FINTECH

NOTES

Cyber Resilience of the Central Bank Digital Currency Ecosystem

Arvinder Bharath, Anca Paduraru, and Tamas Gaidosch

NOTE/2024/003

FINTECH NOTE

Cyber Resilience of the Central Bank Digital Currency Ecosystem

Prepared by Arvinder Bharath, Anca Paduraru, and Tamas Gaidosch

August 2024

Cyber Resilience of the Central Bank Digital Currency Ecosystem

Note 2024/003

Prepared by Arvinder Bharath, Anca Paduraru, and Tamas Gaidosch*

DISCLAIMER: Fintech Notes offer practical advice from IMF staff to policymakers on important issues. The views expressed in Fintech Notes are those of the author(s) and do not necessarily represent the views of the IMF, its Executive Board, or IMF management.

RECOMMENDED CITATION: Bharath, Arvinder, Anca Paduraru, and Tamas Gaidosch. 2024. “Cyber Resilience of the Central Bank Digital Currency Ecosystem.” IMF Fintech Note 2024/003, International Monetary Fund, Washington, DC.

Publication orders may be placed online, by fax, or through the mail:

International Monetary Fund, Publications Services
P.O. Box 92780, Washington, DC 20090, USA
Tel.: (202) 623-7430 Fax: (202) 623-7201
E-mail: publications@imf.org
bookstore.IMF.org
elibrary.IMF.org

This note was written under the supervision of Tobias Adrian and Shirin Hamid. The authors are grateful to Dong He, Herve Tourpe, and Tao Sun for their guidance throughout the process. We would like to thank Victor Budau, Dennis Murathaty, Pierre Passin, Franko Solomon, Ashley Lannquist (all IMF), Cyrus Minwalla (Bank of Canada), and Veljko Andrijasevic (Sveriges Riksbank) for their helpful contributions, and Beju Shah and William Zhang (BIS-Innovation Hub), for their peer review.

Contents

Tables and Figures

Acronyms

AI	Artificial Intelligence
API	Application Programming Interface
CBDC	Central Bank Digital Currency
CLT	Centralized Ledger Technology
CPMI	Committee on Payments and Market Infrastructures
CERT	Cyber Emergency Response Team
DeFi	Decentralized Finance
DoS	Denial of Service (attack)
DDoS	Distributed Denial-of-Service (attack)
DLT	Distributed Ledger Technology
EMDE	Emerging Markets and Developing Economies
FMI	Financial Market Infrastructure
IAM	Identity and Access Management
IOSCO	International Organization of Securities Commissions
NIST	National Institute of Standards for Technology
PII	Personally Identifiable Information
PPT	People, Processes, and Technology
RSA	[Rivest, Shamir, Adleman] Public Key-Encryption Technology
QC	Quantum Computing

Glossary[1]

Term	Definition
Access Control [FSB]	Means to ensure that access to assets is authorized and restricted based on business and security requirements.
Asset[2] [FSB]	Something of either tangible or intangible value that is worth protecting, including people, information, infrastructure, finances, and reputation.
Availability [FSB]	Property of being accessible and usable on demand by an authorized entity.
Compromise [FSB]	Violation of the security of an information system.
Confidentiality [FSB]	Property that information is neither made available nor disclosed to unauthorized individuals, entities, processes, or systems.
Cyberattack [FSB]	Malicious attempt(s) to exploit vulnerabilities through the cyber medium to damage, disrupt, or gain unauthorized access to assets.
Cyber Event [FSB]	Any observable occurrence in an information system. Cyber events sometimes provide an indication that a cyber incident is occurring.
Cyber Incident [FSB]	A cyber event that adversely affects the cybersecurity of an information system or the information the system processes, stores, or transmits resulting from malicious activity.
Cyber Incident Response Plan [FSB]	The documentation of a predetermined set of instructions or procedures to guide the response to, and limit consequences of, a cyber incident.
Cyber Resilience [FSB]	The ability of an organization to continue to carry out its mission by anticipating and adapting to cyber threats and other relevant changes in the environment and by withstanding, containing, and rapidly recovering from cyber incidents.
Cyber Risk [FSB]	The combination of the probability of cyber incidents occurring and their impact.
Cybersecurity [FSB]	Preservation of confidentiality, integrity, and availability of information and/or information systems through the cyber medium. In addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved.
Cyber Threat [FSB]	A circumstance with the potential to exploit one or more vulnerabilities that adversely affects cybersecurity.
Data Breach [FSB]	Compromise of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to data transmitted, stored, or otherwise processed.
Defense-in-Depth [FSB]	Security strategy integrating people, processes, and technology to establish a variety of barriers across multiple layers and dimensions of the organization.

[1] Definitions are primarily aligned with those of the FSB Cyber Lexicon (updated in 2023): Cyber Lexicon: Updated in 2023 (fsb.org), marked by (FSB) and from the CPMI-IOSCO Guidance for FMIs: Guidance on Cyber Resilience for Financial Market Infrastructures (bis.org), marked by (CPMI-IOSCO). Other definitions are aligned with international standards for FMIs (CPMI-IOSCO PFMIs), industry standards such as by private standard setting bodies ISO or NIST or are proposed by the authors.

[2] This term refers to “asset” in a technological sense, not an economic sense such as financial assets or crypto assets.

Generative AI	The class of artificial intelligence (AI) models that emulate the structure and characteristics of input data to generate derived synthetic content. This can include images, videos, audio, text, software code, and other digital content.
Identity & Access Management (IAM) [FSB]	Encapsulates people, processes, and technology to identify and manage the data used in an information system to authenticate users and grant or deny access rights to data and system resources.
Indicators of Compromise (IoCs)	Identifying signs that a cyber incident may have occurred or may be currently occurring.
Integrity [FSB]	Property of accuracy and completeness.
Multi-Factor Authentication [FSB]	The use of two or more of the following factors to verify a user's identity: - Knowledge factor, "something an individual knows." - Possession factor, "something an individual has." - Biometric factor, "something an individual is or is able to do."
Non-repudiation	Ability to prove the occurrence of a claimed event or action and its originating entities and controlling its reversal.
Operational Risk [CPMI-IOSCO PFMI]	The risk that deficiencies in information systems or internal processes, human errors, management failures, or disruptions from external events will result in the reduction, deterioration, or breakdown of services provided.
Patch Management	Methodical notification, identification, deployment, installation, and verification of software code revisions commonly known as patches, hot fixes, and service packs.
Penetration Testing [FSB]	A test methodology in which assessors typically working under specific constraints, attempt to circumvent or defeat the security features of an information system.
Phishing [FSB]	A digital form of social engineering that attempts to acquire private or confidential information by pretending to be a trustworthy entity in an electronic communication.
Reliability	Consistent intended behavior and results.
Smart Contracts	Self-executing code based on agreed terms and conditions. Generally used on distributed ledger platforms.
Technology Risk	Risk associated with the use, ownership, or adoption of information and associated technologies.
Threat Actor [FSB]	An individual, a group or an organization believed to be operating with malicious intent.
Threat Vector	A path or route used by the threat actor to gain access to the target.
Zero-day Vulnerability	A previously unknown vulnerability within an information system.
Zero-Trust Principle	Zero trust is a security design approach that eschews the security perimeter concept ("perimeterless"). Instead, it focuses on never trusting and always verifying users and systems throughout their interactions.

Introduction

Over 100 central banks around the globe are exploring central bank digital currencies (CBDCs) to modernize payment systems. They aim to explore potential benefits, risks, and the broad range of new capabilities CBDCs might offer. Some view CBDC exploration as an opportunity to rethink their existing, legacy payment systems and build a resilient and secure infrastructure using modern technologies. However, a CBDC creates a vast and complex ecosystem that amplifies existing risk exposures and surfaces new ones. Given the implications of issuing a CBDC, it should be seen as a fundamental change in the way the central bank operates.

It can be said that without security, there is no trust, and without trust, there is no money.[3] A CBDC ecosystem will be a high-value target for a range of threat actors including nation-states and cyber criminals, and any successful attack or operational failure resulting in a service outage, data breach, or fraud will erode public trust and confidence with systemic implications. A well-functioning CBDC system therefore requires a resilient and efficient infrastructure, with the ability to onboard, authenticate, and support users on a large scale. It will necessitate an architecture that is flexible and scalable, expandable for future functionalities, and one that has security at its core.

CBDC implementation involves a range of new, technical and operational considerations which do not apply to existing payment systems. These include the use of digital tools for life-cycle management of the currency, and the use of programmability and smart contracts for its utility and efficient transfer. To maintain service continuity, seamless switching between online and offline modality may also be necessary. In addition, it requires foundational factors to be in place at a national level, such as stable and efficient communication networks, digital and financial literacy and cyber risk awareness of payment system users, technological maturity of institutions, collaboration between stakeholders, and a stable geopolitical environment.

CBDC design choices have *policy* and *security* implications, and this note covers the latter. CBDCs can be retail or wholesale, token or account-based. The underpinning architecture can be direct or intermediated; centralized or distributed; can use programmability and smart contracts; and be available offline or online. They could also use new technologies such as distributed ledgers (DLT) and artificial intelligence (AI) and be hosted in-house or in a cloud environment. These choices have different implications for operational and cyber resilience of a CBDC and the ecosystem within which it operates.

The design choices considered in this note relate to a retail CBDC given its higher complexity. A retail CBDC ecosystem is vast, complex, and highly interconnected. It includes participants who are outside the central bank's purview and governed by a different rule book. It's efficient operations are also highly reliant on telecom networks and national infrastructures. On the other hand, a wholesale CBDC ecosystem is only available to financial institutions and therefore comprises fewer participants who are

[3] Why Does Money Depend on Trust? Bank of England.

largely within the supervision of financial sector authorities and can operate within closed loop managed networks. Cyber and operational risks related to wholesale CBDC ecosystems could almost be seen as a subset of those confronted by its retail counterpart. Essentially, the key risks in a wholesale CBDC come down to “insider” threats.[4]

Although there are examples of some live CBDCs, their adoption has been very low. Many countries are at various stages of exploration and experimentation which is largely focused on policy goals and functionality with little or no testing for cyber resilience. This limits practical intelligence required for the development of specific security guidance. However, lessons can be derived from existing information security frameworks for critical financial systems and services. Some work in this regard has already been completed by the BIS Innovation Hub. Insights from this work and from the results of CBDC experiments underway, will be leveraged in future updates to this note.[5,6]

This note considers experiences from live CBDCs and is informed by experiments conducted by central banks and international institutions for domestic use. It also draws from cybersecurity and resilience frameworks from standard-setting bodies. It is organized into four sections. Sections I and II introduce digital risks including cyber risks and their impact on an interconnected CBDC ecosystem. Section III describes the attributes and examines pros and cons of commonly considered design options in a domestic, retail CBDC implementation, and suggests potential mitigations. Section IV delves into best practices for developing a cyber-resilient CBDC ecosystem.

[4] Hence, the increased focus of authorities and standard setters on end-point security guidance, such as Reducing the Risk of Wholesale Payments Fraud Related to Endpoint Security: A Toolkit (bis.org).

[5] Central Bank Digital Currency (CBDC) Information Security and Operational Risks to Central Banks (bis.org).

[6] Project Polaris: Closing the CBDC Cyber Threat Modelling Gaps (bis.org).

Section I. Cyber Risk: Context and Overview

As a payment instrument in digital form, CBDCs are exposed to digital risks as well as payment systems risks. Digital risks encompass a broad range of threats and vulnerabilities associated with the use of digital technologies and digital transformation initiatives. They sit at the intersection of people, process, technology, and data, both internal to the institution and within its supply chain (Annex 1).

Cybersecurity is generally managed along three core principles, also called the "CIA Triad" or Information Security *Trust principles*. These are:

- **Confidentiality,** that data is only visible and accessible to authorized users and for specific purpose(s).
- **Integrity,** that data is accurate and complete. Integrity needs to be ensured for data at rest and in motion and of code or logic used for its processing.
- **Availability,** that the system and data are accessible and usable as needed, and functioning as expected. Availability controls should extend to all underlying components and interconnections that could cause outages or delays to an expected service.

Vulnerabilities in people, process, and technology can be exploited by cyber threat actors to launch cyberattacks, resulting in service outages, data breaches, and fraud. It should be noted that people vulnerabilities due to errors, malintent, or manipulation can significantly impact the effectiveness of processes and technology. Reportedly, over 80 percent of cyberattacks are due to the human element.[7] In addition, 99 percent of cyberattacks can be avoided by practicing foundational security hygiene and organization-wide training and awareness.[8,9] There are several types of cyberattacks relevant to the financial sector (Table 1).

Table 1. Types of Cyberattacks

Type of Attack	Impact
Denial of service (DoS)/Distributed denial of service (DDoS)	Denial of access to legitimate users by artificially overwhelming the network bandwidth. A variant of this is DDoS which is executed from various and widely dispersed sources. It is larger in scale with more severe impact.
System intrusion and data infiltration	Unauthorized access to data, programs, protocols, and configurations, resulting in data breaches and leakage of sensitive information, code, and logic corruption.
Malware, ransomware, and wiperware	Injection of malicious code to disrupt operations and encrypt sensitive data until a ransom is paid.
Phishing and social engineering attacks	Related to people risks where social engineering techniques are used for behavior manipulation and credential theft.
Third-party and supply chain attacks	Disruption or unauthorized access to key supplier systems resulting in cascading effects.
Cryptographic key compromise	Unauthorized access to "secret" cryptographic key, leading to data breaches and fraud.

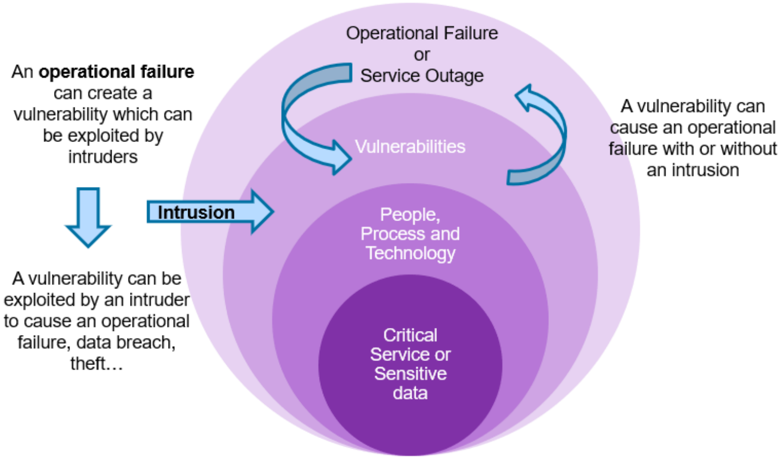
[7] Human Error Drives Most Cyber Incidents. Could AI Help? (hbr.org).

[8] Microsoft Digital Defense Report 2023 (MDDR).

[9] The threat landscape is changing rapidly due to the advent of new technologies such as AI and therefore this metric is dynamic.

Cyber risk can be a source, or a consequence, of failure of processes, people, or technology, and is a subset of operational risk (Figure 1). A cyber event can cause operational disruptions leading to reputational and financial risks. Conversely, operational events can create vulnerabilities that can be exploited by cyber threat actors, for example, an outage can facilitate unauthorized access or harvesting of credentials, resulting in fraud, data breaches, and service interruptions leading to a loss of user confidence.

Figure 1. Link between Cyber Risk and Operational Risk


An **operational failure** can create a vulnerability which can be exploited by intruders
A vulnerability can be exploited by an intruder to cause an operational failure, data breach, theft…
Intrusion
Operational Failure or Service Outage
Vulnerabilities
People, Process and Technology
Critical Service or Sensitive data
A vulnerability can cause an operational failure with or without an intrusion

Source: Authors.

Cyber risks have some unique features and require an approach and treatment that differs from traditional operational risk frameworks. This is because:

- Cyber-attackers are motivated, persistent, patient, and oftentimes well resourced. In addition, the origins of malicious cyberattacks are often difficult to detect or eradicate due to lack of geographical boundaries in cyber-space.
- The extent of damage caused by a cyberattack is difficult to fully quantify, as remnants or backdoors may remain open post recovery.[10] Losses due to cyber incidents, as highlighted in the recently published IMF Global Financial Stability Report (GFSR), are in the order of millions of US$, but under extreme scenarios they could exceed billions.[11]
- In an interconnected environment, every connection, however small or insignificant in the supply or value chain, can create exposures and vulnerabilities for the ecosystem.

[10] Different methodologies have been established to try and compute the costs. For example, in the paper “Estimating the Global Cost of Cyber Risk: Methodology and Examples (rand.org)” the cost ranges outlined by applying different methods are between 1.1 percent and 32.4 percent of global GDP.

[11] The Last Mile: Financial Vulnerabilities and Risks (imf.org).

- Certain types of cyberattacks can withstand traditional risk management and business continuity arrangements and render them ineffective. For example, a ransomware attack in an environment of real-time data replication will also impact backup data stores simultaneously.
- Cyber risks are difficult to predict as they continue to evolve due to rapid digitalization, increasing zero-day vulnerabilities[12], and fragmentation of control measures. Traditional prediction methods, which rely on past data, struggle to keep up with the fast-paced changes in technologies deployed by cyber criminals.
- Attackers make use of the tools to attack systems that are also used by the defenders to protect them, such as AI,[13] machine learning (ML), and, down the road, quantum computing (QC).
- Unlike other operational risks, a significant proportion of cyberattacks are down to the human element due to a mix of poor security hygiene, low risk awareness, and increasing sophistication of attacks. This results in poor detection and higher exploitation by cyber threat actors.[14]

Cyberattacks can be perpetrated by a variety of threat actors with financial, political, intellectual, or societal motivations and different levels of resources (Table 2). A malicious cyber event can be initiated directly, by attacking an organization's core systems, through insiders with privileged access, compromise of less secure systems in the supply chain or through disablement of supporting infrastructure such as telecommunication networks, or power grids. Sophisticated exploits are becoming commonly accessible on the dark web, lowering barriers to entry for those who want to cause harm. This is amplified with the use of AI which further lowers the entry barriers for cyberattacks (Box 1).

Table 2 Threat Actor Categories

Category	Description	Motivation	Main Impact	Resources
Nation-states and affiliated groups	Government institutions, intelligence agencies, and defense services with cyber espionage capabilities.	To gain political advantage.	Disruptions to critical services, financial and social instability, and loss of citizen trust.	Likely to be highly skilled, well resourced, and persistent. They may also influence insiders, further amplifying the threats.
Organized crime groups	Cyber gangs and individual criminals with technical know-how.	Financial gain through ransom and bullying tactics.	Fraud, loss of funds, data breaches and leakage, and reputational damage.	Usually well resourced in terms of skills and know-how but not always in IT equipment to pursue cybercrime.
Insiders	Employees of an institution or of its key suppliers who have privileged access to systems and deep knowledge of business processes.	Retribution for financial gain or to cause reputational damage. Often this group is manipulated by actors in other categories.	Service outages, data breaches, fraud, reputational damage, and loss of funds.	Not well resourced but often with privileged access. Some can cause vulnerabilities by careless behavior rather than malintent.

[12] Zero-day vulnerabilities are typically unknown to the vendor and for which no update, patch, or remedy has been developed.

[13] Generative-AI is proving particularly effective in improving the efficacy of phishing attacks.

[14] Human Error Drives Most Cyber Incidents. Could AI Help? (hbr.org).

Hacktivists	Groups of technology and cyber experts, geographically dispersed and working for a cause.	Advancing a political or social cause (for example, freedom of speech).	Discrediting institutions and reputational damage.	Not well resourced but persistent depending on the pursued cause.

Box 1. Impact of Artificial Intelligence (AI) on Cybersecurity

AI has served to improve cyber defenses in many industries including the financial sector; however, there are risks. Central banks have been using AI tools such as machine learning, deep learning, and natural language processing for a long time to detect anomalies in data, systems, and behavioral patterns in an effort to reduce unauthorized access, data exfiltration, and fraud. However, the use of AI is a double-edged sword in that its evolution is lowering barriers of entry for cyber-attackers. AI can facilitate finding exploitable vulnerabilities and improve hit-rates of attacks. In addition, Generative AI (Gen-AI)[15] can be exploited to: (1) support effective social engineering attacks (such as phishing, deep fakes in voice and images) on a large scale with potential financial stability implications;[16] (2) quickly analyze large amounts of stolen data to identify valuable subsets, mount further attacks, and train models; (3) improve malware generation; and (4) support post intrusion activities, such as lateral movement and exfiltration. Another risk of AI in critical systems is its creation of large data sets and models for their analysis which are an attractive target for attackers. Sophisticated use of AI in cyberattacks in the short term is confined to well-resourced threat actors; however, new threats are likely to emerge over time as the technology evolves. Efforts are being made by large technology companies to curb improper use of AI tools and models.[17]

Skill sets to prevent, detect, and contain cyber incidents using AI are in short supply. Based on a recent studies, significant investments may be needed to develop human capital for effective use of AI tools.

[15] Gen-AI comprises AI models that emulate the structure and characteristics of input data to generate derived synthetic content including images, videos, audio, text, software code, and other digital materials, which increase the risks of social engineering attacks and unauthorized data disclosure. To mitigate these risks and harness the benefits of Gen-AI, substantial investments will be needed in human capital not only in model development but also in oversight and assurance for its ethical and responsible use.

[16] The Rise of Artificial Intelligence: Benefits and Risks for Financial Stability, as part of ECB's Financial Stability Review, May 2024 (europa.eu).

[17] Staying Ahead of Threat Actors In The Age of AI – Microsoft Security Blog

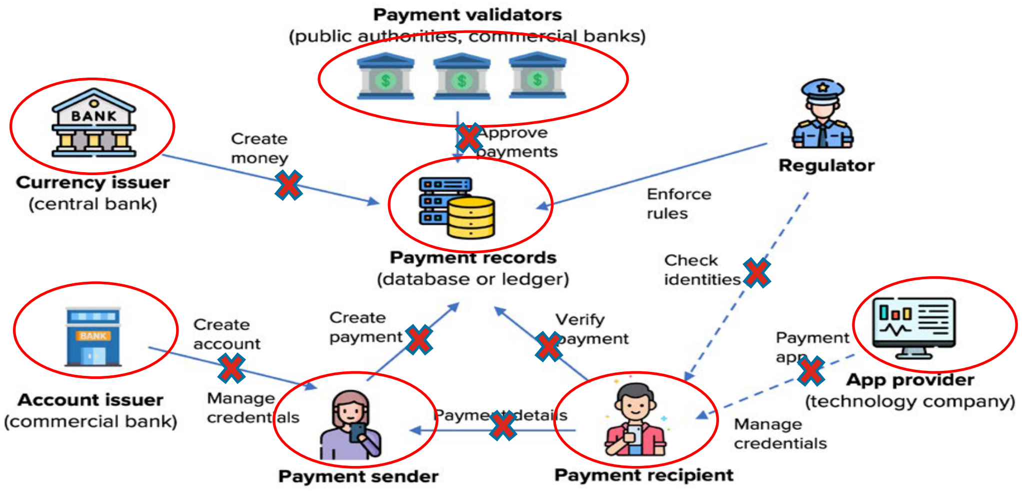
Section II. Cyber Risk in the CBDC Ecosystem

A well-designed CBDC ecosystem built at the technological frontier presents an opportunity to enhance operational and cyber resilience of a country's payments infrastructure. However, such an interconnected and high value system could face additional exposures not commonly experienced by other forms of digital money. A CBDC involves complex interconnections between intermediaries (banks and nonbank financial institutions) and other financial market infrastructures, with each being vulnerable to cyber risks to varying extents. This section aims to explain how each part of the CBDC ecosystem is exposed to cyber risks and how this exposure differs from other digital means of payment such as e-money. A retail CBDC ecosystem is more complex than a wholesale CBDC and has therefore been used for illustration.

2.1. CBDC: A Highly Interconnected Ecosystem

CBDCs exist in an ecosystem comprising many participants and interconnections, often with blurred boundaries of oversight, supervision, and assurance. Each of these can be a point of failure and exposed to cyberattacks within their organization (Figure 2).[18] Many of these participants are outside the central bank's purview, potentially masking a build-up of risks. However, the overall responsibility for the secure and resilient operations of the CBDC ecosystem primarily lies with the central bank as issuer of the currency.

Figure 2. Interconnected Retail CBDC Ecosystem



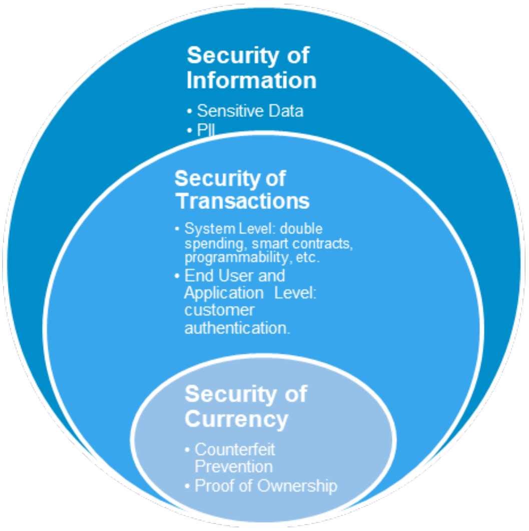
Source: Adapted from "The Missing Key" by the Atlantic Council.
Note: Red circles and crosses represent entry points for a cyber event and a potential point of failure.

[18] Missing Key: The Challenge of Cybersecurity and Central Bank Digital Currency—Atlantic Council.

2.2. Cyber Risk Perimeter of a CBDC

The cyber risk perimeter of a CBDC has three broad elements (Figure 3). The first is the currency itself throughout its life cycle—creation, storage, dissemination, and destruction. The second is transactions or movement and transfer of value between individuals and merchants. The third element relates to sensitive information that a CBDC collects from the users, merchants, and transactions. This information needs to be protected both in transit and at rest.

Figure 3. Elements of Security in a CBDC



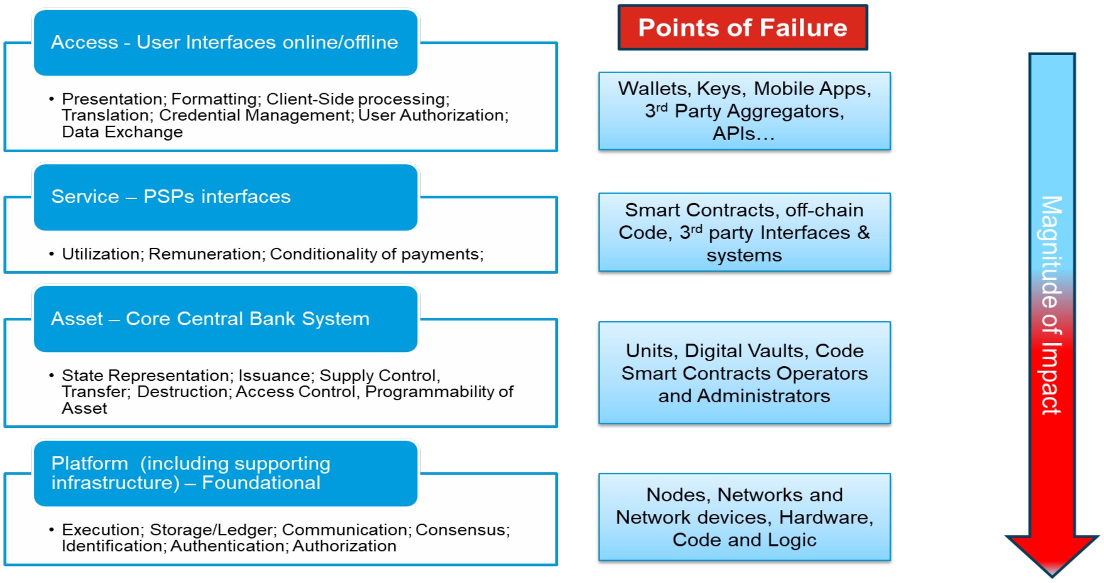
Source: Authors.

Mapping this to a digital asset technical stack such as the one depicted in IMF's ASAP[19] model (Figure 4) helps with understanding where vulnerabilities could exist, the magnitude of impact if these were exploited, and where protections can be layered. In the ASAP model, security of CBDC (the core circle of Figure 3) sits in the asset layer; the security of transactions (the middle circle in Figure 3) can be mapped to the access and platform layers. The security of sensitive information (the outer circle in Figure 3) can be compromised at any and all stages and therefore relates to all layers of the ASAP model.

Protection of the currency and transactions will be explored in greater detail in Section III while the security of sensitive information is the subject of a forthcoming IMF Fintech Note titled *CBDC Data Use and Privacy Protection*.

[19] ASAP: A Conceptual Model for Digital Asset Platforms (imf.org).

Figure 4. Risk Mapping to ASAP Model


Access - User Interfaces online/offline
• Presentation; Formatting; Client-Side processing; Translation; Credential Management; User Authorization; Data Exchange
Service – PSPs interfaces
• Utilization; Remuneration; Conditionality of payments;
Asset – Core Central Bank System
• State Representation; Issuance; Supply Control, Transfer; Destruction; Access Control, Programmability of Asset
Platform (including supporting infrastructure) – Foundational
• Execution; Storage/Ledger; Communication; Consensus; Identification; Authentication; Authorization
Points of Failure
Wallets, Keys, Mobile Apps, 3rd Party Aggregators, APIs…
Smart Contracts, off-chain Code, 3rd party Interfaces & systems
Units, Digital Vaults, Code Smart Contracts Operators and Administrators
Nodes, Networks and Network devices, Hardware, Code and Logic
Magnitude of Impact

Source: Authors, adapted from IMF ASAP model.

CBDC could be subject to similar types of cyber threats as other digital means of payments, including:

- Compromises of core servers dedicated to the issuance (minting), holding, and redemption of digital money leading to fraud, unauthorized issuance (printing) or exceeding intended money supply.
- Compromises of payment systems leading to redirection of funds to unintended recipients and mismatched balances.
- Corruption or exploitation of code, or bugs in core or enabling systems leading to service disruptions, fraud, data breaches.
- Direct attacks on underpinning infrastructure such as the “cloud” or power grids, internet, and mobile networks leading to service disablement.
- Insider threats arising from human errors, manipulation, or malintent leading to compromised data, service outages or loss of funds.

Additionally, CBDCs could face unique cyber risk exposures that are not necessarily encountered by other types of digital money. Three factors could be considered as proxies for comparing the increased exposure across digital money types (see Annex 2): (1) factors that can increase the likelihood of both malicious and non-malicious cyber events (for example, due to complexity of interconnections and trade-offs involving security), (2) factors that increase attractiveness for a cyber-attacker, and (3) factors that can expand the cyberattack surface. A CBDC, compared to e-money or stablecoins for instance, may involve a larger number of intermediaries and third parties, a wider and less cyber risk-aware user base, and a design intended to meet multiple goals increasing complexity (for example, asset tokenization, financial inclusion, efficient disbursements, conditional payments, and several payment initiation methods). As the national currency in digital form, it may also be more attractive to sophisticated cyber-attackers, such as nation-states. It is therefore crucial to consider security and resilience requirements from early design stages (see Section IV).

In addition to people, process, and technology at the central bank and the financial sector, resilience and security of digital payment systems are heavily reliant on a nation's core infrastructure. This includes underpinning critical services such as consistent power supply, stability, and security of national and international communication networks and span of mobile, broadband, and internet connectivity. The existence of national cybersecurity strategies and coordination bodies such as Cyber Emergency Response Teams (CERTs) also affect the responsiveness to a security incident in digital payment systems and their resilience in recovering from an attack.

Emerging market and developing economies (EMDEs) may face more pronounced challenges in securing a CBDC ecosystem. These include but are not limited to:

- Legacy and out-of-date IT environments developed before modern technologies such as smart devices and cloud services. New services and controls are often layered in response to consumer demand, real or perceived weaknesses, or cyber threats. This can create conflicts between tools and vulnerabilities in interfaces leading to unintended outcomes. Although such conditions may exist in advanced economies, issues in EMDEs are exacerbated due to a paucity of skilled resources.
- Suboptimal critical national infrastructure which is prone to power and network outages resulting in service disruptions and cyber exposures.
- Inadequate skills in deployment of IT best practices and containment of corresponding threats.
- Supplier concentration risks for critical services such as the cloud, 24 × 7 digital perimeter monitoring, and management of security operation centers. Additionally, central banks may lack the legal power to insist on the right to oversee or audit vendor technology environments or security controls, potentially resulting in an undetected build-up of risks in the supply chain.[20]
- Some EMDEs are less mature in their cybersecurity posture and display limited adoption of modern security frameworks. There is also a general lack of national cybersecurity strategies, incident response, and information exchange mechanisms.

Materialization of cyber risks in a CBDC system could have far-reaching consequences. Any service disruption or outage, loss of funds, compromise or leakage of sensitive data, counterfeiting, and double spending can individually and collectively result in reputational damage to the central bank and erosion of consumer confidence and trust. Sustained adoption requires building security and resilience into the

[20] Several examples of operational issues and cyberattacks can be mentioned in EMDEs—for CBDCs, Bahamas' Sand Dollar had operational issues due to the limited digital infrastructure on some of the islands that led to accessibility problems; for e-money, during Nigeria's MTN Mobile Money Service outage users were unable to perform transactions, access their funds, or receive money, leading to widespread inconvenience and financial disruption; the Kenya's M-Pesa Unauthorized access cyberattack led to service disruption and users were unable to access their accounts or perform transactions; in a Mobile Money fraud case in Ghana, scamming with promotional messages to users prompted them to provide personal information or transfer money that lead to significant financial loss.

design from initial stages of the CBDC project. It is good practice to strengthen general IT governance and controls and address cybersecurity vulnerabilities from the start to avoid expensive rollbacks and bolt-on measures. This analysis should consider the clear demarcation of responsibilities for all stakeholders in the ecosystem given that some are supervised by authorities other than the central bank. Further details on activities related to cyber resilience at each stage in the CBDC development are provided in Section IV.

Section III. Design and Technology Choices: Cybersecurity Implications

Delivering a CBDC is a large-scale and complex undertaking which involves choosing appropriate designs that support the desired objectives. Such design choices will affect the risk profile of a CBDC and will require relevant safeguards to ensure confidentiality and integrity of information and availability of expected levels of service. A CBDC system should be resilient to faults and failures of different components within the ecosystem. These include people or users, infrastructure, networks and interfaces, hardware, software, protocols, logic, and control failures—either accidental or intentional. This section briefly explains the commonly considered design options and supporting components for a retail CBDC and examines the security risks of each. It also evaluates the pros and cons of relying on third-party services using the example of cloud technology for CBDC experimentation.

3.1. Design Option 1: Distribution Model

A retail CBDC is a claim on the central bank available to individuals and entities in the country. It can be distributed in two ways:[21]

1. Direct or single tier whereby a CBDC is issued by the central bank directly to end users. In such a model, the central bank handles all payments and keeps records of retail holdings by all participants in real time. Adopting this model would signify a new approach and investment for the central bank and necessitate the creation of new infrastructure and functions such as Identity and Access Management (IAM), User and Transaction Authentication, Wallet Provision and Management, Private Key Management, and Dispute Resolution. In addition, this model will give the central bank full visibility and control of personally identifiable information (PII) and transaction history. Besides data privacy issues, this approach creates reservoirs of rich data attractive to hackers. While all elements that could threaten security will be under its direct control, these activities place a great deal of new, unfamiliar burden on the central bank and can onboard unseen risks. For these reasons, most countries have ruled out the adoption of a direct or single-tier model.

2. Intermediated or two-tier: The central bank provides the core ledger/system and life-cycle management of the CBDC to assure soundness and singleness of money. It also provides a secure and resilient platform or infrastructure for the CBDC ecosystem. All other activities are delegated to private-sector participants. This mimics the traditional role separation and fosters innovation and competitiveness within the private sector to the benefit of the consumer. In such a model, the central bank processes and records wholesale payments and balances but could also opt to periodically record retail balances. Management of risks within the wider ecosystem

[21] Although there are some hybrid variants of these, the two broad categories have been used for simplicity.

are delegated to intermediaries such as banks and nonbanks or other payment service providers and overseen by the central bank or an equivalent supervisory authority.

3.2. Design Option 2: Token or Account-Based

Security considerations in this design option relate to the *protection of currency* through its life cycle.

Account-based CBDC models entail electronic holding of funds in a user account and follow debit and credit methods to facilitate instantaneous transfers. This is akin to traditional bank accounts and electronic payments. In an account-based model, the key area of protection is the user's identity which could be achieved by strong access and identity management tools using passwords, passphrases, biometrics, or a combination of similar tools. Although security requirements in this model are similar to those used in traditional e-money systems, a new infrastructure presents an opportunity to strengthen control measures with advanced tools such as data sharding, granular permissions management, zero-trust architecture, and quantum-safe cryptography[22] (Box 2). However, this approach, based on prevailing laws and regulations around account opening, could impair universal access to a national currency.

Token-based CBDC is emerging as an important option. In a token-based CBDC, tokens are issued by the central bank and transferred over distributed ledgers for payment transactions. This is akin to having banknotes and coins in a physical wallet which provide assurance of ownership. Like cash, tokens can more easily meet the requirements of universal access and offer some controllable level of anonymity. A key risk factor for token-based systems is protection of the digital token throughout its life cycle.

Protection of currency includes the currency itself (issuance, distribution, and destruction), its programmability (if used) which controls some aspects of its use, and smart contracts which influence its supply and transfer. Central banks are well experienced in managing the life cycle of fiat currency and have implemented multilayered controls spanning technology, people, processes, and facilities. However, managing the life cycle of a digital currency is a novel territory which requires logical protection using technology tools, processes, and governance. The issuance of a token-based CBDC involves the creation of digital tokens by the central bank based on supply parameters. Each unit or token is uniquely identified using cryptographic mechanisms such as digital signatures and public-private key encryption. Private keys are used at the time of issuance to secure the authenticity and uniqueness of the tokens and public keys for verification at the time of use.

Key Issues

- Compromise of cryptographic keys, digital signatures, and other cryptographic algorithms used for authentication and authorization.

[22] A concept or architecture used to segment or partition data sets into smaller, faster, more easily managed parts called "shards."

- Quantum computing (Box 2) is a future threat to the cryptography used to protect digital assets. Elliptic curve keys, which are the gold standard for digital signatures, can potentially be computed by quantum attackers using publicly visible keys thereby threatening the safe custody of CBDC. (See further details below under the subheading of Digital Wallets.)

Box 2. Impact of Quantum Computing on CBDC Cybersecurity

Quantum computing makes it possible to solve difficult problems much faster, which has a direct impact on cybersecurity in general, and CBDC in particular. Cryptography is essential to ensure confidentiality and integrity of CBDC. The strength of the cryptographic algorithms, that is, the difficulty to break them, is vital for CBDC's cybersecurity.[23] Several widely used algorithms such as elliptic curves or RSA share characteristics and form the basis for digital signatures. They are considered strong but were shown to be easily broken with QC. Although this threat may not be immediate, as the first quantum computers are not expected before 2030, CBDC projects need to address the issue now because transitioning to quantum-safe cryptography is likely to be a long and arduous process. Specifically, the security architecture of the CBDC must make it possible to change to newer and stronger algorithms quickly and seamlessly as the older ones become vulnerable to QC-based attacks. This feature is often referred to as cryptographic agility and should be an essential requirement in any CBDC implementation project.[24] Experimentation is under way in this regard with positive early results.[25]

Potential Mitigations

- General strengthening of security defenses involving user risk awareness, comprehensive industry collaboration, physical and logical protections, and some specific measures as detailed in the following sections.
- Data centers that house systems involved in currency issuance should be air-gapped and access should be strictly controlled using strong IAM processes.
- Use of secure hardware elements for key storage and multilayered, strongly secured digital signatures supported by rigorous oversight and surveillance.
- Use of mutable tokens which live for only one use and are destroyed at the end of that transaction. These are being considered in some experiments.
- Use of cryptographic keys and algorithms that conform to well-established international standards. Although based on current research, the threat of QC is not imminent, a breached encryption

[23] A cryptographic algorithm is considered secure ("strong") for a certain purpose if it is practically impossible to break it within the period in which the data it protects must remain confidential or must retain integrity. Thus, cryptographic algorithms may become insecure as computing power grows. Since CBDC, especially the DLT-based variants, are fully reliant on cryptography, the strength of the algorithms deployed is a crucial factor in their overall security.

[24] Quantum Computing and the Financial System: Spooky Action at a Distance? (imf.org).

[25] Project Leap: Quantum-Proofing the Financial System (bis.org); Project Tourbillon Demonstrates Cash-Like Anonymity for Retail CBDC (bis.org).

algorithm will need a swift response from the authorities. Efforts should be made to integrate post-quantum cryptographic schemes early in the design process.[26,27]

3.3. Design Option 3: Ledger Design

Integrity of payments and money transfers require maintaining a record of transactions and user balances. Similarly, at the core of a digital currency system, there must be a digital record of all transactions that have taken place. A digital ledger could be implemented using a conventional, centralized system controlled by the central bank or a trusted third party, or a decentralized ledger with no single, central point of control. Regardless of the degree of centralization, a digital ledger should provide assurance of a verifiable transfer of value.

Centralized Ledger Technology (CLT)

Centralized systems are efficient and mature with proven and fit-for-purpose supervisory and regulatory rule books to govern their operations. Solutions or controls that overcome unexpected or arbitrary behavior, outages, bugs, and system breaches have stood the test of time and continue to be enhanced to accommodate new or novel technologies and threats.[28] Protection, detection, and recovery mechanisms are well established and can be monitored efficiently. Governance arrangements entrust control to a central authority and can be amended expeditiously as the need arises. For business continuity, centralized systems adopt "distributed" principles through use of real-time replication (and sometimes additional delayed replication) across multiple data centers in different and dispersed locations.

Centralized systems offer consumers recourse in the face of errors, breaches, or outages and enable full visibility of risks, allowing efficient mitigation and management. Connectivity to such systems can be holistically mapped, tracked, and appropriately guarded. Centralized systems therefore can offer high levels of confidentiality, integrity, and availability.[29]

Key Issues

- A central authority, or a malicious insider, can potentially change all rules and rewrite ledger history and censor or delay transactions impacting public trust.
- Centralized ledgers are attractive targets for hackers and represent a **single point of failure**, as a successful attack can disable the entire system and lead to data breaches and leakages on many

[26] How Does Post-Quantum Cryptography Affect Central Bank Digital Currency? (arxiv.org).

[27] Safeguard CBDC Systems in the Post-Quantum Computing Age | World Economic Forum (weforum.org).

[28] Based on evolution in payment systems which now include online and mobile functionality and use of pre-paid and chipped cards, QR codes, and so on.

[29] Jam-Dex, the digital currency issued by Jamaica, uses CLT. This design option was chosen for future seamless interoperability with the existing payment systems. Due to very low adoption of Jam-Dex, insights on the pros and cons are limited to date.

customers via a single attack. For replicated databases, a ransomware attack could impact all live and backup systems simultaneously, making recovery difficult.

- Malicious insiders with privileged access to centralized systems can make unauthorized amendments to transactions, system configurations, or communications protocols, which can remain undetected, leading to integrity issues, disruptions, and fraud.
- A large-scale power or network outage could impact production and backup servers within the primary data center simultaneously. The risk would be amplified if the secondary data center used for replication is also located in the vicinity.

Possible Mitigations

There is extensive guidance on mitigating the above issues from standard-setting authorities such as the CPMI. This includes but is not limited to:

- Use of secure, military-grade, air-gapped data centers for issuance or minting with strong IAM controls supported by frequent auditing of access logs to detect unauthorized access attempts.
- Periodic profile checks on privileged users to detect malintent driven by changes in circumstances.[30]
- Appropriately designed replication to reduce impact of ransomware attacks, for example, real-time replication to a secondary environment supported by periodic syncing to a third.
- Geo-replication and off-site back-ups to reduce the impact of large-scale outages of enabling critical infrastructure such as power grids.

Distributed Ledger Technology (DLT)

Distributed ledger technology is relatively new. A distributed ledger is spread across several computers or servers known as “nodes.” Participating nodes can have a shared ability to maintain the ledger and perform various functions through voting—known as the consensus process. DLT can be open and permissionless, that is, anyone can become a node and all nodes have voting rights to make decisions such as transaction validation or, it could be “permissioned” where only certain “trusted” parties can vote. The choice of consensus mechanism involves a trade-off between robustness and efficiency. For example, there could be a single node to confirm the validity of each transaction. This is efficient because it requires no coordination between multiple nodes, but not robust, as if the node goes offline or misbehaves, integrity and availability will be severely impacted. On the other hand, there could be many nodes. The efficiency of this approach would be limited by network latency and bandwidth. However, higher numbers would be more robust to misbehaving or unavailable nodes.

DLT may offer opportunities for innovation in the financial sector as it can facilitate efficient settlements, programmability of transactions, and sophisticated execution of conditional payments (discussed in detail in the following section). It also makes asset tokenization simpler. While these opportunities maybe possible with centralized ledgers, DLT affords coordination benefits that come with shared governance.

[30] Similar to controls introduced by SWIFT Customer Security Program.

DLT networks may arguably be natively more “available” than fully centralized systems as failure of one or a few nodes does not automatically lead to the failure of a complete system.[31] Relatedly, common attacks, such as ransomware, maybe less applicable unless executed at scale, which would be difficult as each node is independently managed and may not contain the same exploitable vulnerabilities as the others. To maintain integrity, the DLT network is governed by ground rules. A set of protocols describes how the nodes will authenticate access, authorize, and store transactions securely and consistently. For confidentiality, nodes can have varying levels of visibility of transaction details, depending on the system’s design. Public/permissionless DLTs offer full visibility whereas private or permissioned DLTs impose limitations.

Key Issues

- DLT is a relatively recent technology. It is more complex than the traditional database infrastructure and requires specialized skill sets which are in short supply**.** In addition, DLT has not been tested at the national payment system scale and therefore its vulnerabilities and design flaws are not fully understood in that context. This hinders predictive threat modeling and development of specific preventative protections and frameworks.
- DLT, while more available than a traditional centralized environment, is not *hardened* to the same extent. It is also not immune to certain cyberattacks such as distributed denial of service (DDoS), or collusion among nodes (51-percent attack). This may result in fraud, double spending, or create delays in transaction settlement.
- DLT makes extensive use of APIs and software code. A failure of software, malicious or due to errors, could compromise the integrity of the entire network.
- Crash faults could occur if a large fraction of validators go offline, for example, due to a disruption in power or network infrastructure. This is likely if validators or nodes are geographically concentrated.
- Byzantine faults could occur if some validators actively misbehave or deviate arbitrarily from protocol. In a CBDC, the financial incentives for misbehavior are high.[32]
- Given extensive replication and ongoing authentication and synchronization, scalability, and response times of DLT could be suboptimal**.**

Potential Mitigations

- Use of permissioned DLT where nodes are limited to trusted parties. This continues to be tested by several central banks to support CBDC deployment with ongoing, albeit slow improvements in scalability and performance.
- In the absence of specific threat modeling, a combination of policies, strength of oversight and governance, and robustness of the IT internal control environment may be used (see Section IV). An area which as stated earlier, is being advanced through project Polaris and others.

[31] In reality, many other factors affect availability outside of the question of centralization.

[32] A situation where nodes fail in ways that are erratic or not immediately obvious, making it difficult to diagnose the cause of failures. Particularly important in DLT-based systems reliant on achieving consensus despite existence of faulty or misbehaving nodes.

- To guard against crash faults, to the extent possible, nodes should be geographically dispersed using different power sources and network links.
- To avoid collusion and corruption, nodes should be independently monitored and governed by algorithms that can withstand a certain number of misbehaving nodes.[33]

Integrity of a CBDC ecosystem places a high reliance on the integrity of software code used to run its operations and security of end points (wallets) that access it. Each of these is discussed in the following sections.

Software Code: Programmability and Smart Contracts

Programmability is intended to increase a CBDC's utility and expand its features and functionality. It is an option available to authorities to realize policy objectives. While it is not necessary for a CBDC to be programmable or utilize smart contracts to fulfill its primary role as a digital currency, it can be seen as a tool to foster innovation for the entire payment channel.

Programmability of the currency itself could be controversial in some countries, as it might affect trust in the asset.[34] Programming payments can offer powerful options, with smart contracts executing automatically based on specific conditions. For greater efficiency and seamless user experience, smart contracts can also be composable, that is, successful execution of one, can trigger another or the output from one is the input to another.

Programmability involves the use of software code, and any flaws in it—unintended or malicious—can lead to fraud or manipulation. The risk is amplified in the presence of chained or composable smart contracts or simultaneous execution of multiple independent contracts.

Key Issues

- Code corruption or compromise arising from poorly designed programs, accidental coding errors, or malicious alterations can lead to operational failures, data breaches, integrity issues, and fraud.
- Contract manipulation where an "attacker" contract can manipulate a "victim" contract leading to major harm if the outcome of the latter is an input or trigger to multiple other contracts.
- Compromised code or software bugs that remain undetected can mask risk build-up. This could be amplified when using open-source code without appropriate due diligence and ongoing monitoring during execution.
- Interoperability and alignment of smart contracts, particularly if chained, within the CBDC ecosystem could challenge recovery and remediation efforts.

[33] Use of algorithms that that can withstand a certain number of faulty or malicious nodes for example, practical Byzantine fault tolerance (PBFT): An algorithm designed to work efficiently in asynchronous systems, making it possible to reach consensus with a minimum number of message exchanges.

[34] Some central banks, for example, the ECB and the Bank of England, have explicitly stated that they will not introduce programmable features in the digital euro and the digital pound, respectively.

Use of flawed programmability and smart contracts will impact ledger integrity and can erode consumer confidence and trust leading to systemic implications.

Possible Mitigations

- Establish regulatory frameworks and legal standards that define the creation, execution, and enforcement of programs that impact payments using CBDC.
- Promote best practices in code development or use of open-source code through issuance of guidelines on secure coding practices. This could include code signing by developers and certification from established authorities.
- Segment governance into 1) Authorization: who can program and for what purpose and 2) Auditability: who checks the code is performing as designed or intended.
- Mandate regular and comprehensive audits of open-source code and smart contracts by independent security experts to identify and rectify potential vulnerabilities before and after deployment.
- Employ formal mathematical verification techniques to prove that a smart contract's code correctly implements its intended logic and is free from vulnerabilities.
- Encourage reviews by the broader community of developers, security experts, and stakeholders to inspect, review, and contribute to the improvement of code.
- Implement bug bounty programs to incentivize the discovery and reporting of vulnerabilities in smart contracts, facilitating identification and resolution of security issues.

End Points: Digital Wallets

Transactions with DLT-based CBDCs, like other digital payment systems, are facilitated by digital wallets. The design and functionality of digital wallets are crucial not only for usability and convenience but also for security and privacy. Digital wallets have three core functions: *user authentication*, *transaction authentication*, and a *user interface*. In some designs and for offline use, wallets could also be used to store funds.

User Authentication: This overlaps with identity verification in that the former is concerned with identifying the physical person as the legitimate user of the wallet and the latter with the person's existence in the "real" world verified by an address, national identifications, and so on. User authentication is carried out each time the wallet is accessed and can be achieved using passwords, PINs, biometrics, or a combination thereof.

Transaction Authentication: Once authenticated, the user can perform valid CBDC transactions which also require authentication, that is, verification of ownership of tokens, sufficiency of payer's funds to support the payment, and existence of the payee to receive it. Typically, this is done through the use of cryptographic private and public key pairs. The user's private key is a secret key known only to the user. It is used to sign a payment transaction and effectively prove ownership of the digital token associated with the wallet. Public keys are mathematically derived from their corresponding private keys using cryptographic algorithms and are shared with others. The sender uses the recipient’s public key to execute the payment transaction. Transactions are verified by the network through a consensus mechanism (for example, proof of work or proof of stake). Once a transaction is confirmed and committed to the ledger, the wallet updates the user’s balance to reflect sent or received transactions.

User Interface: Design of the user interface is critical for users to navigate the application and make or receive payments. Simplicity and convenience of an interface needs to be balanced with security protocols.

Key Issues

- Compromised Cryptographic Keys: Private keys used to preserve integrity, availability, and confidentiality of the system and prevent unauthorized access can be lost or stolen.
- Compromised IAM: With stolen private keys or credentials, an adversary can gain access to a DLT environment and submit fraudulent transactions.
- Compromised User Interfaces: Ambiguous graphics and icons could be linked to malicious sites and fake addresses to harvest credentials and for theft of funds.

Possible Mitigations

- Use of secure hardware wallets or embedded secure elements designed to store keys securely and make them accessible post user authentication. This could be complemented by trusted execution environments (TEEs),[35] commonly used to protect users’ cryptographic keys and handle the encryption and decryption processes. Another technique is threshold signing,[36] which creates a single digital signature from multiple signatures.
- Clear authorization protocols for key issuance and flexible key management practices involving an authorized set of nodes that can invalidate existing, and re-issue new keys.
- Use of custodians (intermediaries) to manage keys may be appropriate for users who are less familiar with the risks associated with loss of keys.
- Clear user interfaces with concise labeling of graphics and icons for services and actions. These interfaces should build in security prompts and alerts once an external link is activated.

In an intermediated two-tier system, provision, ongoing maintenance, and security of digital wallets are the responsibility of the intermediary who would typically outsource this activity to third-party suppliers.

3.4. Design Option 4: Offline Functionality

Offline access allows transactions to be made in the absence of internet connectivity. The rationale for offline CBDC revolves around resilience against temporary and prolonged outages, and the promotion of

[35] A trusted execution environment (TEE) is a secure area within a main processor. It ensures that sensitive data is stored, processed, and protected in an environment isolated from the main operating system.

[36] Threshold signing is a cryptographic technique that allows a group of participants to collectively sign a document or a message when a threshold number is reached. It guards against key compromises.

financial inclusion in areas with limited telecoms coverage or where outages are frequent. The BIS Innovation Hub has developed a handbook for offline CBDC payments and as part of that work, conducted a survey that shows that 49 percent of central banks consider offline payments with retail CBDC to be vital, while another 49 percent deemed it to be advantageous.[37] Offline access allows users to transfer value where either the payer or payee or both, cannot connect to the ledger at the time of the transaction. Offline features can be designed with varying degrees of payment finality. For example, “fully” offline platforms offer immediate offline settlement, and the payee can immediately spend the money received. Intermittent offline is when risk limits set by the issuer can cap the activity before offline wallets must connect to the ledger. “Staged” offline is where transactions can be made offline but not settled, and as such the payee cannot spend them until connection to the ledger is made.

Offline functionality could be ‘always’ offline for environments where communication infrastructures are weak or have limited coverage or, it can be designed to be offline to cater for short-term outages.

For this note, intermittent offline functionality will be examined as an option for greater resilience of the CBDC ecosystem.

In an offline setting, generally, validation of transactions is reliant on the security of hardware elements and integrity of the software operating on devices being used to transact. In comparison, online transactions are validated in real time to ensure funds are not spent more than once (no double spending) and that the funds were issued by the central bank (no counterfeiting).

Double spending in an offline environment is different to the issue seen for online CBDCs. To enable double spending in an online setting, consensus or approval mechanisms will have to be manipulated while for offline payments, user devices and cryptographic protocols will need to be compromised. Issues of double spending may arise from man in the middle attacks, transaction replay, cloning, jailbreaking, and device tampering.

There are several offline solutions ranging from the use of stored value cards, use of tamper resistant user devices incorporating hardware secure elements such as a chip operating in a trusted execution environment (TEE) or virtual secure elements embedded in mobile applications.

Key Issues

- Counterfeiting and double spending:
    - Some amount of CBDC may need to reside on a device such as a card or a wallet hosted on a smart phone. These can be replicated or manipulated. Without real-time surveillance, an attacker can launch multiple attacks while the device is offline. In addition, such devices may have vulnerabilities that could be exploited by attackers or accidentally (or maliciously) by users themselves.

[37] Project Polaris: Part 1: A Handbook for Offline Payments with CBDC.

  - Transactions protected by cryptography can be reverse engineered[38] to generate fake messages and therefore counterfeit value. Sophisticated side channel attacks can leverage readings of energy consumption or radiation emission to crack cryptographic keys. The resulting replication of the key may remain undetected until after the fraud is committed.

- Device obsolescence, cloning, or stealing of a user device which in expert malicious hands can be unlocked and used by the attacker. Damaged user devices could lead to an inability to access funds. In addition, devices with out-of-date security protocols could lead to security vulnerabilities which can be exploited to harvest credentials which can be used when the system is back online.

- Torn transactions: these occur when communication links that facilitate offline transfers are weak or unstable leading to only one part of the transaction being recorded. This means funds transferred by the sender although sent and deducted from his balance, are not received by the recipient.

Ultimately any data breach or compromise to transactions' integrity will result in reputational damage to the central bank and an erosion of user confidence.

Possible Mitigations

Securing offline functionality technologically can be challenging[39] as typically many of the security features rely on real-time availability of centrally stored data for authentication and authorization. Such features include locking stolen funds, querying suspicious transactions, or freezing breached accounts. Currently there is no complete solution, but active research and experimentation is underway.[40] In the meantime, a combination of policy and technical measures could be adopted for offline security. Policy decisions may include recording transactions but not settling until devices are back online, placing caps on the number or value of transactions that can settle offline or placing limits on how much CBDC can be stored in offline wallets.

Technical measures could include use of established and well-vetted cryptographic algorithms with sufficiently long keys, implementing strong key management practices such as storing keys in hardware security modules,[41] making them harder to extract, key rotation and code obfuscation.[42] However, the keys and the algorithms need to guard against the quantum threat and conform to the concept of crypto-agility.[43] Emerging hardware which has physical unclonable components may provide a solution in the

[38] Reverse engineering refers to the process of deducing or discovering the secret cryptographic keys used in encryption algorithms. This can be done using brute force or cryptanalytic techniques, fault injections, and mathematical algorithms.

[39] Project Polaris: Part 1: A Handbook for Offline Payments with CBDC.

[40] Riksbank and the Bank of Canada among others.

[41] Hardware security modules are specialized physical hardware devices for secure storage of cryptographic keys separately from regular application operations.

[42] Code obfuscation is a technique that modifies software programs to make them difficult to be deciphered by humans and machines without changing their logic or functionality.

[43] Crypto-agility is the ability of security hardware to switch to a new algorithm without the need to rewrite applications or deploy new hardware systems.

future. Developing a complete technology solution for torn transaction is challenging as demonstrated by the recent report on Phase 4 of the e-Krona project[44].

3.5. Design Option 5: Use of Third Parties for Critical Services

A two-tier CBDC will include third-party suppliers ranging from technology providers, wallet developers, government entities, cloud service providers, internet and telecom service providers, and some others. The ecosystem's smooth and secure operations are critical for the adoption of CBDC, so reliance on subject matter experts, service providers or vendors specializing in CBDC implementation is expected. Many of these entities are outside the central authority's regulatory perimeter and governed by a different rule book. This further increases the risk profile of a CBDC as the following issues could arise:

1. Weak visibility of security vulnerabilities in interconnected systems as they may be governed by different regulatory bodies with varying intensity. There is also a high risk of contagion if systems are interconnected and integrated. This can lead to an undetected build-up of risks.
2. Reliance on vendors for critical services could result in unmitigated risk transmission.[45] In addition, inadequate knowledge transfer could result in poor or expensive post implementation security management and remedial actions and vendor lock-in.
3. Digital ecosystems often have blurred boundaries and poor demarcation of role responsibilities which can result in accountability and control gaps. Sharing of too much information with key vendors could result in shifting of control away from the central bank.

Cloud technology is a good example to illustrate these issues.

There are numerous benefits of adopting cloud technology such as:

- **Scalability**: Given a current lack of insights from CBDC implementations, it is important for central banks to avoid expensive mistakes and unnecessary investments. Cloud infrastructure and service propositions can provide flexible and elastic environments that can automatically scale to accommodate unplanned changes in capacity and workload and aid informed decisions to support a desired end state.
- **Resilience**: Large and reputable cloud service providers (CSP) operate a vast infrastructure comprising multiple data centers located across continents and time zones. This is to ensure high availability and effective fault tolerance and disaster recovery capabilities. In the event of a localized outage or disaster, the CSP's infrastructure can automatically redirect traffic to alternate regions, minimizing operational disruptions.
- **Robust security**: Large cloud providers invest heavily in robust security measures and certifications (such as Tier certification of the cloud data center, SOC 1, SOC 2, and so on) to protect data and applications. They offer built-in security features, such as encryption for IAM

[44] Sverigis Riksbank Report on E-Krona Pilot Phase 4, March 2024.

[45] Examples include the Falcon update from CrowdStrike which halted airlines, health services, and media and SolarWinds that pushed a contaminated patch to computer systems worldwide.

and threat detection systems, helping to mitigate security risks and ensure the integrity of data.

However, cloud service providers rely on a shared responsibility model. Security of a CBDC system's application and data requires the central bank to maintain ownership and control of the environment. As such, responsibility for securing the system at those layers sits with the owning entity.

Key Issues[46]

- Cloud-based systems require reliable internet connectivity, and any disruption can hinder access to CBDC services. This could be an issue with countries with weak national communications infrastructure. In such cases it may be necessary to host the solution on premise or in local "cloud" instances where connectivity could be through physical cables.
- Despite robust security measures, cloud platforms remain attractive to perpetrators and have been targeted by malware, including ransomware. This could be due to security vulnerabilities, misconfigurations, compromised or erroneous third-party code, or insider threats. Poor cloud security could result in significant data breaches such as those seen in recent times.[47]
- Effective and secure use of the cloud is a complex shared responsibility between the CSP and the consumer which can be ambiguously demarcated.
- Dependency on a single CSP can result in a single point of failure in the event of an outage or a coordinated data breach. It could also make it difficult to exit or migrate to another provider, leading to increased costs and operational complexities.
- The global nature of cloud services may introduce legal uncertainties and weak remediation of issues, especially when data is stored or processed in an unfriendly jurisdiction.
- Integrating CBDC infrastructure with existing financial systems and services in a cloud environment can pose challenges, particularly with legacy systems.

Possible Mitigations

- Clear strategy and frameworks to determine what data and services can be migrated or hosted in the cloud. For example, mission critical operations such as issuance may be better retained on premise.
- Selection of a reputable cloud service provider with appropriate, verifiable security and resilience certifications.
- Clear definition of roles and responsibilities to ensure there are no gaps in ownership of service components within the value chain.
- Granular access controls and application of zero-trust principles for critical systems and sensitive data.

[46] Many of the large cloud environments are in a handful of jurisdictions and could pose data sovereignty risks. Examination of this is out of scope of this note.

[47] Equifax, Google Cloud, and AWS.

- Clearly designed contracts with exit clauses detailing the treatment of data upon termination or completion of contract. Contracts should also include the right to audit security protocols or an undertaking to share outcomes of independent audits and penetration tests.
- Upskilling of in-house talent with deep understanding of cloud security configuration and integration with systems on-premises.

Although there are some clear advantages and disadvantages of design choices as listed above, the extent to which any is superior is less clear.[48] Design choices should be considered based on jurisdictional needs and motivations to issue a CBDC, and their security should strike an effective balance between functionality, user experience, and convenience. For example, vulnerabilities in CLT and DLT designs are different, but the impact would be equally severe if exploited. In CLT, there are single points of failure such as the controlling, central node could fail due to an attack or outage of the supporting infrastructure. In DLT-based environments, key vulnerabilities are unauthorized use of keys or failure or improper operation of software, or the consensus mechanism (where used) due to crash or "Byzantine" faults. Use of cloud to host the CBDC ecosystem has several benefits but access to the cloud could be impacted by the strength and stability of national infrastructures such as power grids and communication networks. Programmable or conditional payments may be necessary for some countries but be seen as controversial in others. Offline functionality could be a pre-requisite in countries with strong networks and consumer expectation of high availability but a secondary option where CBDCs efficiently co-exist with fiat-based e-money systems. Ultimately, as has been mentioned several times in this note, adoption of currencies and payment systems are heavily reliant on consumer trust which is difficult to build but easy to break. Any chosen architectural or technology option should be carefully designed and tested for vulnerabilities and exposures using a rigorous approach such as the one described by the IMF in its 5P methodology.[49] This should be supported by iterative discussions between security experts and policymakers to ensure that a CBDC deployment strikes an effective balance between policy goals, efficiency, security, user convenience, and resilience.

[48] Consideration can be given to hybrid solutions to meet the stated policy goals. For example, e-CNY uses CLT for transaction processing in order to facilitate scalability and permissioned DLT for reconciliation in order to promote transaction transparency.

[49] IMF Fintech Note, "How Should Central Banks Explore Central Bank Digital Currency?"

Section IV. Foundational Requirements and Good Practices for a Resilient CBDC Ecosystem

Strong security and high availability of a CBDC ecosystem are underpinned by foundational requirements and maintained with best practices that span across its participants. This section proposes high-level principles applicable in CBDC design, regulation, and supervision.[50] It describes a protection framework listing foundational requirements and good practices, based on established risk management, regulatory and supervisory frameworks.

Experience with implementing information systems has shown that it is challenging to meet complex security requirements of a digital product if they are not considered from the conceptual design phase. In other words, bolting security features on a system as an afterthought usually results in avoidable security breaches and costly remedial action. Security breaches can erode customer confidence, undermine the integrity of the instrument, and negatively impact the reputation of the central bank. Therefore, the resilience of the entire CBDC ecosystem should be contemplated and built into the solution design before implementation begins.

Responsibilities for developing and implementing the CBDC resilience framework generally spans several agencies and thus inter-agency coordination is essential. The central bank will have primary responsibility as issuer of the currency, with other financial and nonfinancial sector regulatory and supervisory authorities contributing as needed based on the particulars of the ecosystem, and the legal and institutional framework of the jurisdiction.

4.1. High-Level Principles for Protecting a CBDC Ecosystem

A CBDC is a vast and complex network which amplifies many of the existing issues and risks in digital ecosystems. As such, existing remedies can be adapted or enhanced for its fortification. For instance, smart contracts and programmable CBDC platforms, which are new in the central bank's technology toolbox, are essentially based on programming code and their risks can be addressed by rigorous deployment and potential enhancement, of well-established and secure coding practices. Similarly, it is likely that there is already some coverage of regulatory requirements in the issuing country that are applicable or adaptable to CBDC, as most jurisdictions regulate technology and cyber risk management within the financial sector. These could be adapted to cover CBDC-specific risks ensuring changes are enforceable in a court of law. Although supervisors can resort to broader risk management rules or licensing powers that are legally enforceable, the process typically takes too long to be effective. Approaches for general applicability are difficult to formulate, as the hard and soft power of supervisors,

[50] These principles are based on the authors' analysis and are being proposed to spark further discussion.

the maturity of risk management in the financial sector, and the legal systems vary greatly across jurisdictions.

Given the consequences of eroded or broken trust in the currency and given its high-risk profile, a CBDC should not be launched without robust, fully tested, and continuously monitored safeguards to minimize or eliminate to the extent possible, any lapses in security practices. Once broken, consumer trust will be difficult to rebuild in the context of a new currency instrument. The following principles can guide the design of the security of a CBDC ecosystem.

Principle 1: The resilience of the CBDC ecosystem should be at least to the highest standards that apply to existing payment systems.

Implementation should take a strategic approach to confidentiality, integrity, and availability, and should align to international standards for systemically important payment systems or to Principles for Financial Market Infrastructures.

Adoption may be challenged if CBDC is perceived as less resilient than available alternatives. Innovative payment solutions have historically struggled with perceptions about resilience and security, which have hindered adoption. For example, internet-based card payments struggled to be adopted at the beginning of the e-commerce era. As CBDC has a high-risk profile, with financial stability implications if adopted at scale, the risk of operational or security incidents needs to be proactively minimized. A perception of higher security than other available instruments will more likely achieve policy goals of issuing authorities. Should the CBDC be designed for cross border payments, security requirements should be harmonized across jurisdictions through common standards.

Examples of possible requirements derived from this principle include:

- The maximum tolerable downtimes, recovery time objectives, and recovery point objectives for central elements—core system and processing infrastructure—should be aligned with or surpass requirements for systemic FMIs. The processing infrastructure for CBDC if operated by the same entities as those operating traditional payment systems can make the requirement easier to implement. For instance, central banks often operate real-time gross settlement systems and naturally would operate the core CBDC system.
- The cyber resilience framework of the core system and processing infrastructure operators and intermediaries for CBDC should set out clearly defined risk tolerances, objectives, responsibilities, and risk management processes based on internationally accepted standards and guidelines. These should be rigorously enforced through appropriately adjusted supervisory and regulatory practices.

Principle 2: The protection afforded to elements of the ecosystem should be proportional to the systemic risk they pose, considering severe but plausible threats.

Accordingly, much of the attention in terms of resilience should be focused on the core system, the processing infrastructure, and the intermediaries. Although this is similar to a traditional payment system, CBDCs involve more complex or newer technologies, requiring adaptation of existing standards and possibly additional controls for their resilience. Likewise, and as stated in Section III, specific consideration should be given to the endpoints compared to those in the real-time gross settlement or automated clearing house systems. While the central and intermediary elements can be well controlled, as they are subject to cyber risk regulation, supervision, and oversight, such controls do not always exist for the endpoints, digital wallets and point of sale terminals in this case, making it difficult to strengthen their security. One approach to overcome this difficulty is to pose strict requirements on the endpoint applications or devices, which falls under the responsibility of the intermediaries that distribute them. Central banks, as ultimately responsible for the security of the CBDC, can guide institutions in this respect, for example by issuing business rules and technical standards. Additionally, user awareness of risks associated with vulnerable end points and the impact of compromises should be assured.

Examples of possible requirements derived from this principle are:

- The core system and processing infrastructure operators should run the CBDC systems on a multisite, fully redundant and potentially air-gapped infrastructure with real-time data replication between sites and a separate backup. This is considered best practice for mission critical services and systems in the financial sector.
- The core system and processing infrastructure operators and the intermediaries for CBDC should conduct regular threat intelligence-based red teaming exercises targeting CBDC-related systems at their respective organizations.[51] With the use of threat intelligence relevant to the organization, the requirement on proportionality and considering severe but plausible threats is satisfied.

Investment in high levels of security and resilience as described above while CBDC adoption is still low may be difficult to justify. However, experience shows that it is much more costly and less effective to deal with security issues later. A pragmatic approach is gradual resilience upgrades to the operational environment in line with the rate of adoption, and without any compromise to the security architecture. The latter should be designed for large-scale adoption and with the potential systemic importance in mind.

Principle 3: The attack surface should be minimized through proper design and implementation.

Given the nature of CBDCs and the surrounding ecosystem, the question is not *if* they will be targeted by cyberattacks, but rather *when*. Cyber resilience should be designed with the assumption of facing highly sophisticated threat actors, including nation-states. In an era of high and increasing geopolitical tensions, it is prudent to expect and prepare for focused attacks on CBDCs from such entities, ensuring that resilience measures are robust and well designed.

To effectively counter these highly capable adversaries, especially in scenarios where significant breaches are intolerable, the most effective measure is to minimize the attack surface. This strategy

[51] Threat intelligence-based red teaming refers to testing the cybersecurity posture of a target with actual hacker methods that are guided by an assessment of the real-world threats the target is plausibly exposed to.

requires a sound security architecture, typically under the purview of the CBDC vendor. Minimizing the attack surface entails (1) implementing only strictly necessary functionalities and (2) continuous and methodical identification and remediation of weaknesses in all layers of the ecosystem. For example:

- Governance: organizational hierarchies, responsibilities, and policies should be clear and unambiguous for both in-house and outsourced services.
- Technology components: should not expose any unnecessary service access points; should adopt to the extent possible, a zero-trust approach to any interaction with other components; and use strong, standards-based and potentially quantum-resistant cryptographic algorithms, among other security measures.

Minimizing the attack surface does not mean forgoing functionalities required for optimal operations or deploying controls that discourage broad adoption. It means that a careful balance should be struck between security, efficiency gains, and user experience. Features such as offline availability should be reviewed based on available alternatives and only introduced if necessary to meet policy goals. If introduced, the solution must go through rigorous stress testing to ensure effectiveness of security controls. Similarly, if an API is needed for interoperability with financial institutions, then cybersecurity concerns should not prohibit its implementation. Instead, “nice to have” functionalities of the API should be rigorously weighed against the additional cyber risk they bring if implemented. All input should be validated, race conditions must be eliminated,[52] and other secure program design, coding, integration, test, and validation practices should be enforced.

Principle 4: Resilience requirements of a CBDC should be comprehensive.

Cyber resilience of the CBDC ecosystem is an interplay between risk mitigation across supervision, organization, cooperation, and technology, supported by comprehensive regulation. Risk mitigation measures should exist in each ecosystem element, preferably with some overlap to account for failures. In case of end users who are physical persons, supervision, organization, and cooperation are not directly applicable. Instead, awareness training and user-friendly security recommendations can be used.

On a technical level, the design and implementation of resilient IT and telecommunications infrastructures is a well-established discipline and thus there is no need to reinvent the wheel. Key approaches to be considered from the ground up are built-in redundancies, loose coupling and high cohesion of subsystems, comprehensive exception handling, fault isolation, fast failover, graceful degradation, continuous deployment, and so on. Such practices should be inherent in solution design and comprehensively tested for effectiveness on an ongoing basis.

It should be noted that over 80 percent of cyber incidents are due to the human element reflecting a combination of unintentional errors, reckless practices, manipulation, and malintent. Therefore, ongoing

[52] A race condition occurs when two or more programs try to change the same data at the same time. This can cause unpredictable results. Race conditions are a major source of security vulnerabilities.

training and risk awareness of all personnel involved in managing and supporting a CBDC across all stakeholders should be in place and reinforced by rigorous compliance testing.

4.2. Foundational Requirements

Before introducing a CBDC, it is essential that a jurisdiction has the foundational level of cyber risk management capabilities in place. The following capabilities should be viewed as essential before a CBDC can move to large-scale production.

A widely adopted CBDC could pose significant systemic risk to the financial system. While getting the foundations in place can be challenging and resource intensive, upfront capacity building—which has benefits beyond CBDC—is preferable to managing the financial stability and economic fallout that can result in its absence.

Regulatory Capabilities

1. There is an established legal framework to support enforceable corrections of security noncompliance and to prosecute cybercrime.
2. All legal entities operating the core CBDC infrastructure are clearly within the remit of financial regulatory and supervisory agencies.[53]
3. Regulation or guidance on operational, technology, and cyber risk management in the financial sector exists and has been enforced for some time (for example, two to three years).
4. Licensing requirements for new entrants include operations, technology, and cyber risk management criteria.
5. CBDC-specific regulation that considers operations, technology, and cyber risk is passed.

Supervisory Capabilities

1. Supervisory authorities have the capacity to: (1) regulate technology and cyber risk management in the financial sector; (2) assess technology and cyber risk in payment systems or other FMIs and various financial institutions, both in licensing new entrants and in the supervision of incumbents; (3) assess systemic cyber risk; and (4) take effective action in mitigating such risks.

Organizational Capabilities

1. Financial sector authorities are sufficiently resourced to effectively discharge their regulatory and supervisory responsibilities regarding cyber risk.
2. The following organizations are established and operational in the jurisdiction: (1) Computer Emergency Response Team (CERT), (2) Financial Intelligence Unit, and (3) Data Protection Agency and (4) Customer Protection Agency.

[53] The remit does not necessarily extend across the whole supply chain. However, jurisdictions should consider modalities to supervise critical third-party services for the financial sector, as for example in the EU, with the Digital Operational Resilience Act (DORA) or the US with the Bank Service Company Act (BSCA).

3. Physical security measures are in place to protect systems from physical threats, unauthorized access, disasters, and sabotage.
4. There are mechanisms to test business and service continuity in the face of severe but plausible scenarios.
5. There is organizational capacity in the jurisdiction to provide CBDC first-line technical support and helpdesk services in local language(s).
6. There is relentless focus on ongoing cyber risk training and awareness at all levels of the organization.
7. There is a mechanism to grow a talent pipeline through universities, vocational, and exchange programs.

Cooperation Capabilities

1. There is an established cooperation between financial regulatory, supervisory, law enforcement, data protection, national security, and critical infrastructure authorities; or between branches of authorities with such responsibilities.
2. There are established relationships with peer organizations in relevant foreign jurisdictions that can be leveraged in case of cross-border CBDC issues.

Technical Capabilities

1. Domestic telecommunications services are widely available and reliable (without major/frequent outages).
2. International data communication lines have built-in redundancy, especially if parts of the CBDC infrastructure are cloud-based and located in another jurisdiction.
3. There is data center capacity available for core CBDC IT infrastructure elements in the jurisdiction at Tier III level of resilience; and Tier IV if the CBDC is projected to be systemic as a payment system.[54]

4.3. Good Practices

While experience with operational CBDC is still limited, some practices are likely to be conducive to building better cyber resilience in the ecosystem. Many existing good practices are applicable to CBDC operations and can be distilled from a broad variety of sources. This list is not exhaustive.

Regulatory

1. There is a financial sector cybersecurity strategy, ideally based on a national cybersecurity strategy. The former should ideally address CBDC resilience.
2. Once widely in use, CBDC is designated as critical infrastructure, and its protection is addressed in the sectoral and national strategies.

[54] According to the widely accepted Uptime Institute data center standards, key requirements for Tier III resilience are the use of redundant power feeds and cooling, and the ability to do planned maintenance without downtime. Building on Tier III features, Tier IV requires a completely fault-tolerant infrastructure. Note that the foundational requirement does not imply certification; that would be best practice.

3. Regulators issue clarifications on requirements and expectations of CBDC core system and processing infrastructure operators and intermediaries and consult with the stakeholders on a regular basis.
4. The supervisory or oversight remit is extended to critical third-party service providers of CBDC core system, processing infrastructure operators and intermediaries.[55]
5. In addition to entities within the remit of financial regulators, there are proportional cyber resilience recommendations and requirements for merchants imposed by other authorities with appropriate remit or industry standard setters (for example, Payment Card Industry Security Standards Council).
6. There is easy to understand cybersecurity guidance for end users; and it is widely disseminated over various channels on an ongoing basis.
7. In terms of cyber risk, CBDC regulation imposes at least the same controls as those used in systemic payment systems, clearly delineates the roles and responsibilities of core and intermediary nodes and facilitates a defense-in-depth approach to security.[56]

Supervisory and Oversight

1. There are cybersecurity experts specialized in payment systems and with a sound understanding of CBDC at the supervisory and/or oversight authority.
2. Cyber risk supervision and oversight is risk-based and forward-looking, aligned with the goals of the sectoral cyber strategy, and considers strategic threat intelligence.
3. Off-site supervision and oversight of the CBDC and processing infrastructure operators is performed in a continuous manner and include assessments against the CPMI-IOSCO guidance on cyber resilience for FMIs.[57]
4. On-site examinations of the CBDC and processing infrastructure operators are conducted regularly.
5. The CBDC core system and processing infrastructure operators are required to conduct business continuity and security tests regularly, preferably according to a well-established framework.
6. Cyber risk supervision and oversight of the CBDC and processing infrastructure operators considers supply chain risk.
7. There is a comprehensive cyber incident reporting regime in place including clear definitions of what constitute reportable incidents, deadlines, required content of reports, secure reporting platform, and follow-up process.
8. Supervisors follow up reported cyber incidents and take corrective action to address root causes.
9. Supervisors encourage cyber incident information sharing among financial services entities without inserting themselves in the process.
10. Supervisors facilitate industry-wide cyber crisis exercises, which are conducted on a regular basis, using severe but plausible scenarios, which include attacks against the CBDC.

[55] Bringing large international service providers within the supervisory remit would be very difficult for many jurisdictions. This needs to be considered when deciding on outsourcing elements of the CBDC infrastructure.

[56] In a defense-in-depth approach, layers of protection are built around assets so that all need to be breached sequentially to access them in an unauthorized way or to destroy or steal them. For the approach to be effective, it is important to ensure that an attack cannot progress to an inner layer before the outer layer is breached.

[57] Guidance on Cyber Resilience for Financial Market Infrastructures (bis.org).

Organizational

1. In case of central bank operated CBDC core system, the payment system oversight function is independent from operations.[58]
2. A dedicated CERT for the financial sector ("FinCERT") is established if predefined size and complexity criteria on the financial system are met.
3. Employees and contractors involved in CBDC system or services development, and operations undergo background checks and are required to undertake ongoing cyber risk awareness training.
4. Assurance teams have adequate capacity and skill sets to check compliance to approved policies and standards and to detect anomalous behavior.

Cooperation

1. There is a coordination council or similar mechanism to align approaches to cyber resilience among different authorities, including incident response protocols and crisis management plans of elements of the CBDC ecosystem.
2. The CERT and other relevant stakeholders outside the financial sector (for example, the critical infrastructure protection agency or telecom providers) are involved in financial sector cyber crisis response exercises.
3. The critical infrastructure protection authority consults with the supervisory authority regarding the designation, risk assessment, and protection requirements of critical infrastructure in the financial sector.
4. The agency responsible for the national cybersecurity strategy consults with the supervisory authority regarding strategic goals for the financial sector.
5. Authorities and financial sector entities participate in cyber incident sharing and threat intelligence fora.[59]
6. Information sharing and cooperation in cyber incident response and recovery for business continuity, including law enforcement, extends across jurisdictions. This is important not just because cyber risk does not respect national borders but also due to the potential cross border use of CBDC systems.

Technical

1. The security architecture of the CBDC is multilayered, designed for defense-in-depth; attackers are forced to break protection layers sequentially to reach critical systems and data.
2. The core system and processing infrastructure are fully redundant. For example, operators run CBDC systems in a multisite, fully redundant architecture (Tier III or up) with real-time data replication between sites and a separate backup.[60]
3. The CBDC core system is air gapped from public networks. Access logs are frequently reviewed to detect unauthorized activity.
4. There is a dedicated, secure wide area network connecting the central and intermediary nodes of the CBDC ecosystem.

[58] This is already a common approach to existing payment systems operated by central banks.

[59] Also see the practice of supervisors' facilitating information sharing in the financial sector without direct participation. Practically, the internal cybersecurity team of the agency participates, but the supervisory arm does not.

[60] A DLT-based CBDC would natively have such levels of redundancy, given the distribution of the ledger over several nodes.

5. Data loss related to CBDC stock and flow is not tolerated at the core and the processing infrastructure operators; and system operations are built, run, and controlled accordingly.
6. The cryptography used in CBDC is compliant with internationally accepted standards, employs quantum resistant algorithms; and disallows use of proprietary or un-auditable cryptographic functions.
7. If the CBDC has programmability and smart contracts then these features are strictly controlled; secure coding, version control, review, and testing procedures are enforced with automated controls.
8. CBDC-related production, test, and development IT environments are strictly separated; and migration procedures are enforced with automated controls based on clear segregation of duties.
9. CBDC-related systems interact according to zero-trust principles.
10. Critical CBDC systems are developed using a security-focused methodology and undergo extensive validation and testing before release.
11. CBDC systems are certified against relevant technical security standards.
12. System traffic related to CBDC, and its connections is monitored 24 × 7 with automated alerts to designated persons. Technical tools based on AI to swiftly detect anomalies in large data sets.

4.4. Cyber Resilience and CBDC Project Management

As has been mentioned earlier, trust is at the core of a successful and sustained CBDC deployment. It hinges upon adherence to the information security *Trust Principles* which ensure resilience, and engender confidence. Trust is subjective and can erode quickly. To ensure development of a resilient CBDC ecosystem, it is necessary to follow an iterative and methodical approach and ongoing evaluation of options with policymakers. Based on information gleaned from technology vendors and solution providers involved in live implementations and advanced experimentation, this is not always the case (Box 3).

A five-phase approach is recommended for CBDC implementation, also referred to as the "5P methodology."[61] Table 3 highlights the most relevant workstreams of the 5P methodology for cyber resilience and their relative intensity across the steps.

A key recommendation of the 5P approach is that adequate time is spent in each of the phases of the project. Focused security tests of individual systems and components should be performed as early as possible during the implementation (typically the prototype phase). This will ensure that vulnerabilities and design flaws are discovered in a timely manner, avoiding costly rollbacks, redesigns, and re-coding.

The pilot phase is a key stage that should be underpinned by very clear governance arrangements and success criteria. The outcome of this phase will inform the central bank's decision on whether it is ready

[61] IMF Fintech Note, "How Should Central Banks Explore Central Bank Digital Currency?"

to issue a CBDC. This phase is therefore critical for comprehensive, end-to-end resilience testing including all ecosystem elements, with real actors and actual data.

Some flaws, particularly those deeply embedded in software libraries used in the ecosystem, may remain undetected during regular experimentation. Anticipating all test conditions is complex and will most likely be incomplete. Resilience tests need to be rigorous and iterative with various combinations of plausible scenarios. There are examples of weaknesses that are typically not detected during experimentation but can result in unplanned downtime, such as certificate expiry which caused a prolonged outage of the D-Cash pilot in the ECCB. Another good example is the recent testing of offline functionality by Riksbank,[62] where although progress was made, security inadequacies such as torn transactions were evident in the tested scenarios. A prudent implementation plan should consider such contingencies and set milestones accordingly.

[62] E-krona pilot phase 4 | Sveriges Riksbank.

Box 3. A Candid View from Technology Vendors and Solution Providers

IMF staff engaged with technology vendors and solution providers[63] involved in live and pilot implementations to glean insights into and perspectives on cybersecurity considerations. They consistently reported that cybersecurity tests were often out of scope and deferred to future stages. This is congruent with the experience of technical assistance missions, where cyber assistance in some cases was not included in the scope and only initiated by IMF mission teams based on observed gaps during bilateral discussions.

It was also evident that due to a general lack of skill sets and resources, implementations in some EMDEs are often managed by external service providers with the intention of transferring knowledge at a later stage which could be risky if not properly managed through a contract. This is different for many advanced economies where dedicated teams are typically assembled for this purpose.

Central banks in some EMDEs tend to aim for services at lower cost. This is predominantly because business cases for CBDC are not fully developed due to unclear benefits and unconfirmed costs which could escalate based on the quality of existing network and technology infrastructure, digital readiness in the country, and depth of internal skill sets.

In many cases, engagement with stakeholders commences early, including with financial institutions and other ecosystem participants, but communication gaps exist regarding security thresholds for connectivity, interfaces, and end user devices. Laws in jurisdictions with live CBDC have been adapted to include CBDC as the legal tender but no regulatory guidance has been formalized to strengthen cyber or information security defenses.

The insights above indicate limited awareness of cyber risk and its potential impact on one of the largest public-facing national infrastructures with financial stability implications.

Intended levels of cyber resilience may be achieved by aligning key activities in each step of the methodology, as indicated in Table 3. The suggested list is not exhaustive and should be amended based on specific circumstances in the jurisdiction.

[63] These were mostly IT companies that have obtained procurement contracts for developing a CBDC pilot or live CBDC, or specific component parts of it. Also, the box covers general views of technology vendors expressed in seminars, conferences, and countries’ technical assistance stakeholder engagements, regardless of their contractual relationship vis-à-vis a CBDC project.

Table 3. Cyber Risk Management at Various CBDC Project Phases

Phase	Key activities for cyber resilience
1. Preparation	▪ Assess existing cyber maturity, including regulatory frameworks (data privacy, cloud usage, and so on), organizational governance, and current practices.[64] ▪ Identify and map cyber requirements specific to CBDC use cases across, people, process, and technology including policies, threshold requirements, stakeholders' responsibilities, and governance arrangements. ▪ Assess current readiness and gaps for these use cases. This involves not only the central bank but also any stakeholder involved in the distribution and adoption of CBDC. ▪ Develop initial plan to address the gaps. The plan should aim to fix the gaps on regulation, technology, policy, governance, and so on for all stakeholders.
2. Proof-of-Concept/Proof of Assumption	▪ For each use case, assess feasibility of risk mitigation for all stakeholders. ▪ Evaluate and understand new technology relevant to cyber resilience, such as privacy enhancing technology, DLT-related issues, and AI-related risks, and so on. ▪ Identify key elements of security architecture and test readiness. ▪ Design rulebook and governance framework. ▪ Evaluate relevant cyber resilience measures (for example, technology: infrastructure, ledger, wallet/token, and API security architectures, protocols, and algorithms). ▪ Develop and test (or required in case of third parties) a security-focused system development methodology. ▪ Evaluate existing and required skill sets and capacity to undertake technology experimentation. ▪ Lab test initial versions of systems and cyber components.
3. Prototypes	▪ Document detailed security requirements for RFP or for the development team. ▪ Develop resilient-by-design initial model with key security features. ▪ Test infrastructure and application security against requirements. ▪ Develop and test contingency, incident, and crisis management plans. ▪ Conduct penetration tests and hackathons. ▪ Develop business case for investment in resilience.
4. Pilot	▪ Simulate cyber resilience in a live environment with all ecosystem participants. Create actual outages and attacks for all identified risks, and test rulebook and mitigation plans. ▪ Use a variety of approaches: for example, independent penetration tests, red team exercises, crisis exercises, code reviews, security audits and certifications, or bug-bounties. ▪ Fix gaps identified during tests and repeat simulations.
5. Production	▪ Robust security monitoring. ▪ Regular cyber resilience tests. ▪ Continuous improvement programs.

Source: Authors

[64] This could be done using one of the existing frameworks such as Polaris, Part 2: A security and resilience framework for CBDC systems (https://www.bis.org/publ/othp70.pdf).

Conclusion

Trust is pivotal in the realm of finance, especially when it concerns digital currencies, which are inherently susceptible to a myriad of digital risks throughout their life cycle. The life-cycle functions of digital money, such as issuance, storage, distribution, and eventual destruction, necessitate the use of systems and tools that diverge markedly from those employed for traditional fiat currencies. Despite these differences, it is imperative that the core principles of information security—confidentiality, integrity, and availability—are rigorously maintained. Upholding these principles, both individually and collectively, is crucial for sustaining trust among users and consumers.

In an interconnected and vast ecosystem such as the one surrounding a CBDC with multiple points of exposure to cyber risk, securing all elements for resilience is a complex endeavor but one that must be achieved to ensure a successful deployment.

This note explored the required elements and challenges associated with developing a cyber-resilient CBDC ecosystem which encompasses novel technologies such as distributed ledgers, digital wallets, smart contracts, and technology variants to support offline functionalities. Our analysis reveals that the intrinsic features of such technologies, although promising for transactional efficiency and expanded capabilities, also introduce complex security considerations. It also reveals that experience to date, from live implementations, and experimentation, has not yet provided sufficient insights to develop specific frameworks or guidance for resilient CBDC designs. Initiatives such as BIS-led projects Polaris and Sela and outputs of active experiments in advanced economies show promise, and will be leveraged in future updates to this note.

In the meantime, challenges identified are not unsurmountable. However, given the nature of CBDC—a national currency backed by a central bank—the stakes are high and require targeted mitigation strategies. A commitment to CBDC implementation presents a novel opportunity for central banks to rethink the resilience and security of their critical, often legacy, IT systems, and develop solutions using frontier technologies and safeguards that are future proof. Beyond technical solutions involving quantum resistant cryptography, air-gapped data centers, mutable tokens, secure hardware elements, secure coding practices and enhanced identity and access management controls, a holistic approach to cyber risk management is proposed through overarching principles spanning all areas of the ecosystem.

Furthermore, the critical role of the human element which includes inter alia, users, system or solution designers, developers, operators, custodians, and auditors cannot be underestimated. Human behavior and practices can impact the effectiveness and efficiency of processes and technology, and lead to unintended outcomes that impact public trust. The need for effective project management in navigating the complex landscape of CBDC development and deployment is highlighted, advocating for ongoing training and risk awareness and an early analysis of policy and design choices.

Annex 1: Digital Risks Explained

Digital risks encompass a broad range of potential threats and vulnerabilities associated with the use of digital technologies and digital transformation initiatives. They sit at the intersection of people, process, and technology, both internal to the institution and its supply chain.

People risk refers primarily to risks related to the institution or third-party employees[65] and can manifest as follows:

- Insider fraud or error: A malicious insider with privileged access and deep knowledge of business processes or systems may act individually or in collusion with threat actors to commit financial fraud or sabotage. Alternatively, a well-intended developer may adopt open-source code with security vulnerabilities without appropriate code scanning or security review. Employees may inadvertently respond to phishing emails, click infected links and attachments resulting in cascading effects.
- Data breach or improper disclosure: An employee may gain unauthorized access due to a lack of or poor identity and access (IAM) controls. A third-party service provider may become privy to sensitive information due to poor controls or misconfigurations.
- “Key person risk” where excessive reliance is placed on a single or a small group of individuals without appropriate knowledge transfer or succession planning.

Reportedly, over 80 percent of cyberattacks are due to the human element.[66]

Process risk refers primarily to the risk of inadequate or failed processes leading to loss of efficiency and effectiveness. This risk can materialize due to rapid adoption of technology, failed or incomplete deployment of protection mechanisms, noncompliance with established processes, and inadequate assurance mechanisms. Weak management of the IT estate such as inadequate redundancy in critical hardware and network components, and poor oversight of internal controls such as timely software patching, critical version updates, and infrequent testing of disaster recovery plans can result in avoidable exposures.

Technology risk refers primarily to threats and vulnerabilities associated with the implementation, operation and maintenance of technology systems, supporting infrastructure, and processes. Technology risks threaten the integrity, availability, and performance of technology assets and confidentiality of data and information they store or produce. Examples of technology risks include hardware failures or

[65] While generally people’s risk includes the end users, such as the people using a mobile payment app, this chapter specifically focuses on the risks intrinsic to the system level and excludes exogenous risks such as misuse of an application credentials, a power outage, and so on.

[66] Human Error Drives Most Cyber Incidents. Could AI Help? (hbr.org).

malfunction, software bugs or glitches, network outages and disruptions, and poor compatibility between different technology components and performance degradation due to poor scalability.

Supply chain risk refers to the risk from reliance (sometimes overreliance) on external parties such as suppliers, their supply chains, and their products or services. This can lead to (1) concentration risk, that is, reliance of many entities on a single or a few suppliers whose failure could lead to prolonged service disruption and reputational damage to several entities at the same time and (2) operational risk in that vulnerabilities in business/operating models of suppliers who are governed by a less stringent rule book than the entity they serve may not be fully visible, resulting in unchecked build-up of risks with systemic implications.

Annex 2: Comparison of Cyber Risk Exposure across Digital Means of Payment

The following section compares different digital means of payment from a cyber-risk exposure across three dimensions:

1. Likelihood of malicious and non-malicious events

The more policy objectives digital money is trying to address, the more complex the resulting instrument becomes, thereby increasing vulnerabilities and exposures to cyber and other operational risks.

2. Attacker attractiveness

Typically, the more data is stored and the more sensitive it is, the attractiveness of its exploitation increases. Widely adopted means of payment are usually more attractive to cyber-attackers, as the same vulnerabilities can be exploited at scale and in case of national payment systems, these are attractive to nation-states for political gain and social unrest. Limits on holdings and transactions usually deter attackers since the benefits obtained from fraud would be limited, potentially exceeding the costs of attacks.

3. Attack surface

A wider ecosystem, with many parties involved with different levels of cyber resilience and oversight mechanisms, increases the attack surface and the likelihood of operational incidents and failures. The geographical diversity of the ecosystem adds to vulnerabilities since cyber-attackers operate from a variety of places to replicate attacks across several jurisdictions in an effort to escape law enforcement.

The table below shows a comparison between three different types of electronic payments and rates cyber exposure from high to low.

		E-money	Crypto/Stablecoins	rCBDC[67]
Likelihood of both malicious and non-malicious events	Diversity of use cases. Complexity and therefore risk increases with the number of objectives.	**Medium** (typically, one or few objectives—financial inclusion)	**Medium** (use cases range from DeFi investment to attempts at efficient or inclusive cross-border payments)	**High** (often, a long list of sometimes competing objectives)
	End-user access mechanism. Risk increases in line with diversity of access methods.	**High** (a multitude of access methods—physical card, mobile phone wallet, browser, ATMs)	**Low** (typically browser, and to a lesser extent, mobile phone wallets and ATMs)	**Medium** (a multitude of access methods, but mostly mobile phone wallet; to a lesser extent physical devices such as cards)
	Coverage of supervisory oversight and frameworks. Risk increases if coverage is low.	**Low** (mature supervisory frameworks and enforcement)	**High** (no formal oversight)	**Medium** (some existing frameworks may apply but many components outside the financial sector oversight)
	Maturity of security control frameworks. Risk decreases with maturity of applicable frameworks.	**Low**	**High**	**Medium**
	Adequacy of skill set and capacity required to manage an incident will reduce risk.	**Low**	**High**	**High**
Attacker attractiveness	Amount of data handled or stored. Attraction and therefore risk increases in line with data collection.	**High**	**Low**	**TBC as Design dependent**
	Level of adoption (as above).	**High**	**Low**	**High** (particularly, from nation-states)
Cyberattack surface	Ecosystem complexity and span. Risk increases accordingly	**Medium**	**High**	**High**
	Geographical dispersion. Risk increases accordingly.	**Low-Medium** (some major PSPs have an international footprint—for example, PayPal or Revolut)	**High**	**Medium** (some participants in the value chain may be remote)

[67] A general purpose or retail CBDC (r-CBDC) is, *inter alia,* intended for individuals to enable efficient and secure payments, while a wholesale CBDC (w-CBDC) would facilitate large-scale transfers and only be accessible by financial intermediaries such as banks and payment operators. The cyber risk exposure of the latter is much smaller compared to the former and has not been captured in this overview.

References

Aldasoro, Iñaki; Sebastian Doerr; Leonardo Gambacorta; Sukhvir Notra; Tommaso Oliviero; and David Whyte. 2024. “Generative Artificial Intelligence and Cyber Security in Central Banking.” BIS Papers No. 145, Bank for International Settlements, Basel, Switzerland.

Auer, Raphael, and Rainer Böhme. 2020. “The Technology of Retail Central Bank Digital Currency.” *BIS Quarterly Review*, March.

Bank of England. 2020. “Why Does Money Depend on Trust?” Explainers, Bank of England, May 19.

Budau, Victor, and Herve Tourpe. 2024. “ASAP: A Conceptual Model for Digital Asset Platforms.” IMF Working Paper 24/19, International Monetary Fund, Washington, DC.

Bank for International Settlements and CPMI 2018 : “Reducing the risk of wholesale payments fraud related to endpoint security”:

“Central Bank Digital Currency (CBDC) Information Security and Operational Risks to Central Banks: An Operational Lifecycle Risk Management Framework.” Bank for International Settlements, Basel, Switzerland.

Chamorro-Premuzic, Tomas. 2023. “Human Error Drives Most Cyber Incidents. Could AI Help?” *Harvard Business Review*, May 3.

Deodoro, Jose; Michael Gorbanyov; Majid Malaika; and Tahsin Saadi Sedik. 2021. “Quantum Computing and the Financial System: Spooky Action at a Distance?” IMF Working Paper 21/71, International Monetary Fund, Washington, DC.

Dreyer, Paul; Therese Jones; Kelly Klima; Jenny Oberholtzer; Aaron Strong; Jonathan William Welburn; and Zev Winkelman. 2018. “Estimating the Global Cost of Cyber Risk: Methodology and Examples.” RAND Corporation, Santa Monica, California.

Fanti, Giulia; Kari Kostiainen; William Howlett; Josh Lipsky; Ole Moehr; John Paul Schnapper-Casteras; and Josephine Wolf. 2022. “Missing Key: The Challenge of Cybersecurity and Central Bank Digital Currency.” The Atlantic Council, Washington, DC.

Financial Stability Board. 2023. “Cyber Lexicon.” Financial Stability Board, Basel, Switzerland.

“Guidance on Cyber Resilience for Financial Market Infrastructures.” Bank for International Settlements, Basel, Switzerland. 2016

Huber, Nick. 2024. “Why Cyber Risk Managers Need to Fight AI with AI.” *Financial Times*, May 2.

Hupel, Lars, and Makan Rafiee. 2023. “How Does Post-Quantum Cryptography Affect Central Bank Digital Currency?” *Communications in Computer and Information Science* 2034: 45–62.

International Monetary Fund. 2024. *Global Financial Stability Report: The Last Mile: Financial Vulnerabilities and Risks*. Washington, DC, April.

Leitner, Georg; Jaspal Singh; Anton van der Kraaij; and Balázs Zsámboki. 2024. “The Rise of Artificial Intelligence: Benefits and Risks for Financial Stability.” *Financial Stability Review*, May.

Microsoft. 2023. “Microsoft Digital Defense Report: Building and Improving Cyber Resilience.” Microsoft Corporation, Redmond, Washington.

Microsoft. 2024. “Staying Ahead of Threat Actors in the Age of AI.” Microsoft Security Blog, February 14.

Nili, Cameron; Tom Patterson; and Carl Dukatz. 2024. “Safeguard CBDC Systems in the Post-Quantum Computing Age.” World Economic Forum, May 21.

“Project Leap: Quantum-Proofing the Financial System.” Bank of France, Deutche Bundesbank, Bank for International Settlements, Washington, DC.

“Project Polaris Part 1: A Handbook for Offline Payments.” Bank for International Settlements, Basel

”Project Polaris Part 3: Closing the CBDC Cyber Threat Modelling Gaps.” Bank for International Settlements, Basel, Switzerland.

“Project Sela: An Accessible and Secure Retail CBDC Ecosystem.” Bank of Israel, and Hong Kong Monetary Authority. Bank for International Settlements, Base,.

“Project Tourbillon Demonstrates Cash-Like Anonymity for Retail CBDC.” BIS Innovation Hub, November.

Soderberg, Gabriel, John Kiff, Marianne Bechara, Stephanie Forte, Kathleen Kao, Ashley Lannquist, Tao Sun, Herve Tourpe, and Akihiro Yoshinaga. 2023. “How Should Central Banks Explore Central Bank Digital Currency?: A Dynamic Decision-Making Framework.” IMF Fintech Note 2023/008, International Monetary Fund, Washington, DC.

Sveriges Riksbank. 2024. “E-Krona Pilot Phase 4.” Sveriges Riksbank, Stockholm, Sweden.

World Economic Forum. 2024. “Quantum Security for the Financial Sector: Informing Global Regulatory Approaches.” World Economic Forum, Geneva, Switzerland.

PUBLICATIONS

Cyber Resilience of the Central Bank Digital Currency Ecosystem
NOTE/2024/003