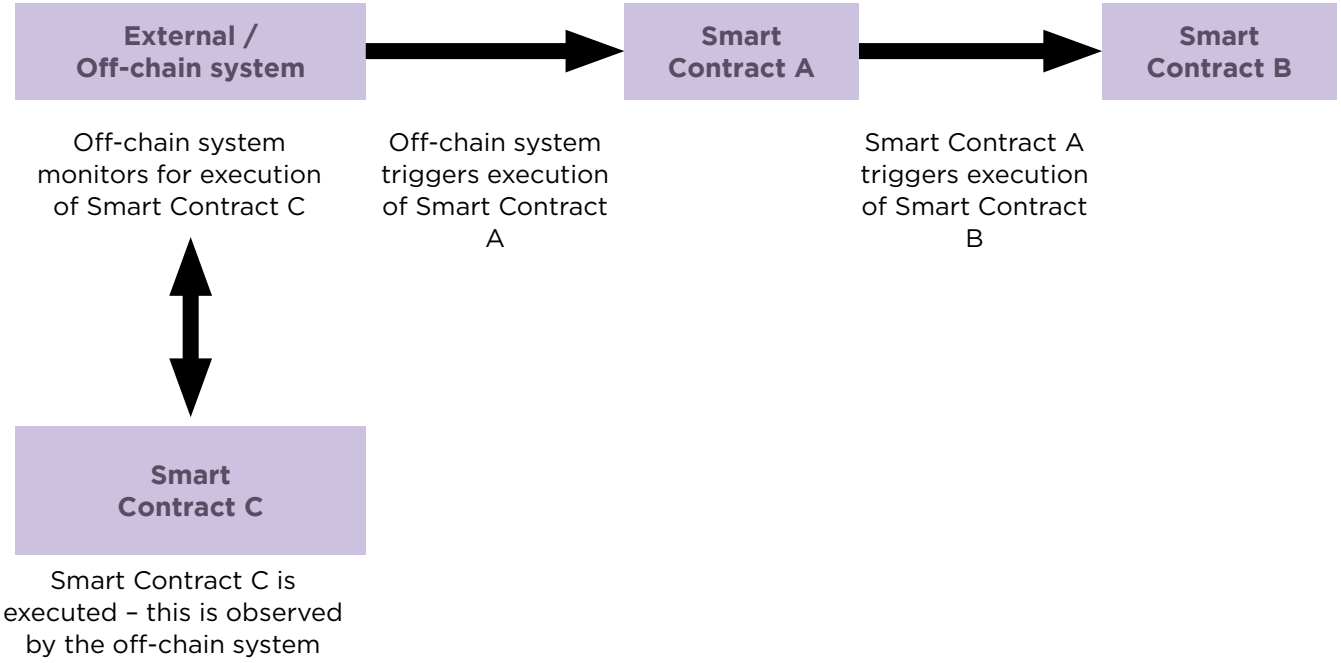
What is meant by "automatic execution"?

The definition of smart contracts in this primer refers to software code that is designed to *"automatically execute"* upon the occurrence of predefined conditions. It is worth noting that "automatic execution" does not necessarily mean that a smart contract "waits or "listens for" the occurrence of an event, and then **self-executes** upon the occurrence of such an event. Technically, execution of a smart contract on a blockchain may be **initiated** by (i) an external component or third party (which may be a human or a system), or (ii) by another smart contract.

For example, Smart Contract B can be set to be triggered by Smart Contract A. In this case, Smart Contract B does not simply "observe" the performance and outputs of Smart Contract A, and then self-initiate or self-execute accordingly. Rather, Smart Contract A initiates the execution of Smart Contract B as part of its processing, and passes on the relevant data to Smart Contract B.

Smart Contract A triggers the execution of Smart Contract B, and passes along the relevant data to Smart Contract B

Further, it is also possible that an off-chain component (e.g. a system that is external to the blockchain) watches for the execution of a smart contact (e.g. Smart Contract C), and such component then triggers the execution of another smart contract (e.g. the aforementioned Smart Contract A):



In summary, on an individual level, each of these smart contracts do not automatically self-execute upon the mere occurrence of an event, without being triggered in accordance with pre-defined conditions. On an overall system level, smart contracts can be made to execute based on pre-defined conditions, through the use of off-chain components or by being initiated by another smart contract.

Programmability refers to the ability for smart contracts to be pre-programmed to automatically execute a logical process, where a given input will lead to a defined output. This does not mean that code is left entirely to its own devices, as human input will remain crucial in terms of ongoing code development, audits, and ensuring continued regulatory compliance, as well as any manual intervention contemplated by relevant governance for the smart contract. Programmability has the potential to revolutionize financial services in a number of ways, including:

- streamlining processes and reducing costs through automation;
- saving time and facilitating simultaneous actions and value transfers, as well as enabling new financial products and services;
- mitigating human error during processing through programmatic instructions;
- enhancing trust between contractual parties, reducing the likelihood of disputes, and mitigating the need for intermediaries, by objectively and programmatically determining whether obligations were met and automatically executing desired outcomes;[9] and
- increasing transparency and security through tamper-proof records and through attaching additional terms as metadata.

More specifically, as noted in a recent report on programmability in the context of commercial banking and payments (authored by Onyx by J.P. Morgan and the Massachusetts Institute of Technology's ("MIT") Digital Currency Initiative ("DCI")),[10] a key feature of programmability is to allow (corporate) clients or users of banks' services to deploy self-contained executable instructions which reside on the same environment as the bank and that would interact or compose directly with the services of the bank. This model could provide benefits over the conventional model (i.e., where code is typically deployed and executed within a client's environment, such as its own applications, which then interacts with the bank's systems through APIs or other channels). These benefits include:

1. **Faster, more responsive transactions:** By performing triggers, logic and actions within a single environment, programmability reduces both the technical lag of cross-platform communication and the business lag of batch updates or limited polling frequency.
2. **Improved operational reliability and predictability:** Instructions are housed and executed within a single environment, reducing dependency on clients' systems and minimizing the risk of failures.
3. **Clearer and more reliable transaction audit trails:** Use within a single environment ensures that data is maintained in a consistent format, enhancing traceability and auditability.
4. **Expanded range of programmability:** Access to previously unavailable data and event triggers allows for more sophisticated programmable instructions to be embedded directly into payments. Improved execution time and certainty enable these instructions to be processed within the payment flow, rather than afterward, without negatively impacting overall processing time.
5. **Increased operational hours:** Programmable instructions can be used with higher certainty and lower failure rates, which allows for payment instructions to be performed close to or even after typical bank cut-off times. This flexibility reduces the need for extensive time buffers and external inputs.

[9] Note, however, that smart contracts are not expected to eliminate or replace the role of intermediaries entirely (BIS, "Finternet: the financial system for the future" (15 April 2024)).
[10] "Application of Programmability to Commercial Banking and Payments", Onyx by J.P. Morgan and the Massachusetts Institute of Technology's (MIT) Digital Currency Initiative (DCI) (2024). Available at: https://dci.mit.edu/application-of-programmability-to-commercial-banking-and-payments

6. **Support for complex use-cases** and composability: Programmable instructions can interact with each other, supporting more complex financial operations. Atomic operations—those program operations that run completely independently of any other processes—ensure that linked instructions either completely succeed or fail, which is crucial for transactions like delivery-versus-payment (DvP) or payment-versus-payment (PvP). This minimizes counterparty risk and ensures consistency, reducing system complexity and the need for manual reconciliation and recovery processes.

This Primer discusses smart contracts in the context of DLT and of tokenization—in other words, the process of recording claims on financial or real assets that exist on a traditional ledger on a distributed ledger or otherwise programmable platform. Importantly, it is combination of the advent of tokenization with the programmability of smart contracts—in such a way that a "token" can capture within it both the information about the underlying asset (e.g., what the asset is, who the owner is), and the rules and logic governing the transfer of such assets (e.g., what the asset can do, such as conditions on an asset being transferable only to an approved set of recipients),[11] —which gives rise to the opportunities and efficiency gains offered by DLT-based solutions in financial services.

A recent IMF Working Paper on Programmability in Payment and Settlement also concludes that "programmability holds substantial promise to make financial services more innovative, open, interconnected, and resilient"[12], and further points to the related concept of *composability,* which is "the capacity to programmatically combine operations"[13] - in other words, the ability to bundle multiple components into one executable package. In particular, the IMF Working Paper notes that "another advantage of programmable systems is their ability to execute transfers and enable automation, conditionality, and composability of financial transactions"[14] [emphasis added]. The GFMA's previous report on DLT in capital markets similarly described composability as the "ability to build an ecosystem of applications that are interoperable because they have back-end integrations with a common distributed ledger and a means of exchange to transact on the ledger", where the back-end of such a system "delivers services by using software code known as smart contracts."[15]

[11] "Blueprint for the future monetary system: improving the old, enabling the new"", Chapter III of BIS Annual Economic Report (2023). Available at: https://www.bis.org/publ/arpdf/ar2023e3.pdf
[12] "Programmability in Payment and Settlement", IMF (Aug 2024), p. 28. Available at: https://www.imf.org/en/Publications/WP/Issues/2024/08/15/Programmability-in-Payment-and-Settlement-553493
[13] Id. p.6
[14] Id. p.19
[15] "Impact of Distributed Ledger Technology in Global Capital Markets", GFMA (2023)

In a similar vein, the aforementioned report on programmability by JPMorgan's Onyx and MIT's DCI notes that the composability of smart contracts "could improve interoperability and lead to the provisioning of a richer suite of products and services".[16] Also, of particular interest, a recent Bank for International Settlements ("BIS") Working Paper co-authored by the General Manager of the BIS shared the concept of the "Finternet", a vision of "multiple financial ecosystems interconnected with each other, much like the internet" such that individuals and business would be able to make secure, cheap, and near-instantaneous transactions relating to any type of financial asset at any time, to anywhere in the world. Presented as a topic of interest, but not necessarily the position of the BIS, the Finternet is envisioned as a token-based system, where "unified ledgers" form the building blocks:

Unified ledgers have two defining characteristics. The first is that they combine all the components needed to complete financial transactions–financial assets, ownership records, rules governing their use and other relevant information–in a single venue. The second is that money and other financial assets exist on the ledgers as executable objects. This means that they can be transferred electronically using pre-programmed "smart contracts". Together, these design features allow individuals and businesses to move money and other assets safely and securely, with less need for external authentication and verification processes or reliance on external clearing, messaging or settlement systems.[17]

Given the significant role that smart contracts are expected to play in DLT-based financial ecosystem, we propose that "smart contracts" occupy a key area that requires focus to drive industry and regulatory cooperation to move towards smart contract standardization. This would be a crucial next step towards scaling DLT implementation and moving the needle on the broader digitalization of financial services.

[16] "Application of Programmability to Commercial Banking and Payments", Onyx by J.P. Morgan and the Massachusetts Institute of Technology's (MIT) Digital Currency Initiative (DCI) (2024). Available at: https://dci.mit.edu/application-of-programmability-to-commercial-banking-and-payments

[17] "Finternet: the financial system for the future", BIS Working Papers No 1178 (15 April 2024). Noting that BIS Working Papers are written by members of the Monetary and Economic Department of the Bank for International Settlements, and from time to time by other economists, and are published by the Bank. The papers are on subjects of topical interest and are technical in character. The views expressed in them are those of their authors and not necessarily the views of the BIS. Available at: https://www.bis.org/publ/work1178.htm

II. B. Interoperability and Smart Contract Standardization

Similar to the vision of the Finternet, the GFMA May 2023 report highlighted the importance of interoperability to enable scaling of a DLT-based ecosystem. Specifically, it is crucial to have both interoperability between DLT systems and "traditional" systems (so that, for example, data can be shared between DLT-based and traditional books and records systems), as well as between different DLT platforms.[18]

One of the recommendations (*"Enable Interoperability"*) in the GFMA report set out the need for market participants to align in terms of technical design, standards, and core governance considerations. One aspect of technical design and governance is how smart contracts can drive and enable such interoperability in a DLT-based capital market ecosystem. In order for this to occur, market participants feel that smart contracts themselves would benefit from standardization approaches across industry, both in smart contract implementation as well as risk management to avoid the development of siloed and incompatible solutions within the market. Among other things, this Primer proposes the following three key areas be prioritized for development of smart contract standardization across industry:

1. **Technical standards** such as standards for developing tokens (e.g., ERC-3643, FINP2P, IVMS101),[19] messaging standards or protocols that allow for cross-chain interoperability, bridge solutions, etc.;

2. **Standardization of smart contract provisions and template-based approaches to smart-contract development** with respect to specific products or asset classes, where appropriate, for example by leveraging the initiatives ISDA has taken to develop standardized approaches to smart derivative contracts (noting that ISDA documentation[20] is widely adopted and accordingly there is already a relatively high degree of contract standardization in the context of derivatives trading, such that it may be possible to develop standardized approaches on a logic-level, at least to provide a foundation which developers may draw upon to enable specific functionality—however, this level of standardization may not be appropriate for other types of products or services). It is also important to note other existing relevant projects working towards standardization undertaken across industry such as the Common Domain Model,[21] the International Capital Market Association Bond Data Taxonomy (ICMA BDT)[22], and the Digital Token Identifier (DTI)[23]. Additionally, standardization needs to take place for the legal / product documentation. This may require separate enhancements based on a specific "tokenization" model; and

3. **Best practices and risk-mitigation** for audit and verification of smart contract code, responsibility and liability for design and execution of smart contracts, use of external data feeds, transparency, the extent of manual intervention required within automated processes, and dispute resolution mechanisms. Smart contract risks and mitigation strategies, and how these can be addressed via existing regulatory frameworks for mitigating operational and technical risk, are discussed and expanded upon in Section III below.

[18] "Impact of Distributed Ledger Technology in Global Capital Markets" (2023)
[19] ERC3643 :https://www.erc3643.org/, FINP2P: https://finp2p-docs.ownera.io/docs/introduction-1, IVMS101: https://www.intervasp.org/
[20] Including the ISDA Master Agreement and templates for ancillary documentation, and ISDA Taxonomy and Clause Library
[21] Common Domain Mode: https://www.finos.org/common-domain-model
[22] ICMA BDT: https://www.icmagroup.org/fintech-and-digitalisation/fintech-advisory-committee-and-related-groups/bond-data-taxonomy/
[23] DTI: https://dtif.org/

Primary and secondary markets are in the early stages of adoption of DLT, and it will be important for emerging regulatory frameworks to support such adoption without inhibiting responsible innovations for the legitimate use of DLT. Scaling and reaching critical mass for DLT implementation can be supported by introducing clear "best practices" to reduce regulatory ambiguity, while avoiding the imposition of overly prescriptive rules and punitive standards. This Primer aims to serve as a guide to work towards one piece of responsible innovation for smart contract implementation. As it is already evident that certain asset classes and use cases (as identified in the GFMA May 2023 report)[24] stand to benefit from the efficiency and liquidity benefits DLT could offer (See Exhibit 1), the **following discussion considers how to support smart contract implementation and mitigate risks in the context of high readiness asset classes within regulated capital markets.**

[24] "Impact of Distributed Ledger Technology in Global Capital Markets" (2023)

Exhibit 1

Potential Future Developments of a DLT Ecosystem: Summary of GFMA May 2023 Report

High readiness & high opportunity asset classes

- Private debt
- Money market funds
- Syndicated loans
- OTC derivatives
- Corporate bonds
- Sovereign & semi-sov. bonds
- Illiquid & real asset funds

Common drivers:

(1) a clear financial opportunity from efficiency gains or innovation;

(2) market readiness for innovation and adoption around specific market structure attributes, workflow inefficiency, and the maturity of electronification.

Notable characteristics of a DLT-based system

- Tokenisation
- Immutable, distributed ledger
- Programmabilitcontractsy via smart
- Interoperability with other systems

Examples of smart contract usage

- **Back-office settlement/payment servicing:** Smart contracts can be used to streamline processes in bond issuance, coupon and principal payments, and custody.
- **Corporate actions:** Smart contracts are well-suited to operationalize corporate actions by providing a mechanism to automate and execute based on predefined conditions ("if...then" coding).
- **Withholding tax:** Smart contracts can enable correct withholding at source, replacing document-based manual workflows.
- **Proxy voting:** Custodians can leverage automation provided by smart contracts to extend voting cut-off times and reduce operational risk such as over / under-voting.

Recommendations from the GFMA Report

Recommendation #1
Drive towards legal certainty and regulatory clarity

Recommendation #2
Enable interoperability (e.g. interoperability across DLT networks, smart contract standards, governance)

Recommendation #3
Establish viable Primary and Secondary markets for high-potential asset classes

Recommendation #4
Collaborate on the advancement of DLT to promote new technical solutions

Recommendation # 5
Work towards sound, safe, and compliant DLT-based Payment Instruments

Key enablers for long term growth								
	Cross-industry, public-private partnerships	Regulated, accepted, DLT-based cash	Industry-aligned taxonomy and educative materials	Updated fund and investment mandates	Global legal and regulatory framework	Interoperable networks and markets	Interoperable networks and markets	DLT-specific FMI

Source: Adapted from GFMA, 'Impact of Distributed Ledger Technology in Global Capital Markets' May 2023

III. BEST PRACTICE FOR SMART CONTRACT IMPLEMENTATION AND ANALYSIS OF THE EXISTING REGULATORY TOOLKIT FOR RISK MITIGATION FRAMEWORKS

III. Best Practice for Smart Contract Implementation and Analysis of the Existing Regulatory Toolkit for Risk Mitigation Frameworks

As discussed in both the GFMA May 2023 report and the recent research commissioned by GDF - the institutional adoption of DLT is already underway.[25] The adoption of new technology and increasing automation have long been a feature of financial markets and their infrastructure to serve clients' needs globally.[26] As with the advent and implementation of any new technology or automated process, smart contracts present significant potential benefits to markets and their participants. They also present considerations for users and regulators alike, including the assessment of any associated risks. These concerns are not new to digital asset technology.[27] As regulated institutions approach technology change management, and aim to implement responsibly, they have found that in many cases, existing laws, regulations, and guidance, along with existing risk management approaches, are sufficient for the operation and use of smart-contract technology.

For example, while there are some risks that may be unique, as well as additional legal and regulatory clarifications to be addressed as technology continues to evolve, overall, institutions have been steadily working towards developing best practices for utilizing smart contracts within business lines and have already been able to mitigate most related risks. This is primarily because using smart contracts does not, by default, mean that new forms of regulated financial services activities are being carried out; rather, by streamlining and automating existing business logic through the implementation of smart contracts, financial services may be provided in a more efficient and effective manner that, among other things, obviates manual processes that can be a source of operational risk.

Firms that have already begun implementing smart contracts have done so in accordance with existing regulatory guidance for DLT. For example, given that global regulatory approaches to permissionless public ledgers are still evolving, firms have instead implemented smart contracts in permissioned environments. In recent years, many institutions are starting to embrace permissionless public ledgers as permissioned networks reaches their limits for interoperability. However, the use of public platforms is not a prerequisite to smart contract use. The benefits of programmability, as highlighted in Section II, can be achieved in permissioned systems with varying degrees of centralization in terms of operation and governance. As a result, in a number of respects, smart contract implementation is already compatible with the principles of existing legal and regulatory frameworks.[28]

As the industry matures, smart contract usage is becoming increasingly common and advanced. The following Section III. A. sets out principles for establishing best practices, while also highlighting how existing risk mitigation practices and regulatory frameworks can be applied in the context of smart contracts. The next Section III. B. analyzes where regulators and policymakers could support the future evolution and scaling of digital markets through adjustment and clarification to existing requirements and legal regimes. It will be important for regulators and market participants to be cognizant of relevant risks that are non-specific as well as those unique to smart contracts. The development of best practices or industry standards can enhance regulatory clarity to assist with industry adoption of digitalization and mitigate the growing risk of market fragmentation.

[25] "Real-World Asset Tokenization is moving mainstream", GDF (April 2024). Available at: https://www.gdf.io/resources/real-world-asset-tokenization-is-moving-mainstream/ ; https://www.gdf.io/resources/private-debt-will-be-first-asset-class-to-be-tokenized-and-routinely-traded/

[26] LabCFTC's "Smart Contract Primer" (p. 10) (November 2018). Available at: https://www.cftc.gov/sites/default/files/2018-11/LabCFTC_PrimerSmartContracts112718.pdf

[27] For example, in the context of virtual currencies, preliminary smart contract discussions highlighted that DLT "could significantly alter how bilateral margining and clearing works today…" See, "Digital Currencies", Committee on Payments and Market Infrastructures (Nov. 2015). Available at https://www.bis.org/cpmi/publ/d137.pdf.

[28] For example, where a financial entity implements an internal DLT-based solution to support its recordkeeping systems, or where participants to a decentralized network agree to be governed by a set of rules and a defined entity takes on the responsibility of operating and maintaining the network.

III. A. Smart Contract Best Practice: Operational and Technical Risk Mitigations and Application of Existing Regulation

This Section provides an overview of the most crucial areas where best practices in technical and operational risk mitigation for the use of smart contracts can be applied. It aims to map risk types that may arise from smart contract implementation to functional policy areas within existing risk management frameworks. This Section does not aim to be prescriptive in how smart contract code should be developed, but rather to set out guiding principles, mapped to existing regulatory frameworks, that can serve as a guide of best practices for standardized risk mitigation across industry. This Section III.A. discusses how regulated market participants are approaching smart contract implementation similarly to implementing other new technologies through the years (e.g., cloud) and how existing regulatory frameworks and best practices can be used to mitigate risks. Section III. B. looks to the future and considers what adjustments and clarifications to existing frameworks could be provided for smart contract scaling as the industry continues to evolve.

As with any technology change management program, this Primer outlines the existing functional policy areas and processes that will enable market participants to identify risks, including risks unique to smart contracts. This Primer's aim is to discuss how both traditional technology risks and these unique challenges are already being addressed to support smart contract and DLT scaling in the financial services ecosystem in a compliant and responsible manner. (It is also worth noting that smart contracts used for books & records, as internal functions, will not have the same risk profile as external facing smart contracts.)

This Primer proposes the following eight key areas of standardization for firms implementing smart contracts as well as some of the relevant regulatory frameworks for each principle.[29] Each principle is also accompanied by practical examples of risk identification and mitigation, as well as some of the relevant regulatory frameworks governing the risk approach.

[29] A full analysis of the frameworks which map to the eight principles can be found in Annex 1 with an expanded discussion on global frameworks in Annex 2.

1. Development and growth of internal risk and control or compliance function with appropriate resourcing: Firms will need to consider how to develop and scale their internal operational risk and/or compliance departments to oversee, support and advise business lines with sufficient personnel to audit, maintain and upgrade any necessary coding issues. This will vary based on a firm's size, business model, and activities, proportionate to its business needs.

Functional Area	Relevant Regulatory Framework / Guidance	Existing Industry Best Practice / Mitigation Strategy	Why this Matters: The Risk Being Addressed
Operational / Technological & Compliance / Regulatory	European Banking Authority (EBA) – Guidelines on ICT and security risk management (November 2019) FSB – Principles for an effective risk appetite framework (November 2013) Monetary Authority of Singapore (MAS) - Guidelines on Risk Management Practices – Technology Risk (January 2021) FCA Principles for Business, Principle 2 & Principle 3 FCA - SYSC (Senior Management Arrangements, Systems and Controls) rules, in particular SYSC 3 (Systems and Controls) and SYSC 7 (Risk control) Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (DORA) HKMA - Supervisory Policy Manual on Operational Risk Management (July 2022) HKMA - Circular on risk management considerations related to the use of distributed ledger technology (April 2024) HKMA - Supervisory Policy Manual on General Principles for Technology Risk Management (June 2024)	• Implement and maintain adequate risk management policies and procedures, including procedures for risk assessment, identifying risk tolerances, and risk mitigation. • Implement and maintain an effective compliance function to monitor, identify, mitigate and address compliance risks. • Leverage on-chain data to track ownership, using verifiable credentials to enforce compliance while protecting privacy by validating eligibility without exposing private data. • Risk control and compliance functions should have oversight of, where appropriate, the full development cycle, from proposal to deployment and ongoing monitoring. • Risk management and compliance functions should monitor compliance of and provide advice to persons / business lines developing, managing, and deploying smart contracts. • Appoint a chief risk officer and compliance officer, and establishing relevant committees (with individuals assigned to key roles and responsibilities, and relevant reporting lines). • Monitor on a regular basis the adequacy of such measures and take steps to address deficiencies. • Risk control and compliance functions should be directly accountable to the management body. • Risk control and compliance functions should have the necessary authority, resources, expertise and access to all relevant information. • Risk control and compliance should be independent of the business they control.	Firms need to have effective risk governance structures in place to identify, understand and manage risks associated with the development and use of technology generally, including smart contracts. An effective risk management system reduces the likelihood of incidents occurring as well as mitigates the impact of incidents. Such practices also reduce compliance risk—the financial services sector is a highly regulated one, where there are numerous regulatory frameworks/ legislation which are technology-neutral (e.g., laws applicable to automation, use of data, artificial intelligence, digital operational resilience and business continuity, may all be applicable to the use of smart contracts, depending on the use case). The potentially cross-border application of smart contracts also increases compliance risk.

2. Have a clear and proportionate incident response mechanism/policy: These policies should include how and what should be done once an incident starts, and firms should have a clear business continuity plan ("BCP") as well as an information and communication technology ("ICT") plan to minimize the damage, as well as appropriate steps in place to maintain the continuity of any smart contract supporting important business services. The following table includes examples of policies and best practices that can mitigate risk:

Functional Area	Relevant Regulatory Framework / Guidance	Existing Industry Best Practice / Mitigation Strategy	Why this Matters: The Risk Being Addressed
Operational / Technological	NFA Interpretive Notice 9070 and NFA Compliance Rules 2-9, 2-36 and 2-49 FCA – PS21/3 Policy Statement on Building Operational Resilience FCA - Senior Management Arrangements, Systems and Controls (SYSC) rules in particular SYSC 15A (Operational Resilience) and SYSC 8 (Outsourcing) Bank of England, Prudential Regulation Authority (PRA) – Operational resilience: Impact tolerances for important business services Federal Financial Institutions Examination Council – Information Security Program Management (Information Security Handbook) Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, Office of the Comptroller of the Currency – Sound Practices to Strengthen Operational Resilience (October 2020) Basel Committee on Banking Supervision (BCBS) – Principles for Operational Resilience (August 2020)	• Have clear and proportionate incident response mechanism/ policies and procedures, including: procedures to identify, track, log, categorize and classify incidents (e.g., by prioritizing based on business criticality); procedures to identify, analyze and solve the root cause behind one or more incidents; processes to mitigate impacts and harm of incidents and to ensure continuation of critical business functions and processes when disruptions occur (including, if appropriate, the ability to continue operating certain functions and services without the use of smart contracts); and post-incident review processes to analyze causes of disruption and need for improvements. • Maintain up-to-date inventory of smart contracts and relevant ICT systems, devices, databases in relation to which such smart contracts are used, and document interdependencies between different ICT assets to facilitate efficient response to security and operational incidents. • Integrate smart contracts with existing workflows (see also principle 7 below) with human intervention at critical points for added security. • Define, implement, and regularly test data and systems backup and restoration procedures to ensure that they can be recovered as required. • Establish effective communication plans, both internally (e.g., escalation procedures) and externally (e.g., notifications to stakeholders) • Design at the outset smart contracts which are able to be upgraded as the need arises to mitigate any new and evolving risks or to solve post-deployment bugs etc.	Regardless of what technology is being used (e.g., smart contracts or otherwise), financial institutions may suffer ICT incidents—in the case of smart contracts this could include errors / mistakes in code, software bugs, malfunctioning of related systems or devices, and cyberattacks.

Functional Area	Relevant Regulatory Framework / Guidance	Existing Industry Best Practice / Mitigation Strategy	Why this Matters: The Risk Being Addressed
Operational / Technological	Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (DORA) MAS – Notice on Technology Risk Management (May 2024) MAS – Guidelines on Risk Management Practices – Technology Risk (January 2021) MAS – Guidelines on Business Continuity Management (June 2022) Security Exchange Commission (SEC) – Regulation Systems Compliance and Integrity (Regulation SCI) (February 2015) Bank of England – Financial Stability in Focus: The FCP's macroprudential approach to operational resilience (March 2024) HKMA - Supervisory Policy Manual on Operational Resilience (May 2022) HKMA - Supervisory Policy Manual on Business Continuity Planning (May 2022) HKMA - Supervisory Policy Manual on General Principles for Technology Risk Management (June 2024)		

3.Standardized requirements for smart contract audits, including for completeness and robustness while working towards a template-based approach for broader smart contract standardization: Such requirements should incorporate best practices that exist for smart contract auditing, and should promote transparency between regulators and market participants with respect to audit processes and outcomes. Examples of best practices are described below:

Functional Area	Relevant Regulatory Framework / Guidance	Existing Industry Best Practice / Mitigation Strategy	Why this Matters: The Risk Being Addressed
Operational / Technological	European Banking Authority (EBA) – Guidelines on ICT and security risk management (November 2019) Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (DORA) An example of a non-supervisory authority's guidance is the National Institute of Standards and Technology Internal Report 8202: Blockchain Technology Overview (October 2018) HKMA - Whitepaper 2.0 on Distributed Ledger Technology (October 2017) HKMA - Circular on sale and distribution of tokenised products (February 2024) HKMA - Circular on risk management considerations related to the use of distributed ledger technology (April 2024)	• Audits should be undertaken by independent auditors with sufficient knowledge, skills and expertise in smart contracts and blockchain. • Given the transparent nature of blockchain networks (including permissioned networks), it may be possible for certain audits to occur on an automated and constant basis, as opposed to taking place on a periodic basis. • Where smart contract code is developed / provided / managed by third party providers, appropriate audit and access rights should be granted to financial entities and their regulators in the relevant vendor contracts. • Firms can integrate international standards applicable to software more broadly, such as ISO/IEC 27001. • Audits can also be conducted in line with smart contract-specific standards which may be developed by industry.[30] In addition to audits around software code, carry out audits relating to external data which feeds into the smart contract such as via data oracles, as well as audits on internal governance, risk controls and compliance functions around smart contract development and deployment processes	Generally, a financial entity's ICT systems and processes would be audited on a periodic basis, particularly those that support critical business functions and operations. Given that smart contracts are designed to execute autonomously and may be used in combination with sensitive data, smart contract code should in particular be audited for security issues or errors. Smart contracts may also consume off-chain data through external systems such as data oracles, which themselves may be susceptible to manipulation– appropriate auditing practices will therefore help to mitigate security and data accuracy risks in relation to such oracles.

There is, however, still further work that can be done to progress and codify smart contract and token standardization. As discussed under Section II.B., interoperability will simplify interactions among participants, extend functionality, and reduce risks related to complicated interactions across smart contracts, applications and cross-network operations. Looking to the future, standardization work should include an analysis of key features of widely used standards and a review of missing features or functions suitable for the types of assets and transactions that tokens and smart contracts intend to represent.[31]

[30]An example is the "Smart Contract Security Verification Standard" (v2), a free checklist "created to standardize the security of smart contracts for developers, architects, security reviewers, and vendors". Available at: https://www.jpmorgan.com/onyx/documents/portfolio-management-powered-by-tokenization.pdf

[31]See "The Future of Wealth Management", Project Guardian, Onyx by JPMorgan and Apollo (2023), pp. 45-47. Available at: https://www.jpmorgan.com/onyx/documents/portfolio-management-powered-by-tokenization.pdf (describing the rationale for developing ODA-FACT token standard and the implementation of the standard cross-network)

4. Ensure smart contracts are written in clear, well-documented code that is easy to understand and audit: Best practices in documentation should describe, for example: intended functionality of the application, what properties and invariants should be maintained under execution, controls, and cross-contract dependencies. A smart contract should have a clear scope and use regular naming conventions and in-line comments. This should also be captured in product documentation.

Functional Area	Relevant Regulatory Framework / Guidance	Existing Industry Best Practice / Mitigation Strategy	Why this Matters: The Risk Being Addressed
Operational / Technological	Financial services regulators typically take a principles or outcomes-based approach and would not regulate code readability specifically, due to the technical nature of software development, the variety of programming practices, and to avoid stifling innovation by industry.	Some practices which industry broadly accepts to be good/ best practice, and which are generally applicable to the software code development include: • Using consistent coding style such as naming conventions, indentations and commenting. • Using in-line comments to explain the purpose of a particular line of code and the relevant logic. • Using meaningful variable names, function names, and clear logic structures where possible to ensure readability of the code. • Avoiding excessively deeply nested structures. • Integration of smart contracts with existing workflows (see also principle 7 below) with human intervention at critical points for added security.	As many smart contracts have self-execution coded in, this could lead to self-execution of errors. This may cause the unintended consequences, including the violation of contractual terms and provisions. Clear and readable code helps to reduce risks of errors in code development, as well as to mitigate risks around code interpretation in the event of a dispute in the context of the associated legal agreement. More broadly, clearly written and readable code also facilitates code audits, maintenance and updates, which can help to mitigate compliance risks as well as technical/operational risks of failures.

5. Extensively test smart contracts before deployment using various scenarios and stress tests: This testing should include verifiable test coverage. Smart contract tests should methodically cover maximum existing use cases and functionalities to minimize unexpected and untested edge cases. Test coverage should also be transparent for both regulators and market participants.

Functional Area	Relevant Regulatory Framework / Guidance	Existing Industry Best Practice / Mitigation Strategy	Why this Matters: The Risk Being Addressed
Operational / Technological	HKMA - Circular on risk management considerations related to the use of distributed ledger technology (April 2024) FINRA's Regulatory Notice 15-09 Recommendations for Standard Procedures which clearly catalogued, labelled, and isolated code both for implementation and for testing. BCBS general principles for stress testing IOSCO cyber resilience guidelines which provide some guidance on the kind of stress testing that private market participants can deploy when using or developing smart contracts.	• Ensure all code is reviewed, tested, and audited as appropriate by third parties. • Consideration of "best practice" standards for the review of smart contracts pre-deployment. • Ensure that smart contracts are written in clear, easy-to-audit, well-documented code (see also principles 3 & 4 above). • Extensively test smart contracts before deployment using various scenarios and stress tests with external third parties where appropriate (see also principles 3 & 4 above). • Ensure technology and cybersecurity policies allow for code review and testing, where appropriate.	Lack of pre-deployment consensus of the business logic represented in the smart contracts could result in errant or inadvertent business logic execution. Erroneous code could result in potential breach of contractual terms, and risk of voidability of contract.

6. Implement strong access controls to restrict who can modify or interact with the smart contract: This should also include Privileged Access Management and firms should ensure that there are strong access controls for any privileged access or admin activity. This should also be captured in product documentation.

Functional Area	Relevant Regulatory Framework / Guidance	Existing Industry Best Practice / Mitigation Strategy	Why this Matters: The Risk Being Addressed
Cybersecurity	SEC and NFA have eight regulations on safeguarding the privacy of consumer information given to third parties. SEC recently adopted final rules requiring a general cybersecurity risk management and incident disclosure and a small entity compliance guide. CFTC required risk management programs that include operational risk and information security. See 17 C.F.R. §§ 1.11, 23.600. Federal Reserve Board, the FDIC, and the OCC of Treasury interagency guidance on third-party risk management. HKMA - Whitepaper 2.0 on Distributed Ledger Technology (October 2017) HKMA - Circular on managing cyber risk associated with third-party service providers (December 2023) HKMA - Circular on risk management considerations related to the use of distributed ledger technology (April 2024) MAS – Notices on Cyber Hygiene (May 2022) set out requirements on securing administrative accounts.	• Implement a standardized secure software development lifecycle that includes smart contract security audit and formal verification of sensitive functions. • Regularly perform smart contract-focused threat modeling to capture, communicate, and remediate the risk of each use case.	Lack of smart contract security audit and review process, as well as lack of appropriate lifecycle development programs could lead to potential for exploitation of vulnerable code and flawed business logic leading to denial of service attacks, fraud or theft.[32]

[32] An Introduction to Smart Contracts and Their Potential and Inherent Limitations," Levi, Stuart; Lipton, Alex (May 26, 2018). Available at: https://corpgov.law.harvard.edu/2018/05/26/an-introduction-to-smart-contracts-and-their-potential-and-inherent-limitations/.

7. Integrate smart contracts with existing workflows with human intervention at critical points for added security: This risk mitigation should also be streamlined with the test coverage principle noted above. Ideally, human intervention should be required whenever there is activity outside the test coverage. This should also include ledger security monitoring and alerting capabilities as well as a key management solution with appropriate cybersecurity and enforcement controls.

Functional Area	Relevant Regulatory Framework / Guidance	Existing Industry Best Practice / Mitigation Strategy	Why this Matters: The Risk Being Addressed
Cybersecurity	MAS – Guidelines on Risk Management Practices - Technology Risks (Jan 2021) contains requirements on privileged access management. MAS – Guidelines on Risk Management Practices - Technology Risks (Jan 2021). US Federal Reserve and the FDIC proposed guidelines establishing a "three-lines-of-defense" model of risk management as a standard of general risk management governance for all depository institutions. HKMA - Circular on risk associated with third-party IT solution, Annex (September 2024)	• Implement ledger security monitoring and alerting capabilities. • Leverage a key management solution with transaction level policy enforcement capability. • Implement a defense-in-depth strategy with multilayer access controls to restrict who can manage or interact with the smart access controls to restrict who can modify or interact with the smart contract and its middleware. • Implementing a mechanism that requires certain access privileges for approving orders that exceed pre-determined volume and price thresholds that are pre-set within the code.	Malicious threat actors (with an increased risk of this on public-permissionless networks) could exploit vulnerable code via third-party hacking, leading to fraud/theft.[33]

[33] Id.

8. Agreement of contractual obligations between relevant parties: Firms should also consider how, particularly in respect of smart contracts that are used in the context of legal agreements between counterparties, to mitigate risks in smart contract integration through incorporation of certain provisions in legal contracts between the parties, to avoid legal ambiguities. In addition, the obligations on each party to an agreement to comply with applicable laws, rules and regulations (e.g., resolution regimes and related regulations such as qualified financial contract resolution stay rules in the US or the Bank Recovery and Resolution Directive (BRRD) in the EU, international sanctions, data protection legislation, etc.) should be clearly understood between the parties. Dispute resolution mechanisms as well as procedures for complying with applicable laws, rules and regulations should be considered and put in place at the outset and initial coding of a smart contract, so that appropriate mechanisms are built into the system and the parties' regulatory obligations are appropriately addressed, as would be necessary for other types of transactions in regulated financial markets.

It is important to note, some smart contracts may only be used internally (e.g., in the case of Books and Records Smart Contracts), so dispute resolution mechanisms may not be relevant in all instances. Furthermore, the risk assessment may be significantly minimized if smart contracts are only being used within private permissioned systems where a transactional issue may be more easily addressed, such as in the event of an error by the administrator.

Where there may be a potential dispute between relevant counterparties to a smart contract, the parties' agreement could also mandate certain operational and technological mitigation strategies discussed in this Section, such as requiring pre-deployment code review including user acceptance testing and scenario testing, to identify code-specific issues. An independent audit/verification of the smart contract code (see principles 3&4) or a third-party oracle (where applicable), may help to ensure that execution error is minimized. Features like time locks, kill switches, fail safes, and monitoring, which are further described in the GFMA May 2023 report, may allow for real-time oversight to verify ongoing transactions according to the agreement, such as by checking the transaction values and data in ongoing transactions against values in the agreement.[34] Both the underlying agreement and the smart contract code can also require that both parties use multi-signature authentication to prevent premature or inadvertent execution.

These are guiding principles for risk mitigation strategies, which should be proportionate to the size, scope, and relation to other business activities of the smart contract use case.

Functional Area	Relevant Regulatory Framework / Guidance	Existing Industry Best Practice / Mitigation Strategy	Why this Matters: The Risk Being Addressed
Legal	The law of contracts of the local jurisdiction would govern provisions identifying valid smart contracts.[35] For a more in-depth adiscussion of this issue, see Section III.B.1 below.	• Consider the governing contract law principles prior to reaching contractual agreement on governing law and jurisdiction provisions. • Ensure that all parties have identified the valid smart contract. • Include contractual provisions allowing for the creation of valid smart contracts that satisfy requirements for legal agreements of that type.	Agreeing to a favorable governing law and jurisdictional provisions mitigates enforceability risk and, in the event of a disagreement between counterparties to an agreement, facilitates quicker dispute resolution by ensuring the jurisdiction of the legal agreement is not in question.

[34]"Impact of Distributed Ledger Technology in Global Capital Markets," at p. 24. Available at: https://www.gfma.org/wp-content/uploads/2023/05/impact-of-dlt-on-global-capital-markets-full-report.pdf.
[35]For example, in the United States, the Illinois legislature adopted a law providing that no otherwise legally enforceable contract is unenforceable simply because a blockchain was used to create, store, or verify it. Certain domestic regulators, such as the CFTC and SEC, require registered swap dealers and security-based swap dealers to agree to governing law provisions prior to entering into OTC derivative contracts. See 17 C.F.R. § 23.504(b), 17 C.F.R. § 240.15Fi-5.

III. B. Looking to the Future: Regulatory Adjustments Where Further Clarity May be Beneficial

The previous Section detailed how existing operational and technology risk management processes (such as code audits, static analysis, and unit testing), as well as financial risk management programs, sound governance structures and prudent contractual review, can mitigate risks.

Two legal risks that are highlighted frequently by regulatory bodies in reference to smart contracts are: **1) jurisdictional uncertainty, and 2) lack of legal contractual certainty.** The potential consequences and risk mitigants of these risks are better identified and mitigated in jurisdictions where there is emerging or clear(er) guidance on perimeters, regulations, and laws, as they relate to DLT, digital assets, and the rights and obligations of assets owners and those counterparties involved in the handling of digital assets on behalf of asset owners.

While, as discussed above, some risk considerations emerge from the innate nature and creation of smart contracts, existing operational and technical regulatory frameworks (see Annexes) can help mitigate such risks. In addition to these existing frameworks, this Section aims to discuss areas where adjustments, clarification and guidance could further support the scaling of DLT within the broader financial ecosystem. This Primer identifies three key areas where adjustments may be beneficial and where the public sector can support smart contract implementation and standardization. It also discusses existing best practices within industry, further expanding on how they are already being used to support the scaling taking place today and the steps being taken to mitigate risks.

1. Legal Clarifications:
While this Primer's focus is smart contracts and not "smart legal contracts" (as mentioned in Section II above), whether an agreement which involves the use of smart contract code can withstand legal scrutiny (i.e., to operate as a legally binding and enforceable contract in a court of law) is an area where the public sector could provide further certainty to complement the best practices the industry is developing to date.

For the avoidance of doubt, this is not a reference to a need for legal certainty regarding the use of "electronic" contracts (versus hard-copy/paper contracts)—in fact, the validity of electronic contracts and e-signing mechanisms is well established in major jurisdictions around the world, as demonstrated by legislation such as the E-SIGN Act in U.S., UETA at U.S. state level, and Regulation (EU) No 910/2014 otherwise known as "eIDAS" in the EU. The use of electronic contracts has also been considered in the context of key industry-standard master agreements in the global financial markets—for example, ISDA has procured "e-contract" opinions covering industry-standard master agreements (e.g., ISDA Master Agreement, Global Master Securities Lending Agreement, Global Master Repurchase Agreement, Master Repurchase Agreement, Master Securities Loan Agreement, and Master Securities Forward Transaction Agreement) across a wide variety of jurisdictions.

Legal uncertainty (such as challenges in contractual interpretation and issues around whether a contract is legally binding and enforceable) is more likely to arise where mutual agreement permits and enables some, or all, of the terms of an agreement to be defined in software code rather than "natural language". The risk of legal uncertainty, therefore, exists on a continuum, depending on the extent of the contractual obligations being written in code form. Where contractual terms are defined wholly in natural language (even if only represented electronically), the use of smart contract code would be unlikely to raise novel issues of legal uncertainty, as the role of software would be merely to operationalize elements of the agreed terms.

Where the parties mutually agree to utilize a "hybrid" contract which incorporates terms in both natural language and software code, the use of smart contract code may give rise to some uncertainty in cases where the code portion of the arrangement is not readily interpretable, or not recognized as valid or enforceable under a court of law in a particular jurisdiction. Risks around legal uncertainty would be particularly significant if contractual provisions on applicable choice of law, dispute resolution and similar foundational matters were not clearly agreed and defined by the parties prior to execution, such as by means of a protocol or rulebook that specifies mutually agreed requisites for contract formation or other form of written agreement.

Finally, a contract which is expressed entirely in code could present the most significant level of legal uncertainty, as there is less established legal guidance or precedent on such issues. It is worth noting, however, that there are currently no industry trends to suggest a complete departure from the use of "natural language" to replace the use of industry-recognized master agreements (such as the ISDA Master Agreement) at a portfolio-level with purely coded arrangements, which mitigates the risk of uncertainties arising in relation to certain important contractual terms (e.g., close-out netting provisions).

Notably, the Law Commission of England and Wales has undertaken significant efforts to explore the legal treatment of smart contracts and, in 2021[36] , concluded that the existing legal framework (due to the flexibility of the common law) is able to support the use of smart legal contracts, without the need for statutory reform (although the Law Commission noted the uncertainties around the creation of deeds, as opposed to contracts, which are wholly or partly defined by code, due to the strict formalities which apply to the execution of deeds). Instead of changes to legislation, the Law Commission suggests ways in which market participants could themselves anticipate and address potential uncertainties in the legal treatment of smart legal contracts, such as by considering issues around the interplay between natural language terms and coded terms upfront, and expressly addressing them in the relevant agreement.

[36]Law Commission of England and Wales, "Smart legal contracts – Advice to Government" (Nov. 25, 2021)

Such public sector insight published by the Law Commission is helpful to facilitate and to complement industry's development of best practices, as the financial services industry progresses towards broader digitalization. Examples of such best practices include those mentioned in Part 8 of Section III.A above, such as ensuring the parties are clear on the governing law and jurisdiction of the smart legal contract, and put in place appropriate dispute mechanism procedures.

Steps the regulatory community could take to support smart contract scaling and to reinforce industry best practices include:

- Updating legal guidance to support legal enforceability or to otherwise clarify the legal treatment of smart contracts in their jurisdictions;

- Acknowledging that DLT-based smart contracts can be legally binding and enforceable contracts; and

- Adopting digital dispute resolution tools, as well as digital insolvency guidance to support broader enforceability.

Industry Best Practice

Industry currently works to the best of their ability to ensure that smart contracts are integrated into legal agreements that satisfy existing jurisdictional contract law, and that a valid smart contract is defined or identified in the legal agreements. Industry can also work together to develop digital dispute resolution best practice in line with existing global principles for dispute resolution.

It is also considered best practice that the form of smart legal contract which is least likely to lead to issues of enforceability would be made up of natural language, which is external to smart contract code and is, in and of itself, a legally enforceable contract. Parties should also agree and document the connection of these natural and technical obligations.

Most smart legal contracts are either made up of (1) a natural language agreement in which some obligations are performed automatically by computer code, or (2) a hybrid contract in which some contractual obligations are defined by natural language, and other terms are defined in code. In such cases, it is essential that the parties are clear on the boundaries between code and natural language. Where appropriate, parties should agree (in natural language) which contractual obligations are automated via smart contract code, the relationship between coded and non-coded terms (e.g., in the case of a hybrid contract) the relevant hierarchy in the event of a conflict, mechanisms to sever or modify coded contractual terms (e.g. if the coded terms are central to the agreement/relationship) in order to preserve the arrangement should the software code component be deemed unenforceable under a court of law, and, crucially, how to redress erroneous code in the event the smart contract code does not accurately perform the obligations as intended (e.g., where altering a transaction is impossible, for example, the parties might require that smart contracts are voided).

2. Jurisdictional Cooperation: As industry continues to evolve and digitize, it is important, as discussed in the previous Section, for different domestic regulatory regimes to cooperate to uniformly enforce and regulate DLT-based smart contracts, contract validity and enforceability of transfers. For example, without adequate jurisdictional cooperation, the legal framework regarding enforcement of smart contracts may be finalized in one jurisdiction but remain unfinished or different in another (e.g., some legal contracts may be required to comply with regulations from one jurisdiction which contradict those in another jurisdiction).[37]

Certain jurisdictions have begun to consider some aspects of smart contracts in light of their legal frameworks. For example, as highlighted above, in England and Wales, the Law Commission published a report finding that the English legal system was sufficient to support the use of smart legal contracts.[38] The U.K. Jurisdiction Taskforce also had previously issued a Legal Statement on the legal status of cryptocurrency and smart contracts that "a smart contract is capable of satisfying the basic requirements of an English law legal contract."[39] Separate to issues around the enforceability or legally binding status of smart contract code, some jurisdictions are also considering the implications of digitalization in the context of transferring property rights—for example, in the United States, amendments to the Uniform Commercial Code (UCC) were introduced in 2022 [40] regarding "controllable electronic records", addressing property interest transfers in digital assets, including transfers that may involve the use of smart contracts and DLT). These amendments are working their way through state adoption now. Provisions such as these, provide valuable clarity to the market.

However, other jurisdictions have not yet expressly conveyed that common law precedent is sufficient to support a finding of smart contract enforceability, instead highlighting that an absence of legislation or regulatory decision can forestall the implementation of blockchain technology by financial institutions. One regulator observed that "[i]n the absence of pre-emptive legislation or a regulatory decision on the enforceability of smart contracts," financial institutions in some jurisdictions will not be able to progress with the implementation of blockchain technology.[41]

Other jurisdictions have taken a different approach. Some U.S. states have implemented laws that explicitly provide that no otherwise legally enforceable contract is unenforceable simply because a blockchain was used to create, store, or verify it.[42] While the adoption of blockchain-friendly laws by each individual state should not be viewed as a necessity to resolve questions of legal enforceability, state legislatures could help facilitate the adoption of the technology by enacting similar laws, which would serve to reduce litigation costs, eliminate contractual netting concerns, and help to expedite the development of financial markets deploying smart contracts. As previously mentioned, the adoption of UCC Article 12 at the individual state level is an example of an ongoing effort to provide uniformity with respect to commercial transactions involving digital asset technologies, including blockchain. Still, many states have not adopted these commercial provisions, and state law fragmentation persists in contract default scenarios such as insolvencies where multiple state laws are applied across debtor contracts in insolvency proceedings impacting financial market participants. These types of scenarios create additional complexities

[37]For example, in the United States, the Electronic Signatures in Global and National Commerce Act. 15 U.S.C. 7001.
[38]Law Commission of England and Wales, "Smart legal contracts – Advice to Government" (Nov. 25, 2021)
[39]Sir Geoffrey Vos, Chancellor of the High Court, "The Launch of the Legal Statement on the Status of Cryptoassets and Smart Contracts" (Nov. 18, 2019), para. 19; see also Innovation in post trade services - opportunities, risks and the role for the public sector speech by Sir Jon Cunliffe, Bank of England (Sept. 28, 2022), acknowledging that, "smart contracts carried the status of contracts as understood in law." Available at: https://www.bankofengland.co.uk/speech/2022/september/jon-cunliffe-keynote-speech-at-the-afme-operations-post-trade-technology-innovation-conference.
[40]UCC, 2022 Amendments to, Uniform Law Commission, https://www.uniformlaws.org/committees/community-home?CommunityKey=1457c422-ddb7-40b0-8c76-39a1991651ac.
[41]Whitepaper 2.0 on Distributed Ledger Technology: Annex, HKMA (Oct. 25, 2017). Available at: https://www.hkma.gov.hk/media/eng/doc/key-functions/finanical-infrastructure/infrastructure/20171025e1a1.pdf.
[42]See, e.g., 205 Ill. Comp. Stat. 730 § 10(a).

in applying unified law across the U.S. Similarly, from the EU perspective (where most Member State laws are silent on the legal enforceability of smart contracts governing financial services transactions, and such issues will likely depend on the approaches taken under existing laws on a Member State level), different legal frameworks of individual Member States may also give rise to cross-border issues and barriers to developing interoperable solutions across Member States.

It is also recommended that jurisdictions cooperate to support the utilization of smart contracts on a cross-border basis. Similar to agreements that support legal enforceability of contracts across jurisdictions in broader financial services, it would be beneficial for this type of cooperation to exist for smart contracts. This would support DLT scaling and broader interoperability of smart contracts on a cross-border basis. This type of coordination could also be trialed and scaled in regulatory sandboxes (see Annex 2).

International bodies can support cross-border cooperation by continuing to develop global principles, encouraging cross-border cooperation to reduce fragmentation, and supporting industry-led efforts to work towards standardization. For example, this can be done with respect to:

Industry Best Practice

As permissioned DLT-networks typically feature a supporting legal agreement, this can aid in jurisdictional enforcement of the smart contract (if cross-border cooperation is required, noting this is not a risk factor in private permissioned environments). Similar to the considerations under enforceability, industry can consider that if a legal contract exists in the relevant jurisdiction, a smart contract executing certain obligations set out therein is also likely to be enforceable.

Industry can also ensure that smart contracts make reference to and describe the smart contract, and the contracting parties should consider the appropriateness of the mitigations in this Section.

Finally, a smart contract should (where appropriate) also include "governing law" and "jurisdiction" provisions. The inclusion of these terms is always important, but especially so in cross-border transactions where the law of contracts, and even of smart contracts, may differ. A smart contract-powered agreement in England, for example, may have different requirements than one in New York or Singapore. The underlying agreement and smart contract should also align with these provisions. For example, some jurisdictions may have specific requirements for signatures. Relatedly, firms should consider the impact of the provisions for insolvency and netting purposes. Pre-trade execution should consider the ability to net outstanding transactions and collateral in a counterparty default scenario.

- Development of global principles such as through the Basel Committee on Banking Supervision (BCBS), the Committee on Payments and Market Infrastructures (CPMI), the International Organization of Securities Commissions (IOSCO) and the Financial Stability Board (FSB) which guide regional developments;

- Support for implementation of industry led standards and best practices on a cross-border basis—the ISDA documentation (including the ISDA Master Agreement[43]) is an example of an industry-led, regulator-supported, and globally accepted standard in the context of derivative contracts; and

- Cross-border public and private sector collaboration to consider how to harmonize certifications for applied standards, rather than having audit or certification requirements implemented on a jurisdiction-by-jurisdiction or case-by-case basis.

[43]ISDA Master Agreement: https://www.isda.org/book/2002-isda-master-agreement-mylibrary/

3. Steps to Establish Liability & Intention:

In the case of code-only smart contracts, courts would presumably interpret code to determine intent – a practice best undergone by technical experts. There have also been initiatives in some jurisdictions to put in place liability and digital dispute resolution rules for blockchain-enabled transactions. The U.K. Jurisdiction Taskforce, for example, released its Digital Dispute Resolution Rules in 2021, therefore introducing a mechanism into the existing dispute resolution ecosystem to facilitate resolution of commercial disputes involving new technologies such as cryptoassets, smart contracts, DLT, and fintech applications more broadly.[44] These rules are designed to create arbitration tribunals which operate very quickly, making decisions within thirty days of appointment.[45] Unlike other online dispute resolution solutions, the Rules also allow for anonymous dispute resolution, and for the electronic incorporation of the Rules into smart contracts on the blockchain.

As smart contract usage grows and scales, regulators can also consider how to support industry in building out appropriate reporting requirements for confidential corporate action, tax, and regulatory data if these requirements are not specified.

Industry Best Practice

Industry can consider how the underlying agreement can allow for flexibility in the case of unforeseen incidents giving rise to errors in execution. For example, an agreement might adapt language from traditional force majeure clauses to encompass blockchain-specific events like network outages or forks. A "kill switch" clause that allows parties to hold a smart contract's execution in the case of unforeseen circumstances may also be prudent. Errors may also come from non-contractual parties or sources, such as if the smart contract relies on data from oracles.

Regulators can work with industry to establish liability and intention for smart contract usage by:

- Adopting digital dispute resolution rules, if not in place already;
- Working with industry to identify best practice through public-private sector collaboration (see spotlight section below); and
- Providing specificity and frameworks within which smart contracts are authorized to share the appropriate corporate action, tax, and regulatory data in a compliant manner.

Best practice within industry includes clauses to assign and limit liability. Liabilities for errors and vulnerabilities in the smart contract code can be assigned to the relevant parties rather than being addressed after an error occurs. Contracting parties may wish to consider limiting liability for any smart contract failure to the value of any impacted transaction.

Furthermore, when considering tax, regulatory and corporate data sharing and other requirements firms can mandate operational mitigations to govern the execution of the smart contract within the legal agreement.

[44] "The Digital Dispute Resolution Rules" by the U.K. Jurisdiction Taskforce. Available at https://ukjt.lawtechuk.io/.
[45] Id.

IV. CONCLUSION

Spotlight on Public/Private Sector Collaboration as an Additional Way Forward

Hybrid industry-policymaker initiatives are also beneficial for industry and regulators to develop appropriate provisions. In 2022, the Monetary Authority of Singapore (MAS) launched Project Guardian, a "collaborative initiative between policymakers and the financial industry to enhance liquidity and efficiency of financial markets through asset tokenisation."

Members of the Industry Group individually collaborate with policymakers across a number of asset classes: including fixed income, asset and wealth management, and foreign exchange, and on a wide variety of use cases, including digital issuance of funds, listing frameworks for debt securities, on-chain price and trade execution, and cross border FX settlement. In particular, MAS notes that smart contracts are used to implement a number of services like payments, lending, borrowing, and foreign exchange. These collaborations may result further regulatory guidance and legal certainty from participating policymakers based on their experiences. It could also be a beneficial way to identify the appropriate liability provisions and intent in a "live" transaction, which is a useful way to stress test and prepare for broader scaling of smart contracts and DLT within financial services.

IV. Conclusion

Development of a future digital finance ecosystem can be supported through the cooperation and alignment of policymakers and market participants across jurisdictions on legal and regulatory guidance that provides appropriate protections and promotes innovation. One critical component of this future ecosystem will be smart contracts, as already demonstrated by the initial implementation of this technology within financial markets.

As discussed throughout this Primer, while financial services continue to be digitized and responsible innovation is fostered, smart contracts remain a critical component to this ongoing evolution. Yet it is equally crucial to remember that the current DLT-based ecosystem is still nascent. Primary and secondary markets have yet to reach a critical mass in adoption, as noted in the context provided in Section II of this Primer. At this early, foundational stage, analysis and dialogue between public and private sector participants on how to solve technical challenges and work towards global harmonization, are imperative. The critical priorities are captured below to further clarify dialogue surrounding smart contracts and work towards concrete solutions that can appropriately mitigate risks while still supporting innovation.

IV. A. Calls to Action

These recommendations have been developed with the common goal of providing clarity to both the public sector and market participants and initiating a dialogue on how smart contracts can be implemented in a responsible way, as well as governed within the broader existing and evolving legal, regulatory, and risk management frameworks that ensure safe and secure financial markets innovation. They are each accompanied by specific calls to action, intended as practical next steps to drive impact and continue to foster dialogue across the public and private sectors.

This Primer advocates that regulators can and should use existing frameworks that address operational and technology related risks to regulate smart contracts. While in some cases, the analysis in this Primer found that as smart contract usage continues to scale, regulators can support this future evolution through some clarifications and legal adjustments, market participants also highlight how the compliant and responsible use of smart contracts is already taking place.

The recommendations support existing best practices within industry and also look ahead towards how further cooperation can be achieved in order to enable DLT scaling within financial services.

Recommendation #1: Prioritize Key Drivers of Smart Contract Interoperability Through Technical Standards and Developing a Template-Based Approach to Smart Contract Standardization

Call to Action: Given the significant role that smart contracts are expected to play in DLT-based financial ecosystems, we propose that "smart contracts" occupy a key area that requires focus to drive industry and regulatory cooperation to move towards smart contract standardization. This Primer proposes the following three key areas be prioritized for development of smart contract standardization across industry:

1. **Technical standards** such as standards for developing tokens (e.g., ERC-3643, FINP2P, IVMS101[46]), messaging standards or protocols that allow for cross-chain interoperability, bridge solutions, etc.;

2. **Standardization of smart contract provisions and template-based approaches to smart-contract development** with respect to specific products or asset classes, where appropriate, for example by leveraging the initiatives ISDA has taken to develop standardized approaches to smart derivative contracts (noting that ISDA documentation[47] is widely adopted and accordingly there is already a relatively high degree of contract standardization in the context of derivatives trading such that it may be possible to develop standardized approaches on a logic-level, at least to provide a foundation which developers may draw upon to enable specific functionality—however, this level of standardization may not be appropriate for other types of products or services), as well as other relevant projects undertaken by industry associations in the capital markets space such as the Common Domain Model;[48] and

3. **Best practice and risk-mitigation frameworks** for audit and verification of smart contract code, responsibility and liability for design and execution of smart contracts, use of external data feeds, transparency, the extent of manual intervention required within automated processes, and dispute resolution mechanisms. Smart contract risks and mitigation strategies, and how these can be addressed via existing regulatory frameworks for mitigating operational and technical risk, are discussed and expanded upon in Section III.

Recommendation #2: Support for Utilization of Existing Technology and Operational Risk Frameworks to Regulate Smart Contract Implementation

[46]ERC3643: https://www.erc3643.org/, FINP2P: https://finp2p-docs.ownera.io/docs/introduction-1, IVMS101: https://www.intervasp.org/
[47]Including the ISDA Master Agreement and templates for ancillary doucmentation, and ISDA Taxonomy and Clause Library
[48]Common Domain Model: https://www.finos.org/common-domain-model

Call to Action: Through a detailed analysis this Primer urges industry and policymakers to utilize existing technology and operational risk frameworks to mitigate smart contract risk. This can be done through applying existing frameworks to the eight identified principles to guide best practice in smart contract implementation:

1. *Development and growth of internal risk and control and compliance function with appropriate resourcing*

2. *Have a clear and proportionate incident response mechanism/policy*

3. *Standardized requirements for smart contract audits, including for completeness and robustness while working towards a template-based approach for broader smart contract standardization*

4. *Ensure smart contracts are written in clear, well-documented code that is easy to understand and audit*

5. *Extensively test smart contracts before deployment using various scenarios and stress tests*

6. *Implement strong access controls to restrict who can modify or interact with the smart contract*

7. *Integrate smart contracts with existing workflows with human intervention at critical points for added security*

8. *Agreement of contractual obligations between relevant parties (where applicable[49])*

Recommendation #3: Look to Future-Proof Legal and Regulatory Regimes by Providing Clarity and Support for Responsible Innovation, Addressing Where Unique Risks Arise Without Creating Special New Regimes for Smart Contracts

Call to Action: While existing operational and technology risk management processes, as well as financial risk management programs, sound governance structures and prudent contractual review, can mitigate certain risks, there are areas where the public sector could further support smart contract scaling by providing additional legal and regulatory clarifications as well as adjustments where appropriate, without creating entirely new special regimes relating to smart contracts.

As discussed in full in Section III.B., the three broad areas where industry would urge the public sector to consider how to future-proof regulatory regimes to support smart contract scaling, along with some specific suggestions for each, are:

1. Legal Clarifications

Steps the regulatory community could take to support smart contract scaling and to reinforce industry best practices include:

- Updating legal guidance to support legal enforceability or to otherwise clarify the legal treatment of smart contracts in their jurisdictions;

- Acknowledging that DLT-based smart contracts can be legally binding and enforceable contracts; and

- Adopting tools and guidance on digital dispute resolution and insolvency.

2. Jurisdictional Cooperation

International bodies can support cross-border cooperation by continuing to develop global principles, encouraging cross-border cooperation to reduce fragmentation, and supporting industry-led efforts to work towards standardization. For example, this can be done with respect to:

- Development of global principles which guide regional developments;

- Support for implementation of industry led standards and best practices on a cross-border basis; and

[49]Noting as detailed in Section III.A.8. that this is a reduced risk factor for private permissioned networks.

- Cross-border public and private sector collaboration, to consider how to harmonize certifications for applied standards, rather than having audit or certification requirements implemented on a jurisdiction-by-jurisdiction or case-by-case basis.

3. Steps to Establish Liability & Intention

Regulators can work with industry to establish liability & intention for smart contract usage by:

- Adopting digital dispute resolution rules if not in place already;
- Working with industry to identify best practice through public-private sector collaboration; and
- Providing specificity and frameworks within which smart contracts are authorized to share the appropriate corporate action, tax, and regulatory data in a compliant manner.

V. APPENDICES

V. Appendix

Annex 1 – Smart Contract Best Practice: Operational and Technical Risk Mitigations and Application of Existing Regulation

The below chart is the collated application of existing industry best practice and risk mitigation across the eight themes discussed in the paper in Section III. A.. It identifies the functional area of risk management, relevant regulator frameworks and guidance which could be applied, existing industry best practice, and why this matters for responsible innovation of smart contracts.

Principle 1: Development and growth of internal risk and control or compliance function with appropriate resourcing			
Functional Area	**Relevant Regulatory Framework / Guidance**	**Existing Industry Best Practice / Mitigation Strategy**	**Why this Matters: The Risk Being Addressed**
Operational / Technological & Compliance / Regulatory	European Banking Authority (EBA) – Guidelines on ICT and security risk management (November 2019) FSB – Principles for an effective risk appetite framework (November 2013) Monetary Authority of Singapore (MAS) - Guidelines on Risk Management Practices – Technology Risk (January 2021) FCA Principles for Business, Principle 2 & Principle 3 FCA - SYSC (Senior Management Arrangements, Systems and Controls) rules, in particular SYSC 3 (Systems and Controls) and SYSC 7 (Risk control) Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (DORA) HKMA - Supervisory Policy Manual on Operational Risk Management (July 2022) HKMA - Circular on risk management considerations related to the use of distributed ledger technology (April 2024) HKMA - Supervisory Policy Manual on General Principles for Technology Risk Management (June 2024)	• Implement and maintain adequate risk management policies and procedures, including procedures for risk assessment, identifying risk tolerances, and risk mitigation. • Implement and maintain an effective compliance function to monitor, identify, mitigate and address compliance risks. • Leverage on-chain data to track ownership, using verifiable credentials to enforce compliance while protecting privacy by validating eligibility without exposing private data. • Risk control and compliance functions should have oversight of, where appropriate, the full development cycle, from proposal to deployment and ongoing monitoring. • Risk management and compliance functions should monitor compliance of and provide advice to persons / business lines developing, managing, and deploying smart contracts. • Appoint a chief risk officer and compliance officer, and establishing relevant committees (with individuals assigned to key roles and responsibilities, and relevant reporting lines). • Monitor on a regular basis the adequacy of such measures and take steps to address deficiencies. • Risk control and compliance functions should be directly accountable to the management body. • Risk control and compliance functions should have the necessary authority, resources, expertise and access to all relevant information. • Risk control and compliance should be independent of the business they control.	Firms need to have effective risk governance structures in place to identify, understand and manage risks associated with the development and use of technology generally, including smart contracts. An effective risk management system reduces the likelihood of incidents occurring as well as mitigates the impact of incidents. Such practices also reduce compliance risk—the financial services sector is a highly regulated one, where there are numerous regulatory frameworks/legislation which are technology- neutral (e.g., laws applicable to automation, use of data, artificial intelligence, digital operational resilience and business continuity, may all be applicable to the use of smart contracts, depending on the use case). The potentially cross-border application of smart contracts also increases compliance risk.

Principle 2: Have a clear and proportionate incident response mechanism/policy			
Functional Area	**Relevant Regulatory Framework / Guidance**	**Existing Industry Best Practice / Mitigation Strategy**	**Why this Matters: The Risk Being Addressed**
Operational / Technological & Compliance / Regulatory	NFA Interpretive Notice 9070 and NFA Compliance Rules 2-9, 2-36 and 2-49 FCA – PS21/3 Policy Statement on Building Operational Resilience FCA - Senior Management Arrangements, Systems and Controls (SYSC) rules in particular SYSC 15A (Operational Resilience) and SYSC 8 (Outsourcing) Bank of England, Prudential Regulation Authority (PRA) – Operational resilience: Impact tolerances for important business services Federal Financial Institutions Examination Council – Information Security Program Management (Information Security Handbook) Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, Office of the Comptroller of the Currency – Sound Practices to Strengthen Operational Resilience (October 2020) Basel Committee on Banking Supervision (BCBS) – Principles for Operational Resilience (August 2020) Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (DORA) MAS – Notice on Technology Risk Management (May 2024) MAS – Guidelines on Risk Management Practices – Technology Risk (January 2021) MAS – Guidelines on Business Continuity Management (June 2022)	• Have clear and proportionate incident response mechanism/ policies and procedures, including: procedures to identify, track, log, categorize and classify incidents (e.g., by prioritizing based on business criticality); procedures to identify, analyze and solve the root cause behind one or more incidents; processes to mitigate impacts and harm of incidents and to ensure continuation of critical business functions and processes when disruptions occur (including, if appropriate, the ability to continue operating certain functions and services without the use of smart contracts); and post-incident review processes to analyze causes of disruption and need for improvements. • Maintain up-to-date inventory of smart contracts and relevant ICT systems, devices, databases in relation to which such smart contracts are used, and document interdependencies between different ICT assets to facilitate efficient response to security and operational incidents. • Integrate smart contracts with existing workflows (see also principle 7 below) with human intervention at critical points for added security. • Define, implement, and regularly test data and systems backup and restoration procedures to ensure that they can be recovered as required. • Establish effective communication plans, both internally (e.g., escalation procedures) and externally (e.g., notifications to stakeholders) • Design at the outset smart contracts which are able to be upgraded as the need arises to mitigate any new and evolving risks or to solve post-deployment bugs etc.	Firms need to have effective risk governance structures in place to identify, understand and manage risks associated with the development and use of technology generally, including smart contracts. An effective risk management system reduces the likelihood of incidents occurring as well as mitigates the impact of incidents. Such practices also reduce compliance risk—the financial services sector is a highly regulated one, where there are numerous regulatory frameworks/ legislation which are technology-neutral (e.g., laws applicable to automation, use of data, artificial intelligence, digital operational resilience and business continuity, may all be applicable to the use of smart contracts, depending on the use case). The potentially cross-border application of smart contracts also increases compliance risk.

Functional Area	Relevant Regulatory Framework / Guidance	Existing Industry Best Practice / Mitigation Strategy	Why this Matters: The Risk Being Addressed
Operational / Technological & Compliance / Regulatory	Security Exchange Commission (SEC) – Regulation Systems Compliance and Integrity (Regulation SCI) (February 2015) Bank of England – Financial Stability in Focus: The FCP's macroprudential approach to operational resilience (March 2024) HKMA - Supervisory Policy Manual on Operational Resilience (May 2022) HKMA - Supervisory Policy Manual on Business Continuity Planning (May 2022) HKMA - Supervisory Policy Manual on General Principles for Technology Risk Management (June 2024)		

Principle 3: Standardized requirements for smart contract audits, including for completeness and robustness while working towards a template-based approach for broader smart contract standardization			
Functional Area	**Relevant Regulatory Framework / Guidance**	**Existing Industry Best Practice / Mitigation Strategy**	**Why this Matters: The Risk Being Addressed**
Operational / Technological	European Banking Authority (EBA) – Guidelines on ICT and security risk management (November 2019) Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (DORA) An example of a non-supervisory authority's guidance is the National Institute of Standards and Technology Internal Report 8202: Blockchain Technology Overview (October 2018) HKMA - Whitepaper 2.0 on Distributed Ledger Technology (October 2017) HKMA - Circular on sale and distribution of tokenised products (February 2024) HKMA - Circular on risk management considerations related to the use of distributed ledger technology (April 2024)	• Audits should be undertaken by independent auditors with sufficient knowledge, skills and expertise in smart contracts and blockchain. • Given the transparent nature of blockchain networks (including permissioned networks), it may be possible for certain audits to occur on an automated and constant basis, as opposed to taking place on a periodic basis. • Where smart contract code is developed / provided / managed by third party providers, appropriate audit and access rights should be granted to financial entities and their regulators in the relevant vendor contracts. • Firms can integrate international standards applicable to software more broadly, such as ISO/IEC 27001. • Audits can also be conducted in line with smart contract-specific standards which may be developed by industry.[50] • In addition to audits around software code, carry out audits relating to external data which feeds into the smart contract such as via data oracles, as well as audits on internal governance, risk controls and compliance functions around smart contract development and deployment processes	Generally, a financial entity's ICT systems and processes would be audited on a periodic basis, particularly those that support critical business functions and operations. Given that smart contracts are designed to execute autonomously and may be used in combination with sensitive data, smart contract code should in particular be audited for security issues or errors. Smart contracts may also consume off-chain data through external systems such as data oracles, which themselves may be susceptible to manipulation– appropriate auditing practices will therefore help to mitigate security and data accuracy risks in relation to such oracles.

[50] An example is the "Smart Contract Security Verification Standard" (v2), a free checklist "created to standardize the security of smart contracts for developers, architects, security reviewers, and vendors".

Principle 4: Ensure smart contracts are written in clear, well-documented code that is easy to understand and audit			
Functional Area	**Relevant Regulatory Framework / Guidance**	**Existing Industry Best Practice / Mitigation Strategy**	**Why this Matters: The Risk Being Addressed**
Operational / Technological	Financial services regulators typically take a principles or outcomes-based approach and would not regulate code readability specifically, due to the technical nature of software development, the variety of programming practices, and to avoid stifling innovation by industry.	Some practices which industry broadly accepts to be good/ best practice, and which are generally applicable to the software code development include: • Using consistent coding style such as naming conventions, indentations and commenting. • Using in-line comments to explain the purpose of a particular line of code and the relevant logic. • Using meaningful variable names, function names, and clear logic structures where possible to ensure readability of the code. • Avoiding excessively deeply nested structures. • Integration of smart contracts with existing workflows with human intervention at critical points for added security.	As many smart contracts have self-execution coded in, this could lead to self-execution of errors. This may cause the unintended consequences, including the violation of contractual terms and provisions. Clear and readable code helps to reduce risks of errors in code development, as well as to mitigate risks around code interpretation in the event of a dispute in the context of the associated legal agreement. More broadly, clearly written and readable code also facilitates code audits, maintenance and updates, which can help to mitigate compliance risks as well as technical/operational risks of failures.

Principle 5: Extensively test smart contracts before deployment using various scenarios and stress tests			
Functional Area	**Relevant Regulatory Framework / Guidance**	**Existing Industry Best Practice / Mitigation Strategy**	**Why this Matters: The Risk Being Addressed**
Operational / Technological	HKMA - Circular on risk management considerations related to the use of distributed ledger technology (April 2024) FINRA's Regulatory Notice 15-09 Recommendations for Standard Procedures which clearly catalogued, labelled, and isolated code both for implementation and for testing. BCBS general principles for stress testing IOSCO cyber resilience guidelines which provide some guidance on the kind of stress testing that private market participants can deploy when using or developing smart contracts.	• Ensure all code is reviewed, tested, and audited as appropriate by third parties. • Consideration of "best practice" standards for the review of smart contracts pre-deployment. • Ensure that smart contracts are written in clear, easy-to-audit, well-documented code (see also principles 3 & 4 above). • Extensively test smart contracts before deployment using various scenarios and stress tests with external third parties where appropriate (see also principles 3 & 4 above). • Ensure technology and cybersecurity policies allow for code review and testing, where appropriate.	Lack of pre-deployment consensus of the business logic represented in the smart contracts could result in errant or inadvertent business logic execution. Erroneous code could result in potential breach of contractual terms, and risk of voidability of contract.

Principle 6: Implement strong access controls to restrict who can modify or interact with the smart contract			
Functional Area	**Relevant Regulatory Framework / Guidance**	**Existing Industry Best Practice / Mitigation Strategy**	**Why this Matters: The Risk Being Addressed**
Cybersecurity	SEC and NFA have eight regulations on safeguarding the privacy of consumer information given to third parties. SEC recently adopted final rules requiring a general cybersecurity risk management and incident disclosure and a small entity compliance guide. CFTC required risk management programs that include operational risk and information security. See 17 C.F.R. §§ 1.11, 23.600. Federal Reserve Board, the FDIC, and the OCC of Treasury interagency guidance on third-party risk management. HKMA - Whitepaper 2.0 on Distributed Ledger Technology (October 2017) HKMA - Circular on managing cyber risk associated with third-party service providers (December 2023) HKMA - Circular on risk management considerations related to the use of distributed ledger technology (April 2024) MAS – Notices on Cyber Hygiene (May 2022) set out requirements on securing administrative accounts. MAS – Guidelines on Risk Management Practices - Technology Risks (Jan 2021) contains requirements on privileged access management.	• Implement a standardized secure software development lifecycle that includes smart contract security audit and formal verification of sensitive functions. • Regularly perform smart contract-focused threat modeling to capture, communicate, and remediate the risk of each use case.	Lack of smart contract security audit and review process, as well as lack of appropriate lifecycle development programs could lead to potential for exploitation of vulnerable code and flawed business logic leading to denial of service attacks, fraud or theft.[51]

[51]"An Introduction to Smart Contracts and Their Potential and Inherent Limitations," Levi, Stuart; Lipton, Alex (May 26, 2018). Available at: https://corpgov.law.harvard.edu/2018/05/26/an-introduction-to-smart-contracts-and-their-potential-and-inherent-limitations/.

Principle 7: Integrate smart contracts with existing workflows with human intervention at critical points for added security			
Functional Area	**Relevant Regulatory Framework / Guidance**	**Existing Industry Best Practice / Mitigation Strategy**	**Why this Matters: The Risk Being Addressed**
Cybersecurity	MAS – Guidelines on Risk Management Practices - Technology Risks (Jan 2021). US Federal Reserve and the FDIC proposed guidelines establishing a "three-lines-of-defense" model of risk management as a standard of general risk management governance for all depository institutions. HKMA - Circular on risk associated with third-party IT solution, Annex (September 2024)	• Implement ledger security monitoring and alerting capabilities. • Leverage a key management solution with transaction level policy enforcement capability. • Implement a defense-in-depth strategy with multilayer access controls to restrict who can manage or interact with the smart access controls to restrict who can modify or interact with the smart contract and its middleware. • Implementing a mechanism that requires certain access privileges for approving orders that exceed pre-determined volume and price thresholds that are pre-set within the code.	Malicious threat actors (with an increased risk of this on public-permissionless networks) could exploit vulnerable code via third-party hacking, leading to fraud/theft.[52]

Principle 8: Agreement of contractual obligations between relevant parties			
Functional Area	**Relevant Regulatory Framework / Guidance**	**Existing Industry Best Practice / Mitigation Strategy**	**Why this Matters: The Risk Being Addressed**
Legal	The law of contracts of the local jurisdiction would govern provisions identifying valid smart contracts.[53] For a more in-depth adiscussion of this issue, see Section III.B.1 above.	• Consider the governing contract law principles prior to reaching contractual agreement on governing law and jurisdiction provisions. • Ensure that all parties have identified the valid smart contract. • Include contractual provisions allowing for the creation of valid smart contracts that satisfy requirements for legal agreements of that type.	Agreeing to a favorable governing law and jurisdictional provisions mitigates enforceability risk and, in the event of a disagreement between counterparties to an agreement, facilitates quicker dispute resolution by ensuring the jurisdiction of the legal agreement is not in question.

[52]Id.

[53]For example, in the United States, the Illinois legislature adopted a law providing that no otherwise legally enforceable contract is unenforceable simply because a blockchain was used to create, store, or verify it. Certain domestic regulators, such as the CFTC and SEC, require registered swap dealers and security-based swap dealers to agree to governing law provisions prior to entering into OTC derivative contracts. See 17 C.F.R. § 23.504(b), 17 C.F.R. § 240.15Fi-5.

Annex 2 – Further Detailed Existing Technology Neutral Areas of Regulation and Guidance

This Annex serves to further illustrate the wide range of existing areas of regulation (and associated guidance), it expands upon the eight themes discussed within this Primer and aims to cover a broader thematic overview of existing regulations that could to financial entities' usage of smart contracts. This list is by no means exhaustive but serves as a snapshot of existing functional areas that clearly also may be used to assess and address potential impacts from smart contracts. The following chart is complementary to Annex 1 and aims to serve as a further resource for both the public and private sectors.

Functional Area	Application to Smart Contracts	Examples of Existing Regulations and Guidance in this Area
Model Risk Management	Traditional model-risk management frameworks are applicable to the development, validation, implementation, use and governance of many models. Current regulatory guidelines or frameworks applicable to model risk management are technology neutral - to the extent smart contracts are used in the context of quantitative analysis / modelling by financial entities, such requirements (such as on data integrity, testing etc.) would likely be applicable.	Office of Comptroller of the Currency (OCC) – Model Risk Management: New Comptroller's Handbook Booklet (Aug. 2021) Federal Reserve Board (FRB) & Office of Comptroller of the Currency (OCC) – Supervisory Guidance on Model Risk Management (Apr. 2011) European Central Bank (ECB) - Guide to internal models (February 2024)
Third-Party Risk Management	Third-party risk management (particularly in the context of outsourcing arrangements and digital operational resilience) is of high importance for financial institutions. Where smart contract code is developed or deployed by third party providers, or third-party providers are otherwise involved in the use and development of smart contracts by financial entities, financial entities would need to comply with the relevant regulatory requirements (for example, by ensuring appropriate audit and access rights to monitor the performance of such third party).	Federal Reserve Board (FRB), Office of the Comptroller of the Currency (OCC), Securities and Exchange Commission (SEC) – Interagency Guidance on Third-Party Relationships: Risk Management (June 2023) Financial Stability Board (FSB) – Enhancing Third-Party Risk Management and Oversight: A toolkit for financial institutions and financial authorities (Dec. 2023) International Organization of Securities Commissions (IOSCO) – Principles on Outsourcing: Final Report (Oct. 2021) Money Authority of Singapore (MAS) - Third Party Risk Management Monetary Authority of Singapore (MAS) - Guidelines for financial institutions on risk management of outsourcing arrangements (Oct. 2018) Securities and Exchange Commission (SEC) - Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Customer Information (May 2024) Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (DORA) European Banking Authority (EBA) – Guidelines on Outsourcing Arrangements (March 2019) European Insurance and Occupational Pensions Authority (EIOPA) - Guidelines on outsourcing to cloud service providers (Feb 2020) European Securities Market Association (ESMA) – Guidelines on outsourcing to cloud service providers (Dec 2020) Bank of England – SS2/21 Outsourcing and third party risk management (March 2021) HKMA - Circular on risk associated with third-party IT solution, Annex (September 2024) Financial Conduct Authority (FCA) - FCA Handbook, in particular Principle 3 and SYSC 8 (Outsourcing), FG16/5: Guidance for firms outsourcing to the 'cloud' and other third party IT services

Functional Area	Application to Smart Contracts	Examples of Existing Regulations and Guidance in this Area
Market Protection	Financial firms that use smart contracts in connection with providing services to investors may find that their systems are subject to the requirements of various market protection legislation (including transparency and reporting obligations), such as MiFID II, the Dodd-Frank Act, the Securities and Futures Act, and the Financial Instruments and Exchange Act. For example, financial entities using systems for trading or investment decision-making must ensure that they produce detailed and interpretable logs and records of all decisions and transactions in order to help meet their obligations under such laws. Systems used in trading must be designed to operate in a way that complies with market abuse requirements, and allows such systems to be auditable. Certain market-specific regulations require financial firms to take all sufficient steps to obtain the best possible result for their clients when executing orders. Systems used in automated trading must therefore be designed to consistently consider multiple factors (such as price, cost, speed, and likelihood of execution) to ensure compliance with the best execution policy. Market-specific regulations that apply to general obligations and trading practices would apply regardless of whether smart contracts are used.	Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 (MiFID II) European Securities Market Association (ESMA) – MiFID II/MiFIR review report on algorithmic trading (Sept. 2021) Prudential Regulatory Authority (PRA) - Algorithmic Trading Part of the PRA Rulebook Bank of England - Supervisory Statement 5/18 on Algorithmic Trading (June 2018) Securities and Exchange Commission (SEC) – Investment Management Division Guidance Update on Robo-Advisers (Feb. 2017) Commodity Futures Trading Commission (CFTC) – Electronic Trading Risk Principles (Jan. 2021) Financial Industry Regulatory Authority (FINRA) – Regulatory Notice 15-09: Guidance on Effective Supervision and Control Practices for Firms Engaging in Algorithmic Trading Strategies (Mar. 2015) Financial Conduct Authority (FCA) - FCA Handbook, Principle 6 & Principle 7, MAR 7A.3 Requirements for algorithmic trading Securities and Futures Commission (SFC) - Guidelines on Online Distribution and Advisory Platforms MAS - Guidelines on Risk Management (Market Risk) (February 2006), Guidelines on the Provision of Digital Advisory Services (October 2018), Guidelines on Execution of Customers' Orders (Nov 2022)

Functional Area	Application to Smart Contracts	Examples of Existing Regulations and Guidance in this Area
Governance Structures	Firms need to have effective risk governance structures in place to identify, understand and manage risks associated with applications and systems. Where appropriate, this includes oversight of the full development cycle of technological solutions, from proposal to deployment and ongoing monitoring. While the risks stemming from smart contracts can be novel, the need for effective governance structures is not a new concept. In many jurisdictions, specific requirements already exist to ensure that financial entities have risk controls in place, and that management bodies or otherwise responsible individuals have full coverage of the firm's activities, as well as the appropriate skillsets to perform oversight roles.	Basel Committee on Banking Supervision (BCBS) – Corporate Governance Principles for banks (July 2015) Financial Conduct Authority (FCA) - The Senior Managers and Certification Regime (July 2019) Financial Conduct Authority (FCA) - Senior Management Arrangements, Systems and Controls (SYSC), in particular SYSC 4 (General organisational requirements) European Insurance and Occupational Pensions Authority (EIOPA) – Guidelines on system of governance (January 2014) European Banking Authority (EBA) - Guidelines on Internal Governance (2017) Prudential Regulatory Authority (PRA) - General Organisational Requirements and Allocation of Responsibilities parts of the PRA Rulebook Bank of England (BOE) - Supervisory Statement 21/15 on Internal Governance (April 2017) Federal Reserve Board (FRB) – "Three Lines of Defense" Risk Management Model (Oct. 2023) The Office of the Comptroller of the Currency (OCC) - Heightened Standards for Large Financial Institutions (Sept. 2014) International Association of Insurance Supervisors (IAIS) – Application Paper on Proactive Supervision of Corporate Governance (Feb. 2019) Securities and Futures Commission (SFC) – Guidelines on Online Distribution and Advisory Platforms (Dec. 2016) Financial Conduct Authority (FCA) - Senior Management Arrangements, Systems and Controls (SYSC) 4.1.1R Monetary Authority of Singapore (MAS) - Guidelines on Risk Management Practices – Board and Senior Management (June 2021)

Functional Area	Application to Smart Contracts	Examples of Existing Regulations and Guidance in this Area
Operational Resilience & Business Continuity	Operational resilience requirements help improve the stability and reliability of services so firms can continue to operate and provide critical services in the event of a disruption. Digital operational resilience is becoming an increasingly significant area of focus both for financial entities and their regulators, and the relevant regulatory frameworks will likely be applicable regardless of the technology used—for example, where there are requirements applicable broadly to all technological systems and processes, the use of smart contracts in DLT-based systems and applications will likely be subject to the rules, to ensure the financial entities are resilient and able to remain operational in the event of a failure of such systems and processes.	National Futures Association (NFA) - NFA Interpretive Notice 9070 and NFA Compliance Rules 2-9, 2-36 and 2-49 Financial Conduct Authority (FCA) – PS21/3 Policy Statement on Building Operational Resilience Financial Conduct Authority (FCA) - Senior Management Arrangements, Systems and Controls (SYSC) rules in particular SYSC 15A (Operational Resilience) and SYSC 8 (Outsourcing) Prudential Regulation Authority (PRA) – Operational resilience: Impact tolerances for important business services (SS1/21) Federal Financial Institutions Examination Council – Information Security Handbook – Information Security Program Management Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, OCC – Sound Practices to Strengthen Operational Resilience (Oct. 2020) Basel Committee on Banking Supervision (BCBS) – Principles for Operational Resilience (Aug. 2020) Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (DORA) Monetary Authority of Singapore (MAS) – Guidelines on Business Continuity Management (June 2022), Guidelines on Risk Management Practices – Operational Risk (March 1013) Bank of England – Financial Stability in Focus: The FCP's macroprudential approach to operational resilience (March 2024) Hong Kong Monetary Authority (HKMA) - 2022 Supervisory Policy Manual (SPM): New module OR-2 on "Operational Resilience" and revised module TM-G-2 on "Business Continuity Planning"

Functional Area	Application to Smart Contracts	Examples of Existing Regulations and Guidance in this Area
Risk Monitoring and Management	There are a wide range of risks that can arise from an application of smart contracts; it is important to have an effective risk monitoring and management framework in place to help ensure that key risks are identified and addressed accordingly. However, while there are potentially some novel risks to consider from the use of smart contracts, the objectives of identifying, addressing, and monitoring smart contract-related risks need not be fundamentally different to a firm's existing risk management framework.	European Banking Authority (EBA) – Guidelines on ICT and security risk management (November 2019) Financial Stability Board (FSB) – Principles for an effective risk appetite framework (Nov. 2013) Monetary Authority of Singapore (MAS) - Guidelines on Risk Management Practices – Technology Risk (Jan. 2021) Financial Conduct Authority (FCA) - FCA Principles for Business, Principles 2 & 3 Financial Conduct Authority (FCA) - SYSC (Senior Management Arrangements, Systems and Controls) rules, in particular SYSC 3 (Systems and Controls) and SYSC 7 (Risk control) Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (DORA) (in particular, DORA as supplemented by Regulatory Technical Standards on ICT risk management framework and on simplified ICT risk management framework) Hong Kong Monetary Authority (HKMA) - Supervisory Policy Manual TM-G-1 General Principles for Technology Risk Management (June 2024)
Cybersecurity	As firms consider integrating smart contracts, they must consider cybersecurity and operational implications. Regardless of what technology is being used (e.g., smart contracts, DLT or otherwise), financial institutions may suffer ICT incidents—in the case of smart contracts this could include errors / mistakes in code, software bugs, malfunctioning of related systems or devices, and cyberattacks. Frameworks and guidelines relating to protecting firms against cyber incidents, and incident response management, are likely to be applicable to the use of smart contracts.	Federal Financial Institutions Examination Council – Information Security Handbook – Information Security Program Management Securities and Exchange Commission (SEC) – Requirements to Address Cybersecurity Risks for Public Companies (adopted July 2023), Registered Investment Advisers (proposed Mar. 2022), and Market Participants (proposed Mar. 2023) The Office of the Comptroller of the Currency (OCC) – Computer-Security Incident Notification Requirements (Nov. 2021) Bank of England - SS1/21 Operational resilience: Impact tolerances for important business services (March 2021) Financial Stability Board (FSB) – Effective Practices for Cyber Incident Response and Recovery (October 2020) G7 - Fundamental Elements of Cybersecurity for the Financial Sector (October 2016) G7 – Fundamental Elements for effective assessment of Cybersecurity in the Financial Sector (October 2017) European Central Bank (ECB) - Cyber Resilience Oversight Expectations for Financial Market Infrastructures (CROE) (December 2018) International Association of Insurance Supervisors (IAIS) – Application Paper on Supervision of Insurer Cybersecurity (November 2018) Committee on Payments and Market Infrastructures (CPMI) & IOSCO - Guidance on Cyber Resilience for Financial Market Infrastructures (June 2016)

Functional Area	Application to Smart Contracts	Examples of Existing Regulations and Guidance in this Area
Cybersecurity		Financial Conduct Authority (FCA) – SYSC 13.7 (Processes and Systems) Bank of England – CBEST Threat Intelligence-Led Assessments MAS – Notices on Cyber Hygiene, Notices on Technology Risk Management, Guidelines on Technology Risk Management and Third Party Risk Management Hong Kong Monetary Authority (HKMA) - Cyber Resilience Assessment Framework (C-RAF)
Stress Testing	Stress tests are already a key part of financial entities' training and testing toolkit; they allow firms and regulators to identify and test a range of risk-based scenarios over time to improve resilience. As firms consider deploying smart contracts, it is important for smart contract systems to be tested, to assess their performance and to better understand the related reaction functions. While the scope and content of the rules vary by regulator, broadly speaking, stress-testing enables regulators to probe the resilience of financial systems in the context of emerging threats against financial stability.	Basel Committee on Banking Supervision (BCBS) – Stress Testing Principles (October 2018) European Banking Authority (EBA) - Guidelines on stress testing (July 2018) Bank of England – The Bank of England's approach to stress testing the UK banking system (October 2015) Federal Reserve Board (FRB) - Comprehensive Capital Analysis and Review (CCAR) Federal Reserve Board (FRB) - Comprehensive Liquidity Analysis and Review (CLAR)